GROUPE DE TRAVAIL INTERMINISTÉRIEL
SUR LA LUTTE CONTRE
LA CYBERCRIMINALITÉ

Protéger les INTERNAUTES

*****

Rapport sur la cybercriminalité

Février 2014

Liminaire

Mi juin 2013, les ministres de la Justice, de l'Economie et des finances, de l'Intérieur, ainsi que la ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'Economie numérique constituaient un groupe de travail interministériel chargé de faire des propositions en matière de lutte contre la cybercriminalité.

Cette initiative, qui faisait suite au séminaire gouvernemental sur le numérique du 28 février précédent *(cf. "La feuille de route sur le numérique")*, s'inscrivait, plus généralement, dans la stratégie définie au plan européen, le 7 février.

Bien que le groupe soit, pour l'essentiel, formé de généralistes du droit pénal - avocats généraux à la Cour de cassation et responsables du ministère public - et de spécialistes policiers, gendarmes et douaniers, le mandat donné à son président ne se limitait pas aux questions spécifiquement répressives, puisqu'il s'agissait d'élaborer une stratégie globale de lutte contre la cybercriminalité intégrant notamment les questions de prévention et de sensibilisation des publics, afin de contribuer à créer un espace de confiance sur Internet.

Très rapidement, un quadruple constat s'est imposé :

① par-delà les départements ministériels mandataires, **la question de la cybercriminalité intéresse un grand nombre d'autres acteurs**, tant publics *(parlementaires, administrations techniques, autorités administratives indépendantes...)* que privés, ce qui démontre le caractère transversal de cette problématique mais aussi les limites de l'organisation actuelle. C'est ainsi que, tout au long de ses travaux, le groupe a été sollicité à de nombreuses reprises[1] et a lui-même procédé à de nombreuses auditions pour tenter de mieux cerner les attentes des uns et des autres, tout en s'ouvrant à un interlocuteur incontournable *(la Direction générale de la concurrence, de la consommation et de la répression des fraudes)*. Il est toutefois conscient que seule une enquête généralisée auprès de l'ensemble des administrations de l'Etat et des autorités indépendantes aurait pu permettre une appréhension exhaustive des dispositifs existants ainsi que des attentes sectorielles.

② Si le mandat donné au groupe de travail laissait à penser que l'Etat voulait se donner le temps de la réflexion**, les normes destinées à lutter contre la cybercriminalité n'ont cessé d'évoluer pendant ses travaux**, caractéristique d'un *"droit en marche"* qui se cherche encore.
C'est ainsi que plusieurs questions, à l'étude parfois depuis des années, ont reçu une concrétisation, le plus souvent réglementaire, à l'initiative des départements ministériels concernés.
Parallèlement, plusieurs projets de loi, concernant, pour partie, la cybercriminalité, ont été examinés par le Parlement, dans des domaines les plus divers.

---

[1] Il s'est toutefois refusé à prendre position avant le terme de ses travaux, considérant qu'il appartenait au Gouvernement de décider de la suite à donner à ses recommandations

Dans le même temps, des propositions de loi, intéressant certains aspects de la lutte contre la cybercriminalité, ont été déposées et discutées.
D'autres projets sont encore à l'étude.

Au-delà même de la production normative, certaines décisions juridictionnelles, notamment les arrêts rendus par la chambre criminelle dans le cadre du contrôle de la conventionnalité, tant en matière de réquisitions informatiques que de géo-localisation en temps réel, ont aussi revêtu une importance toute particulière.

Il faudrait enfin citer les nombreuses initiatives prises durant la même période, sous la forme de réunions, de colloques et de missions diverses**.**

Ces quelques exemples illustrent, non seulement, l'actualité de la question et la richesse tant des attentes que des analyses, mais aussi l'hétérogénéité des initiatives et la nécessité de pouvoir disposer tant d'une stratégie globale que d'une grille juridique cohérente.

La richesse de cette actualité a conduit le groupe à étendre quelque peu le champ de son mandat mais aussi à réexaminer, à plusieurs reprises et au fil de l'actualité, certaines des questions dont il était saisi.

③ - durant la même période, de nombreux travaux européens ont rappelé qu'en matière de lutte contre la cybercriminalité, **la solution ne pouvait être exclusivement franco-française.**

C'est ainsi qu'est entrée en vigueur de nouveaux règlement et directive tandis que différents projets sont toujours en discussion.

Le groupe s'est ainsi attaché à entendre certains responsables internationaux et à consulter les spécialistes tant de la coopération internationale que de droit comparé, afin de mieux cerner les synergies actuelles, les perspectives futures, voire les obstacles restant à surmonter.

④ pour autant et la contradiction n'est qu'apparente avec ce qui précède, **l'appréhension de la cybercriminalité est apparue, en l'état, comme une affaire de spécialistes**, d'ailleurs en petit nombre, la majorité des acteurs ayant à en connaître connaissant, au contraire, de réelles difficultés pour cerner ce phénomène, en appréhender le contenu technique comme les aspects internationaux et encore davantage y apporter des réponses pertinentes. Telle est la raison pour laquelle le groupe de travail, bien que saisi, dès l'origine, de nombreuses propositions émanant des services spécialisés, a délibérément fait le choix d'élargir le spectre de l'étude en s'attachant à cerner aussi les attentes des usagers et consommateurs, des victimes individuelles, du monde de l'entreprise, des magistrats, policiers et gendarmes non spécialisés afin de mieux saisir les difficultés qu'ils rencontraient, mais encore des autorités et instances oeuvrant pour la protection des libertés fondamentales.

Cette prise en compte s'est faite, essentiellement, par le biais d'auditions, réalisées en réunion plénière ou en comités restreints, ou sous la forme de communications écrites ou encore de visites effectuées par le président du groupe, les déplacements extérieurs étant exclus pour des raisons tenant aux contraintes de temps.

Ce n'est que dans un second temps qu'ainsi éclairé le Groupe interministériel s'est penché sur les propositions susceptibles d'être émises, avec un double souci : une approche aussi pédagogique que possible et la forte conscience de la nécessité de tenir compte de la surcharge actuelle des services répressifs.

Conformément à son mandat, le groupe de travail s'est focalisé sur la seule cybercriminalité, en écartant les points déjà soumis à l'examen d'autres instances - par exemple, la réflexion initiée, au plan européen, par la Commission nationale de l'informatique et des libertés s'agissant de la protection des données nominatives, ainsi que celle menée sur la contrefaçon commerciale par un Conseiller d'Etat en mission -.
Il lui est toutefois apparu, au cours de ses travaux, d'abord qu'une plus grande synergie devrait être recherchée entre la lutte contre la cybercriminalité, la cyberdéfense et la cybersécurité. Ensuite que, s'agissant des réponses à la cybercriminalité elle-même, elles devraient répondre, au-delà de la spécificité des contentieux et de la nature, administrative et judiciaire, du traitement, à des règles communes, harmonisées et cohérentes, que le groupe s'est efforcé d'esquisser.

Au total, le groupe de travail a tenu 13 séances plénières, auxquelles il convient d'ajouter plusieurs dizaines d'auditions en comité restreint et de nombreux entretiens et visites réalisés par son président. Dans l'intervalle, les communications internes aux membres du groupe ont été assurées par le biais d'une liste de discussion spécifique.

A l'issue de ces quelques mois de travail, je tiens à adresser tous mes remerciements, non seulement à l'ensemble des membres du groupe et aux secrétariats relevant des cabinets de l'Intérieur et de la Justice, mais aussi aux nombreux interlocuteurs qui ont contribué à la réalisation de cette mission.

Marc ROBERT

Plan du rapport

Introduction - Internet : une nouvelle liberté à préserver

Même si la cybercriminalité ne se limite pas à Internet, ce dernier en est le principal vecteur.

Or, Internet, d'abord limité aux relations professionnelles puis étendu à la sphère privée avant de revêtir un aspect universel, a engendré, en quelques décennies, une véritable révolution des comportements et des façons de faire pour la grande majorité des français, désormais incontournable et irréversible.

> Selon l'enquête du CREDOC réalisée en 2012 sur les français âgés de plus de 12 ans,
> - 81% dispose au moins d'un ordinateur au domicile, mais la proportion s'élève à 98% pour les 12-17 ans.
> - 4 français sur 5 sont internautes, 78% disposant d'un accès fixe à Internet à leur domicile et 29% d'un smartphone ; 1 foyer sur 10 possède une tablette tactile.
> - en moyenne, chaque internaute consacre 13 heures par semaine à consulter Internet ; les possesseurs de téléphones portables adressent, en moyenne, 108 SMS par an, mais la moyenne s'élève à 435 pour les 12-17 ans.
> - les réseaux sociaux rassemblent 42% de la population, soit 23 millions de personnes.
>
> Et ces chiffres sont en constante augmentation.

Au plan économique, cette révolution numérique s'exprime notamment par le développement d'un nouveau marché porteur de perspectives de croissance particulièrement précieuses en temps de crise.

> - l'Economie numérique représente désormais 5,2% du produit intérieur brut, concentre 3,7% des emplois *(900.000)* au sein de 100.000 entreprises de 10 salariés ou plus.
> - A lui seul, le commerce électronique concerne 128.000 sites marchands et correspond à 75.000 emplois directs ou indirects, pour un chiffre d'affaires de 56 milliards d'euros en 2012 *(FEVAD, janvier 2013).*
> - la même année, 64% des sociétés disposaient d'un site web ou d'une page d'accueil sur Internet *(INSEE).*

C'est sur la base d'un tel constat que *la feuille de route gouvernementale sur le numérique*, divulguée fin février 2013, entend favoriser la croissance et la création d'emplois dans ce secteur par le développement de technologies, d'infrastructures et de l'usage. Le numérique constitue aussi l'un des 5 axes prioritaires des investissements d'avenir. Enfin, plus d'une dizaine des 34 plans industriels annoncés par le Président de la République en septembre 2013 portent sur l'industrie du numérique *(santé, éducation, objets connectés...)*, notamment sur les filières stratégiques *(données volumineuses, informatique en nuage...)*.

Mais, Internet constitue, d'abord et avant tout, un formidable espace de liberté: liberté d'information, qui abolit les frontières et les barrières culturelles ; liberté d'expression et d'échange, qui contribue à l'essor de la démocratie, au droit d'association et de manifestation ainsi qu'à la diffusion de la pensée ; liberté d'entreprendre, qui favorise l'initiative individuelle comme collective.

La volonté de l'Etat comme des collectivités territoriales de réduire la fracture numérique, notamment en facilitant l'accès au haut débit, manifeste le souci de faire bénéficier le plus grand nombre et de manière équitable de cette liberté.

Toutefois, cette dernière est fragile, compte-tenu même des grandes possibilités qu'offre ce système d'information, à la merci de dérives étatiques - comme l'a illustré récemment l'affaire PRISM - ou de menées malveillantes, voire criminelles inspirées par l'idéologie, la concurrence ou la recherche de gains illicites.

Fragile, celle liberté l'est d'autant plus pour les internautes les moins protégés, et en premier lieu les enfants, mais aussi pour tous ceux qui, plus âgés, maîtrisent mal les précautions élémentaires à prendre, et, par-delà, pour les administrations de l'Etat et les entreprises privées que leurs systèmes ouverts de communication exposent à des risques d'intrusion.

Il importe ainsi d'avoir les yeux ouverts sur ces dangers nouveaux, sans pour autant dramatiser, ni prétendre à un verrouillage sécuritaire d'ailleurs hors d'accès, mais aussi sans tomber dans un discours lénifiant invoquant une évolution inéluctable, un risque acceptable et préconisant le laisser-faire. L'objectif est bien de mieux cerner ces dangers, d'y sensibiliser tout un chacun et d'examiner la meilleure façon de les prévenir ou de les réprimer, sans porter atteinte aux libertés fondamentales auxquelles nous sommes tous attachés.

Cet objectif concerne au premier chef les internautes eux-mêmes, mais aussi ceux des décideurs qui, n'étant pas nés avec Internet, ont du mal à saisir le bouleversement culturel qu'il implique, voire ont tendance à y appliquer des schémas de réponse parfois peu adaptés.

Le constat : la cybercriminalité, une réalité difficile à cerner et confrontée à de fortes attentes

La cybercriminalité apparaît comme une nébuleuse, d'autant plus difficile à cerner qu'elle renvoie à des procédés techniques essentiellement évolutifs maîtrisés par les seuls initiés et que peinent à cerner les dispositifs statistiques traditionnels. (1).

La France a déjà fait beaucoup pour permettre au droit de saisir cette réalité, mais l'effectivité des réponses actuelles prête encore à redire (2).

Compte-tenu de l'aspect essentiellement transnational de cette criminalité, les instruments et les projets européens sont en première ligne, même si le temps de l'action internationale n'est pas toujours à la mesure des légitimes impatiences des acteurs comme des victimes (3).

L'évolution nécessaire doit prendre en compte tant les enseignements du droit comparé (4), que les attentes de l'opinion publique, des acteurs et des victimes (5) ainsi que les exigences tenant à la protection des libertés fondamentales (6).

I.1. - La Cybercriminalité : une réalité protéiforme mal cernée et non définie

Comment prévenir la cybercriminalité ? Comment la punir ? Comment la réparer?

Répondre à de telles question suppose d'abord de décrire le phénomène.

Si, depuis l'affaire PRISM, les médias s'intéressent à la cybercriminalité, rendent compte des affaires d'actualité [2], multiplient les analyses, il relève de la responsabilité de l'Etat de décrire l'étendue comme la complexité de cette délinquance.

Or, **le concept même de cybercriminalité prête à équivoque**.

Trouvant son origine dans le droit anglo-saxon et légitimée par la norme européenne, la cybercriminalité [3] ne renvoie pas à une liste d'infractions bien déterminées, puisqu'elle couvre quasiment l'ensemble du champ infractionnel.

Il s'agit davantage d'une manière d'opérer particulière qui, utilisant ou ciblant un système d'information,

- facilite la commission de l'infraction, puisqu'un simple clic informatique suffit pour passer à l'acte ou atteindre à distance la victime potentielle, même si la mise en scène et les techniques utilisées sont souvent très élaborées
- en démultiplie les effets, en permettant, simultanément, d'attaquer de nombreuses cibles et en bénéficiant de la rapidité de propagation que permet l'outil
- tout en assurant une certaine impunité à son auteur, qui bénéficie, le plus souvent, d'un anonymat fortement protégé et de l'extranéité qui résulte de la localisation des serveurs et du lieu de stockage des données des principaux prestataires d'Internet.

Par voie de conséquence, la cybercriminalité se prête mal à une définition - *celles-ci sont en fait légion mais aucune ne s'est véritablement imposée* -, comme à une quantification exhaustive, deux difficultés qui contribuent au sentiment de flou que suscite ce concept et donc à son appréhension [4].

---

[2] qu'il s'agisse de certaines escroqueries *(les escroqueries par faux ordres de virement, les escroqueries "sentimentales"...)* ou du récent détournement massif de données dont a été victime ORANGE

[3] le terme de *"cyberdélinquance"* serait plus juridiquement exact, mais la notion de *"criminalité"* recouvre, au plan international, toutes les infractions, indépendamment de leur gravité

[4] on pourrait ajouter aussi un 3ème facteur tenant à la prolifération des anglicismes pour décrire les méthodes criminelles utilisées, anglicisme qui signe d'ailleurs le produit d'exportation, raison pour laquelle il est apparu utile d'insérer un glossaire en fin de rapport.

1.- Une définition à visée exclusivement pédagogique

La cybercriminalité n'est pas saisie par le droit interne, même s'il y est fait référence, pour le mandat d'arrêt européen *(décision-cadre du 13.06.2002, art. 695-23 du code de procédure pénale)* et, par renvoi à cette dernière disposition, pour les échanges européens relatifs au gel des avoirs *(décision-cadre du 22.07.2003, art. 695-9-3 et 695-9-17 du même code)*, aux sanctions pécuniaires *(décision-cadre du 24.02.2005, art. D.48-24 du même code)*, aux confiscations *(décision-cadre du 6.10.2006, art. 713-2 et 713-20 du même code)*, aux informations *(décision-cadre du 18.12.2006, art. 695-9-38 et R.49-36 du même code)*, et aux peines privatives de liberté *(décision-cadre du 27.11.2008, art. 728-27 du même code)*.

Pourtant, certaines lois récentes consacrent des développements particuliers à *"la lutte contre la cybercriminalité"*, telles la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Pour autant, pas plus que les instruments internationaux, le droit interne ne définit un tel concept.

La raison en est simple et la Commission européenne s'en est expliquée dans une communication au Parlement européen en date du 22 mai 2007 : *"Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes 'cybercriminalité', 'criminalité informatique' ou 'criminalité liée à la haute technologie' sont souvent utilisés indifféremment"* [5].

Dès lors, le plus souvent, c'est le contenu de la directive ou de la convention internationale qui permet, indirectement, de cerner le concept de cybercriminalité ainsi utilisé, mais sans que cela puisse revêtir une portée générale.

> Toutefois, certaines instances officielles ont tenté de surmonter cette difficulté, d'abord en faisant référence à l'ordinateur ou au système informatique comme objet ou comme instrument de la cybercriminalité [6] ; ensuite, en visant le traitement, la transmission ou la sécurité de données [7] ; d'autres se focalisent sur le caractère non autorisé de l'accès *"à un ordinateur, à un réseau ou à des fichiers à données électroniques"* [8] ; d'autres enfin, et c'est le plus grand nombre, définissent la cybercriminalité au regard d'un système informatique connecté à un réseau.

---

[5] comme l'illustre d'ailleurs le principal instrument international existant, la Convention sur la cybercriminalité adoptée le 23.11.2001 par le Conseil de l'Europe, qui fait mention, tout à la fois, de *"cybercriminalité"*, de *"cybercrime"* ou *"d'infractions liées à la criminalité informatique"*.

[6] ce qui ne résiste pas à l'examen : comme le souligne un expert Canadien, le fait d'asséner des coups à une personne à l'aide d'un ordinateur ne relève, manifestement pas, de la cybercriminalité...

[7] Pour l'OCDE, la cybercriminalité renvoie à *"tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données"* ; pour l'O.N.U., elle a trait à *"tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent"* ; de telles définitions, trop partielles, ne couvrent toutefois pas l'ensemble des infractions concernées, telles la pédopornographie

[8] telle est la définition donnée par les U.S.A. et le Royaume-Uni ; mais se focaliser sur l'accès ne permet pas de rendre compte de toute la cybercriminalité, ne serait-ce que lorsqu'elle prend la forme d'une diffusion de données ou de comportements illicites

Ainsi, dans le cadre du 10˚ Congrès des Nations-Unies (2000), la cybercriminalité était-elle définie comme recouvrant *"toutes les formes d'activités criminelles conduites à partir d'un ordinateur dans l'espace d'un réseau local ou d'une entreprise, ainsi que d'un réseau plus large comme Internet"*, ou encore *"toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique, ou contre un système ou un réseau informatique".*

La Commission européenne, dans la communication précitée, précisait que *"la cybercriminalité devait s'entendre comme des infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'informations ou contre ces réseaux et systèmes".*

Quant à l'Autorité nationale de sécurité des systèmes d'informations *(ANSSI)*, elle vise aussi les *"actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un crime ou d'un délit, ou les ayant pour cible"* [9].

Un point commun essentiel unit l'ensemble de ces définitions : le fait que le mode de commission de l'infraction se fasse à distance, sans contact physique entre l'auteur et la victime.

Pour sa part, le groupe de travail, tout en s'inspirant des définitions précédentes, suggère une formule plus ramassée mais suffisamment large pour appréhender tous les aspects de la réalité actuelle ainsi que l'évolution à venir, et mettant en exergue Internet comme le principal système concerné par la cybercriminalité.

Recommandation n˚ 1
relative à la définition de la cybercriminalité

La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet.

Ceci étant, la portée d'une telle définition est toute relative et, essentiellement, d'ordre pédagogique, car elle ne saurait avoir une vocation juridique ; en outre, dans un domaine qui se caractérise par son caractère transnational et l'importance que revêtent les accords internationaux, seule une définition commune au plan mondial serait véritablement opérationnelle.

[9] Toujours selon l'ANSSI, le système d'information est défini comme *"un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information"*

2.- <u>le contenu du concept de cybercriminalité</u>

Les experts sont plus à l'aise pour déterminer les infractions qui relèvent de la cybercriminalité.

Il y a, en effet, un large consensus pour estimer que ce concept recouvre

⌙d'abord **une catégorie d'infractions totalement spécifiques, celles dirigées <u>contre</u> le système d'information lui-même** et qui regroupent, principalement,

*les attaques contre les systèmes automatisés de traitement de données *(S.T.A.D. [10])*, qui prennent la forme d'intrusion, d'entrave, d'altération ou de destruction de données *(art. 323-1 s. du code pénal français)*

*les atteintes portées aux libertés individuelles par le biais de traitements automatisés de données à caractère personnel, qui correspondent, en France, aux infractions prévues par les art. 226-16 s. du code pénal et résultant de la loi dite *Informatique et libertés*

*des infractions dites *"préventives"* relatives, par exemple, au commerce, à la fabrication et à la diffusion non autorisés d'outils logiciels destinés à de telles activités illégales, notamment la cryptologie.

⌙ensuite, **une deuxième catégorie regroupant l'ensemble des infractions de droit commun commises <u>au moyen de</u> ces nouvelles technologies de l'information et de la communication** ; même si cette catégorie est plus ou moins large selon les systèmes juridiques *(en fonction de l'étendue de la liberté d'expression : cf. les infractions dites de presse en droit français comparées au droit américain résultant du 1er amendement)*, elle recouvre, en Europe,

*l'utilisation de telles technologies pour <u>véhiculer</u> des contenus illicites *(images de pédopornographie, apologie de crimes contre l'humanité ou du terrorisme, provocation à la haine raciale, à la xénophobie, au négationnisme, au révisionnisme : cf., notamment, le protocole additionnel du 7.11.2002 à la Convention de Budapest).*

*l'utilisation de ces technologies en tant que moyen permettant de <u>faciliter</u> la commission de toute autre infraction *(terrorisme, proxénétisme, atteintes à la vie privée, injures et menaces, infractions à la législation sur les stupéfiants, escroqueries, falsifications et usages de cartes de paiement contrefaites, atteintes au secret professionnel, atteintes à la propriété intellectuelle et aux droits d'auteur...).*

Dans le langage courant, ces infractions, lorsqu'elles sont commises au moyen d'un système d'information et de communication, sont dites *"cyber-escroqueries (par exemple)*, pour les distinguer des mêmes infractions commises par les moyens traditionnels.

Si ces cyber-infractions relèvent, ordinairement, du régime du droit pénal général *(cf. l'exemple allemand)*, certains systèmes juridiques, notamment le droit français, aggravent les sanctions encourues pour certaines d'entre elles lorsqu'elles sont commises par le moyen d'un système d'information.

[10] En pratique, le S.T.A.D. recouvre aussi bien une puce électronique *(de carte de paiement, de téléphone mobile...)*, un site Web, une base de données ou un autocommutateur téléphonique électronique

Pour les besoins du groupe interministériel*, le pôle d'évaluation des politiques pénales de la Direction des affaires criminelles et des grâces (ministère de la Justice)* a réalisé une extraction de la table NATINF qui, comme son nom l'indique *(NATure d'INFractions)*, recense l'ensemble des infractions définies par la norme française *(loi, décret-loi, ordonnance, décret),* afin de mieux cerner les types d'infractions concernées par la cybercriminalité *(les listes issues de ces extractions figurent in extenso dans l'annexe terminale du rapport)* [11].

☞ **en France, 248 NATINFs. et donc autant d'infractions, concernent spécifiquement la cybercriminalité, soit par leur objet, soit parce que leur mode de commission est saisi par la loi, le plus souvent au titre des circonstances aggravantes.**

Sont concernées certaines atteintes aux personnes *(infractions du titre 2 du livre 2 du code pénal, avec la circonstance aggravante de commission par réseau de communications électroniques),* les atteintes relatives aux traitements de données personnelles *(infractions dites Informatique et libertés)*, les atteintes aux S.T.A.D., certaines infractions à la loi sur la presse, les infractions techniques et atteintes aux réseaux *(prévues par le code des postes et communications électroniques ou, s'agissant de la cryptologie, par le code pénal)*, certaines atteintes à la propriété intellectuelle commises par voie électronique ou infractions techniques visant à la protection des oeuvres, certaines infractions aux instruments de paiement *(tendant à la contrefaçon de la monnaie fiduciaire ou scripturale)*, les infractions aux jeux en ligne, les infractions relatives à la captation frauduleuse de programmes télédiffusés, et enfin certaines atteintes aux intérêts fondamentaux de la Nation *(atteintes aux secrets de la Défense Nationale, livraison d'information à une puissance étrangère, sabotage)*.

☞ **181 autres NATINFs correspondent à des infractions pour lesquelles le texte d'incrimination ne fait pas de référence expresse à la cybercriminalité, mais dont la commission par ce moyen est constatée par les praticiens.**

On y trouve les infractions relatives à la pédopornographie, partie des menaces contre les personnes ou contre les biens, d'autres atteintes diverses aux personnes, partie des atteintes à la propriété intellectuelle, aux jeux de hasard et à d'autres atteintes aux biens.

☞ **enfin, 46 autres NATINFs paraissent aussi relever de la cybercriminalité.**

Il s'agit, essentiellement, d'infractions concernant les communications électroniques, prévues par le code des postes et des communications électroniques.

[11] En l'état, la table NATINF ne prend pas en compte les infractions prévues par l'article 6 de la loi du 21.06.2004 sur l'économie numérique, eu égard aux difficultés d'interprétation qu'elles posent, ni celles créées par la loi du 18 décembre 2013 relative à la programmation militaire, compte-tenu du caractère récent de cette dernière.

3.- l'importance quantitative de la cybercriminalité : la difficulté de la mesure

Jamais, un phénomène criminel n'a fait l'objet d'affirmations autant péremptoires quant à son importance et quant au préjudice qu'il induit, y compris de la part d'organisations internationales officielles. Pourtant, si l'ensemble des acteurs s'accordent sur cette importance et cette gravité, les sources d'information paraissent parcellaires et approximatives.

Dans tous les Etats *(cf., notamment, l'Allemagne)*, la quantification du phénomène se heurte à des difficultés comparables à celles que rencontre la France :

✓ l'appréhension de la cybercriminalité doit d'abord être fondée sur la définition légale des infractions.

Si le dispositif statistique de la Justice a été conçu autour de ce concept d'infractions, celui du ministère de l'intérieur procède de manière plus globale.

> En France, au plan judiciaire, le base statisticielle est fournie par la table NATINF *(précitée),* dont chacune des quelques 12.000 occurrences répond ainsi à une incrimination, une circonstance aggravante et une peine spécifique. Cette vocation exclusivement juridique s'explique par les finalités de cette table, constituée, à l'origine, pour permettre l'enregistrement des condamnations au Casier judiciaire national automatisé, puis, pour régir les systèmes informatiques des juridictions pénales *(application Cassiopée)*. Le fait qu'aujourd'hui cette table ait une vocation interministérielle, puisqu'elle est utilisée par les administrations et services à vocation répressive, n'a pas modifié sa conception première, bien au contraire, puisque le concept d'infraction constitue le dénominateur commun de l'action de l'Etat en ce domaine. Elle est gérée par *la Direction des affaires criminelles et des grâces du ministère de la Justice.*
>
> Au plan policier, la table dite des 107 index de l'état 4001 géré par *la Direction centrale de la police judiciaire* est constituée par un regroupement de natures d'infractions, même si, à la marge et pour les infractions les plus importantes, elle peut parfois prendre en compte aussi des façons d'opérer. En l'état, seuls deux de ces 107 index se rapportent, et encore partiellement, à la cybercriminalité.

Le 1er défi consiste ainsi, pour le ministère de l'Intérieur, à asseoir son dispositif statistique sur la notion d'infraction, c'est-à-dire sur la table NATINF, ce que ne permettent pas, en l'état, les applications existantes *(Système de traitement des infractions constatées - STIC - pour la Police, et Système judiciaire de documentation et d'exploitation -JUDEX - pour la Gendarmerie).*

✓ Toutefois, la définition légale des infractions est, le plus souvent, insuffisante pour prendre en compte la cybercriminalité lorsqu'elle ne constitue que le moyen de commettre une infraction de droit commun.

Si la table NATINF distingue les cyber-infractions spécifiques relevant de la 1ère catégorie précitée ainsi que les rares infractions de droit commun *(2ème catégorie)* pour lesquelles le *modus operandi* propre à la cyber est visé par la loi en tant que l'un des éléments constitutifs possibles ou encore en tant que circonstance aggravante particulière, il n'en est pas de même pour la grande majorité des infractions de droit commun : la loi ne comportant aucun élément distinctif quant à leur commission au moyen d'un système d'information, la table NATINF ne les isole pas non plus *(cf., par exemple, les*

escroqueries qui constituent pourtant le principal "contentieux de masse" de la cybercriminalité).

Dès lors, le 2ème défi, pour les dispositifs statistiques policier et judiciaire, consiste à prendre en compte, même dans le silence de la loi, ce modus operandi spécifique à la cybercriminalité, lorsqu'il existe ; cela ne peut se faire que sur la base des constatations faites par les enquêteurs.

En résumé, les dispositifs actuels sont donc dans l'incapacité d'appréhender l'ensemble de la cybercriminalité constatée et jugée, comme l'a mis en exergue *l'Observatoire national de la délinquance et des réponses pénales (ONDRP).*

✓ les éléments de solution actuellement mis en oeuvre par le ministère de l'Intérieur

Ils diffèrent, pour des raisons organisationnelles, entre la Police Nationale et la Gendarmerie Nationale.

S'agissant de la police, elle prévoit d'alimenter directement les bases statistiques via l'application opérationnelle mise à disposition des services pour l'enregistrement et la rédaction des procédures *(L.R.P.P.N. : Logiciel de rédaction des procédures de la Police Nationale),* qui intègre, dans la version 3 en cours de déploiement, la table NATINF et donc les infractions spécifiques à la cybercriminalité, mais aussi, s'agissant des infractions dites de droit commun, les indications factuelles *(nature de lieu, mode opératoire)* permettant de savoir lesquelles relèvent aussi de la cybercriminalité.

Dans la mesure où les champs relatifs à la manière d'opérer sont généralement prédéfinis, il conviendra toutefois de veiller à ce que toutes les données intéressant spécifiquement la cybercriminalité soient effectivement prises en compte dans cette application.

Au contraire de la police, la gendarmerie n'envisage pas d'exploiter à des fins statistiques sa base opérationnelle ; elle dispose déjà d'une alimentation statistique particulière, reposant sur l'exploitation des *messages d'information statistique (MIS)* dressés par les unités pour chaque fait enregistré, soit d'office, soit à la suite d'un dépôt de plainte.
Depuis 2012, un indicateur spécifique relatif à la cybercriminalité a été créé dans les MIS, qui doit être sélectionné dès que l'Internet est utilisé comme lieu virtuel de diffusion de contenus illicites ou lorsque les nouvelles technologies numériques sont utilisées comme moyen principal dans la commission des infractions visées. En conséquence, le dispositif valorise une notion factuelle et non celle d'infraction.

Dans un second temps, un nouveau fichier de police judiciaire se substituera aux applications existantes et réalisera notamment l'interface avec les applications judiciaires.

Le traitement d'antécédents judiciaires *(T.A.J.)*

Créé par le décret n° 2012-652 du 4.05.2012 *(cf. art. R.40-23 et s. du code de procédure pénale et la délibération n° 2011-204 du 7.07.2011 de la C.N.I.L.)*, ce fichier de police judiciaire a pour vocation à se substituer, vraisemblablement en 2015, aux applications opérationnelles existantes *(S.T.I.C. et JUDEX)* et à devenir commun à la Police et à la Gendarmerie.

Il a trait aux données recueillies dans le cadre des procédures établies par la Police, la Gendarmerie ou les Douanes judiciaires. S'agissant des mis en cause, l'application ne portera que sur les données recueillies sur les personnes à l'encontre desquelles ont été réunis des indices graves et concordants au sens du code de procédure pénale -. En ce qui concerne les plaintes, seront enregistrées *"les données à caractère non personnel qui concerne les faits, objets de l'enquête, les lieux, dates de l'infraction et modes opératoires ainsi que les données et images relatives aux objets..."*. Il doit être toutefois souligné que, souvent, le plaignant lui-même ignore le moyen utilisé pour le léser *(ex. des fraudes à la carte bancaire, pour lesquelles le détournement des données confidentielles a pu être opéré via Internet mais aussi de bien d'autres façons, ce que la victime ignore dans la grande majorité des cas).*

La collecte s'opère automatiquement par la mise en relation de ce fichier avec les traitements de rédaction des procédures LRPPN *(Police nationale)* et LRPGN *(Gendarmerie nationale)* ; toutefois, si les données renseignées dans ces logiciels de rédaction des procédures relatives aux faits et aux plaignants seront transmises en temps réel au T.A.J., celles concernant les personnes mises en cause ne le seront qu'à la clôture de la procédure, à l'occasion de la validation du compte-rendu d'enquête *(Police)* ou du bordereau d'envoi judiciaire *(Gendarmerie)*, afin d'éviter que les personnes mises en cause par erreur soient fichées.

En l'état, le T.A.J. est totalement déployé pour la Gendarmerie et en cours de déploiement pour la Police.

Le T.A.J. a pour ambition de devenir un véritable outil d'investigation comportant un rapprochement automatisé des données contenues dans des procédures différentes, notamment quant au mode opératoire, ce qui intéresse directement la lutte contre la cybercriminalité. En outre, il devrait permettre aux services enquêteurs d'afficher des alertes correspondant à des enquêtes en cours. Enfin, il poursuit des finalités statistiques.

Le nouveau fichier a vocation à être interconnecté avec l'application CASSIOPEE du ministère de la Justice aux fins de mise à jour automatisée des suites judiciaires.

Dans la mesure où le dispositif Gendarmerie repose sur un système déclaratif distinct des applications opérationnelles, il importe d'en examiner les effets quant à **l'alimentation des applications judiciaires**. En effet, si l'application Cassiopée de la Justice a vocation à être interconnectée avec les applications de la Police ou de la Gendarmerie *(la connexion est déjà opérée, pour partie, avec cette dernière)*, encore faut-il qu'elle puisse aussi disposer des identifiants-cyber relatifs au *modus operandi* et au lieu de commission de l'infraction afin d'être en mesure de les exploiter au regard des décisions judiciaires. Autrement, la continuité statistique ne pourra être assurée.

Il est toutefois à noter, sur un plan plus général, que les dispositifs actuels ou futurs paraissent impuissants à rendre compte de deux types de données intéressant, au plus haut point, la criminologie : le type de victimes et le montant du préjudice, lequel n'est partiellement appréhendé actuellement qu'à travers le prisme des sociétés privées de sécurité informatique.

✓ **Mêmes rendues exhaustives, les statistiques policières et judiciaires seraient impuissantes à rendre compte des cyber-infractions ne donnant lieu ni à plainte, ni à dénonciation, ni à saisine d'office.**

Pour n'être pas propre à la mesure de la cybercriminalité, ce constat prend, la concernant, une importance toute particulière pour deux raisons :

⌞ **la propension à déposer plainte**, bien que plus forte en France que dans nombre Etats étrangers, est fonction des attentes des victimes par rapport au système répressif mais aussi de la représentation qu'elles se font des résultats attendus.
Ainsi, bon nombre d'entreprises sont encore réticentes à rendre publiques les cyber-infractions dont elles sont victimes, essentiellement pour des raisons tenant à leur image.
Les victimes individuelles de petites escroqueries peuvent aussi considérer que le préjudice subi ne justifie pas la démarche.
Quant aux fraudes à la carte bancaire, les détenteurs sont indemnisés par le système bancaire sans devoir justifier d'une plainte préalable.
S'agissant enfin des professionnels de l'Internet, leur obligation de dénonciation est aujourd'hui cantonnée à quelques infractions graves.

Au surplus, nombre de cyber-délits sont *"transparents"* pour l'utilisateur qui peut ignorer son état de victime ou s'en apercevoir longtemps après.

Si la technique des signalements par les internautes, notamment ceux adressés directement à l'Etat *(cf. la plate-forme PHAROS, dont il sera question par la suite)*, permet de pallier, dans une certaine mesure, cette méconnaissance, il n'est pas possible d'en mesurer exactement l'impact.

⌞ **le fait qu'une partie des infractions relevant de la cybercriminalité sont traitées par d'autres modes de régulation des conflits, en-dehors de l'appareil répressif** *(cf. titre I, chapitre 2).*

Une première solution consiste alors à prendre en compte aussi les informations provenant d'autres sources que celles de la police, de la gendarmerie ou de la justice : les administrations spécialisées qui disposent de pouvoirs transactionnels, voire de sanctions administratives *(Douane, Concurrence, consommation et répression des fraudes...) ;* les Autorités indépendantes ; les organismes partenariaux ou professionnels *(G.I.E. cartes bancaires, professionnels du e-commerce, éditeurs anti-virus, assurances...)* ; il y a toutefois difficulté à disposer d'une nomenclature commune et à éviter les doubles comptages entre les différentes sources.

Une autre solution consiste, comme l'a initié, dès les années 1970, le C.E.S.D.I.P. *(laboratoire C.N.R.S. de recherche socio-criminologique rattaché au ministère de la Justice)* et comme s'y emploie l'ONDRP depuis 2007, à mener des enquêtes de victimation ; toutefois, certaines des cyber-infractions se prêtent mal à une telle enquête pour les raisons déjà exposées tenant à l'absence de dépossession matérielle et visible; encore faudrait-il aussi que, comme le font déjà les pays anglo-saxons, ces enquêtes visent, non seulement les ménages, mais aussi les entreprises *(cf. plus loin, toutefois, le rôle joué par le CLUSIF)* [12].

[12] *cf.* Home Office, *"Crime against businesses : Headline findings from the 2012 Commercial Victimisation Survey",* January 2013 ; cette enquête de victimation, menée en 2012 auprès des entreprises commerciales d'Angleterre et du Pays de Galles, est brièvement résumée dans le rapport 2013 de

⌙ **enfin, les constatations faites d'office, notamment pour les cyber-infractions qui ne font pas de victimes directes, dépendent de l'importance des enquêtes d'initiative et donc, pour une bonne part, des veilles réalisées sur Internet.**

L'ensemble des développements précédents expliquent pourquoi la France ne dispose actuellement que d'une vision très partielle de la réalité de la cybercriminalité, au risque de minorer son importance. Elle est donc dépendante des éléments diffusés au plan international voire de ceux mis en exergue, pour leurs besoins propres, par quelques sociétés de sécurité, souvent elles aussi étrangères.

Il est vrai que la prise de conscience de l'importance d'une telle mesure est récente. Elle a été initiée, il y a deux ans, par l'ONDRP, dans son rapport 2011sur la délinquance. Comme l'a déjà souligné cet Observatoire, il est aujourd'hui urgent de se doter des moyens nécessaires pour appréhender plus précisément cette criminalité.

Recommandation n° 2
relative à l'appréhension statistique de la cybercriminalité

1.- créer, dans le cadre de la Délégation interministérielle préconisée plus avant, un observatoire chargé de rassembler et de mettre en cohérence toutes les données relatives à la cybercriminalité, y compris en terme de préjudice subi,

2.- définir, au plan interministériel et sous l'égide de la Justice, un agrégat précis des infractions relevant de la cybercriminalité, à partir de la table dite NATINF,

3.- mener à terme les réformes engagées par le ministère de l'Intérieur pour la mesure de la cybercriminalité, en veillant à l'exhaustivité de l'alimentation judiciaire en terme de données,

4.- prévoir une exploitation statistique judiciaire de la cybercriminalité, reposant, d'une part, sur le Casier judiciaire, d'autre part sur l'application judiciaire Cassiopée alimentée par la police judiciaire et aménagée à cet effet, afin de prendre en compte toutes les manifestations de cette délinquance et l'ensemble des réponses judiciaires qui lui sont apportées,

5.- développer, en liaison avec l'ONDRP, les enquêtes de victimation sur la cybercriminalité auprès tant des ménages que des entreprises,

6.- favoriser une meilleure appréhension de la cybercriminalité en suscitant, à cet effet, les organismes de recherche.

---

l'INHESJ/ONDRP sur la criminalité en France : 180.000 entreprises se sont dites avoir été victimes d'intrusion dans leur système d'information, de phishing, de vol en ligne d'argent ou d'informations, d'altération de leur site Internet, ou d'infection de leurs machines par un virus ou un programme malveillant ; l'infection par virus s'avère prédominante *(135.000 entreprises victimes)* ; dans 86%, l'infiltration ou l'infection s'est faite à distance. Seules 2% de ces infractions ont donné lieu à dépôt de plainte.

4.- les données statistiques actuellement disponibles sur la cybercriminalité

Sont ici recensées les données statistiques les plus importantes dont on dispose pour la dernière année de référence (2012).

□ les données de la Police Nationale et de la Gendarmerie Nationale

Compte-tenu de l'impossibilité d'exploiter l'état statistique 4001, l'ONRDP a extraites les données qui suivent des systèmes d'information opérationnels de la Police nationale *(STIC)* et de la Gendarmerie Nationale (JUDEX), avec des réserves tenant au fait que ces systèmes n'ont pas de vocation directement statistique [13]. Même si les résultats ne sont pas exhaustifs, il en résulte les tendances suivantes pour 2012 :

> ↗ une progression constante des atteintes aux systèmes de traitement automatisé des données (STAD) : 419 en 2009, 626 en 2010, 1105 en 2011, 1427 en 2012, quasi-exclusivement sous la forme d'un accès ou d'un maintien frauduleux.
>
> ↗ une augmentation sensible des atteintes à la dignité et à la personnalité commises par le biais d'Internet *(injures, diffamations, discriminations...)* : 1.235 en 2009, 1.528 en 2010, 1.691 en 2011, 2.300 en 2012 ; dans ce total, les atteintes aux droits de la personne résultant des traitements informatiques *(infractions Informatique et liberté)* progressent moins fortement : 248 en 2009, 245 en 2010, 312 en 2011, 334 en 2012.
>
> ↗ une hausse des atteintes sexuelles commises par le biais d'Internet *(exhibitions, racolage, agressions sexuelles, pédopornographie) :* 385 en 2009, 330 en 2010, 263 en 2011, 455 en 2012 ; parmi elles, les infractions pédopornographiques *(diffusion ou détention d'images à caractère pornographique d'un mineur)* occupent une place majeure : 277 en 2009, 226 en 2010, 194 en 2011 et 362 en 2012.
>
> → un maintien à niveau des escroqueries et abus de confiance commises par le biais d'Internet : 28.044 en 2009 ; 27.225 en 200 ; 27.259 en 2011 et 27.928 en 2012
>
> ↘ une diminution sensible des falsifications et usages de cartes de crédit commises par le biais d'Internet, conséquence directe de la politique pénale mise en oeuvre en la matière : 9.313 en 2009 ; 6.703 en 2010 ; 6.685 en 2011 et 1.868 en 2012.

Toutefois et comme il a déjà été indiqué, la Gendarmerie dispose, depuis 2012, d'informations plus précises résultant de la prise en compte d'un indicateur propre à la cybercriminalité.

Si l'ONDRP a déjà effectué une première présentation des principaux résultats, le groupe interministériel a aussi procédé à leur analyse [14], étant souligné que les chiffres qui suivent doivent être interprétés avec prudence compte-tenu de l'introduction récente de cet indicateur et du temps nécessaire aux enquêteurs pour se l'approprier pleinement. En outre, aucune comparaison avec les années précédentes n'est possible.

---

[13] Source : INHESJ/ONDRP, *"Rapport sur la délinquance constatée en 2012"*

[14] Source : note dressée par la Direction générale de la Gendarmerie Nationale le 18.07.2013

33.428 faits relevant de la cybercriminalité ont été enregistrés par la Gendarmerie en 2012.

☞ 63% d'entre eux concernent des escroqueries et abus de confiance *(21.077 soit 34% du total des escroqueries et abus de confiance constatés)*
☞ 5% sont des atteintes à la dignité et à la personnalité *(1703 faits, soit 19% du total)*
☞ 4% ont trait aux falsifications et usages de carte de crédit *(1.423 faits, soit 42% du total des infractions constatées)*
☞ 4% concernent des menaces ou chantages *(1374 faits, soit 6,4% du total mais la proportion est bien plus forte pour ceux de ces faits qui sont motivés par une volonté d'extorsion de fonds : 22%)*
☞ 2% ont trait à des atteintes sexuelles *(568 faits, dont 15% du total)*
☞ 2% sont des atteintes aux systèmes de traitement automatisés de données *(775 faits, soit 100% du total)*
☞ les 20% restants correspondant à d'autres faits délinquantiels *(6.543 faits).*

A la demande du groupe interministériel, la Direction centrale de la police judiciaire *(DCPJ)* s'est livrée à un exercice similaire en ce qui concerne la Police Nationale [15]; les données ci-dessous sont issues de la base "STATS OP", base qui est aujourd'hui alimentée partie de manière traditionnelle *(par le S.T.I.C.)*, partie par le logiciel de rédaction des procédures de la Police Nationale *(L.R.P.P.N. version 3)* en cours de déploiement dans les services ; le visa du code NATINF permet d'évaluer l'importance de la cybercriminalité constatée sur la base de la centaine de codes NATINF identifiés comme relevant de cette délinquance particulière. Il s'agit d'une exploitation provisoire jusqu'au déploiement généralisé du L.R.P.P.N. en juillet 2014, d'autant plus qu'en l'état la qualification de l'infraction sur la base de la table NATINF est celle retenue en début d'enquête : elle peut évoluer par la suite.
Les données obtenues sont ainsi fournies à titre de simple information.

En 2012, 51.346 infractions concernant la cybercriminalité auraient été ainsi constatées, par la Police Nationale, que l'on peut regrouper en trois catégories :

☞ les infractions spécifiques aux technologies de l'information et de la communication - T.I.C. - *(1.590)* [16], dont :
*les atteintes aux S.T.A.D. *(1.273)*
*les infractions à la loi informatique et libertés *(282)*
*les chiffrements non autorisés : -
*les violations de correspondance *(16)*
*les infractions à la loi sur l'économie numérique : -
*les autres infractions au code des postes et des communications électroniques *(19)*

[15] L'extraction réalisée en janvier 2014 par la D.C.P.J. *(Service central d'étude de la délinquance)* porte, aussi bien, sur les données 2013 que sur les données 2012 ; toutefois, par souci de cohérence avec les autres données disponibles, compte-tenu aussi de la nécessaire consolidation des chiffres de 2013 et de l'impossibilité de procéder, pour l'instant, à des comparaisons entre années, seuls les éléments relatifs en 2012 ont été retenus

[16] la D.C.P.J. intègre aussi dans cette catégorie les fraudes aux cartes bancaires ; il semble toutefois que ces dernières relèvent davantage de la catégorie 3 *(autres infractions dont les T.I.C. sont utilisées comme moyen principal de commission)*, qui comprend déjà les escroqueries, extorsions et abus de confiance

☞ les infractions de diffusion de contenu illicite par voie électronique *(1.327)*, dont
*les infractions liées à la pédopornographie *(189)*
*les infractions à la loi sur la presse *(267)*
*les usurpations de fonction, de titre et d'identité *(455)*
*les autres atteintes aux personnes *(408)*
*les atteintes aux biens : -
*les diffusions de procédés pour la fabrication d'engins explosifs *(8)*

☞ les autres infractions dont les technologies de l'information et de la communication sont utilisées comme moyen principal de commission *(48.429)*, dont
*les infractions aux cartes bancaires *(39.553)*
*les escroqueries, extorsions et abus de confiance *(8.780)* [17]
*les infractions au code de la propriété intellectuelle *(38)*
*les infractions à la législation des jeux en ligne *(1)*
*les violences sexuelles *(2)*
*la traite des êtres humains et le proxénétisme *(1)*
*la mise en péril des mineurs et personnes vulnérables *(54)*
*les provocations au suicide : -

Même si ces exploitations propres à la Gendarmerie et à la Police doivent être consolidées et mises en cohérence dans le futur, elles permettent déjà d'avoir une image plus exacte de l'importance de la cybercriminalité et de son contenu.

Estimation globale des cyber-infractions constatées par les services de Police et de Gendarmerie en 2012

84.774 infractions,
dont 84% sont constituées par des escroqueries, abus de confiance et fraudes aux cartes bancaires.

Sur ce total, il n'est pas possible de savoir le nombre des infractions constatées que les services de police déclarent avoir élucider.

Toutefois, pour les raisons déjà exposées, les infractions constatées par les services de Police et de Gendarmerie n'épuisent pas la réalité de la cybercriminalité ; il faut donc se référer aussi à d'autres sources, sans prétendre cependant à une quelconque exhaustivité dans le cadre de ce rapport. Certains des éléments qui suivent rendent compte de l'activité de services ou d'autorités ; les autres sont issus d'enquêtes auprès de diverses catégories concernées.

[17] Manifestement, la part des escroqueries relevant de la cybercriminalité est, en l'état, appréciée différemment par la Police Nationale et la Gendarmerie Nationale

□ la cybercriminalité à travers l'action des services de la Concurrence, de la Consommation et de la répression des fraudes (DGCCRF)

L'action de contrôle de la D.G.C.C.R.F exercée dans le e-commerce lui permet de mettre en évidence un certain nombre d'infractions au droit de la concurrence et de la consommation [18].

-Les 15.199 contrôles de sites de commerce électronique effectués en 2012 ont permis de constater **3.742 infractions**, soit un taux de 24,6% en progression par rapport à 2011 (13%).

-30% de ces infractions concernaient la réglementation sur la vente à distance, 25% des pratiques commerciales trompeuses *(art. L.121-1 du code de la consommation)*, 17% des carences d'information en matière de commerce électronique, 9% des infractions aux arrêtés en matière d'affichage des prix, 4% des clauses abusives *(art. L.131-1 du code précité)* et 2% le non-respect d'obligations relatives aux soldes.

-Au total, 226 de ces infractions ont donné lieu à réalisation d'un procès-verbal, le reste étant traité par la voie de l'avertissement.

□ la contrefaçon en ligne à travers l'action des Douanes

Le *Comité national anti-contrefaçon (CNAC)*, à l'occasion de sa dernière assemblée plénière qui s'est tenue le 10 décembre 2013, chiffrait le manque à gagner, sur le plan fiscal, de la contrefaçon en France à 6 milliards d'euros.

Au plan douanier, les saisies opérées dans le fret postal et le fret express - mode privilégié de la contrefaçon vendue via Internet - représentaient, en 2012, 30% des saisies totales opérées *(correspondant à 1,4 millions d'objets saisis)* contre à peine 1% en 2005.
Outre les contrefaçons classiques portant sur la mode ou le tabac, celles relatives aux médicaments sont en très forte augmentation : les saisies en la matière ont augmenté de 45% en 2012 *(95.000 objets saisis)*.

Dans l'activité de Cyberdouane pour 2012, la contrefaçon correspond à 52% de l'activité du service, bien avant les stupéfiants (9%),

□ Les atteintes aux données personnelles à travers l'action de la Commission nationale de l'informatique et des libertés (CNIL)

Comme chaque année, la C.N.I.L. a dressé le bilan de ses actions dans le cadre de son rapport d'activité 2012. Les éléments qui suivent n'ont trait qu'aux plaintes reçues et aux sanctions ordonnées par cette Autorité.

[18] Source : DGCCRF, *"Bilan de l'action de la DGCCRF sur la Toile en 2012"*

-6017 plaintes ont été reçues par la C.N.I.L. en 2012 ; ce chiffre est en augmentation constante.

-31% d'entre elles concernaient Internet ou le domaine des télécommunications, essentiellement pour revendiquer un droit à l'oubli *(sous la forme de suppression de photographies, de vidéos, de commentaires, de coordonnées, notamment sur les réseaux sociaux ou dans les réfèrencements des moteurs de recherche*) ; toutefois de nombreuses plaintes avaient aussi trait à la réception de spams non sollicités et au harcèlement sur les réseaux sociaux
21% concernaient le secteur du commerce
15% le domaine du travail
10% les organismes bancaires
8% les libertés publiques et les collectivités locales

-Tous domaines confondus, l'opposition à figurer dans un fichier constituait le principal motif de saisine de la CNIL.

-43 mises en demeure ont été effectuées, 13 sanctions ordonnées à l'encontre de sociétés, de collectivités locales, d'écoles...et prenant la forme soit d'un avertissement, soit d'une sanction pécuniaire, soit d'une injonction de cesser le traitement.

□ Les jeux en ligne illicites à travers l'action de l'Autorité de régulation des jeux en ligne (ARJEL)

Créée par la loi n° 2010-476 du 12 mai 2010 ouvrant à la concurrence les jeux d'argent et de hasard en ligne, l'ARJEL a pour mission de réguler ce secteur - qui concernait, en 2012, 2 millions de joueurs ayant misé 45 millions d'euros - et de lutter contre les sites illégaux.

Depuis sa création, l'ARJEL a envoyé 1.400 mises en demeure correspondant à autant d'infractions, qui ont été suivies d'une mise en conformité dans 92% des cas.
S'agissant des récalcitrants, 85 sites illégaux ont été assignés et 49 d'entre eux ont été bloqués sur décision judiciaire ; les parquets ont été aussi saisis de plusieurs dénonciations.

□ l'exploitation des signalements reçus par la Plate-forme PHAROS *(Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements, gérée par l'Office central*

Même si cette exploitation n'a pas de valeur statistique, puisque PHAROS reçoit, pour l'essentiel, des signalements effectués d'initiative par les internautes et que les *"qualifications"* auxquelles ces derniers procèdent requièrent une vérification juridique, l'importance des signalements reçus *(près de 120.000 pour 2012 [19])* mérite que l'on y prête attention.

[19] Source : OCLCTIC, *"PHAROS, bilan de l'année 2012"*, note du 14.06.2013

Extraits du bilan 2012 de la plate-forme PHAROS

↗ 56% des signalements ont trait à des **escroqueries et extorsions**, proportion en hausse par rapport aux années antérieures ; en valeur absolue, la croissance est forte *(67.349 faits en 2012 contre 49.262 en 2011) ;*

↘ 12% concernent des atteintes aux mineurs *(essentiellement pédopornographie et atteintes sexuelles)*, qui sont en forte baisse tant en valeur relative qu'en valeur absolue*(14.696 en 2012 contre 21.912 en 2011) ;*

↗ 8% ont trait à des **actes xénophobes ou racistes ou encore discriminatoires**, qui sont à un niveau équivalent en valeur relative mais qui continuent à croître en valeur absolue par rapport aux années antérieures *(9.431 en 2012 contre 8.967 en 2011).*

□ les fraudes à la carte bancaire selon l'Observatoire de la sécurité des cartes de paiement (OSCP)

L'Observatoire a été créé par la loi n° 2001-1062 du 15 novembre 2001. Composé d'élus, du Gouverneur de la Banque de France, de représentants des ministères, d'émetteurs de cartes de paiement, du Conseil national de la consommation, d'entreprises de commerce, il a essentiellement pour mission de favoriser la concertation sur la question de la sécurité des cartes de paiement, de sensibiliser les émetteurs et commerçants, d'assurer une veille technologique en matière de cartes de paiement et de suivre l'évolution des fraudes.

Cette évolution est mesurée annuellement à partir des données des établissements financiers.

Extraits du 10ème rapport annuel d'activité relatif à l'exercice 2012 de l'Observatoire de la sécurité des cartes de paiement

-Le nombre de cartes mises en opposition en 2012 suite à au moins une transaction frauduleuse s'élève à **767.000**, soit + 3% par rapport à 2011, chiffre qui était déjà en forte progression (+ 16%) par rapport à 2010.

-Le montant moyen d'une transaction frauduleuse était de 125 €.

-Le taux de fraude à la carte bancaire sur l'ensemble des paiements s'élevait, en 2011 comme en 2012, à 0,08%, pour un préjudice global évalué, respectivement, à 413,2 et à **450,7 millions d'euros**.

-La fraude sur les transactions internationales augmente de 11,2%, que l'Observatoire explique par la recrudescence, lors des séjours à l'étranger, des vols de cartes et des compromissions des données de cartes, mais aussi par une très forte croissance de la fraude sur Internet s'agissant des sites situés à l'extérieur des frontières nationales (+ 37%).
Le montant de cette fraude internationale atteint 224 millions d'euros.
Le risque de fraude de ce type s'avère beaucoup plus fort que la fraude nationale, puisqu'il représente, au regard du montant des opérations en jeu, près de 0,4%.
La fraude sur les paiements à distance auprès de e-commerçants étrangers réalisés avec des cartes françaises a très fortement augmenté, vraisemblablement parce que les sites situés à l'étranger sont moins bien protégés que les sites de commerce en ligne situés en France.

-La fraude sur les transactions nationales s'accroît de 7,1%, progression qui serait due à une hausse très forte des attaques de distributeurs automatiques de billets *(+ 73% par rapport à 2011)* et des points de vente, devenus des cibles privilégiées pour les réseaux de fraude organisés, auxquelles s'ajoute un nombre élevé des vols de cartes avec leur code confidentiel. Si le taux de fraude sur les paiements à distance est en baisse tout en demeurant 20 fois plus élevé que celui constaté à propos les paiements de proximité, ces fraudes concentrent 61% des opérations frauduleuses nationales.
Plus précisément, le taux de fraude de paiement sur Internet diminue, suite au déploiement de dispositifs d'authentification renforcés du porteur de la carte, mais il continue à augmenter pour les paiements à distance effectués par courrier ou par téléphone.

-L'origine de la fraude dans les paiements nationaux : dans 61% des cas, il s'agit de numéros de carte usurpés ; les pertes et vols de cartes représentent 35% ; la contrefaçon n'est à l'origine que de 2,6% des fraudes et l'ouverture frauduleuse d'un compte que de 1%.

□ les fraudes à la carte bancaire résultant de l'enquête nationale annuelle de victimation menée par l'INSEE et l'ONDRP

Depuis 2011, cette enquête, menée auprès de 17.000 ménages, permet d'appréhender les débits frauduleux sur carte bancaire dont s'estiment victimes les personnes résidant en France métropolitaine *(hors litiges avec des créanciers, vols de chèque ou de carte bancaire, omissions de carte dans un distributeur, ou extorsion de données confidentielles par la violence ou la menace)* [20].

Extraits de l'enquête annuelle de victimation *"cadre de vie et sécurité"* réalisée en 2013 par l'INSEE et l'ONDRP

-1,8% ménages *(soit 501.000 ménages pour 868.000 débits frauduleux estimés)* déclaraient avoir été victimes, en 2010, d'au moins un débit frauduleux sur un de leurs comptes bancaires; la proportion s'est élevée à 2,3% en 2011 *(soit **649.000 ménages** ayant déclaré **1,134 million de débits frauduleux estimés**)*, ce qui correspond à une augmentation très significative.

-Pour 52% des ménages, le débit frauduleux le plus récent a été effectué dans un commerce en ligne, localisé le plus souvent en France, ce qui signifie que des informations bancaires confidentielles ont été utilisées pour procéder à un achat sur Internet.
-Pour 13% d'entre eux, ce même débit a été effectué dans un commerce traditionnel situé, majoritairement, à l'étranger et à l'aide, par exemple, d'une carte contrefaite.
-Pour 7%, il s'agissait d'un virement effectué par l'auteur depuis leur compte bancaire.
Une proportion identique déclarent avoir été victimes d'un retrait frauduleux à un distributeur automatique de billets.

-Le préjudice subi est variable selon les enquêtes 2011-2012 cumulées : dans 27% des cas, il est égal ou inférieur à 100 € ; dans 25% des cas, il est compris entre 100 et 300 € ; 29% entre 300 et 1.000 € et 19% supérieur à ce dernier montant.

-70% des ménages ont pris conscience de la fraude à la consultation de leurs relevés bancaires, 22% ont été avisés par leur établissement bancaire.

[20] Source : GUILLANEUF (Jorik), chargé d'études statistiques à l'ONDRP, *"les débits frauduleux sur comptes bancaires déclarés par les ménages au cours des enquêtes "Cadre de vie et sécurité"*, in Repères 20, publication de l'Institut national des hautes études de la sécurité et de la justice *(INHESJ)* et de l'ONDRP; n°20, janvier 2013

-56% des ménages ignorent les conditions dans lesquelles les informations bancaires confidentielles leur ont été dérobées, mais 15% déclarent que cela a fait suite à un achat ou à une réservation sur Internet.

-En 2011, **42% des ménages victimes ont déposé plainte** *(taux en baisse)* et 9% ont fait une déclaration de main courante.

-77% des ménages victimes ont été remboursés par leur banque *(6% étaient en attente de réponse, 7% s'étaient heurtés à un refus et 9% n'avaient formulé aucune demande de ce type).*

Toutefois la tendance à la plainte comme à la demande d'indemnisation est directement fonction du montant du préjudice.

□ la cybercriminalité et l'enquête annuelle réalisée par le CLUSIF

Le Club de la sécurité de l'information Français (CLUSIF) est une association indépendante rassemblant des entreprises, des collectivités territoriales mais aussi des administrations, qui s'est fixée pour objectif d'agir pour la sécurité de l'information et de sensibiliser à cette question tous les acteurs concernés ; elle aide les entreprises à mieux sécuriser leurs réseaux et leurs systèmes d'information.

Chaque année depuis 2002, elle publie les résultats d'une enquête sur les menaces informatiques et les pratiques de sécurité effectuée auprès des entreprises de plus de 200 salariés, des collectivités d'une certaine taille, des hôpitaux mais aussi de 1000 internautes ; elle réunit enfin des assises pour dresser un panorama de la cybercriminalité.

Extraits des résultats de l'enquête du CLUSIF sur les menaces informatiques et pratiques de sécurité en France, édition 2012

-la technique du stockage des informations dans *"l'informatique dans les nuages" (cloud computing)* est encore peu utilisée par les entreprises questionnées *(14%)*, essentiellement pour des raisons tenant à la problématique de la sécurité des données.

-**les infections par virus** restent la première source d'incidents d'origine malveillante pour les entreprises *(23% des entreprises concernées)*, avant les vols ou disparitions de matériels *(19%)*. Quant aux attaques logiques ciblées, elles n'ont concerné que 3% des entreprises, de même que les fraudes informatiques ou touchant aux systèmes de télécommunication. On dénombre aussi 2% d'entreprises concernées par des actes de dénigrement ou d'atteintes à l'image, autant d'intrusions sur les systèmes d'information, ainsi qu'1% d'entreprises victimes de sabotages physiques.

- **seules 6% des entreprises déposent plainte** suite à un incident de sécurité.

□ la cybercriminalité réprimée à travers les statistiques judiciaires

A la demande du groupe interministériel, *le pôle d'évaluation des politiques pénales* déjà cité a mis en exergue, au regard de chacune des infractions définies par la loi comme relevant, par leur objet ou en fonction du moyen utilisé, de la cybercriminalité, le nombre de condamnations prononcées en 2008, 2009, 2010, 2011 et 2012, ainsi que les peines principales [21]. Il s'agit donc des infractions élucidées, qui ont donné lieu à poursuite *(les alternatives aux poursuites ne sont pas prises en compte).*

En revanche, les condamnations relatives aux nombreuses infractions qui, bien que souvent commises par le biais d'un système d'information et de communication, ne font pas l'objet d'une incrimination spécifique au plan légal n'ont pas été comptabilisées, le Casier judiciaire national automatisé ne disposant d'aucun moyen pour les isoler.

-En 2012, **2222 condamnations ont été prononcées pour des crimes (5) ou délits spécifiquement visés par la loi comme faisant partie de la cybercriminalité.**

-Un gros tiers concerne des atteintes aux personnes *(817 condamnations)*, en forte augmentation depuis 2010 compte-tenu d'une répression accrue de la pédopornographie mais aussi du proxénétisme aggravé en cas de contact par le biais d'un réseau de communications électroniques

-Les infractions à la loi sur la presse font quasiment jeu égal *(800 condamnations),* mais leur nombre, en augmentation par rapport à 2011, régresse par rapport aux années antérieures; prédominent les injures racistes, les diffamations et les autres types d'injures.

-Puis viennent les infractions aux instruments de paiement *(321 condamnations)*, dont le nombre diminue par rapport à la période 2008-2010 suite à la modification de la politique pénale ; l'usage d'instrument de paiement contrefait ou falsifié prédomine, suivi de l'usage d'instrument de paiement contrefait ou falsifié, de la détention d'équipements destinés à la contrefaçon-falsification ou de la contrefaçon-falsification elle-même

-Les atteintes aux S.T.A.D. *(182 condamnations)* sont en nombre plus important que les années antérieures, à l'exception de 2010 *(252 condamnations)* ; cette progression concerne moins les intrusions que les modifications frauduleuses de données.

-La captation frauduleuse de programmes télédiffusés *(47 condamnations)*.

-Les infractions dites Informatique et liberté *(44 condamnations)*, qui progressent.

-Toutefois nombre d'infractions ne donnent lieu qu'à quelques condamnations par an, voire à aucune.

[21] L'intégralité de cette exploitation figure dans les annexes terminales du rapport

5.- Les tendances actuelles de la cybercriminalité

Nonobstant les difficultés de comptage, les principaux acteurs étatiques spécialisés dans la lutte contre la cybercriminalité relèvent que le nombre de cyber-délinquants augmente de manière significative et que leurs modes opératoires se sont, tout à la fois, diversifiés et complexifiés.

Le nombre de cybercriminels augmente en raison, notamment, d'une offre technique qui évolue, se vulgarise et s'avère désormais facilement accessible : l'époque où le cybercrime était le fait de quelques férus d'informatique est désormais révolue : aujourd'hui, tout un chacun peut se fournir sur le marché parallèle d'Internet [22] en virus et autres programmes malveillants. En particulier, l'utilisation croissante de moyens d'anonymisation des connexions *(tel TOR)* engendre une forte progression des comportements délinquantiels du fait du sentiment d'impunité qu'elle génère.

La cybercriminalité se diversifie. Schématiquement, l'on peut distinguer

- **les cybercriminels de droit commun**, de loin les plus nombreux, parmi lesquels prédominent :

*Les **délinquants sexuels**, avec la pédopornographie, véritable plaie d'Internet contre laquelle le monde entier se mobilise, qui s'accompagne parfois de passages à l'acte ; par-delà, l'on trouve aussi du proxénétisme organisé.

*Les **cyberviolents** qui s'en prennent aux personnes *(menaces, insultes, diffamations, harcèlements via Internet)* : comme l'énonce Marc KNOBEL, l'Internet devient, trop souvent, un exutoire à la haine contre des catégories entières ou contre une personne déterminée ; l'on y décèle aussi des risques sectaires qui se cachent sous les nombreuses offres à caractère soit-disant thérapeutique ou de développement de la personnalité.

*Les **cyberescrocs** motivés par l'appât du gain et qui relèvent, pour l'essentiel, d'une délinquance à grande échelle, très organisée mais aussi très imaginative: d'une part, toute la masse des escroqueries, qui prennent des formes de plus en plus diverses pour convaincre l'internaute de commettre l'erreur qui lui sera fatale *(le hameçonnage, l'escroquerie aux emplois d'appoint, le blocage avec demande de rançon, l'amende fictive à payer, l'escroquerie à la réservation de la chambre d'hôtel, l'escroquerie à la Nigériane ou à la fausse loterie, l'escroquerie sentimentale, le chantage à la "web-cam"...et la plus lucrative d'entre toutes qui fait actuellement des ravages dans les entreprises françaises : l'escroquerie par faux ordres de virement)* ; d'autre part, les fraudes par cartes bancaires avec l'interception des données sur Internet, le *skimming* qui s'attaque aux distributeurs automatiques de billets, ou encore le piratage des terminaux de paiement chez les commerçants ; mais aussi, les fraudes téléphoniques par détournement des services surtaxés ; et enfin tous les types possibles de contrefaçons liés à l'extension du commerce en ligne *(contrefaçons de marques, de logiciels, de produits relevant de la propriété intellectuelle, de médicaments...)* ; sans oublier les jeux illégaux.

[22] et notamment sur le *"web profond" (Deep web)* et les *"réseaux sombres" (Darknets)* auxquels s'intéresse le nouveau *Centre européen de lutte contre la cybercriminalité*

Il faut toutefois prendre aussi en compte les nombreux trafics qui prospèrent sur Internet, tel le florissant marché des drogues de synthèse ou le blanchiment du produit du crime..

⌞ **les cybercriminels qui concentrent leurs attaques sur les entités étatiques et les opérateurs d'importance vitale** *(cf. titre II, chapitre 1 sur la cybersécurité)* ; parmi ces cybercriminalité, la Direction centrale du renseignement intérieur *(DCRI)* distingue

*Les **cybermercenaires,** qui proposent leurs services sur un marché Internet souterrain, afin de perpétrer des attaques pour le comptes d'Etats, d'individus ou d'organisations ne souhaitant pas apparaître ou ne possédant pas la technicité ou la ressource nécessaire; ce système fonctionne exclusivement par cooptation et sous "contrat". Il n'y a toutefois pas de frontières étanches avec la catégorie précédente puisque ces mercenaires peuvent se livrer aussi bien à des activités d'espionnage qu'à de la criminalité de nature financière.

*Les **cyberespions**, qui réalisent des intrusions afin de s'approprier des informations stratégiques et économiques. Ces attaques sont principalement commanditées par des Etats, alliés ou non de la France. En parallèle, le cyberespionnage économique *(vol de données par un concurrent)* constitue aussi une menace majeure.

*Les **cyberterroristes,** animés par des idéologies extrémistes, qui utilisent Internet, de manière plus intensive depuis quelques mois, comme une tribune et un moyen de radicalisation. Ils ont recours, par exemple, à des forums islamiques dédiés et de plus en plus sécurisés compte-tenu du niveau technique élevé de leurs développeurs, pour diffuser leur propagande, recruter et échanger des informations opérationnelles. Suite au *"Printemps arabe"*, la propagande islamiste s'est aussi répandue via les réseaux sociaux, tels Facebook, Twitter et Youtube, chaque groupe armé et chaque brigade possédant désormais un compte qu'il alimente par "l'actualité" en provenance du terrain.

Les cibles de la cybercriminalité n'épargnent aucune catégorie de victimes potentielles, depuis les particuliers eux-mêmes, utilisateurs d'Internet, jusqu'au monde de l'entreprise et les services de l'Etat.

⌞Les enfants, les personnes vulnérables et les personnes âgées sont particulièrement visés par les délinquants sexuels et les cyber-escrocs.

⌞Les petites et moyennes entreprises comme l'industrie sont, quant à elles, les cibles privilégiées des cyber-attaques contre les systèmes de traitement automatisé de données.

Selon une étude récente réalisée par la société éditrice de logiciels anti-virus KAPERSKY, plus d'un tiers des entreprises françaises de moins de 250 salariés auraient été victimes de telles attaques en 2013, en augmentation de 42% par rapport à l'année antérieure. Le choix de ces PME comme des sous-traitants n'est pas anodin car il permet aussi d'atteindre indirectement des grands groupes normalement mieux armés contre ces menaces.

⌞L'Etat et les entreprises sensibles au titre de la souveraineté nationale ne sont pas davantage épargnés, pour les raisons déjà mentionnées, ainsi que l'illustrent les attaques menées, ces dernières années, contre le ministère de l'Economie et des Finances *(décembre 2010)* mais aussi contre AREVA, E.D.F.

(Avril 2011), la Gendarmerie, le ministère de la Justice, le Sénat *(janvier 2012)* et bien d'autres, car peu ont été rendues publiques.

Les modes opératoires se diversifient et se complexifient.

⌞Les attaques contre **le matériel** ont des visées principalement financières.

Parmi les plus citées, figurent le *skimming (copie de carte de paiement par capture de bande magnétique ou vol du support des cartes elles-mêmes)*, le piratage croissant des terminaux de paiement et des autocommutateurs téléphoniques *(afin de passer des appels surtaxés)*.
La mise à disposition sur le marché de moyens de paiement incluant une puce RFID augmente l'exposition à cette menace, dans la mesure où le protocole régissant ces puces est toujours en cours de sécurisation.
La mise en ligne de tutoriaux pour pirater du matériel de loisir *(console de jeux, équipements de communication : téléphone portable, tablette)* s'avère aussi extrêmement lucrative et représente un préjudice financier non négligeable ; en outre, certains constructeurs paraissent aujourd'hui être les vecteurs de ce type d'attaques, lorsque l'on constate que le matériel certifié est différent du matériel réellement mis sur le marché, des composants majeurs susceptibles de favoriser des actes malveillants ayant été introduits.

⌞Sur **le plan logique**, si tous les systèmes d'exploitation sont touchés, *Android* est le plus affecté car il est majoritairement utilisé.
Les architectures informatiques restent vulnérables aux attaques de type *défiguration* ou *DdoS*, les réseaux d'ordinateurs *"zombies"* étant toujours facilement accessibles et bon marché.
Les cyberdélinquants profitent par ailleurs de l'utilisation de matériels personnels sur les réseaux d'entreprise pour attaquer ces équipements connectés.
En revanche, la contrefaçon de logiciels reste à un niveau stable.

⌞**Les données** sont les cibles finales des attaques organisées. A coté du traditionnel envoi de courriels piégés, les techniques de *l'hameçonnage (phishing)* et du point d'eau *(waterholing)* permettent aux cyberescrocs et au cyberespions, souvent après une phase *"d'ingénierie sociale"*, de pénétrer plus ou moins en profondeur les infrastructures, pour en dérober des données à fort potentiel stratégique ou financier.

Le chantage par la rétention volontaire des données de l'utilisateur *(ransomwares)* est aussi un mode d'attaque qui prend de l'essor du fait de sa facilité de mise en oeuvre et des bénéfices susceptibles d'en être retirés. L'utilisateur *(privé ou professionnel)* qui navigue sur un site piégé voit ainsi l'accès à son ordinateur et/ou à ses données partiellement ou totalement entravé, et ne peut espérer obtenir le code de déblocage que contre un paiement en ligne.

Sur un plan plus général, l'avenir de la cybercriminalité sera fonction de la capacité à limiter les effets néfastes d'un cyber-espace qui est appelé à brasser de plus en plus de données, rendues ainsi plus vulnérables.

D'ores-et-déjà, les données personnelles ou professionnelles n'ont jamais été aussi nombreuses sur Internet. Le *"big data"* connaît son âge d'or. L'arrivée, dans les quatre ans à venir, d'un milliard et demi d'internautes supplémentaires au plan mondial va encore accroître ce marché.

Les sociétés de service de l'Internet *(les prestataires techniques au sens du droit français)* stockent, suivent, analysent et recoupent en permanence ces données, à des fins économiques, et en facilitent l'accès quelle qu'en soit la nature.

Parmi ces dernières, les réseaux sociaux sont les grands acteurs du monde connecté. Le réseau Facebook, fondé il y a juste 10 ans et qui compte en France 26 millions d'utilisateurs actifs, vient ainsi de mettre en ligne l'ensemble des 1.273.873.443 profils existants. Twitter, qui vient de s'introduire en bourse, a comptabilisé, depuis sa création, en 2006, plus de 170 milliards de tweets et 500 millions d'utilisateurs au plan mondial.

Au-delà de l'utilisation qui peut être faite de ces données et des questions de souveraineté qu'elles posent, leur transport comme leur stockage de masse constitue un point de faiblesse qui intéresse les cyber-délinquants *(cf. le piratage dont vient d'être victime Orange)* comme les Etats *(cf. l'affaire Prism).*

La technologie dite de *"l'internet en nuage" (cloud computing)*, de plus en plus prisée pour des raisons de facilité et de coût par les entreprises et les consommateurs qui veulent héberger leurs données sensibles sur des serveurs extérieurs, constitue aussi un nouveau défi, eu égard au risque d'intrusion qu'elle génère [23].

Parallèlement, le nouveau marché des objets connectés est en pleine expansion. Appliqué au secteur de l'automobile, au domaine médical ou à des systèmes techniques du quotidien *(chauffage central, climatisation...)*, il va révolutionner nos modes de vie à court terme, en accentuant le recours à la robotisation et à l'automatisation. D'ores-et-déjà, un informaticien de 28 ans a mis au point un moteur de recherche *(SHODAN)* qui a repéré sur Internet plus de 1,5 milliard d'appareils déjà connectés au réseau. On estime qu'en 2020, ce chiffre dépassera les 50 milliards d'objets...
Comme les données déjà présentes sur Internet, ces nouvelles techniques poseront la question de la sécurisation de ces outils intelligents mais aussi de leur contrôle, car l'usurpation de profils Internet susceptibles de favoriser des prises de contrôle à distance a déjà débuté.

▬▬▬▬▬

[23] Toutefois, certains professionnels d'Internet *(notamment OVH)* ont conçu des *clouds* sécurisés, intégrant des solutions de cryptographie ; cf., sur ce point, les analyses et synthèses de *l'Autorité de contrôle prudentiel de la Banque de France* sur *"les risques associés au Cloud computing" (n°16, juillet 2013).*

I.2.- Les réponses actuelles à la cybercriminalité en France : de l'appréhension normative à la spécialisation de la police judiciaire pour une efficacité relative

Confrontée à ce phénomène nouveau que constitue la cybercriminalité, la France s'est dotée d'un "arsenal" juridique important ainsi que de services d'investigation performants. Néanmoins, l'efficacité de son action reste encore relative.

1.- Un droit riche et souvent novateur

Pionnière en cela au plan européen, la France disposait déjà d'une loi régissant les données informatiques au regard de la nécessaire protection des libertés *(loi n°78-17 du 6.01.1978 relative à l'informatique, aux fichiers et aux libertés)* qu'elle a su mobiliser pour faire face aux nouvelles contraintes générées par le développement des traitements automatisés de données à caractère personnel *(cf., notamment, les modifications résultant de la loi n° 2004-801 du 6.08.2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel)* ; elle s'attache aujourd'hui à adapter ce cadre juridique au nouveau défi posé par les systèmes d'information et de communication, notamment Internet et ses différents prestataires [24].

Dix ans plus tard, la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite loi Godfrain, définissait et réprimait, pour la première fois, les atteintes aux systèmes de traitement automatisé de données *(cf., depuis la refonte du code pénal, les art. 323-1 s.)*.

Par la suite, et au fur et à mesure que des instruments européens étaient adoptés, le législateur français les a transposés en droit français tout en continuant son travail d'adaptation de la norme à cette nouvelle forme de délinquance.

En 2004, la loi pour la confiance dans l'économie numérique *(loi n° 2004-575 du 21.06.2004)* constitua une avancée décisive dans la communication en ligne ; tout en proclamant le principe de liberté de communication, elle définissait le régime juridique des prestataires techniques, encadrait le commerce et la publicité électroniques ainsi que le recours aux moyens de cryptologie, et énonçait les bases du développement des technologies de l'information et de la communication.

C'est aussi en 2004 que furent posés les principes et modalités du système de nommage sur Internet *(cf. loi n° 2204-069 du 9.07.2004 relative aux communications électroniques et aux services de communications électroniques et son décret d'application n° 2007-162 du 6.02.2007 relatif à l'attribution et à la gestion des noms de domaine de l'Internet et modifiant le code des postes et des communications électroniques)*.

---

[24] A noter toutefois que les dispositions de cette loi *"ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises" (cf. art.4)*.

Cette même décennie 2000 vit plusieurs lois successives adapter le droit pénal à certaines formes de cybercriminalité et créer des moyens d'investigation spécifiques pour la combattre *(cf. loi n° 2001-1062 du 15.11.2001 relative à la sécurité quotidienne, loi n° 2003-239 du 18.03.2003 pour la sécurité intérieure, loi n° 2004-204 du 8.03.2004 portant adaptation de la justice aux évolutions de la criminalité, loi n° 2206-64 du 23.01.2006 relative à la lutte contre le terrorisme, loi n° 2007-297 du 5.03.2007 relative à la prévention de la délinquance, loi n° 2011-267 du 14.03.2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite "LOPSI II"...)*.

Et cela, sans compter les lois spécifiques, relatives, par exemple, à la protection du droit d'auteur contre la contrefaçon et la copie numérique illicite *(loi n° 2009-669 du 12.06.2009 favorisant la diffusion et la protection de la création sur Internet ; loi n° 2009-311 du 28.10.2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet - dites loi "Hadopi")*, ou encadrant l'ouverture à Internet de nouveaux produits ou services réglementés *(cf. loi n° 2010-476 du 12.05.2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne),* ou encore transposant certaines directives européennes.

Pour l'essentiel, la France dispose d'outils juridiques abondants, dans tous les domaines affectés par la cybercriminalité.

Les instruments européens, qu'ils émanent du Conseil de l'Europe ou de l'Union européenne, ont complété, très utilement, les normes internes, notamment en terme d'investigations transnationales et de coopération *(gel des données, équipes communes d'enquête, mandat d'arrêt européen...).* Et la France a aussi souvent joué un rôle important dans leur élaboration.

2.- <u>des mécanismes de régulation variés</u>

Outre le recours au droit pénal et aux institutions répressives de l'Etat, le législateur et l'autorité réglementaire firent appel à plusieurs types de mécanismes de régulation, souvent complémentaires :

- l'auto-discipline des professionnels, l'Etat les incitant à se doter de chartes de déontologie ou de codes de bonne conduite et à mettre en oeuvre des mécanismes de prévention et de réaction adaptés

- la co-régulation de ces mêmes professionnels, illustrée notamment par le développement du partenariat public/privé dans le cadre d'instances spécifiques, le plus souvent sous la forme associative ou d'observatoires, à l'exemple du *"Forum des droits sur Internet"* créé, d'initiative publique, en décembre 2004 ; un tel partenariat s'est révélé particulièrement intense dans les domaines où les sociétés privées ont, elles-mêmes, économiquement intérêt à lutter contre la cybercriminalité, par exemple dans le domaine du commerce en ligne ou dans la lutte contre les spams [25]

[25] cf., à titre d'exemple, le livre blanc publié par la FEVAD *(Fédération e-commerce et vente à distance)* en octobre 2013 sur *"les moyens de sécurisation des paiements sur Internet - la lutte contre la fraude vue par les e-marchands".*

⌙le renvoi à des mécanismes indemnitaires particuliers, comme, par exemple, en matière de fraudes aux cartes bancaires

⌙la création de dispositifs de contrôle/sanction mis en oeuvre par certaines administrations spécialisées

⌙le recours à des autorités administratives indépendantes, dont la plus ancienne mais aussi la plus importante est la *Commission nationale de l'informatique et des libertés*, dotée d'un pouvoir d'avis a priori mais aussi d'un pouvoir de contrôle a posteriori ainsi que d'un arsenal de sanctions qui vont de l'avertissement et de l'injonction jusqu'à la sanction pécuniaire.
Relèvent aussi d'un tel dispositif la *Haute autorité pour la diffusion des oeuvres et la protection des droits sur Internet (HADOPI)* et l'*Autorité de régulation des jeux en ligne (ARJEL).*

⌙enfin la Justice civile, avec ses procédures de référé et de requête, en toute matière où les droits de la personne sont lésés, en particulier pour les infractions en matière de presse.

Evolutifs dans le temps, parfois redondants et à l'action pas toujours coordonnée, ces dispositifs ont toutefois été à l'origine d'avancées décisives et d'une amélioration progressive de la lutte contre la cybercriminalité prise globalement, sur le plan de la prévention, de la sensibilisation comme des sanctions.

Il reste, sans doute, à mieux déterminer le rôle de la Justice - d'abord civile, ensuite pénale - dans la lutte contre la cybercriminalité au regard de l'ensemble des autres modes de réponse existants, et notamment des modes alternatifs de règlement des conflits comme des sanctions de nature administrative dont le champ progresse dans certains secteurs. Si l'on attend plus de réactivité de la Justice pénale, il semble de bonne politique que, sauf pour les atteintes graves, elle ne soit saisie qu'en cas d'échec ou d'ineffectivité des autres modes.

3.- des services d'investigation spécialisés

Comme la cybersécurité ou la cyberdéfense *(voir Titre II, chapitre 1., s'agissant notamment de l'ANSSI)*, la lutte contre la cybercriminalité repose sur des services spécialisés à très haute compétence technique [26].

31 - Deux d'entre eux relèvent, au plan central, du ministère de l'Intérieur.

[26] Dans les développements qui suivent, il n'est question que des services spécialisés : bon nombre d'autres services relevant du ministère de l'Intérieur, notamment plusieurs Offices centraux, constituent aussi des acteurs privilégiés dans la lutte contre la cybercriminalité

◆ l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

Ce service a été par décret du 15 mai 2000 et placé au sein de *la Direction centrale de la police judiciaire (sous-direction de la lutte contre la criminalité organisée et la délinquance financière)*. Il est composé de policiers et de gendarmes.

Il s'agit d'une structure mixte d'enquête et d'assistance ; en outre, son statut d'office central national lui confère une mission interministérielle de centralisation, d'analyse et de communication.

⌞Au plan opérationnel, doté d'une compétence judiciaire nationale, l'office peut procéder à tous les actes d'enquête à la demande des autorités judiciaires, seul ou en assistance d'autres services d'investigation. Il a vocation à connaître des affaires présentant soit une spécificité technologique novatrice, soit un caractère national nécessitant une vision centralisée, soit encore une composante internationale forte dans laquelle sont impliquées des équipes de malfaiteurs relevant de la criminalité organisée.

A cette fin, sa section opérationnelle comprend 4 groupes d'enquête spécialisés

*dans les atteintes portées aux systèmes de paiement et cartes à puce *(contrefaçon, falsification et utilisation de cartes bancaires falsifiées ; acquisition frauduleuse de données bancaires par skimming, carding ou phishing ; nouvelles attaques technologiques détectées par le GIE cartes bancaires sur les cartes à puce)*,
*les fraudes aux opérateurs de communication électronique *(virus sur les smartphones, escroqueries aux micro-paiements : SMS et numéros de téléphone surtaxés, attaques des standards téléphoniques d'entreprise, spams par sms),*
*le piratage via les atteintes aux systèmes de traitement automatisé de données,
*enfin les escroqueries sur Internet *(particulièrement en ce qui concerne l'identification d'équipes organisées sévissant sur le territoire national, à l'aide de réseaux de complices qui hébergent les virements à réexpédier ou réceptionnent temporairement les colis de marchandises acquises frauduleusement, et dont les commanditaires sont principalement basés dans les pays d'Afrique de l'Ouest).*

⌞Au titre de l'assistance technique, sa section spécialisée - qui rassemble des enquêteurs hautement qualifiés dans le domaine informatique, dispose d'un matériel informatique performant et qui est dotée d'un laboratoire Forensic [27] dédié à l'exploitation et à la recherche de la preuve numérique - apporte son aide aux services d'enquête, centraux ou territoriaux, relevant tant de la police que de la gendarmerie ou des douanes, ainsi qu'aux autorités judiciaires.
Cette section assure en outre la formation des enquêteurs spécialisés de police au plan territorial.

⌞En tant qu'office centralisant l'information opérationnelle en matière de cybercriminalité, il a vocation à assurer la coordination opérationnelle entre les services de police judiciaire au niveau national.

[27] L'inforensique ou l'informatique légale désigne la recherche et l'exploitation des données présentes dans un support numérique

⌞Enfin, sa section des relations internationales lui permet d'activer l'ensemble des canaux de coopération internationale nécessaires à la lutte contre la cybercriminalité. Elle est aussi le point de contact national pour les demandes venant de l'étranger et redistribue les informations en France et vers l'étranger, par le biais du bureau central national d'Interpol, de l'unité nationale Europol ou du groupe d'alerte "G8-cybercrime" institué par la Convention de Budapest..

Depuis janvier 2009, l'office gère aussi **la plate-forme publique nationale de signalement**, en provenance tant des Internautes que des professionnels, dite plate-forme **PHAROS** *(Plate-forme d'harmonisation, d'analyse, de recoupements et d'orientation des signalements)*.

Il assure enfin une mission d'information du public confronté à des contenus illicites, à travers une autre plate-forme - *la plate-forme téléphonique d'information et de prévention sur les escroqueries sur Internet, dite* ***"Info-escroqueries"***.

En raison de sa place centrale dans la lutte contre la cybercriminalité, l'Office entretient des relations suivies avec les autres services d'enquête de la Police nationale, de la Gendarmerie nationale, mais aussi des Douanes, de la Direction générale de la concurrence et de la répression des fraudes et de la Commission nationale informatique et des libertés.

Il a aussi mis en oeuvre un partenariat étroit, en particulier dans le cadre de PHAROS, avec une centaine d'associations, d'hébergeurs et de fournisseurs de services communautaires sur Internet *(OVH, La Centrale, Vivastreet, Overblog, la LICRA, E-Enfance...)*, partenariat qui peut prendre une forme conventionnelle.

Il a enfin signé une convention avec une école d'ingénieurs *(EPITA)*, qui développe, pour son compte, des outils spécifiques dédiés à la lutte contre la cybercriminalité.

◆ Le Plateau d'investigation cybercriminalité et analyses numériques (PICyAN) du Pôle judiciaire de la Gendarmerie nationale (PJGN)

Il s'agit d'une structure mixte d'investigation et de criminalistique coordonnant *le Département informatique et électronique de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN)* et *la Division de lutte contre la cybercriminalité du Service technique de recherches judiciaires et de documentation (STRJD).*

Cette structure

⌞assure la coordination et le pilotage du dispositif global de la Gendarmerie en matière de lutte contre la cybercriminalité qui, du niveau local au niveau nationale, associe investigation et criminalistique,

⌞constitue le point de contact pour la Gendarmerie avec les offices centraux, pour les affaires traitant de la cybercriminalité.

Son activité est de trois ordres :

⌞ au plan des investigations, le PICyAN assure

*la surveillance, principalement pro-active, des différents espaces de l'Internet en vue de détecter et de caractériser les infractions ; cette surveillance peut prendre la forme d'enquêtes sous pseudonyme. Il coordonne, en outre, les enquêtes sous pseudonymes réalisées par les unités territoriales.
*La direction d'enquêtes ou l'appui aux offices centraux de la Gendarmerie et aux unités territoriales, ainsi que la direction d'opérations présentant une particulière envergure, gravité ou sensibilité.
*Au plan national, il a la responsabilité du *Centre national d'analyse des images de pédopornographie (CNAIP)* et administre la base nationale constituée à partir des enquêtes de police et de gendarmerie, aux fins d'identification des victimes et de leurs auteurs, cela en lien avec INTERPOL et les homologues étrangers du CNAIP.

␣ En matière de criminalistique, le PICyAN réalise, à la demande des magistrats et des enquêteurs, les expertises et examens techniques complexes relatifs à la preuve numérique : l'extraction de données à partir de supports électroniques, magnétiques ou optiques, et l'analyse de systèmes et de réseaux.

␣ De manière transversale, le PICYAN

*gère un guichet unique téléphonie et Internet *(GUTI)* assurant l'interface entre les opérateurs et les enquêteurs de la gendarmerie ainsi que le lien avec la future plate-forme nationale des interceptions judiciaires.
*Assure une mission de soutien de la communauté des enquêteurs spécialisés des unités territoriales de Gendarmerie en termes de formation, d'équipement et d'information
*Met en oeuvre une mission de recherche et de développement.

32 - **La Direction centrale du renseignement intérieur (DCRI)** occupe une place particulière compte-tenu de sa mission générale qui consiste à *"lutter, sur le territoire de la République, contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la Nation" (cf. art. 1er du décret n° 2008-609 du 27.06.2008).*

S'agissant de la lutte contre la cybercriminalité, elle se concentre ainsi sur les atteintes relevant de la cyberdéfense comme de la cybersécurité *(cf. titre II, chapitre 1)*, détectant et identifiant les cyber menaces ; elle est, en outre, chargée spécifiquement de *"la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'Etat"* ainsi qu'en ce domaine de *"la lutte contre la cybercriminalité".*

Cette mission statutaire s'illustre à travers différentes facettes de son activité :

␣Les enquêtes judiciaires relatives au piratage informatique des systèmes d'information sensibles
La DCRI a une compétence judiciaire pour les atteintes aux systèmes de traitement automatisé de données concernant les opérateurs d'importance vitale, les établissements disposant de zones à régime restrictif (ZRR) ou les réseaux gouvernementaux.
En outre, et de manière générale, la DCRI met à la disposition des autres services d'enquête ainsi que de l'autorité judiciaire ses capacités de déchiffrement de contenus cryptés, par le biais du *Centre technique d'assistance (CTA).*

⌞Le recueil du renseignement pour prévenir la menace informatique.
En tant que service de renseignement intérieur, la DCRI a vocation à recueillir et à traiter diverses sources d'information pour permettre à l'Etat de se prémunir contre les risques informatiques.
Elle appuie d'abord sa stratégie sur son réseau de sources humaines qui l'alerte régulièrement sur l'émergence de nouvelles menaces informatiques et leurs acteurs.
Elle entretient aussi des relations régulières avec ses partenaires étrangers, qui la préviennent des menaces susceptibles de viser la France, mais qui peuvent aussi être mobilisés pour accroître ses propres moyens d'investigation.
Elle tire enfin de précieux renseignements de ses échanges avec la communauté du renseignement français dans ses différentes composantes.
Le renseignement ainsi recueilli est analysé par les propres experts de la DCRI *(policiers spécialisés en cybercriminalité, techniciens et ingénieurs)* puis donne lieu à des synthèses et notes d'alerte à l'attention des autorités étatiques ou des opérateurs privés.

33 - Au plan des services territoriaux de police et de gendarmerie, seule la Préfecture de police de Paris dispose, au sein de la direction régionale de la police judiciaire, de services spécialisés à compétence régionale

⌞ au premier rang desquels **la Brigade d'enquête sur les fraudes aux technologies de l'information *(BEFTI)***, qui a une compétence spécifique s'agissant des atteintes aux systèmes de traitement automatisé de données, des infractions à la loi Informatique et libertés et à la loi du 21 juin 2004 pour la confiance dans l'Economie numérique, la contrefaçon numérique logicielle ou de bases de données, les atteintes aux droits d'auteur, la captation frauduleuse de programmes télédiffusés et les usages frauduleux de lignes téléphoniques.

Elle est, en outre, chargée d'assister les services d'enquête pour des investigations informatiques techniques, de sensibiliser les partenaires privés ou publics et de former les fonctionnaires de la Préfecture de police. Elle assure enfin de nombreuses interventions, aux fins de sensibilisation du grand public ou des entreprises.

⌞ bien qu'elles ne se consacrent pas exclusivement à la lutte contre la cybercriminalité, d'autres structures de la PP y contribuent activement : la brigade des fraudes aux moyens de paiement (BFMP), compétente pour l'utilisation de moyens de paiement par Internet ; la brigade de répression de la délinquance astucieuse (BRDA), dédiée à la lutte contre les escroqueries ; la brigade de répression de la délinquance contre la personne (BRDP), qui connaît notamment des infractions de presse ; et la brigade de protection des mineurs (BPM), compétente pour les infractions contre les mineurs commises, notamment, via Internet, et qui assure de nombreuses actions de sensibilisation auprès des écoles et des collèges.

⌞ Enfin, la Direction de la sécurité de Paris et de l'agglomération Parisienne (DSPAP) comprend des brigades des mineurs de la petite couronne, à compétence départementale, et deux petites cellules d'assistance technique dans les Hauts de Seine et le Val de Marne.

<u>En province,</u> il n'existe pas de services spécialisés dans la lutte contre la cybercriminalité. Toutefois, les services territoriaux de la police et de la gendarmerie *(directions interrégionales de police judiciaire, directions départementales*

des sûretés urbaines, sections de recherche, brigades départementales de renseignements et d'investigations judiciaires) disposent d'enquêteurs spécialement formés à cette lutte et très impliqués *(voir, pour plus de détails, le titre II, chapitre 3 sur la formation des acteurs).*

34 - Hors ministère de l'Intérieur, le ministère de l'Economie et des Finances a créé, au sein de la Direction générale de la concurrence, de la consommation et de la répression des fraudes, un service spécialisé - **le Service national des enquêtes (SNE).**

Outre un **Centre de surveillance du commerce électronique (CSCE)** basé à Morlaix, qui effectue une veille permanente, ce service est composé d'enquêteurs spécialisés dans la lutte contre la cybercriminalité sur l'ensemble du territoire national, regroupés en majorité à Paris mais aussi en poste dans les directions régionales. Il a vocation à procéder à des investigations sur des priorités définies au plan central, voire à l'échelon européen, en fonction des nécessités tenant à la régulation du marché mais aussi de l'actualité, tandis que les directions départementales de la population, qui ne disposent que d'un ou de deux personnels spécialisés, se focalisent davantage sur les actes de commerce courants.

> En plus de la surveillance des principaux secteurs marchands en ligne, le SNE assure une action préventive auprès des secteurs identifiés à risque - notamment les nouveaux sites du commerce électronique - et contrôle de manière systématique les sites faisant l'objet de plaintes réitérées ; à titre d'exemple, il s'est focalisé, ces derniers temps, sur les réservations d'hôtel en ligne, les prix personnalisés évolutifs, les opérations de solde sans réduction, la vente de billets d'avion à prix cassés, d'éthylotests *(après l'obligation réglementaire de détention à bord des véhicules)* ou de ventes de compteurs Geiger et de pastilles d'iode *(après l'incident nucléaire du Japon)*, les loteries publicitaires, les applications de géo-localisation sur les smartphones, les faux avis de consommateurs....
>
> Le SNE travaille en liaison étroite avec Cyberdouane pour les contrefaçons, la C.N.I.L., la plate-forme PHAROS, les réseaux européens spécialisés, par exemple, RAPEX s'agissant de la sécurité des produits *alimentaires (le SNE sert de point de contact national)*, EUROPOL...et l'ensemble des professionnels présents dans le secteur.

Sur un plan plus global, le projet de loi sur la consommation, actuellement en discussion, devrait autoriser la DGCCRF à utiliser la technique dite *"du coup d'achat"* dont dispose déjà la Douane.

35 - Au sein du ministère du Budget, la Direction générale des Douanes et des droits indirects *(Direction nationale du renseignement douanier et des enquêtes douanières - DNRED)* s'est dotée, elle aussi, d'un service spécialisé dans la lutte contre la cybercriminalité : **Cyberdouane.**

C'est un service de renseignement qui intervient exclusivement en amont de l'enquête, son rôle étant de détecter les transactions illicites sur Internet et de les transmettre, après instruction, à un service opérationnel, soit au plan central,

soit au niveau territorial, aux fins de contrôle douanier et d'enquête approfondie.

> Son action s'exerce ainsi dans tous les secteurs intéressant l'action de la douane *(trafics de contrefaçons, de stupéfiants, de cigarettes, d'armes, de médicaments, d'espèces protégées, d'oeuvres d'art...)*, à partir des priorités sectorielles définies par le ministère, des déclarations de cible effectués par les douaniers de terrain ou même d'initiative. Il dispose d'un monopole national s'agissant des investigations à opérer sur Internet lorsqu'elles ont trait à des dossiers importants. Son objectif consiste à déceler les fraudes, à effectuer des rapprochements, puis à identifier les personnes, physiques ou morales, utilisant Internet sur le territoire national pour vendre en ligne ou poster des annonces relatives à des marchandises prohibées ou fortement taxées. Enfin, lorsque plusieurs services sont saisis, il joue un rôle d'orientation.
>
> Outre les enquêteurs spécialisés de la DNRED, Cyberdouane travaille avec chaque direction régionale des Douanes, grâce à un agent relai présent dans les cellules régionales d'orientation des contrôles. Par-delà, il oeuvre en étroite liaison avec PHAROS et l'ensemble des administrations spécialisés, mais aussi avec les enseignes du commerce en ligne, les entreprises de fret et les intermédiaires financiers, avec lesquels ont été conclus des protocoles. Enfin, Cyberdouane est très impliqué dans les projets européens relatifs à la lutte contre la cyber-contrefaçon.

La DNRED dispose aussi d'une **Cellule de recueil de la preuve informatique (CRPI)**, qui intervient en appui technique des enquêteurs douaniers, lorsque ces derniers effectuent des visites domiciliaires, aux fins d'examen du contenu des disques durs d'ordinateurs et de recherche et de conservation des éléments de preuve.

36 - enfin, sur le plan judiciaire, seul **le parquet de Paris** dispose d'une section spécialisée dans la lutte contre la cybercriminalité : la section dite S2 dédiée à *"la lutte contre la délinquance astucieuse et la cybercriminalité"*, qui comprend *un pôle cybercriminalité* composé de plusieurs magistrats et d'un assistant spécialisé ; elle a à connaître, notamment, de l'essentiel des atteintes aux S.T.A.D. commises à l'encontre des administrations comme des entreprises ayant leur siège à Paris *(en l'état, le parquet de Paris est saisi de 600 affaires de cette nature, dont 16 ont donné lieu à saisine de la JIRS)* ; quant aux escroqueries et fraudes aux cartes bancaires, elles sont aussi traitées par la même section, qui peut ainsi, les concernant, bénéficier du soutien du pôle spécialisé. Les affaires poursuivies au titre des STAD relèvent ensuite de la compétence de deux chambres correctionnelles dont les membres se sont formés à cet effet.

Quant aux autres parquets des ressorts des cours d'appel de Paris et de Versailles, ils disposent de magistrats référents mais pas de services spécialisés.

En ce qui concerne enfin les parquets de province, si certains peuvent compter sur les magistrats ayant suivi une formation permanente dans le domaine de la cybercriminalité, il n'existe pas, à proprement parler, ni de référents, ni de services spécialisés, bien que les juridictions inter-régionales spécialisées *(J.I.R.S.)* montent, peu à peu, en puissance, s'agissant de certaines formes de cybercriminalité *(ex. des escroqueries par faux ordres de virement).*

Grâce à l'ensemble de ces services spécialisés, à la motivation et au professionnalisme de leurs membres, mais aussi à l'ensemble des fonctionnaires et magistrats de terrain qui ont acquis une compétence spécialisée, tant l'action de renseignement que l'action répressive ont incontestablement marqué des points ces dernières années.

4.- La lutte contre la cybercriminalité : une efficacité encore relative

Même si la montée en puissance des dispositifs de signalement des activités et contenus illégaux sur Internet constitue une source d'information précieuse ; même si l'action des Autorités indépendantes permet d'encadrer de plus en plus les pratiques des professionnels de l'Internet ; même si nombre de juges civils jouent un rôle décisif dans l'évolution de la jurisprudence ; même si enfin la mobilisation de l'ensemble des acteurs répressifs aboutit à des résultats non négligeables, force est de constater que la lutte contre la cybercriminalité rencontre encore bien des obstacles.

Le constat comme l'élucidation des formes les plus organisées de cette délinquance doivent être renforcés.

Quant aux décisions judiciaires, les décisions civiles peinent à être effectives compte-tenu des difficultés rencontrées dans leur mise à exécution ; les réponses pénales, quant à elles, ne sont pas toujours adaptées à la gravité de l'infraction ou au préjudice des victimes.

Le constat peut étonner eu égard à l'importance des outils juridiques disponibles.

Il a toutefois de multiples causes :

❖l'insuffisance de la prévention, dans la mesure où nombre d'actes délinquantiels reposent sur la contribution involontaire des internautes, sous la forme, par exemple, de la fourniture de données sensibles, ou sur un manque de prudence des entreprises ou de leurs salariés.

❖Des mécanismes de "veille" ou des investigations d'initiative insuffisants par rapport au volume des données circulant sur Internet et qui sont essentiellement le fait de quelques Autorités ou services centraux spécialisés en fonction des moyens qui leur sont dévolus.

❖Des dispositifs de signalement, certes précieux, mais multiples et ignorés de la majorité des internautes.

❖La technicité de cette délinquance, dont l'appréhension requiert une sensibilisation et une formation beaucoup plus généralisées.

❖L'évolution incessante des procédés délinquantiels, de plus en plus sophistiqués, par exemple en matière de virus malfaisants ou d'escroqueries, qui requièrent une adaptation quotidienne de la part des services d'investigation et de justice.

❖ Au plan juridique, le droit spécifique, qui relève de corpus différents, reste peu accessible aux non initiés ; il est, de plus, essentiellement mouvant [28], les multiples initiatives normatives peinant, au surplus, à s'inscrire dans un cadre cohérent et consensuel sur le moyen terme.

❖Un mode inadapté de traitement d'un contentieux qui, souvent massif, exige des recoupements car il est bien rare qu'un cyber-escroc se limite à quelques victimes, ce qui nécessite une évolution des organisations, qui a commencé mais qui est loin d'être achevée.

❖L'impuissance des mécanismes classiques d'investigation, fondés sur un accès physique au suspect comme aux éléments de preuve, en regard de l'anonymat comme de l'extranéité des cyber-délinquants ainsi que de la volatilité des moyens de preuve qui caractérisent la cyber-délinquance organisée.

Comme l'a déclaré, de manière quelque peu lapidaire, M. Michel QUILLE, directeur adjoint d'Interpol, *"nous combattons un crime du futur avec des outils du passé"*, même si tout bon enquêteur sait tirer le meilleur parti des moyens juridiques mis à sa disposition.

Les résultats en terme d'élucidation illustrent ce dernier constat puisque, si les services d'investigation n'ont aucune difficulté pour mener à terme leurs enquêtes lorsque la cyber-délinquance s'inscrit dans un cadre inter-personnel *(une partie des infractions à al loi sur la presse, certains types d'harcèlements, la détention d'images pédopornographiques)* ou se limite au territoire français, les obstacles s'accumulent lorsqu'il s'agit d'attaques contre les systèmes automatisés de données, d'escroqueries organisées ou encore de fraudes à la carte bancaire.

❖Le caractère transnational tant de la cybercriminalité que de ses acteurs, qui se jouent de la notion de frontière, alors que les législations internes peinent à s'harmoniser, sinon en Europe, du moins dans le reste du monde.

Il en résulte notamment, pour les services de police et de justice, une véritable dépendance à l'égard des opérateurs, en particulier des prestataires techniques d'Internet, qui sont les seuls à pouvoir faciliter la levée de tels obstacles ; encore faut-il que tous le veuillent faire...

❖Un manque de stratégie et de cohérence d'ensemble enfin.

Mais, c'est d'avant tout, d'une prise de conscience dont la lutte contre la cybercriminalité a besoin, qui ne saurait se limiter à quelques spécialistes si bon soient-ils, ni même aux seuls agents de l'Etat. Or, force est de constater qu'il est plus facile de mobiliser contre le terrorisme que contre la cybercriminalité dans son ensemble, même si cette dernière devient l'un des vecteurs privilégiés de la délinquance organisée.

---

[28] L'annexe jointe au présent chapitre sur *"le droit en marche"* illustre ce phénomène en recensant les nombreux textes votés ou en débat, au plan interne comme international, durant les six mois de travail du groupe interministériel

Finalisation de textes réglementaires ou de circulaires relatifs à la lutte contre la cybercriminalité

⌙ *arrêté du 24.06.2013 relatif à l'habilitation d'officiers ou d'agents de police judiciaire mettant en oeuvre des techniques d'enquête sous pseudonyme portant sur les infractions mentionnées au 6ème alinéa de l'article 24 de la loi du 29.07.1881 sur la liberté de la presse lorsque celles-ci sont commises par le moyen de communications électroniques.* Cette disposition réglementaire a trait à la mise en oeuvre des dispositions des art. 706-25-2 du code de procédure pénale et 24, al.6. de la loi du 29.07.1881 relatives à *la cyber-infiltration*.
L'arrêté a été suivi d'une circulaire d'application du ministère de la Justice *(Direction des affaires criminelles et des* grâces) du 10.09.2013.

⌙ *Circulaire interministérielle du 19.07.2013 relative au dispositif national de signalement des contenus illicites de l'Internet.* Son objet concerne la plate-forme dite PHAROS, qui n'avait pas fait l'objet jusqu'ici d'une circulaire officielle concernant sa saisine et son objet.

⌙ *Arrêté du 21.08.2013 pris en application des art. R.213-1 et R.213-2 du code de procédure pénale fixant la tarification applicable aux réquisitions des opérateurs de communication électronique.* Il comporte, pour la première fois, un début de tarification concernant la fourniture de données relatives à Internet qui, jusque là, faisait l'objet de tarifs hétérogènes de la part de chaque opérateur.

⌙ *Arrêté du 3.10.2013 modifiant l'arrêté du 16.06.2009 portant création d'un système dénommé "Pharos"(Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements).* Il amplifie le rôle de cette plate-forme.

Projets de loi intéressant, pour partie, la lutte contre la cybercriminalité

⌙ *projet de loi devenu la loi n° 2013-1168 du 18.12.2013 relative à la programmation militaire pour les années 2014 à 2019* et comportant des dispositions relatives à la cyberdéfense *(cf. art.20 relatif à l'accès administratif, notamment en matière de terrorisme et de criminalité organisée, aux données de connexion et de* ***géo-localisation*** *stockées par les opérateurs de communication électronique, les hébergeurs et les fournisseurs d'accès)* et d'autres ayant trait à la cybersécurité *(cf. art.. 20 à 25 sur la protection des infrastructures vitales contre la cybermenace, consacrant le rôle de l'Agence devenue l'Autorité nationale de sécurité des systèmes d'information et lui reconnaissant un droit d'accès, à des fins de prévention et de protection aux coordonnées correspondantes aux adresses IP)*, le rapport annexé à la loi prévoyant de porter le nombre des agents de cette Autorité à 500 en 2015 et d'accroître de 350 le nombre des agents oeuvrant dans la cyberdéfense.

⌙ *Projet de loi sur la consommation*, qui, à l'origine, prévoyait la possibilité d'obtenir une décision judiciaire de blocage en vue de prévenir ou de faire cesser un dommage pour un consommateur consécutif au contenu illicite d'un site sur internet, mais qui s'est traduit par la suppression du blocage administratif résultant de l'art.18 de la **loi du 21.06.2004** *(art. 25bis et ter)* ; en l'état, ce texte réglemente aussi la vente à distance et prévoit la répression administrative des **spams** utilisés à des fins commerciales, autorise les agents à recourir à une fausse identité aux fins de contrôle *(cf. art. 48, 52)* et permet à l'administration de saisir la juridiction civile, sur le fondement de l'art.

[29] Cet état n'a aucune valeur d'exhaustivité et ne vise que les textes ou projets de textes sur lesquels le groupe interministériel a dû se pencher dans le cadre de ses travaux ; il faudrait notamment y ajouter les nombreux forums, colloques, assises, rencontres et débats portant sur la cybercriminalité qui témoignent de l'actualité de la question.

6-I.8 de la loi du **21.06.2004**, afin qu'il soit prescrit aux hébergeurs et fournisseurs d'accès Internet toutes mesures proportionnées propres à prévenir ou à faire cesser un dommage causé par le contenu d'un service de communication au public en ligne pour certaines infractions *(art. 25, qui renvoie à un décret d'application)*. - texte en l'état après C.M.P. du 6.02.2014

⌙ *Projet de loi pour l'égalité réelle entre les hommes et les femmes* à l'occasion duquel a été déposé un amendement concernant la répression du harcèlement dans le cadre de la vie privée commis via Internet, amendement qui a été, dans un premier temps, retiré en commission en attendant les propositions du groupe de travail puis, en définitive, adopté *(art. 17 quater)* : serait constitutif d'un délit le fait de soumettre une personne à des harcèlements ou intimidations répétées ou à des atteintes répétées à sa vie privée, l'utilisation d'un service de communication au public en ligne étant érigé en circonstance aggravante ; en outre, en cours de navette parlementaire, le délit réprimant les appels téléphoniques malveillants *(art. 222-16 du code pénal)* a été étendu aux *"envois réitérés de messages malveillants par la voie de communication électronique" (art. 11bis - **spams**)* ; enfin, l'article 6-I-7 de la **loi du 21.06.2004** a étendu la surveillance spécifique imposée aux hébergeurs et fournisseurs d'accès à l'incitation *"à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap"*.

⌙ *Projet de loi devenu la loi du 6.12.2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière*, à l'occasion de l'examen duquel un amendement destiné à réprimer l'incitation à la fraude fiscale commise notamment via Internet par le biais d'une modification de la **loi du 29.07.1881** sur la liberté de la presse a été repoussé *(cf. Débats Assemblée Nationale, 20.06.2013)* ; en outre, le texte prévoit une protection spécifique pour les *"lanceurs d'alerte"*.

⌙ *Loi n° 2014-56 du 27.01.2014 visant à harmoniser les délais de prescription des infractions prévues par la loi sur la liberté de la presse du **29.07.1881**, commises en raison du sexe, de l'orientation et de l'identité sexuelle ou du handicap* porte à 1 an le délai de prescription s'agissant des délits de provocation à la discrimination, de diffamation ou d'injure publique commis en raison de l'une des circonstances précitées.

⌙Enfin, le Gouvernement a déposé un projet de loi sur **la géo-localisation** en matière judiciaire, qui fait suite aux récents arrêts de la Chambre criminelle.

Propositions de loi intéressant, pour partie, la lutte contre la cybercriminalité

⌙ *la proposition de loi "renforçant la lutte contre le système prostitutionnel"*, adoptée en première lecture par l'Assemblée Nationale en décembre 2013, prévoit, en son art. 1er, une modification de l'art. 6.I.7 de la **loi du 21.06.2004** afin d'étendre la surveillance spécifique imposée aux hébergeurs et fournisseurs d'accès aux cas de la traite des êtres humains ainsi qu'au proxénétisme et assimilé *(art. 225-4-1, 225-5 et 225-6 du code pénal)* ; en revanche, les autres dispositions projetées autorisant l'administration à notifier à ces prestataires les adresses électroniques des services illicites aux fins de blocage n'ont pas été adoptées en l'attente du rapport du Groupe de travail.

⌙ *La proposition tendant "à renforcer la lutte contre la contrefaçon",* qui, en son art.9 - voté conforme par les deux chambres -, prévoit de modifier l'art.67 bis du code des douanes afin d'étendre l'infiltration douanière et la technique dite du coup d'achat..

....

Projet d'ordonnance intéressant, pour partie, la lutte contre la cybercriminalité

Concomitamment, faisant suite à la ratification de la Convention MEDICRIM, *le projet d'ordonnance relatif à l'harmonisation des sanctions pénales et financières relatives aux produits de santé et à l'adaptation des autorités et agents chargés de constater les manquements* comporterait des dispositions relatives à l'enquête sous pseudonyme pour les infractions d'exercice illégal de professions réglementées de santé et de vente illégale ou de contrefaçon de médicaments.

Missions

⌙ A la demande du ministre de la Culture, Mme. IMBERT-QUARETTA, conseillère d'Etat, devrait déposer, courant février 2014, un rapport de proposition dans le domaine de la contrefaçon commerciale.

⌙ A la demande du gouvernement, *la Commission nationale informatique et libertés* anime un groupe de travail sur un programme national de sensibilisation à la protection des données personnelles.

Instruments internationaux

⌙ le *Règlement de l'Union européenne n° 611/2013 du 24.06.2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.*

⌙ La *Directive 2013/40/UE du 12.08.2013 relative aux attaques contre les systèmes d'information et remplaçant la décision cadre 2005/222.JAI du Conseil*

⌙ différents projets européens s'agissant de la protection des données nominatives ou de la protection du secret des affaires :
**la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*
**la proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulguées (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.*

Ces quelques exemples illustrent, non seulement l'actualité de la question et la richesse des analyses, mais aussi la nécessité d'une approche plus coordonnée et sans doute plus globale de la lutte contre la cybercriminalité.

I.3.- Les outils européens de lutte contre la cybercriminalité : réalités et espérances

L'efficacité de la lutte contre la cybercriminalité repose, en grande partie, sur une véritable coopération internationale, élément incontournable qui doit s'inscrire dans le prolongement de l'activité opérationnelle des services d'enquête et des autorités judiciaires.

Dans ce contexte, l'espace européen a vu, depuis le début des années 2000, le lancement progressif d'initiatives politiques, institutionnelles et juridiques qui, pour beaucoup, ont permis des premières avancées concrètes au niveau international, dans la coopération contre la cybercriminalité.

Alors que cette menace ignore, par nature, la notion de frontière géographique, la dimension européenne permet ainsi à la France d'assurer le prolongement de ses capacités au plan international avec l'émergence progressive, chez ses principaux partenaires, d'un espace-cyber mieux sécurisé et mieux adapté aux besoins d'enquêtes, dans une véritable logique de sécurité collective.

Ces avances internationales sont d'abord le fait du Conseil de l'Europe, véritable précurseur, qui a produit, dès 2001, la convention internationale de référence sur la cybercriminalité *(Convention dite de Budapest)*, avec son protocole additionnel de 2002.

Au fil des années 2000, l'Union européenne s'est ensuite dotée d'une succession de cadres normatifs [30]. Ces textes juridiques ont été intégrés, en février 2013, dans un ensemble cohérent ayant vocation à traiter le plus largement possible de la problématique cyber : *la stratégie de cybersécurité de l'Union européenne*, qui ambitionne de devenir une référence mondiale en ce domaine.

Cette volonté européenne est d'autant plus d'actualité depuis l'affaire PRISM. Désormais, l'Europe ambitionne de développer son indépendance technologique *(cf. l'industrie européenne du "nuage dans les étoiles" ou "cloud computing" notamment)* et négocie avec Washington un projet d'accord sur la protection des données.

Les outils européens mis à la disposition de la France et des autres membres de l'Union sont, non seulement des dispositifs permettant la coopération des services répressifs et judiciaires, des bases d'incriminations pénales communes, mais aussi des services, des politiques et des structures.

Non exempts de limites et de blocages inhérents à la dimension internationale des travaux, ces moyens, qui sont *a minima*, restent, par nature, perfectibles et sont l'objet de négociations régulières dans les enceintes Bruxelloises.

---

[30] concernant les infractions visant les systèmes de traitement automatisé des données *(STAD)*, les formes traditionnelles de criminalité, les infractions dites de contenu *(diffusion via Internet de pédopornographie, de messages racistes et xénophobes...)*

La coordination des positions des administrations françaises dans les négociations avec l'Union européenne est assurée par *le Secrétariat général des affaires européennes (SGAE)*, dépendant du Premier ministre [31]. Il constitue, à ce titre, l'interface interministérielle de coordination avec l'environnement communautaire européen.

1.- <u>des moyens au service des enquêtes et de l'échange d'informations entre services</u>

En premier lieu, le Conseil de l'Europe et l'Union européenne ont élaboré, au profit des Etats-membres, des dispositifs reconnus au plan international pour faciliter la coopération, en particulier :

- la mise à disposition des informations par l'obligation de mesures conservatoires comprenant le **gel des données**, ou par l'instauration d'un **délai minimum de conservation** en ce qui concerne les données de connexion
- un échange de ces informations, opéré dans le strict respect des libertés individuelles, notamment grâce à la législation de l'Union sur la protection des données personnelles et au rôle joué par la Cour européenne des droits de l'homme
- un traitement en temps réel garanti par un dispositif opérationnel
- une extradition des mis en cause facilitée par le mandat d'arrêt européen.

De manière plus générale, les instruments européens déterminent les principes prévalant pour les relations entre professionnels traitant les données et administrations *(absence d'obligation générale de surveillance des contenus, mais devoir de coopération pour identifier les auteurs)***.**

Elles créent une dynamique de coopération entre les entreprises elles-mêmes *(notamment dans le domaine de la lutte contre la contrefaçon)*, avec le souci de la protection du consommateur/victime.

En résumé, l'approche européenne se veut soucieuse d'un certain équilibre entre libertés individuelles et efficacité des pouvoirs d'enquête.

11. - la Convention sur la cybercriminalité du Conseil de l'Europe

Cette *Convention dite de Budapest* [32], seul instrument international contraignant dédié spécifiquement à la cybercriminalité, reste, de ce fait, l'instrument de référence pour tout développement de la coopération internationale.

Elle a vocation à servir de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre de coopération contre cette délinquance entre les Etats-parties.

---

[31] Le SGAE n'assure pas, toutefois, une telle position d'interface entre les administrations et le Conseil de l'Europe, entité complètement distincte de l'Union européenne

[32] entrée en vigueur le 1er juillet 2004, elle est ouverte à la signature des Etats-membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration, à Budapest, le 23.11.2001

Ce texte s'articule autour de trois points essentiels :

⌞ l'harmonisation des législations nationales, notamment par le biais de la définition d'incriminations communes : elle traite des infractions à la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ainsi que les nombreuses infractions connexes souvent facilitées par l'usage de tels systèmes *(falsification informatique, fraude informatique, pornographie enfantine, atteintes à la propriété intellectuelle, discriminations - cf. II).*

⌞ l'adaptation des moyens procéduraux au support spécifique que constitue, entre autres, Internet, dans le respect et la garantie des droits et libertés individuelles.
Elle reconnaît notamment à l'Etat Partie une possibilité d'accès direct à toutes données accessibles au public quelle que soit leur localisation, mais également la capacité *à accéder ou à recevoir, au moyen d'un système informatique situé sur son territoire, des données informatiques stockées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique" (art.32).*
Elle impose aussi l'adoption de mesures aux fins de conservation et de divulgation rapide des données informatiques stockées *(gel des données informatiques)*, si la partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition, de la saisie, de l'obtention ou de la divulgation de ces données informatiques. Elle prévoit également la collecte en temps réel des données relatives au trafic et d'interception de données relatives au contenu *(art. 29).*
Enfin, au plan de l'entraide pénale internationale, elle facilite l'extradition entre les Etats Parties. Elle constitue même un fondement possible aux demandes d'entraide et d'extradition entre ces Etats lorsqu'il n'existe pas d'autre traité international applicable.

⌞ la mise en place de moyens d'action rapides et efficaces au titre de la coopération internationale : elle oblige ainsi à l'instauration d'un réseau de points de contact, dit G8/H24, dédiés et disponibles 24h. sur 24 et 7 jours sur 7

En 2002, le Conseil de l'Europe a complété son dispositif en adoptant un protocole additionnel, ainsi que la Convention de Lanzarotte *(cf. II).*

Depuis l'adoption de ces instruments, le Conseil de l'Europe s'est engagé dans un travail important de mise en oeuvre de ces textes et de traitement de nouvelles problématiques intéressant la cybercriminalité. Le projet *cybercrim/Octopus* cherche, notamment, à développer les capacités juridiques *(le respect de la protection des données personnelles, la promotion de l'état de droit...)* et opérationnelles des pays qui ne se sont pas encore dotés de structures adaptées dans la lutte contre la cybercriminalité ; l'approche s'appuie sur un partenariat entre pouvoirs publics et organismes privés agissant dans le domaine de l'informatique *(fournisseurs d'accès, concepteurs de logiciels...)* [33].

La dernière conférence Octopus, qui s'est tenue les 4-6 décembre 2013, a porté sur la sauvegarde et la protection des données à des fins de justice pénale ou de sécurité nationale, ainsi que sur la protection des enfants contre l'exploitation sexuelle en ligne.

En 2013, dans le sillage de Budapest, l'Union et le Conseil de l'Europe ont aussi organisé, conjointement, deux projets régionaux [34] dont l'objectif était de renforcer les capacités des autorités de justice pénale pour une meilleure coopération contre la cybercriminalité.

[33] cf., par exemple, l'accord de coopération signé, le 3.12.2013, entre le Conseil et Microsoft.

[34] concernant les Balkans et les pays du partenariat oriental *(Biélorussie, Ukraine, Moldavie, Géorgie, Arménie, Azerbaïdjan)*

A ce titre, le Conseil de l'Europe demeure actuellement l'enceinte internationale majeure de coopération pour la lutte contre la cybercriminalité.

Problématique française :

La France a promulgué la loi du 19 mai 2005 autorisant l'approbation de la Convention sur la cybercriminalité et du protocole additionnel à cette Convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Un an après cette loi, les décrets d'application n° 2006-580 et 2006-597ont été publiés.

La France soutient résolument le dispositif résultant de la Convention, quelle a mis en oeuvre par la loi n° 2004-575 du 21 juin 2004. La systématisation de points de contact 24/7 dans les pays partenaires est, pour elle, essentielle notamment dans les échanges en matière pénale avec les Etats-Unis vers lesquels les demandes d'entraide française sont en forte augmentation, puisque, à la différence de la législation française, la législation américaine n'impose pas aux opérateurs privés d'obligation de conservation minimale des données.

S'il demeure le plus abouti, le dispositif de la Convention n'en reste pas moins qu'un instrument encore partiel dans sa mise en oeuvre :

- Même s'il s'étend au-delà des seuls Etats membres du Conseil de l'Europe et si 55 pays l'ont adopté, il ne couvre que les 40 pays qui l'ont ratifié

- il ne concerne qu'un nombre restreint de types de criminalité

- la capacité légale, pour les services enquêteurs, d'accéder aux données stockées dans un autre Etat, dans l'hypothèse où elles ne sont pas publiques *(art. 32)* connaît des difficultés d'application en l'absence de consensus entre les Etats parties à la Convention quant à l'interprétation à donner au texte. L'enjeu est d'importance, puisqu'il s'agit de lever l'un des principaux blocages à la coopération pénale internationale en matière de lutte contre la cybercriminalité, mais aussi de la capacité des Etats à conserver un contrôle juridique total sur les informations non publiques, par nature les plus sensibles

  En effet, cette disposition autorise les enquêteurs français à consulter, télécharger ou recevoir des données stockées à l'étranger en dehors du cadre de l'entraide judiciaire à la seule condition du consentement soit du titulaire du compte de messagerie, soit du fournisseur d'accès à Internet. Le contrôle juridique, préservé dans l'hypothèse d'une demande d'entraide, n'est, dès lors, maintenu qu'en cas du refus de l'un ou de l'autre..

Telles sont les raisons pour lesquelles l'Union et le Conseil de l'Europe préparent actuellement le lancement d'une nouvelle campagne visant à la mise en oeuvre de la Convention dans le monde entier.

S'agissant du Conseil de l'Europe proprement dit, la priorité consiste, incontestablement, à tenter de trouver un accord en ce qui concerne l'article 32 précité, accord qui pourrait donner lieu à **l'adoption d'un nouveau protocole additionnel mais spécifiquement consacré à la question de l'accès transfrontalier aux données électroniques.**

A noter aussi la création d'un bureau du Conseil de l'Europe sur la cybercriminalité à Bucarest (Roumanie), annoncée en octobre 2013 ; il est destiné à permettre au Conseil de répondre de manière efficace au nombre croissant de demandes d'assistance en ce domaine.

12.- La directive de l'Union 2000/31 du 8 juin 2000 sur le commerce électronique

Cette directive définit notamment le degré de responsabilité des opérateurs techniques et fournisseurs d'accès dans leur relation avec l'autorité publique *(art. 15) :*

- elle dispense ces opérateurs de tout devoir de surveillance générale des contenus, induisant leur absence de responsabilité civile ou pénale à deux exceptions près en ce qui concerne l'hébergeur *(art. 14.1)* : si ce dernier a eu effectivement connaissance de l'activité ou de l'information illicite ou de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente et qu'il n'a pas agi promptement pour retirer les informations ou en rendre l'accès impossible ;
- elle autorise une obligation d'information des autorités compétentes en cas de découverte d'activités illicites ;
- elle oblige à fournir aux autorités compétentes des informations permettant l'identification des clients mis en cause ;
- elle encourage enfin *(considérant 40) "l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible"*, mais sans imposer de notification spécifique aux Etats membres.

Problématique française :

En vertu de cette directive, transposée par la loi n° 2004-575 pour la confiance dans l'économie numérique du 21.06.2004, la France n'a donc pu imposer aux opérateurs qu'un devoir de surveillance limité, concernant des infractions limitées *(pédopornographie, propos racistes, apologie des crimes contre l'humanité).*

Une telle limitation européenne a eu une incidence, plus ou moins directe, sur plusieurs législations françaises adoptées par la suite, notamment lors des débats sur la loi HADOPI de 2009, concernant la question de la suspension de l'accès Internet et le rôle imparti aux opérateurs dans la lutte contre le piratage des oeuvres artistiques ; lors des débats similaires sur la loi relative aux jeux en ligne de 2010 ; enfin, lors de l'examen précédant le vote de la loi n° 2011-267 du 14.03.2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui s'est conclu par l'octroi, à la seule autorité administrative, de la capacité de bloquer des contenus pédopornographiques.

Sur ce dernier point, la directive, en accordant la possibilité de bloquer des sites, a ouvert en France un débat complexe sur l'octroi à l'autorité administrative d'une telle capacité, qui est loin d'être terminé compte-tenu de l'abrogation récemment décidée par le Parlement.

(cf., sur ce point, le titre III, chapitre 2 in fine).

13.- le protocole d'accord du 4 mai 2011 sur la vente de contrefaçons sur Internet

Ce protocole avait pour but d'établir un code de bonnes pratiques pour lutter contre la vente de contrefaçons sur Internet et pour renforcer la collaboration entre ses signataires *(33 entreprises et associations professionnelles représentant 39 sites différents).* La Commission européenne assume le rôle de facilitateur d'un dialogue voulu transparent et animé par un esprit de confiance mutuelle entre partenaires.

Il détermine trois principaux axes de coopération entre les entreprises et les sites :

- la mise en oeuvre de mesures proactives de protection comme de mesures techniques visant à empêcher la mise en ligne d'offres illicites *(par le biais, par exemple, du contrôle préalable des projets d'annonce)* ;

⌙ l'instauration de processus de signalement à disposition des entreprises et des consommateurs *(procédures dites de notification et de retrait)* ainsi qu'un mécanisme de partage d'informations *(sous la forme, par exemple, du signalement des personnes vendant des produits de contrefaçon) ;*

⌙ enfin, un processus permettant l'élimination accélérée de l'offre en ligne de produits contrefaits, sur la base de la directive 2000/31 du Conseil de l'Europe *(chapitre II, section 4).*

Il préconise également des actions d'information/sensibilisation des vendeurs et acheteurs potentiels, de protection du consommateur ainsi que des mesures dissuasives à l'encontre des contrevenants récidivistes qu'il convient d'identifier.

La Commission a prorogé le protocole de 2 ans et a institué un suivi périodique sous sa propre égide.

En 2014, la mise en oeuvre de ce protocole devrait voir la poursuite des réunions bilatérales entre les signataires, qui visent à déboucher sur des actions concrètes et ciblées.

En outre, la Commission se propose, au-delà de son rôle actuel de facilitateur, d'assumer une fonction de médiateur sur certaines questions spécifiques.

Enfin, les signataires et la Commission se proposent, toujours en 2014, de renforcer leur action de communication à l'égard du public et de tous nouveaux partenaires potentiels *(associations de consommateurs, groupes représentatifs de la société civile, plate-formes Internet non encore signataires...)* afin de trouver de nouveaux partenaires.

14.- Les directives de l'Union 2002/58 du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques, et 2006/24 sur les conditions de conservation des données

La première prévoit, en termes généraux, que la conservation des données de connexion est possible si elle constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique pour sauvegarder la sécurité nationale, la défense et la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisation non autorisée d'un système de communications électroniques, mais cela sans fixer de délais.

Celle de 2006 oblige, en revanche, les Etats membres à contraindre les opérateurs de télécommunications de conserver les données de trafic pour une durée que les Etats membres peuvent fixer de 6 mois à 2 ans.

Elle reste encore à être transposée dans quatre Etats de l'Union *(Allemagne, Autriche, République Tchèque et Suède)*, qui invoquent des difficultés d'ordre constitutionnel. Les positions allemandes pourraient toutefois évoluer suite à la conclusion récente d'un accord de coalition gouvernemental qui prévoit expressément la mise en oeuvre de cette directive pour instaurer une conservation de 3 à 6 mois.

De 2010 à mai 2012, la Commission européenne a initié une série de consultations en vue de réformer ce texte. Cette démarche a été suspendue compte-tenu des fortes réticences de la majorité des Etats membres à remettre en cause le statu quo. Sous la pression de certains fournisseurs européens d'accès à Internet mais aussi de défenseurs des droits de l'homme [35], une réflexion est toujours en cours

[35] Récemment, un avocat général de la Cour de justice de l'Union européenne, dans le cadre des recours exercés en Irlande et en Autriche, a ainsi exprimé le souhait, au regard du principe de proportionnalité et au nom de la protection de la vie privée, que la directive soit modifiée pour abaisser la durée prévue en-dessous

à ce sujet aux fins de proposer une minoration du délai de conservation, vraisemblablement à 6 mois. A cet effet, la Commission a créé, en avril 2013, un groupe d'experts chargé d'identifier les difficultés rencontrées dans l'application de cette directive.

Problématique française :

La France a instauré un délai de conservation d'un an *(art. L.34-1 du code des postes et télécommunications électroniques),* donc inférieur au délai de prescription en matière délictuelle.

Dans le débat européen, notamment dans le cadre du groupe d'experts auquel elle participe, elle soutient résolument le maintien, a minima, de la réglementation actuelle, en faisant valoir que le recours aux données de connexion est devenu essentiel pour la résolution d'affaires particulièrement sensibles *(crime organisé, terrorisme)*, tant sur le fond que de par leur valeur probante dans les procédures judiciaires.

15.- Le règlement de l'Union européenne 611/2013 du 24 juin 2013, dit *"data breach"*, concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58 du Conseil de l'Europe

Entré en vigueur le 25 août 2013, ce règlement encadre l'obligation faite au fournisseur de services de communications électroniques d'informer tant l'autorité nationale de protection des données que le client concerné de toute violation de données à caractère personnel.

Harmonisant les procédures de notification dans les Etats membres, le texte fixe des modalités de notification, un délai *(si possible 24 h. après le constat de la violation)* ainsi que l'obligation, pour l'autorité nationale précitée, de créer un moyen électronique sécurisé pour ces notifications.

Problématique française :

Cette obligation de notification figure à l'art. 34 bis de la loi du 6 janvier 1978 relative à l'informatique et aux libertés, suite à l'ordonnance modificative 2011-1012 du 24 août 2011, qui érige aussi en délit le fait, pour un fournisseur, de ne pas y procéder *(art. 226-17-1 du code pénal).*

16.- La législation de l'Union européenne sur la protection des données et la proposition de directive et de règlement

Compte-tenu de l'obsolescence, au regard d'Internet, des directives 95/46/CE du 24 octobre 1996 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, 97/66/CE du 15 décembre 1997 sur le traitement des données à caractère personnel et protection de la vie privée dans le secteur des télécommunications, l'Union travaille depuis 2012 à leur refonte ainsi qu'à celle de la Décision-cadre 2008/977/JAI

L'objectif est, non seulement, d'adapter la législation en matière de traitement des données personnelles, mais aussi de renforcer le contrôle des transferts de données hors de l'Union européenne.

---

d'un an.

La proposition de règlement du 25 janvier 2012 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données *(COM (2012) 11 final)* vise à remplacer la directive de 1995. **Ce projet entend notamment s'appliquer à tout responsable de traitement de l'information assurant une offre de biens ou de services, même établi hors de l'Union, dès le moment où les données gérées sont celles d'un résident de l'Union**.

A la décision-cadre précitée est appelée à succéder la proposition de directive présentée le 25 janvier 2012 *(COM (2012) 10 final)* relative à la protection des personnes physiques à l'égard du traitement des donnés à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation des données.

Cette proposition de directive prévoit, en son article 4, que *"les données à caractère personnel doivent être*
a) traitées loyalement et licitement
(b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités
(c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées
(d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai
(e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées
(f) traitées sous la responsabilité du responsable du traitement qui veille au respect des dispositions adoptées en vertu de la présente directive".

Problématique française :

Ces instruments, une fois adoptés, offrent un cadre légal général que le législateur se doit d'optimiser et de rendre totalement opérationnel, dans les deux sens, avec nos partenaires européens. Leur mise en oeuvre, notamment dans le domaine des fichiers utilisés en matière répressive, doit permettre de renforcer la légitimité et la confiance dans l'action de l'Etat.

Il est à noter qu'un autre projet de règlement a trait à la protection des données des entreprises.

17. - le mandat d'arrêt européen

Le mandat d'arrêt européen complète utilement les possibilités d'extradition déjà offertes par la Convention de Budapest.

La cybercriminalité figure parmi les infractions mentionnées à l'article 695-23 du code de procédure pénale français, *"punies d'une peine privative de liberté d'une durée égale ou supérieure à trois ans d'emprisonnement"* et permettant la remise des personnes recherchées.

18.- la problématique constante de l'équilibre entre libertés individuelles et capacités d'enquête

- pour mémoire - *(cf. le chapitre I.6. consacré au contexte de l'action)*

2.- l'instauration d'outils normatifs communs

Outre l'instauration du cadre propice à la coopération contre la cybercriminalité, le Conseil de l'Europe et l'Union européenne ont également oeuvré à la création de bases communes, *a minima*, d'incriminations spécifiques.

21.- les attaques contre les systèmes d'informations et les systèmes de traitement automatisé de données (STAD) [36]

Dés 2001, l'atteinte aux STAD est la première des infractions prévues et définies par la Convention de Budapest [37], qui l'appréhende sous l'angle de l'accès illégal, de l'interception illégale, de l'atteinte à l'intégrité des données ou d'un système, de l'abus de dispositif ou de la falsification de données.

L'approche spécifique de l'Union s'est traduite récemment par l'adoption de la directive 2013/40/UE du 12 août 2013, qui se substitue à la décision-cadre 2005/222/JAI ; devant être transposée par chaque Etat membre avant le 4 septembre 2015, elle leur impose :
- d'incriminer l'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système d'informations et à l'intégrité de données, l'interception illégale de transmission non publique de données informatiques, avec des minima de peines
- de répondre à de nouveaux modes d'atteinte à la sécurité des réseaux d'information, telle que l'utilisation de *"réseaux-zombies".*

Elle prévoit aussi, à l'instar de la Convention de Budapest, la mise en place de contacts nationaux opérationnels 24 heures sur 24 et 7 jours sur 7 et l'instauration de procédures permettant de répondre à une demande urgente d'assistance émanant d'un autre Etat membre dans les 8 heures à compter de la réception de cette dernière, puisque la célérité des cyber-attaques impose une mobilisation rapide des services enquêteurs.

> Problématique française
>
> La France dispose déjà, depuis la loi du 5 janvier 1998, d'un socle répressif non négligeable *(cf. art. 323-1 à 323-7 du code pénal)*, qui semble prendre en compte les nouvelles exigences. Ces dernières présentent toutefois l'intérêt d'inciter certains de ses partenaires à combler leur retard en la matière.

22.- la protection des réseaux et la directive dite *"cyber-sécurité"*

La proposition de directive COM(2013) 48 final du 7 février 2013, qui doit assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union Européenne, est en cours de négociation.

Elle vise à renforcer les capacités intérieures des Etats membres de l'Union, la coopération européenne en matière de gestion de crise cyber et de réponse aux incidents. Elle projette aussi d'étendre des dispositions de la directive-cadre concernant les télécommunications à un ensemble *"d'opérateurs de marché"*, incluant, notamment, les secteurs d'importance critique.

---

[36] déni de service, piratage, *"réseaux zombies"*...

[37] cf. Le chapitre II, section 1, titres 1 et 2 *: "infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques"*

Trois moyens sont proposés dans ce but :

- imposer l'instauration, dans chaque Etat membre, d'une autorité nationale compétente sur la sécurité des réseaux d'information, d'une stratégie nationale de cyber-sécurité, d'un C.E.R.T. *Computer Emergency Response Team)* et d'un plan national de réponse aux crises ;
- créer un *"réseau européen des autorités nationales de cyber-sécurité"*, instaurer le principe d'une notification obligatoire des incidents de sécurité informatique décelés au niveau national à l'ensemble des homologues européens, adopter un *"plan européen de coopération durant les crises cyber"*, constituer un réseau informatique d'échange d'informations sensibles ;
- instaurer le principe de la notification obligatoire d'incidents informatiques significatifs par les opérateurs économiques visés par la directive, introduire la possibilité, pour l'autorité nationale de cyber-sécurité ou pour des prestataires qualifiés, de conduire des audits réguliers et d'exiger la mise à disposition par les opérateurs des informations nécessaires, introduire un principe de sanction en cas de non-respect de ces dispositions.

Problématique française

La France dispose déjà d'une agence, devenue autorité nationale suite à la loi de programmation pour la Défense, s'agissant de la sécurité des systèmes d'informations, notamment pour les opérateurs d'importance vitale.
L'adoption, au niveau européen, de mesures législatives destinées à renforcer, partout en Europe, les capacités nationales conforte cette politique. Toutefois, la proposition de directive s'avère aussi, en l'état et de l'avis de nombreux Etats membres, trop intrusive en terme de déclaration obligatoire et de réponse opérationnelle coordonnée, au regard du principe de souveraineté des Etats en matière de sécurité nationale garanti par l'art. 346 du Traité de l'Union.

23.- La protection de l'intelligence économique et le secret des affaires

Le 28 novembre 2013, la Commission européenne a présenté un projet de directive visant à protéger les *"secrets d'affaires" (technologies ou savoir-faire particuliers)* contre le vol par des entreprises concurrentes. Ce projet devait être présenté au Parlement dès février 2014 mais son examen sera retardé eu égard aux élections prochaines.

Bien qu'abordant l'infraction de manière générale, ce texte prend aussi en considération l'atteinte cyber en visant: *"L'accès non autorisé à tout document (...) ou ficher électronique ou copie non autorisée de ces éléments".*

Outre la remise au détenteur légal et la destruction des fichiers concernés, le projet prévoit des dommages et intérêts pour les entreprises victimes d'un vol ou d'une appropriation illicite d'informations confidentielles.

Problématique française

Contrairement à l'Allemagne, l'Italie et l'Espagne, la France ne dispose pas d'une législation spécifique s'agissant du secret des affaires. Si une proposition de loi avait été adoptée le 23.01.2012 par l'Assemblée nationale afin de créer, dans un nouvel art. 325-3 du code pénal, un délit de *"violation du secret des affaires",* ce texte n'a pas prospéré. *La délégation à l'intelligence économique* travaille actuellement sur un projet de texte plus ambitieux.
(cf., sur ce point, le titre III, chapitre 1er)

24.- La vente de contrefaçons et le piratage sur Internet

La Convention de Budapest incrimine les atteintes à la propriété intellectuelle en renvoyant aux principaux accords internationaux existants : *Convention universelle sur le droit d'auteur* (Paris, 24.07.1971) ; *Convention dite de Berne pour la protection des oeuvres littéraires et artistiques ; Accord sur les aspects commerciaux des droits de propriété intellectuelle* ; *Traité de l'OMPI sur la propriété industrielle.*

Dans le cadre de *l'Observatoire européen de la contrefaçon et du piratage, un* groupe de travail relevant du secteur privé procède, actuellement, à une évaluation de l'ensemble de ces instruments.

Suite à une consultation réalisée fin 2012, la Commission a décidé de ne pas proposer de révision de la directive 2004/49/CE relative au respect des droits de propriété intellectuelle, ni de celle relative au commerce électronique, afin de privilégier la question de la responsabilité des intermédiaires d'Internet.

25.- Les abus sexuels et l'exploitation sexuelle des enfants, la pédopornographie

La Convention de Budapest demeure la première et principale base internationale de référence incriminant, sous ses différents angles, la cyber-exploitation de la pornographie infantile *(possession, stockage, mise à disposition, diffusion, transmission de contenus pédopornographiques).*

Une autre convention du Conseil de l'Europe, dite *"Convention de Lanzarote"*, a trait à la protection des enfants contre l'exploitation et les abus sexuels ; ouverte à la signature le 25.10.2007, elle a été signée et ratifiée par 28 Etats, dont la France, mais les Etats-Unis n'en font pas partie ; elle est entrée en vigueur le 1er juillet 2010.

Elle impose notamment aux Etats Parties d'incriminer le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine, ou encore le fait, pour un majeur, de solliciter un mineur à des fins sexuelles par l'intermédiaire de ces nouvelles technologies.

Elle constitue, en outre et à défaut d'autres instruments, une base légale adaptée pour l'entraide judiciaire en matière pénale.

La directive n°2011/92/UE du 13 décembre 2011 reprend les dispositions de la convention précitée, en les approfondissant et en les harmonisant, également en terme de sanctions encourues.

Elle fait ainsi obligation aux Etats membres d'incriminer le fait d'accéder, en connaissance de cause et par le biais des technologies de l'information et de la communication, à de la pédopornographie, quand bien même cet accès ne serait pas habituel [38], ou encore le fait de solliciter un mineur à des fins sexuelles au moyen de ces technologies.

Elle impose à ces mêmes Etats de prendre les mesures nécessaires pour faire supprimer rapidement les pages Internet hébergées sur leur territoire et contenant ou diffusant de la pédopornographie, et de **bloquer l'accès par les internautes aux pages internet contenant ou diffusant de la pédopornographie.**

[38] le droit français a été adapté en conséquence par la loi n° 2013-711 du 5 août 2013 *(art. 227-23 du code pénal)*

La résolution du Parlement européen sur la protection des enfants dans le monde numérique, en date du 20 novembre 2012, si elle souligne le niveau élevé de coopération entre les autorités policières et judiciaires des Etats membres, regrette la lenteur des procédures de notification et de retrait de pages Internet dans certains Etats membres, souhaite que l'Union se dote d'une approche commune en matière de recevabilité et d'admissibilité des preuves et appelle à redoubler d'efforts pour renforcer la coopération avec les pays tiers en ce qui concerne le retrait rapide des pages Internet illicites hébergées sur leur territoire.

Enfin, l'Alliance mondiale contre la pédopornographie constituée le 5 décembre 2012 a été lancée à l'initiative des Etats-Unis et de l'Union européenne et regroupe aujourd'hui 48 Etats. Il s'agit d'une déclaration politique d'intention visant à réaliser un plan d'action comportant 4 objectifs : l'identification et le soutien aux victimes, la réduction de la présence de matériel pédopornographique sur Internet, l'identification des auteurs et leurs poursuites, la sensibilisation du public sur les risques que représentent les activités des enfants sur Internet.

Une évaluation sera dressée en juillet 2014, suivie de la tenue d'une conférence mondiale aux Etats-Unis en septembre suivant.

Problématique française

Si la création d'une telle Alliance ne peut qu'être accueillie très favorablement, il reste nécessaire de préciser les modalités de son articulation avec Interpol, Europol et le nouveau centre européen contre la cybercriminalité *(voir plus loin)*.

26.- les discriminations

Le protocole additionnel à la Convention de Budapest, adopté le 7 novembre 2002, ouvert à la signature en janvier 2013 et immédiatement signé par la France, demande aux Etats de lutter contre la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques et préconise, à ce titre, une harmonisation du droit pénal et l'amélioration de la coopération internationale.

La décision-cadre 2008/913/JAI du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie demande aux Etats-membres d'incriminer tout fait, propos ou comportement constitutif de racisme, d'incitation à la haine, de négation ou de banalisation des crimes de génocide, et de les réprimer de peines comprises entre un à trois ans de prison. Plus précisément sont visées *"l'incitation publique à la violence ou à la race visant un groupe de personnes ou de membres d'un tel groupe, défini par référence à la haine, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique"*, en particulier lorsqu'une telle incitation se fait *"par diffusion ou distribution publique d'écrits, d'images ou d'autres supports" (par référence à Internet),* ainsi que *"l'apologie, la négation ou la banalisation grossière publique des crimes de génocide, crimes contre l'humanité et crimes de guerre tels que définis par la Cour pénale internationale".*

Toutefois, l'ensemble des Etats de l'Union n'ont pas encore transposé cette décision-cadre dans leurs législations respectives.

3.- La stratégie de l'Union européenne en matière de cyber-sécurité : une réponse globale au défi cyber

Outre les acquis juridiques précités, l'Union européenne a voulu élaborer, en février 2013, une stratégie d'ensemble visant toutes les problématiques cyber, stratégie dans laquelle la lutte contre la cybercriminalité est toutefois traitée comme une composante garantissant une cyber-sécurité collective [39].

La lutte contre la cybercriminalité y est ainsi abordée au côté de quatre autres piliers que sont la protection/résilience des réseaux et de l'information [40], le développement de capacités de cyber-défense, le partenariat avec le secteur industriel afin de développer une véritable technologie européenne, notamment pour les produits de cyber-sécurité, et l'élaboration d'une véritable diplomatie européenne en matière de cyber [41].

Si le document stratégique intègre les actions déjà engagées, il en envisage aussi de nouvelles de nature à soutenir l'action des Etats-membres sous la forme d'outils européens de soutien technique, d'aide à la formation et à la prévention, de soutien opérationnel aux enquêtes, de financement, d'aide au développement d'outils technologiques...

Cette stratégie, qui sert désormais de fondement à la politique de l'Union en la matière, fait l'objet d'un suivi au sein du *"Groupe des amis de la présidence"* qui entend veiller à la synergie des travaux dans le domaine juridique et dans celui de la défense [42]. Elle s'est déjà traduite par un projet de directive sur la sécurité des réseaux et de l'information en cours de négociation ; une autre priorité concerne la lutte contre les réseaux *"zombies"* et les logiciels malveillants.

Il est à noter que le mandat confié au présent groupe interministériel s'inscrit dans cette stratégie européenne.

31.- Un enjeu global : l'adaptation rapide à l'évolution des technologies de l'information et la communication

En réponse à l'émergence de nouveaux modes d'utilisation d'Internet, l'Union a identifié des filières stratégiques en terme de protection des données *(les données volumineuses dites "big data" ou l'informatique en nuage)*, qu'il s'agit de développer en Europe.

---

[39] Une telle approche a été voulue par la Commission, en dépit de la position de certains Etats-membres préconisant une approche plus équilibrée.

[40] À cet égard, le projet de directive relative à la cyber-sécurité *(cf. II.2)* fait partie intégrante de cette stratégie

[41] cf., notamment, sur cette stratégie la résolution votée par le Sénat le 19.04.2013

[42] La délégation française est composée de représentants du ministère des Affaires Etrangères, de l'ANSSI et du ministère de l'Intérieur *(Direction de la coopération internationale)* ; le ministère de la Justice n'est pas représenté

32.- Des approches sectorielles dédiées spécifiquement à la lutte contre la cybercriminalité

Le plan de lutte stratégique pluri-annuel contre la grande criminalité organisée érige en action prioritaire la cybercriminalité ; celle-ci est visée tant au titre des fraudes en ligne et aux cartes de paiement, de l'exploitation sexuelle en ligne des mineurs et des cyber attaques portant atteinte à des infrastructures et à des systèmes d'informatique critiques de l'Union, que comme vecteur de criminalité *(recours à Intranet pour la traite des êtes humains, le trafic de drogues de synthèse, la contrefaçon de biens, le trafic d'armes à feu, la fraude aux taxes infra communautaires)* [43].

Problématique française

Au sein des groupes de travail, la France, représentée par l'O.C.L.C.T.I.C., l'O.C.V.R.P. et le S.T.R.J.D. de la Gendarmerie, est pleinement impliquée dans les priorités ainsi définies.

Elle mène, également, et cela en concertation avec la Commission et EUROPOL, une étude sur les obstacles juridiques handicapant la lutte contre les fraudes aux cartes bancaires ; elle diligentera aussi une étude, début 2014, auprès des services enquêteurs de l'Union en vue de définir les possibilités d'améliorer l'entraide pénale internationale au plan européen.

En outre, le 7ème plan d'action douanier européen fixe, pour 2013-2017, un cadre stratégique d'action pour les Douanes, en privilégiant quatre objectifs stratégiques, notamment la lutte contre le commerce de contrefaçons résultant de la vente sur Internet et le renforcement de la coopération avec l'Observatoire européen des atteintes aux droits de propriété intellectuelle. Ces objectifs sont eux-mêmes déclinés en actions concrètes, comme l'organisation d'échanges avec les pays tiers ou encore la production de lignes directrices en matière de lutte contre la vente de contrefaçons sur Internet.

33.- La fourniture d'outils de formation et de prévention

La stratégie de l'Union intègre un objectif de sensibilisation des entreprises, des administrations et du grand public *(sous l'angle notamment de la formation en milieu scolaire)* qui n'est toutefois pas nouveau.

□ s'agissant de **la protection de l'enfance**,

⌙ Le programme *"Internet sans crainte" (safer internet)* créé par la Commission soutient le développement d'un Internet responsable et sûr pour les enfants, qui associe, dans 38 pays, les parents, les enseignants, les éducateurs et les enfants eux-mêmes.

Chaque année, le *"Safer Internet Day"*, organisé simultanément dans trente pays de l'Union, permet la mobilisation d'un grand nombre de partenaires autour d'un thème commun qui, en 2014, sera *"Ensemble pour un meilleur Internet"*.

[43] Au sein du Conseil, le groupe COSI, compétent sur les questions de sécurité intérieure, est chargé de la mise en oeuvre de ce plan qui concerne les années 2014-2017. La priorité donnée par le Conseil à la lutte contre la cybercriminalité a été approuvée par le Conseil Justice-Affaires Intérieures des 6 et 7 juin 2013.

En France, ce programme est placé sous l'égide de *la Délégation aux usages de l'Internet* et fédère trois services complémentaires en matière d'éducation et de protection des mineurs *(cf. titre II, chapitre 4 sur le partenariat public/privé).*

⌞ De manière plus générale, la recommandation de l'Union en date du 18 décembre 2006 incite chaque Etat, dans le cadre de la lutte contre la fracture numérique, à intégrer les compétences clés définies au plan européen dans ses stratégies d'éducation et de formation tout au long de la vie ; parmi les 8 compétences clés ainsi définies, la quatrième, visant la compétence numérique, implique l'usage sûr et critique des technologies de la société de l'information *(TSI)* au travail, dans les loisirs et dans la communication.

□ s'agissant de **la formation des personnels enquêteurs**

Le groupe de travail européen ECTEG *(Européan cybercrime training and éducation group)*, composé de représentants des services enquêteurs des Etats membres, d'organisations internationales, d'universités et d'industriels, entend promouvoir l'harmonisation des référentiels des métiers et qualifications.

Son acte vise notamment à favoriser des démarches de formation commune entre les services répressifs par la mise à disposition de supports de formation et le partage d'expertise en la matière. Cette approche implique également les organisations internationales, les partenaires académiques *(sous la forme de la création de formations diplômantes reconnues au plan international)* et les partenaires industriels. Elle bénéficie du soutien d'EUROPOL et s'appuie notamment sur le Collège européen de police (CEPOL).

34.- La création d'un outil européen de soutien technique et opérationnel dédié à la lutte contre la cybercriminalité

EUROPOL est l'une des agences européennes impliquées dans le dispositif anti-cybercriminalité de l'Union Européenne, avec l'ENISA *(Agence européenne chargée de la sécurité informatique des réseaux)*, EUROJUST, le CERT de l'Union Européenne et le CEPOL. Elle est, plus spécifiquement, chargée d'analyser la réalité du phénomène par le biais de ses bases de données [44].

Dans ce cadre, EUROPOL a créé récemment **le *Centre européen de lutte contre la cybercriminalité (EC3)*** [45], qui a pour mission d'apporter aux services d'enquête un soutien dans la lutte contre les fraudes bancaires, les escroqueries financières en ligne, la pédopornographie, les cyber-attaques contre les infrastructures d'intérêt vital et le piratage d'informations de l'Union. Il fournit à ce titre conseils et assistance technique, analyse criminelle, soutien technico-légal, coordination opérationnelle, analyse stratégique que les nouvelles menaces [46], formation, mise en réseau d'experts, travail avec le privé et les universités...

Plus précisément, un groupe de discussion - *l'European cybercrime task force* d'EUROPOL -

[44] La France est représentée au sein du conseil d'administration d'EUROPOL par la direction centrale de la police judiciaire, mais l'ensemble des services répressifs travaille étroitement avec cette agence.

[45] Inauguré le 11 janvier 2013 dans les locaux d'EUROPOL, EC3 compte actuellement une quarantaine d'experts et dispose d'un budget de 4,6 millions d'euros.

[46] Programme SOCTA *(Serious organized crime threat assessment)*

permet aux chefs des unités nationales de la lutte contre le cybercrime d'évoquer avec les instances européennes *(EUROPOL, EUROJUST, la Commission)* les problèmes stratégiques et opérationnels liés aux enquêtes et à leur poursuite pénale, à l'intérieur comme à l'extérieur du territoire de l'Union.

Les fichiers CYBORG *(piratage),*TERMINAL *(fraudes aux cartes de paiement)* et AWF COPY *(contrefaçon)* facilitent les recoupements pour les enquêtes.

Le 10 février 2024, la Commission européenne a présenté le premier rapport sur la cybercriminalité élaboré par le centre EC3 ; son service opérationnel a participé, en un an, à 19 opérations internationales d'envergure contre la criminalité organisée

En terme de perspective, EUROPOL entend fédérer un réseau des plates-formes de signalement des Etats-membres ; **dans ce cadre, la plate-forme PHAROS, gérée par l'O.C.L.C.T.I.C., devrait être intégrée dans une plate-forme européenne, dénommée I-CROS,** dont le projet a été initié par l'office français dans le cadre de la présidence française de l'Union en 2008. Ce projet a connu des retards liés au déménagement d'EUROPOL mais aussi au fait que son contenu exact est encore débattu, certains Etats souhaitant se limiter aux contenus pédopornographiques, d'autres l'étendre plus largement *(racisme, escroqueries...).*

35.- Les institutions relais à l'échelle européenne

Au-delà des structures déjà énoncées, l'Union favorise l'émergence de forums ou d'observatoires destinés à prolonger les débats nationaux s'agissant des principaux thèmes liés à la lutte contre la cybercriminalité.

□ **le Forum européen "SecurePay"** s'inscrit dans le prolongement européen des débats nationaux qui ont lieu dans le cadre de *l'Observatoire français de la sécurité des cartes de paiement.*

Problématique française

Le champ de compétence de l'instance européenne est plus large que celui de son homologue français, puisqu'elle couvre l'ensemble des instruments de paiement *(virements, paiements mobiles...) - (cf., sur ce point le titre II, chapitre IV).*

□ **l'Observatoire européen des atteintes aux droits de propriété intellectuelle** s'intéresse, en ce qui le concerne, à l'ensemble des questions relatives à la lutte contre la contrefaçon. Il a pour mission d'améliorer la qualité des informations et des statistiques concernant le marché intérieur de l'Union, la définition et la diffusion des meilleurs stratégies et techniques de contrôle mises en oeuvre dans les secteurs public et privé de l'Union, et la sensibilisation de l'opinion publique.

Problématique française

Cet observatoire, initialement coordonné et dirigé par la Commission européenne, a été créé en 2009 suite à une initiative de la présidence française de l'Union. Il est rattaché à *l'Office d'harmonisation du marché intérieur (OHMI)* depuis 2012.

L'Institut national de la propriété intellectuelle (I.N.P.I.), en tant qu'il assure le secrétariat général du *Comité national anti-contrefaçon (C.N.A.C.),* représente la France à l'observatoire, participe aux réunions entre les Etats-membres ainsi qu'à la réunion plénière associant le public et le privé ; l'UNIFAB, la DGCIS et la direction générale des douanes et des droits indirects contribuent aussi activement à ces travaux en étant présent dans les différents groupes de travail.

Le CNAC, par l'intermédiaire des groupes "sensibilisation" et "cybercontrefaçon" devrait lancer en 2014 une campagne de communication sur la contrefaçon sur Internet à destination des consommateurs. Il s'agira également, en leur communiquant une liste d'indices et de bonnes pratiques, d'éviter d'être les victimes d'achat de contrefaçons sur Internet.

36.- Le soutien à la coopération pénale internationale

L'Union s'attache à élargir les possibilités de coopération institutionnelle.

Cette action se concrétise, notamment, dans le cadre de la lutte contre la contrefaçon; c'est ainsi que l'Union va lancer un nouveau programme européen sur la protection de la propriété intellectuelle en Chine comme en Asie du Sud Est [47].

S'agissant spécifiquement de l'entraide pénale internationale, la Commission a également chargé EUROJUST d'identifier les obstacles actuels à la coopération judiciaire au sein de l'Union en matière de cybercriminalité.

37.- Les possibilités de financement

Dans le cadre de la stratégie cyber, l'Union met à disposition des moyens de financement *(programme MIE, Horizon 2020, Fonds pour la sécurité intérieure, PEST et coopération extérieure...).*

A titre d'exemple, l'Union finance notamment l'IWF [48], agence indépendante de régulation des contenus sur Internet, qui constitue une autorité internationale de référence pour la lutte contre la pédopornographie sur Internet.

---

[47] Le projet Union Européenne - Chine IPR2 vise principalement à former les acteurs concernés par la propriété intellectuelle et sa mise en oeuvre et à améliorer le respect des droits de propriété intellectuelle par la mise en oeuvre d'actions administratives, civiles et pénales. L'I.N.P.I. participe à la logistique de ce projet. Quant au programme Union Européenne -Asie du Sud Est *(la Birmanie, le Brunei, le Cambodge, l'Indonésie, le Laos, la Malaisie, les Philippines, Singapour, la Thailande et le Vietnam)*, son troisième volet a été lancé le 1er janvier 2010 *(UE - ASEAN ECAP III)* ; financé par la Commission et l'Office européen des brevets *(0EB)*, il s'étale sur 4 ans ; il est piloté, depuis le début 2013, par l'OHMI

[48] Cette agence *(Internet watch foundation)* met notamment à la disposition de ses partenaires (fournisseurs d'accès à Internet, fournisseurs de solution de blocage et moteurs de recherche) une liste noire d'URLs pointant vers des sites contenant potentiellement des contenus d'abus sexuels sur mineurs, et en particulier des images.

Problématique française

Si les capacités européennes de financement existent bien, elles sont gérées par des procédures à long terme, qui répondent à des logiques parfois complexes ou éloignées du temps opérationnel. Le contexte budgétaire actuel conduit aussi la Commission à revoir son engagement dans certains programmes ; c'est ainsi qu'elle envisage, dès 2014, de mettre progressivement un terme aux subventions qu'elle alloue aux dispositifs de signalements européens. Une telle politique pourrait devenir critique *pour l'Association des fournisseurs d'accès (AFA)*, qui espère que les pouvoirs publics français prendront le relais en s'engageant financièrement pour la protection des mineurs sur Internet et la lutte contre la pornographie enfantine.

38.- Les perspectives européennes pour 2014

La Commission Européenne n'envisage pas, dans le cadre de sa stratégie cyber, de créer de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace.

La priorité est ainsi mise sur l'adoption des instruments déjà préparés, notamment les projets de directive déjà cités portant sur la protection des données ou sur le secret des affaires, ainsi que le projet de règlement européen sur l'identification électronique [49]. Toutefois, comme on l'a vu, l'ambition consiste aussi à améliorer certains instruments existants et à leur donner une plus grande portée en terme d'adhésions nouvelles.

En juin 2014, le Conseil de l'Union doit établir une feuille de route pour le domaine Justice-Affaires intérieures pour les quatre prochaines années ; les travaux préparatoires témoignent déjà de la priorité que les Etats-membres souhaitent donner à la lutte contre la cybercriminalité.

Problématique française

Pour la France, les efforts normatifs entrepris par l'Union visant à rapprocher les législations nationales à des fins d'échange d'informations et de coopération policière en matière de lutte contre la cybercriminalité sont prioritaires.

En outre, suite à l'adoption des conclusions du Conseil de juillet 2013, les Etats-membres de l'Union se sont accordés, le 30 octobre 2013, pour traduire plus avant la stratégie sous la forme d'une feuille de route détaillée. Au plan stratégique, cette démarche devrait donc se traduire, dans les mois à venir, par la déclinaison des orientations politiques déjà adoptées sous la forme de priorités, d'actions à mener et d'acteurs à impliquer.

Problématique française

L'une des priorités françaises, énoncées publiquement par les plus hautes autorités de l'Etat, consiste à favoriser l'émergence d'une industrie européenne spécialisée susceptible de fournir, en matière de cyber, les dispositifs nécessaires à toute indépendance technologique.

En outre, l'échange de bonnes pratiques que le *"groupe des Amis de la présidence de l'Union européenne"*, en charge de la mise en oeuvre de la stratégie de cybersécurité, entend développer, pourrait être l'occasion de promouvoir au plan international les améliorations du dispositif français dans la lutte contre la cybercriminalité.

[49] Ce projet COM(2012) 238, en cours de discussion au Parlement européen, traite, entre autres, de la notion d'authentification électronique mais sous le seul angle de la reconnaissance mutuelle entre Etats.

Les priorités actuellement arrêtées pourraient connaître, en cours de l'année 2014, des évolutions importantes du fait du renouvellement des commissaires de la Commission européenne et des élections au Parlement européen.

*****

Si l'Union européenne comme le Conseil de l'Europe jouent ainsi un rôle majeur dans la lutte mondiale contre la cybercriminalité, les instruments européens adoptés dans différents secteurs offrent un cadre légal général que l'on se doit de renforcer, tant au plan international qu'au plan interne.

En outre, l'affaire PRISM a souligné la nécessité d'un positionnement européen plus cohérent et plus volontariste s'agissant de la protection des données personnelles.

I.4.- Les enseignements du droit comparé

La France n'est pas seule à se heurter à des difficultés dans l'appréhension de la cybercriminalité et à vouloir passer à une seconde étape : l'étude réalisée, à la demande du groupe de travail, par *le Service des affaires européennes et internationales (S.A.E.I.)* de la Chancellerie *(bureau du droit comparé)* [50] en atteste, tout en mettant en exergue, ici et là, des précédents utiles.

□ Dans les Etats comparables, nul ne paraît être parvenu à surmonter le défi que pose **la définition de la cybercriminalité** ou, lorsque certains l'ont fait *(cf. Grande Bretagne et U.S.A.)*, la définition donnée paraît trop restrictive, voire peu opérationnelle *(cf. Canada)*.

Une telle difficulté s'explique par le fait que, partout, si certains comportements spécifiques à la cybercriminalité ont été érigés en infractions autonomes - en particulier s'agissant des atteintes aux systèmes de traitement automatisé de données, et l'on voit là l'influence de la directive européenne sur la cybercriminalité -, la majeure partie des poursuites reste fondée sur les incriminations de droit commun.

Toutefois, à la marge, il y a des distinctions dans la mesure où, en matière d'atteintes aux biens, **la tendance à l'incrimination spécifique est parfois plus forte qu'en France** *(cf. l'Allemagne qui incrimine l'escroquerie commise au moyen de la manipulation de données informatiques; certains Etats fédérés des U.S.A. font de même avec l'extorsion en ligne ou l'envoi de spams massifs quantitativement définis en fonction des périodes de temps ; l'Espagne qui vise spécialement la diffusion ou la révélation de photographies ou d'images sur Internet portant gravement atteinte au droit de la vie privée de la personne ainsi que la révélation des secrets d'entreprise faisant l'objet de transcriptions informatiques ; la Belgique qui incrimine le cyber-harcèlement depuis 2005 ; le Canada s'agissant de la fraude informatique ou du vol élargi au crédit d'un compte bancaire ou encore de la possession d'outils de piratage informatique...).* Une telle tendance est perceptible dans de nombreux Etats lorsqu'il est question de cyber-intimidation, de cyber-harcèlement, de vol d'identité, de *"spamming"*, d'acquisition ou de distribution de données illégales...

Il n'en demeure pas moins que, comme en France, on se heurte partout à de véritables difficultés lorsqu'il s'agit de **décompter les infractions relevant de la cybercriminalité** *(cf., notamment, l'Allemagne, en situation comparable).*

Le travail législatif d'incrimination est lui-même confronté à un dilemme difficile, puisque la cyber-infraction doit être définie de manière assez large pour que l'évolution technologique ne la rende pas immédiatement obsolète ou du moins insuffisante, tout en respectant le principe de légalité qui requiert précision et clarté. Selon les systèmes, la priorité est donné à l'une ou à l'autre des considérations. Enfin, la difficulté à prouver l'élément intentionnel de la cyber-infraction conduit certains systèmes juridiques à préconiser des infractions matérielles ou à privilégier la voie administrative qui fait l'économie d'une telle exigence *(cf. WEIGEND, op. cit.).*

---

[50] voir, en annexe, l'intégralité du rapport de synthèse ; parmi les autres sources utilisées, cf. WEIGEND (Thomas), *"Rapport général sur la société de l'information et le droit pénal au XIXème congrés de l'Association internationale de droit pénal"*, Revue internationale de droit pénal, 2013/1, vol.84, p). 19-47

Il est à noter que les efforts des systèmes juridiques ne portent pas seulement sur les incriminations mais aussi parfois sur **l'adaptation des sanctions** ; ainsi, le droit Belge prévoit-il la confiscation des dispositifs malveillants et reconnaît au procureur du Roi le droit d'utiliser tous les moyens techniques pour rendre les données inaccessibles si ces données *"constituent l'objet de l'infraction ou en sont le produit et si elles sont contraires à l'ordre public ou aux bonnes moeurs, ou constituent un danger pour l'intégrité des systèmes informatiques ou des données stockées, traitées ou transmises par un tel système"* , par exemple en ordonnant à un fournisseur de services Internet de supprimer le nom de domaine d'un site qui viole la loi *(cf. WEIGEND, op. cit.).*

□ **la place donnée à la réponse pénale** diffère fortement selon les systèmes juridiques *(cf. WEIGEND, op. cit.).*

Ainsi certains donnent la prédominance à des réponses de nature administrative en reconnaissant à des organismes le droit d'ordonner la suppression de tel ou tel contenu ou de fermer un site ; un tel dispositif, qui va jusqu'à ordonner à un fournisseur d'accès de bloquer un site, est fréquent pour lutter contre la pédopornographie *(Finlande, Hongrie, Italie, Roumanie, Turquie...)* ; en sens inverse, en Allemagne, en Grèce et en Pologne, les lois votées à cette fin ne sont jamais rentrées en vigueur - ce qui un peu aussi la situation de la France.

Dans la plupart des systèmes juridiques, les victimes peuvent agir au civil en réparation de leurs dommages ; mais une telle voie paraît souvent complexe et donc peu utilisée *(Pologne, Turquie...).*

Telle est la raison pour laquelle d'autres systèmes préconisent une troisième voie, faisant appel à l'auto-régulation des prestataires de service de l'Internet, par le biais de notifications faites par les internautes *(cf. Les Pays-Bas, la Hongrie).*
A cet égard, certains Etats s'interrogent sur l'opportunité d'élargir la responsabilité des fournisseurs d'accès à Internet.

Un autre moyen de faire du droit pénal l'ultima ratio consiste à en exclure les cas où l'infraction a été autorisée ou facilitée par la négligence de la victime en terme d'auto-protection *(Allemagne, Espagne, Hongrie, Italie, Pologne).*

□ **la compétence territoriale à l'égard de la cybercriminalité** pose difficulté mais les systèmes juridiques l'ont résolu différemment *(cf. WEIGEND, op. cit.).*

Ainsi, lorsque l'auteur a agi à ou de l'étranger, la plupart des Etats reconnaissent compétence à leurs propres juridictions si l'effet de l'infraction s'est produit sur le territoire national *(cf. Autriche, Brésil, Allemagne, Italie, Roumanie).* Toutefois, cet "effet" est défini plus ou moins largement : dans certains systèmes juridiques, la simple visualisation d'un contenu pénalement répréhensible sur un site étranger est attributive de compétence pour la juridiction concernée *(Allemagne, Turquie)* ; d'autres requièrent un préjudice plus direct et plus matériel.

Manifestement, la connexion traditionnelle entre la question de compétence et celle du territoire d'un Etat-nation est, peu à peu, bouleversée par la cybercriminalité, comme elle l'est déjà d'ailleurs par la criminalité organisée à l'échelle internationale.

□ En ce qui concerne **l'organisation des services d'enquête**, les Etats hésitent entre le recours à des enquêteurs spécialisés et la création de véritables services dédiés à la lutte contre la cybercriminalité ; toutefois, la croissance de cette délinquance les incite actuellement à privilégier la seconde solution, quitte à créer, dans le cadre de tels services, des groupes plus spécialement assignés à lutter contre telle ou telle forme de cyberdélinquance.

Le cadre constitutionnel s'avère, en revanche, déterminant lorsqu'il s'agit de confier tout ou partie de cette lutte à un ou à des services centraux *(Espagne, Pays-Bas, Royaume-Uni)* ou, au contraire, aux Etats fédérés *(U.S.A.)* aux landers *(Allemagne, les services fédéraux n'ayant compétence qu'en matière de soutien technique ou pour effectuer une veille permanente),* ou aux provinces *(Canada, bien que la Gendarmerie Royale dispose d'une direction spécialisée).*

Certains modèles organisationnels méritent attention, tel le service central créé par le Royaume-Uni pour connaître de toute la délinquance relative aux cartes bancaires, ou le centre de gestion des plaintes en ligne que l'on trouve aux U.S.A. pour certaines infractions spécifiques à la cybercriminalité *(usurpation d'identité, intrusion informatique, violation des droits de propriété intellectuelle, extorsion en ligne...),* étant noté qu'outre les plaintes des victimes dressées sur la base de formulaires-type, ce centre a aussi vocation à recevoir les signalements portant sur des contenus illicites ou des comportements dangereux. La composition même de ces services fait parfois largement appel à des analystes privés, voire à des hackers susceptibles d'infiltrer les systèmes potentiellement dangereux *(Grande-Bretagne).*

□ En terme de **coordination et de pilotage centralisés**, l'hétérogénéité prédomine, certains pays la confiant à l'armée *(cf. le Brésil où la lutte contre la cybercriminalité relève de la stratégie nationale de Défense)*, d'autres à une agence publique sur le point d'être créée pour pallier l'éparpillement des services *(cf. le Royaume-Uni),* d'autres encore à la police judiciaire *(cf. les Pays-Bas, même si, en cas de menace grave, peut intervenir aussi une force interministérielle regroupant services de police, parquet national et centre de protection des infrastructures nationales)*, d'autres enfin à un procureur général spécialisé *(Espagne, cette autorité disposant d'un parquet autonome comprenant 70 magistrats).*

□ Pour ce qui concerne **les moyens juridiques d'investigation**, la distinction la plus notable concerne les Etats - les plus nombreux - qui obligent les gestionnaires à conserver les données relatives aux échanges sur Internet mais pendant des périodes de temps très variables, et ceux qui s'y refusent pour l'instant *(Allemagne, Grande-Bretagne, Japon et U.S.A. notamment)*, pour des raisons tenant essentiellement aux droits constitutionnellement reconnus s'agissant de la liberté d'expression; les Etats du second groupe tentent de pallier les difficultés qui en résultent s'agissant du recueil de la preuve numérique soit en misant sur la prévention de la fraude et son signalement rapide *(Grande-Bretagne et Pays de Galles)*, soit en recourant à une veille permanente à grande échelle sur Internet et à la cyber-infiltration à dose massive *(U.S.A.).*

Pour autant, la tendance générale consiste à doter les services d'enquête de moyens d'investigation jugés nécessaires à la lutte contre la cybercriminalité.

Certains Etats disposent déjà, et parfois depuis une décennie au moins, de moyens légaux récemment reconnus en France ou qui font toujours discussion, notamment en matière de blocage de sites en matière de pédopornographie *(cf., par ex., le juge d'instruction Belge qui peut ordonner aux fournisseurs de bloquer leurs services en cas de danger pour la sécurité publique, la*

sécurité publique, la sécurité nationale, la défense nationale ou l'intérêt des consommateurs - (cf. WEIGEND, op. cit.).

D'autres Etats sont sur le point d'introduire de pareils moyens dans leurs normes internes, par exemple l'Espagne, qu'il s'agisse de l'usage de fausses identités et de la cyber-infiltration ou de la possibilité reconnue au juge d'instruction d'ordonner la fermeture des sites de pornographie infantile ou le blocage de leur accès s'ils sont situés dans un pays étranger, ou encore le Canada qui, bien que doté d'une législation depuis 1985, entend renforcer la coopération des prestataires privés, élargir les possibilités d'interception et créer de nouveaux outils d'enquête adaptés aux délits informatiques...

Quoiqu'il en soit, il semble que, de manière générale, les débats sur ce point soient moins tendus qu'en France. Néanmoins, le consensus existant consiste parfois à réserver l'obligation de stockage des données *(Espagne, même si cette limitation est aujourd'hui contestée)* ou les mesures les plus intrusives aux infractions dites graves *(5 ans d'emprisonnement encourus pour l'Espagne, l'Allemagne se référant, quant à elle, à une liste d'infractions assez pléthorique*).

□ En ce qui concerne **les victimes**, rares sont les Etats qui disposent d'une véritable politique en la matière, à l'exception notable des actions mises en oeuvre en terme d'information et de sensibilisation, notamment à l'égard des mineurs et des entreprises à propos desquelles l'on constate partout une certaine réticence à déposer plainte pour des raisons d'image ; ces actions sont conduites soit par la police *(Espagne)*, soit par une autorité indépendante *(Royaume-Uni)*, soit par des instances public/privé *(Canada, s'agissant tant du télémarketing frauduleux, que de l'exploitation sexuelle des enfants, avec des possibilités de signalement en ligne).*

□ **La coopération internationale** rencontre, dans tous les Etats, des difficultés du même ordre que celles constatées en France et même davantage pour ceux qui ne sont pas signataires de la convention du Conseil de l'Europe sur la cybercriminalité *(Brésil)* ou qui ne l'ont pas encore ratifié *(Canada)* ou transposé intégralement dans leur législation interne *(Espagne).* Certains de ces Etats mènent une politique très volontariste dans le domaine international *(Pays-Bas, Canada...).*

Le pilotage de ces questions est fonction de l'architecture interne retenue ; ainsi, le ministère fédéral de l'Intérieur joue-t-il un rôle prééminent en Allemagne, alors que les questions de coopération sont confiées, par le Royaume-Uni, à une agence spécifique.

□ Mais c'est sans doute en ce qui concerne **la stratégie globale dans la lutte contre la cybercriminalité** que les enseignements du droit comparé sont les plus intéressants pour la France, d'autant plus que, s'agissant des Etats européens qui l'ont mise en oeuvre, elle s'inspire directement de la stratégie recommandée par l'Union européenne lorsqu'elle ne l'a pas précédée.

Ainsi, la "stratégie de cyber-sécurité" mise en oeuvre en Allemagne à compter de février 2011 repose sur la détermination de 10 objectifs qui englobent, aussi bien, des questions de cybersécurité, de cyberdéfense et de lutte contre la cybercriminalité au sens français de ces termes.

Sur le plan organisationnel, cette stratégie Allemande

-est pilotée par un *"Conseil national de cyber-sécurité"*, associant, outre la Chancellerie, les ministères fédéraux des Affaires étrangères, de l'Intérieur, de la Défense, de l'Economie, des Finances, de la Justice et de l'Education et de la Recherche, avec la possibilité d'associer les milieux économiques et des universitaires.
-lequel est assisté par *un Conseil de cyber-sécurité*, association composée de personnalités politiques, économiques et universitaires
-est mise en oeuvre par *l'Office fédéral pour la sécurité des techniques d'information*, déjà existant, mais dont le rôle a été renforcé afin, outre la mise au point et la surveillance de l'application des protocoles et standards de sécurité s'agissant de l'administration fédérale, d'informer le public sur les failles de sécurité existant dans les logiciels ou systèmes informatiques et de mener des actions de sensibilisation auprès des milieux économiques ou financiers ; cet Office, qui comprend 550 personnes, essentiellement des informaticiens et scientifiques, est rattaché au ministère de l'Intérieur.
- ainsi que par *le Centre national de cyber-protection* qui, assistant l'Office fédéral, traite des dossiers concernant la sécurité nationale, notamment celle des infrastructures dites critiques, et assure la coopération entre les différentes autorités *(policières, douanières, de renseignements ainsi que l'armée).*

Plus récemment, les Pays-Bas ont créé un *Centre national de cyber sécurité*, structure associant notamment la Défense, la police, le ministère public et le laboratoire central de médecine légale ; il est principalement chargé de suivre les tendances en matière de cybercriminalité, de menaces, d'incidents et de vulnérabilités.

Le Royaume-Uni prépare, lui aussi, une nouvelle stratégie en matière de lutte contre la cybercriminalité, principalement axée sur la protection des intérêts industriels, financiers et commerciaux du pays. Il est le fait de l'agence déjà citée.
Toutefois, cet Etat, a depuis longtemps mis l'accent sur la prévention à travers une série d'organismes permettant au Gouvernement, aux autorités judiciaires et aux entreprises appartenant aux secteurs économiques sensibles d'échanger les informations utiles sur les cyber-menaces, l'un d'entre eux étant plus spécialement dédié aux questions de défense et aux industries de l'armement.
Une dernière structure, qui prend la forme d'une agence publique, laquelle associe aussi des représentants de la société civile, a pour but de prévenir et de lutter contre la fraude, notamment sous la forme de campagnes publicitaires et d'informations des usagers.

Le Canada, s'il n'a pas encore défini de stratégie globale, sauf pour la protection des infrastructures essentielles, dispose toutefois d'un *Comité de coordination des hauts fonctionnaires* destiné à aider la police et les administrations habilitées à évaluer leur capacité d'enquête et la prise en compte de la cybercriminalité.

▬▬▬▬▬

I.5.- Les attentes de l'opinion publique, des victimes et des acteurs

Toutes trois sont singulières, raison pour laquelle il convient de les passer successivement en revue.

1.- Lorsque l'on évoque Internet et la nécessité de lutter contre la cybercriminalité,l'ambivalence domine dans **l'opinion publique**, partagée qu'elle est entre une exigence très forte que l'on n'émarge pas sur les libertés d'expression et d'usage d'Internet *(cf. les débats qui ont précédé la loi Hadopi ou certaines réactions suscitées par la question de la géo-localisation)* et une demande non moins forte de protection lorsque l'internaute, lui-même, devient victime ou se sent menacé *(cf. l'affaire PRISM)*.

Une telle ambivalence a notamment pour origine le fait que seul l'apport d'Internet est mis en évidence, les internautes n'étant pas suffisamment sensibilisés sur les risques induits par ce nouveau mode de communication et d'expression, que mettent en exergue tous les experts entendus [51] :

- la mémorisation considérable induite par Internet et sans limitation de durée, niant le droit à l'oubli, et qui fait en sorte que toutes données, les plus personnelles comme celles susceptibles de servir de support à un éventuel acte de délinquance, seront fichées et exploitées, sans possibilité de récupération ni d'effacement ;

- l'effet amplificateur d'Internet en terme d'informations, partagées à l'infini même si elles sont sensibles, qui peut conduire jusqu'à la mort sociale, voire au suicide.

L'éducation, la sensibilisation de l'opinion à la nécessité d'adopter de nouveaux comportements, afin de mettre un terme à la confusion existante entre l'espace privé et l'espace public, tout en fournissant moins d'armes aux délinquants, revêt ainsi une importance cruciale.

[51] source : notamment, l'audition de Mme. Christiane FERAL-SCHUHL, alors bâtonnière de l'Ordre des avocats de Paris, spécialiste du cyberdroit et présidente de l'Association pour le développement de l'informatique juridique

2.- S'agissant des **victimes individuelles** [52], leurs attentes, de manière générale, dépendent de la nature de l'atteinte subie, selon qu'elle porte sur l'intégrité physique ou psychique *(pédopornographie, atteinte à l'image...),* sur l'atteinte à la vie privée, l'identité, l'intimité, la réputation *(injures, diffamations, harcèlement...)*, ou sur le patrimoine *(escroqueries...).*

Il existe toutefois des facteurs aggravants spécifiques aux cyber-victimes, qui tiennent aux particularités de cette délinquance :

- la peur de l'inconnu et donc de la réitération, puisqu'à l'exception de certaines atteintes à la vie privée et des pratiques d'harcèlement entre mineurs, l'auteur agit anonymement et le restera pour l'essentiel, et que, même identifié, il est un étranger pour la victime ;

- l'effet démultiplicateur du préjudice, puisqu'un message attentatoire à l'image ou à la vie privée d'une personne peut se répandre de façon massive et instantanée et toucher ainsi un large public. La victime se sent totalement désarmée face à cette reprise de l'information en chaîne, dans l'espace et le temps *("l'effet miroir" d'Internet).*

- Le sentiment d'impuissance, car la victime n'a aucune possibilité de maîtrise sur l'événement et attend tout de l'Etat, sentiment renforcé par l'efficacité relative de ce dernier eu égard aux difficultés d'identification et de preuve qui font obstacle au principe de responsabilité, mais surtout lorsqu'il s'agit de faire cesser l'infraction ou de la réparer.

- Parfois même un sentiment de honte, voire de culpabilité, qui peut faire obstacle au dépôt de plainte, notamment dans l'hypothèse d'une escroquerie sentimentale qui révèle les failles intimes et les fragilités de la victime ou même de l'escroquerie banale lorsqu'elle se fonde sur la naïveté, la crédulité ou même l'appât du gain de la victime *(ex. des escroqueries à l'héritage)*, ou qui résulte de la violation de la sphère privée dévoilée à tout un chacun.

...mais aussi au fait que ces cyber-victimes sont souvent des personnes isolées socialement et fragiles psychologiquement, réticentes à se confier même à leurs proches et encore davantage à des professionnels, silence qui peut être à l'origine de véritables drames.

Un tel constat fonde les attentes des victimes individuelles, telles que résumées par l'INAVEM :

- la première attente des victimes c'est qu'il soit mis un terme à l'infraction, en particulier en cas d'atteinte à la vie privée, et cela le plus rapidement possible et sans attendre de très éventuelles poursuites. Toutefois, leur méconnaissance des dispositifs existants, l'efficacité réduite de certains d'entre eux s'agissant notamment des mécanismes de dénonciation aux hébergeurs, la nécessité

[52] source : *Institut national d'aide aux victimes et de médiation (INAVEM),* réseau regroupant les 135 associations d'aide aux victimes habilitées par la Justice, gérant la plate-forme téléphonique nationale d'aide aux victimes (08victimes) et dont le dernier congrès, qui s'est tenu les 20 et 21.06.2013 à ROUBAIX, a précisément porté sur les cyber-victimes.

d'engager des frais pour le référé civil, le fait que le système pénal ne soit pas en capacité de prendre des mesures provisoires en urgence ne facilitent pas la situation des victimes.

⌴ La seconde attente a trait à une meilleure prise en considération et à une plus grande reconnaissance, notamment au niveau du dépôt de plainte, dans la mesure où, faute de sensibilisation suffisante à ce type de délinquance mais aussi eu égard à un certain sentiment d'impuissance ressenti par les enquêteurs eux-mêmes par exemple en matière d'escroqueries, certaines plaintes se heurtent encore à des refus d'enregistrement, voire à un accueil inadapté eu égard à l'état de faiblesse ou à la honte ressentie par l'intéressé.

⌴ La troisième attente concerne la réparation, d'abord au regard d'Internet lui-même afin de reconstruire une image salie et d'éviter qu'elle continue à se répandre, ensuite en terme financier, s'agissant des escroqueries commises au préjudice de victimes en situation de détresse et de fragilité particulière, le peu d'efficacité de la réponse répressive n'étant pas compensée par les possibilités d'indemnisation sur fonds publics, faute d'adaptation de ces dernières à ce nouveau type de délinquance.

Par-delà, le renforcement des actions de prévention et de sensibilisation, notamment dans les établissements scolaires, ainsi que l'extension des délais de prescription pour les infractions dites de presse dans la mesure où les victimes ont souvent connaissance de l'infraction alors que le délai de trois mois est déjà acquis, sont jugés hautement nécessaires.

La question des mineurs victimes[53] mérite une approche particulière puisque la vie numérique fait désormais partie intégrante de leur vie réelle et que chaque évolution technique en ce domaine a des répercussions sur leurs droits - celui d'être protégé contre les violences et contre les atteintes à leur vie privée, celui de ne pas être exploité, celui de s'informer et de penser librement...Or, les enfants et les adolescents, objet de nombreuses sollicitations, sont directement concernés par les contenus illicites, l'usurpation d'identité, le harcèlement et le dénigrement, le prosélytisme et la désinformation. Les principales attentes formulées en ce domaine se fondent sur les constats suivants :

⌞ plus que tous autres, les mineurs ont besoin d'être sensibilisés aux risques numériques et informés de la protection réelle dont ils peuvent bénéficier, ce que *la Commission nationale consultative des droits de l'homme (CNDH)* qualifie de nécessaire *"culture de la prudence et de la sécurité".*

⌞Mais il faut aussi que leur environnement immédiat *(le monde éducatif, les parents)* ainsi que les policiers et les magistrats *(afin de faciliter le recueil des plaintes et leur traitement)* soient davantage formés à ces questions.

[53] sources : contribution de *la Défenseure des enfants* à la suite d'une réunion regroupant, le 10.01.2014, de nombreux acteurs, tant publics que privés *(cf. aussi le rapport "Enfants et écrans, grandir dans le monde numérique", novembre 2012)*; de l'association *Enjeux e-médias* ; de l'Education nationale...

⌞Si, sur ces deux points, de nombreuses actions sont quotidiennement mises en oeuvre, il faut encore qu'elles soient évaluées, coordonnées, pérennisées, ce qui passe par une implication suffisante des pouvoirs publics.

⌞Encore faut-il s'interroger sur l'efficacité des mécanismes préventifs existants, tel l'avertissement demandant une simple déclaration de majorité pour l'accès et l'achat sur les sites proposant des contenus pornographiques, des produits alcoolisés... ; telles les conditions d'accès des mineurs au e-commerce et le recueil de leur consentement et de celui de leurs parents ; telles les conditions posées aux pratiques de profilage et de géo-localisation ; telle la reconnaissance, toujours attendue, du droit à l'oubli, que revendiquent, entre autres, la CNDH et la CNIL.

⌞La spécificité de ces questions comme la multiplicité des acteurs conduisent la Défenseure des enfants à suggérer la création d'une plate-forme spécifique de réflexion, de proposition et d'intervention, rassemblant l'ensemble des acteurs publics et privés, afin d'instaurer une co-régulation des politiques du numérique en direction des mineurs.

Ceci rejoint les préoccupations de nombreux autres acteurs, qui souhaiteraient plus de coordination et d'impulsion de la part des pouvoirs publics, de véritables formations aux médias pour les personnels travaillant avec les jeunes, une modification de la classification des contenus sur le web, une meilleure prise en compte des chartes européennes spécifiques, une incitation à la recherche...

⌞Les attentes ont aussi trait à une plus grande responsabilité des opérateurs, notamment des fournisseurs d'accès ou de messages pornographiques ou haineux afin qu'ils ne puissent plus s'exonérer de leur responsabilité vis-à-vis d'un mineur par le biais d'un simple avertissement.

D'autres catégories de victimes méritent une attention particulière, sans aucune prétention sur ce point à l'exhaustivité.

Les propos discriminatoires et haineux [54] qui se multiplient sur Internet ont déjà été à l'origine de la création de la *Délégation interministérielle à la lutte contre le racisme et l'antisémitisme*, le 25 mars 2012. Là encore, est souhaitée une plus grande implication des services de l'Etat, notamment de l'appareil répressif. Au titre des propositions émises, l'on peut citer, par delà les actions de sensibilisation, de prévention et d'éducation,

⌞ l'amélioration des outils de mesure statistique du phénomène,

⌞ une auto-régulation des fournisseurs d'accès et de contenu plus effective, par exemple par des procédés de filtrage en amont, et la création d'un modérateur qui devrait pouvoir ordonner la suppression des propos haineux ; sur ce point et de manière générale, la CNDH s'inquiète de l'importance prise par les grands opérateurs, devenus quasiment des régulateurs et insiste sur le fait que, s'il faut les responsabiliser, il convient aussi d'éviter une sorte de privatisation du

[54] sources : auditions du *Délégué interministériel à la lutte contre le racisme et l'antisémitisme* ; de M. Marc KNOBEL, historien-chercheur...

contrôle de la liberté d'expression.

- L'adaptation de la loi de 1881 sur la presse aux nouvelles formes d'expression, nécessité toutefois contestée par la CNDH soucieuse de l'équilibre posé par cette loi entre la lutte contre le racisme et le respect de la liberté d'expression,

- une plus grande traçabilité de la suite réservée aux signalements à la plate-forme PHAROS afin que cette dernière, dotée des moyens nécessaires, devienne, comme le résume la CNDH, *"plus pédagogique",*

- la création d'un Observatoire de l'antisémitisme et du racisme sur Internet, réunissant professionnels, agents de l'Etat et organisations non gouvernementales [55],

- un soutien plus effectif des associations de lutte contre le racisme, qui portent en justice les atteintes les plus graves dont elles peuvent avoir connaissance mais qui ne disposent pas suffisamment de moyens pour être présentes sur tous les fronts,

- une politique plus volontariste de poursuite, avec un recours plus systématique par les parquets aux dispositions de l'art. 50-1 de la loi du 29.07.1881 permettant d'obtenir, en référé, l'arrêt d'un service illicite,

- une action résolue sur le plan international pour éviter l'évasion vers des *"paradis Internet"*, notamment en incitant les Etats-Unis, qui hébergent une part importante des contenus racistes, à ratifier le protocole additionnel à la Convention sur la cybercriminalité.

La discrimination sexiste [56], à travers la multiplication de tweets homophobes, comme les dangers que fait parfois peser le web sur les jeunes filles, avec, notamment, **le développement du proxénétisme et de la traite humaine**, suscitent des attentes souvent du même ordre que celles précitées, même s'il faut y adjoindre la recherche de nouveaux moyens juridiques destinées à faire de l'Internet un espace plus sûr et plus respectueux des femmes comme des hommes.

L'influence des mouvements à caractère sectaire [57] est aussi l'occasion, pour les acteurs concernés, de formuler de fortes attentes à l'attention des prestataires techniques de l'Internet et notamment des moteurs de recherche, mais aussi en ce qui concerne le renforcement des moyens publics consacrés à la veille et à la *"cyber-patrouille"* sur Internet et à la lutte contre la cybercriminalité

---

[55] Une telle création avait été projetée mais elle semble avoir été reportée en l'attente des conclusions du présent groupe de travail

[56] sources : entretien avec les représentants du Cabinet de la ministre des droits des femmes ; projet de loi pour l'égalité entre les hommes et les femmes...

[57] sources : rapports de la Haute autorité de santé ; rapport de la Mission interministérielle de vigilance et de lutte contre les dérives sectaires (MIVILUDES), avril 2013 ; rapport de la commission d'enquête du Sénat sur l'influence des mouvements à caractère sectaire dans le domaine de la santé, 3.04.2013...

Les attentes des **associations de consommateurs** [58] sont plus aisées à cerner car elles se situent dans un cadre plus circonscrit, même si l'on retrouve, dans les dénonciations qu'adressent les consommateurs à leurs associations, nombre d'infractions déjà évoquées par les associations de victimes *(notamment le phishing, les escroqueries en ligne, la fraude au SMS ou à la carte bancaire, ou les usurpations de données d'identité).*

⌙ Pour elles, la 1ère priorité relève de l'éducation de la population au numérique qui doit être érigée en grande cause nationale en commençant par l'école mais aussi, avec l'aide des services sociaux, en direction de certains publics défavorisés victimes de la fracture numérique, et qui doit prendre la forme d'une campagne audio-visuelle répétée. Une telle action devrait allier les moyens publics et privés.

⌙ Faire de l'internaute un acteur pour une meilleure régulation d'Internet constitue une autre exigence. Encore faut-il que les internautes soient convaincus que les dispositifs de signalements sont d'accès direct et facile pour eux et efficaces. Or, si de nombreux dispositifs existent déjà, certains sont jugés en déshérence, d'autres peu efficaces ou insuffisamment connus, d'où la nécessité de fédérer les interfaces sous la forme d'un numéro d'appel simple et unique à destination d'une seule plate-forme. L'incitation à la régulation passe aussi par l'amélioration de l'information de l'internaute sur les suites données à son signalement, une pareille exigence concernant également les plaintes.

Toutefois, l'efficacité d'un tel réseau d'information opérationnel entre la société civile et les services de l'Etat en charge de la prévention et de la répression nécessite de mieux associer les associations de consommateurs, qui, au-delà de leur rôle de veille, peuvent jouer un rôle de filtre, se substituer ou soutenir des consommateurs réticents à agir, ou fournir un relais utile aux pouvoirs publics en cas de menace grave.

⌙ La prévention suppose que les solutions techniques déjà existantes, par exemple pour se prémunir contre les spams, soient configurées par défaut, ou que la solution *"3DSecure"* destinée à prévenir les fraudes à la carte bancaire soit généralisée, et que les internautes soient mieux informés par les opérateurs et les entreprises du e-commerce sur les risques qui pèsent sur eux et les moyens de les pallier.

Elle requiert aussi que, par-delà une auto-régulation jugée insuffisante, les pratiques de confiance, mise en place par quelques entreprises - comme celles, en matière de e-commerce, consistant à encaisser le prix d'un bien acquis qu'une fois que ce dernier a été effectivement expédié - soient généralisées ; et que les opérateurs mobiles contrôlent davantage les prestataires bénéficiant de numéros spéciaux et avec lesquels sont conclues des conventions de remboursement avec, à la clé, un remboursement systématique des préjudices subis du fait des sms frauduleux.

Mais la prévention concerne aussi les nouvelles sources de risque pour les consommateurs, que constituent le développement des technologies du cloud

[58] source : auditions des associations de consommateurs *(C.L.C.V., Indecosa-C.G.T., Familles rurales, U.F.C.-Que choisir).*

en terme de sécurité des données, les échanges en télé-médecine, les offres de vente de médicaments, la multiplication sur les réseaux sociaux d'offres de prêts sur gage, les modes de paiement par terminal mobile, l'apparition prochaine des paiements mobiles sans contact...

Encore faut-il que l'Etat fixe les règles et que celles-ci ne soient pas le fait des prestataires techniques les plus puissants sur le marché...

Le dernier sondage Eurobaromètre publié par la Commission européenne en 2012 [59] confirme partie des attentes précitées puisque 59% des utilisateurs d'Internet ne s'estiment pas bien informés des risques liés à la cybercriminalité, que 40% d'entre eux craignent un usage abusif de leurs données personnelles et que 38% s'estiment préoccupés par la sécurité liée aux paiements en ligne. La dernière enquête du CREDOC, relative au déploiement des équipements et usages numériques en France, montre combien les français se disent aussi préoccupés par ces risques.

3.- Quant aux **entreprises**, victimes d'attaques de plus en plus nombreuses prenant pour cibles soit leurs systèmes d'information, soit les données détenues, soit même leur image et leur réputation, alors même qu'elles sont de plus en plus dépendantes d'un outil numérique et informatique qui évolue *"à la vitesse de la lumière"* et que leur véritable richesse tient pour une part dans l'information produite, elles doivent faire face à des questions de sécurité et de préjudice nouvelles, tant en interne qu'en externe, et s'interrogent sur la meilleure façon de préserver le modèle économique.

Si les plus importantes d'entre elles ont déjà mis en oeuvre un effort d'investissement important, tant en terme d'organisation, de méthode, de formation, de sécurité et d'équipements, c'est ce même monde de l'entreprise qui formule les attentes les plus précises de l'Etat, dont il attend une aide tant en terme de prévention, qu'au plan de la sécurité informatique et de la réponse pénale [60].

A l'égard des services étatiques, les attentes exprimées sont de plusieurs ordres:

- la 1ère est d'ordre technique, s'agissant de la prévention, de l'identification par le recours à des systèmes d'alerte efficaces [61] et de la réponse aux agressions, quelle qu'en soit l'origine *(entreprises mafieuses, entreprises concurrentes étrangères, services étatiques étrangers, ou criminels motivés par l'appât du gain)* ; ce rôle est en partie joué par *l'Autorité nationale de sécurité des systèmes d'information*, en partie seulement compte-tenu de ce que l'insuffisance de ses moyens actuels ne lui

[59] enquête portant sur 27.000 personnes dans l'ensemble des Etats membres de l'Union

[60] sources : cf., notamment, l'audition de M. Alain JUILLET, président du *Club des directeurs de sécurité des entreprises (C.D.S.E.)*, qui regroupe les 101 entreprises françaises les plus importantes, tant en terme d'emploi qu'au plan stratégique ; et la contribution du *Forum des compétences*, qui regroupe les établissements de la banque et de l'assurance

[61] Selon une récente étude américaine, la plupart des attaques ne sont détectées que très postérieurement à leur commission et à une époque où le pillage des données a déjà eu lieu.

permet pas de répondre à toutes les sollicitations [62] et qu'elle ne couvre pas l'ensemble du champ entrepreneurial.

⌞ La 2ème est d'ordre juridique, et renvoie à un manque de lisibilité comme d'adaptation du droit au regard, notamment, du caractère international de la menace mais aussi compte-tenu de la superposition de normes édictées par la loi et par de nombreuses autorités administratives sans recherche suffisante de cohérence. Sont aussi soulignées des carences d'interface avec le ministère de la Justice et les juridictions, faute de pôles spécialisés et d'une suffisante formation et sensibilisation des magistrats, ainsi que le prononcé de peines jugées inadaptées par rapport au préjudice causé par les cyber-attaques.

⌞ La 3ème relève des relations entre les entreprises et les services d'enquête, dans la mesure où beaucoup d'entrepreneurs sont réticents à déposer plainte par souci de leur réputation ou par crainte d'un manque de confidentialité, mais aussi faute, là encore, d'une interface suffisante entre les entreprises et les services d'enquête - interface indispensable lorsque l'infraction dépasse le cadre d'une seule société ou impacte un grand nombre de clients sur le territoire - [63]; d'autres obstacles mis en exergue tiennent à la complexité des procédures et à la lenteur des enquêtes souvent jugées incompatibles avec les besoins économiques.
Enfin, les entrepreneurs souhaitent une meilleure information sur l'évolution des enquêtes et les suites données, voire un accès direct à une base centralisée d'informations à des fins de prévention.

De manière générale, il est à noter que les entrepreneurs réclament davantage de coordination entre les trois différents pôles que constituent, en France, la cyberdéfense, la cybersécurité et la lutte contre la cybercriminalité, compte-tenu de la porosité croissante entre ces thèmes, les entreprises étant confrontées concomitamment à ces trois types de problématiques.

Toutefois, la situation des entreprises moins importantes, et a fortiori des petites et moyennes entreprises, souvent mal outillées en ressources de sécurité et qui ne peuvent disposer, au plan technique comme juridique, d'un réseau de nature à leur apporter une aide efficace en cas d'agressions numériques *(assistance d'urgence en cas d'attaque, préservation des preuves, nettoyage des systèmes, reconstitution des données...)*, est encore moins enviable.

Là, les besoins relèvent d'abord d'une sensibilisation et d'une formation aux risques, souvent méconnus ou minimisés, mais aussi d'une aide technique afin de prévenir et de répondre aux agressions, ce qui suppose une organisation, inexistante en l'état. Cette assistance devrait porter sur les questions urgentes qui se posent à une entreprise agressée, sur les mesures de préservation des preuves, de nettoyage des systèmes, voire de reconstitution des données.

---

[62] La récente loi de programmation sur la Défense devrait permettre de répondre à cette insuffisance, en ce qu'elle prévoit une montée en charge significative des effectifs de cette Autorité *(360 effectifs en l'état, 500 à l'horizon 2015).*

[63] même si, sur ce point, *la Direction centrale du renseignement intérieur* joue un rôle non négligeable

Les réponses attendues pourraient être le fait de CERT *(Computer emergency response team)*, dont la création est suggérée en associant les professionnels et les services étatiques.

4.- S'agissant enfin des **acteurs répressifs**, si les services spécialisés appellent essentiellement de leurs voeux des moyens d'investigation de nature à renforcer leur efficacité mais aussi une clarification des règles de compétence comme des obligations des prestataires techniques notamment étrangers, les services de droit commun, tant policiers que judiciaires, appréhendent encore mal la menace spécifique que fait peser la cybercriminalité ou s'estiment, le plus souvent, impuissants pour répondre à certaines manifestations de cette délinquance compte-tenu de sa spécificité et renverraient volontiers ces enquêtes aux instances spécialisées, existantes ou souhaitées.

Toutefois, à entendre ces dernières, certaines formes de cybercriminalité s'accommodent bien d'un traitement pénal classique, soit que les services de droit commun bénéficient déjà d'un processus de tri et d'orientation opéré en amont *(notamment en matière de pédopornographie où les infractions de détention d'images illicites font l'objet souvent de dénonciations de la part de services spécialisés, à l'échelle nationale ou internationale)*, soit, plus généralement, lorsqu'elles s'inscrivent dans des rapports inter-personnels où l'identification de l'auteur relève de mécanisme d'enquête traditionnels *(une partie notable des atteintes à la vie privée ou des harcèlements entre mineurs).*

C'est donc pour les infractions commises de l'étranger par des auteurs difficilement identifiables car anonymes, a fortiori pour la délinquance organisée et notamment pour les escroqueries, que les attentes sont les plus fortes, notamment en provenance des services de police qui souhaitent pouvoir disposer de davantage d'enquêteurs formés aux technologies numériques et être à même de travailler en liaison avec des magistrats eux aussi formés.

Plus généralement, l'ensemble des acteurs souhaitent, eux aussi, une action préventive plus intensive, une meilleure lisibilité de la législation applicable et une plus grande effectivité de l'entraide pénale internationale.

<u>En résumé</u>, plusieurs point forts résultent de ces attentes :

*l'existence d'une très forte demande vis-à-vis de l'Etat, même si la nécessité d'associer toutes les parties privées concernées et les internautes eux-mêmes n'est contestée par personne ;

*l'adaptation de la gouvernance interministérielle au plan national [64] avec, notamment, le renforcement du rôle du ministère de la Justice ;

*la nécessité que soit mise en place une stratégie globale de prévention comme de lutte contre la cybercriminalité mais aussi des stratégies sectorielles correspondant aux différents domaines qu'elle concerne, et avec toute la transparence nécessaire ;

*l'urgence de mieux cerner le phénomène ainsi que l'efficacité des moyens déjà disponibles ;

*le sentiment que, malgré la prolifération des actions de prévention, de sensibilisation, voire de formation, beaucoup reste encore à faire et que la solution est à rechercher dans une meilleure mise en cohérence de l'action des différents acteurs ;

*des attentes non satisfaites à l'égard des opérateurs, dont l'implication n'est généralement pas jugée à la hauteur de ce que l'on serait en droit d'en attendre ;

*une action plus efficace des services de police et de justice, qui requiert d'abord de la formation, ensuite l'adaptation des moyens d'investigation et de coopération internationale dans le respect des principes fondamentaux du droit *(CNDH)* et de manière transparente vis-vis du public *(association Cyber Lex)*, alors même qu'à quelques exceptions près, le droit pénal de fond est jugé adapté quoique peu accessible.

*Enfin, des actions résolues à l'égard des différentes catégories de victimes.

▬▬▬▬▬

[64] exigence que soulignent, par exemple, tant *le Forum des compétences* que *l'association Cyber Lex* et, plus encore, M. Daniel GUINIER

I.6.- Le contexte de l'action : les exigences tenant à la protection de la vie privée et à la liberté d'expression

Si la lutte contre la cybercriminalité suppose une plus grande effectivité, elle doit, dans le même temps, prendre en compte les exigences tenant aux libertés publiques, qui constituent le cadre dans lequel doit nécessairement s'inscrire toute proposition en la matière.

1.- le principe de la primauté du droit européen

Comme on l'a vu, le droit de fond commandant les règles du commerce électronique sur Internet ou la protection des données personnelles sont largement issues du droit européen

Ainsi, *la directive 2000/31 CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur* a-t-elle énoncé les principes directeurs applicables en cette matière où il s'agit d'abord de créer un réel espace sans frontières pour les services de la société d'information tout en respectant la liberté d'expression consacrée par l'article 10 de la Convention européenne et la jurisprudence de la Cour européenne des droits de l'homme ainsi que les règles relatives à la protection des mineurs et des consommateurs.

Quant au préambule de *la Convention de Budapest*, il énonce la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits fondamentaux garanti par la Convention précitée du Conseil de l'Europe et le Pacte international relatif aux droits civils et politiques, notamment le droit de ne pas être inquiété dans ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature sans considération de la frontière, ainsi que le droit à la vie privée.

La matière est également soumise à la protection des données personnelles régie par les *directives 95/46 CE du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel, 97/ 66 CE du 15 /12/1997 traitement des données à caractère personnel et protection de la vie privée dans le secteur des télécommunications et 2006/24/CE du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communication accessibles au public ou réseau public de communications*.

Enfin, les articles 8 et 10 de *la Convention européenne des droits de l'homme* justifient les ingérences de l'autorité publique dans l'exercice du droit au respect de la vie privée et du droit d'expression, à la condition que ces ingérences soient prévues par la loi et qu'elles constituent, dans une société démocratique, une mesure nécessaire à la sécurité nationale, au bien-être économique du pays, à la prévention des infractions pénales ou à la protection des droits et libertés d'autrui.

Ces principes européens revêtent d'autant plus d'importance que la jurisprudence de la Cour de Justice des Communauté européennes *(C.J.C.E.)* puis de l'Union européenne *(C.J.U.E.)* dénie aux juridictions nationales, y compris constitutionnelles, le pouvoir

de déclarer invalides les actes du droit dérivé. Dans l'arrêt Simmenthal [65], la Cour a ainsi énoncé le principe selon lequel *"Le juge national chargé d'appliquer dans le cadre de sa compétence les dispositions du droit communautaire a l'obligation d'assurer le plein effet de ces normes en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle ci par voie législative ou par tout autre procédé constitutionnel".*

En consentant à l'instauration de l'ordre juridique communautaire, les Etats membres ont admis que le régime contentieux des actes communautaires suivrait des règles propres : un acte de droit dérivé ne peut avoir qu'un seul juge qui est le juge communautaire. Il bénéficie auprès des juges nationaux d'une immunité constitutionnelle.

A l'occasion d'une contestation de la constitutionnalité des dispositions de la loi du 21 juin 2004 sur l'économie numérique, définissant le régime de responsabilité des "hébergeurs", dont l'activité consiste à stocker les informations fournies par un destinataire du service de communication au public en ligne, le Conseil constitutionnel en a tiré la conséquence que, lorsque les dispositions législatives se bornent à tirer les conséquences nécessaires des dispositions inconditionnelles et précises d'une directive, le grief d'inconstitutionnalité ne peut être utilement présenté devant lui [66].

Il rappelle qu'aux termes de l'article 88-1 de la Constitution *"la République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont institués d'exercer en commun certaines de leurs compétences"* et qu'ainsi *"la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la constitution"*[67], ce qui revient à dire qu'un Etat membre ne saurait exciper de difficultés internes ou des dispositions de son ordre juridique national, même constitutionnel, pour justifier le non respect des obligations et délais résultant des directives communautaires.
Il n'appartient qu'au juge communautaire, saisi, le cas échéant, par voie préjudicielle, de contrôler le respect par une directive communautaire des compétences définies par les traités ainsi que des droits fondamentaux garantis par le Traité de l'Union.

Ce principe vaut aussi bien pour le régime de responsabilité civile que pour le régime de responsabilité pénale des opérateurs et le législateur national ne peut le modifier.

---

[65] arrêts C.J.C.E. 106/77 en date du 9 mars 1978 ; C.J.C.E., 11 avril 1978, C. 100/177 et 6 mai 1980 C 102/79

[66] décision du Conseil constitutionnel 2004-496 D.C. du 10.06.2004 *(cons. 6)* sur la loi pour la confiance dans l'économie numérique ; cf., dans le même sens, la décision n° 2004-499 DC du 29.07.2004 sur la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ; décision n° 2004-498 DC du 29.07.2004 sur la loi relative à la bioéthique

[67] De cette décision du Conseil, il se déduit qu'il n'existe que deux tempéraments qui sont l'existence d'une disposition expresse contraire de la constitution, et le cas où les dispositions transposées de la directive ne sont pas inconditionnelles et suffisamment précises et laissent une latitude à l'autorité nationale.

2.- **La liberté d'expression et de communication**

La liberté d'expression et de communication est l'une des libertés des plus protégées à raison du rôle fondamental qu'elle tient dans la vie démocratique.

Or, et au delà des autres usages qui peuvent en être fait, Internet est devenu principalement un vecteur d'expression, de communication et de transmission des idées et des opinions.

Outre ceux déjà cités, cette liberté est explicitement visée par plusieurs instruments internationaux.

L'article 19 du *Pacte international relatif aux droits civiques et politiques de l'Organisation des Nations-Unies* dispose que l'exercice de la liberté d'expression, qui comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix ne peut être soumis qu'à des restrictions qui doivent être expressément fixées par la loi et qui sont nécessaires au respect des droits ou de la réputation d'autrui ou à la sauvegarde de la sécurité nationale, de l'ordre public, de la santé ou de la moralité publiques.

Dans *la Recommandation 2008/2160(INI), adoptée par le Parlement européen le 26 mars 2009*, il est expressément dit que les Etats doivent participer aux efforts visant à l'établissement d'une démocratie informatique à travers un accès à Internet sans réserve et sûr. Le Parlement recommande notamment aux Etats membres de condamner la censure, imposée par le gouvernement, du contenu qui peut être recherché sur les sites Internet, et il les invite *"à garantir que la liberté d'expression ne soit pas soumise à des restrictions arbitraires provenant de la sphère publique et/ou privée et éviter toute mesure législative ou administrative qui pourrait avoir un effet dissuasif sur tous les aspects de la liberté d'expression".*

Le 4 avril 2012, le Comité des Ministres du Conseil de l'Europe a adopté *la recommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche*, qui souligne l'importance de cette liberté publique s'agissant des moteurs de recherche, lesquels *"permettent au public du monde entier de rechercher, de recevoir et de communiquer des informations, des idées et d'autres contenus, en particulier, d'avoir accès au savoir, de prendre part à des débats et de participer aux processus démocratiques."*

La même idée générale est énoncée, en droit interne, par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, ainsi libellé : *"la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme: tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi".*

C'est cette même liberté qui fait l'objet d'une jurisprudence protectrice du Conseil constitutionnel à raison du rôle fondamental qu'elle tient dans la vie démocratique, et tout particulièrement en ce qui concerne Internet.

□La liberté d'accès à internet, partie intégrante de la liberté d'expression

Dans la décision rendue le 10 juin 2009 à propos de la loi favorisant la diffusion et la protection de la création numérique sur internet [68], le Conseil constitutionnel affirme que l'accès à Internet entre dans le champ du droit constitutionnel de s'exprimer et de communiquer librement, ce qui assure la protection constitutionnelle de la liberté de communication et d'expression tant dans sa dimension *"passive"*, le citoyen étant récepteur d'information [69], que dans sa dimension *"active"* d'exercice dans laquelle le citoyen est émetteur d'information : le droit de *"parler, écrire, imprimer librement"* énoncé à l'article 11 de la Déclaration des droits de l'homme et du citoyen se réalise dans la transmission du courrier électronique, le Web 2.0, les blogs…

Le Conseil juge que cela implique *"la liberté d'accéder à internet"* en raison *de "l'état actuel des moyens de communication" et "eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation de la vie démocratique et l'expression des idées et des opinions".*
Cependant la reconnaissance de la liberté d'accéder à internet ne revient pas à garantir à chacun un droit de caractère général et absolu d'y être connecté, mais consiste à affirmer qu' *"en l'état"*, les atteintes à la liberté d'accéder à Internet s'analysent, au regard de la Constitution, comme des atteintes à la liberté garantie par l'article 11 de la Déclaration de 1789. Cela n'exonère pas toutefois le titulaire de l'abonnement d'exercer une obligation de surveillance sur l'usage de son accès à Internet.

Cela induit, s'agissant d'Internet, une **affirmation claire des fondements de l'action de l'Etat et de ses limites, comme du régime de responsabilité des prestataires.**

□L'obligation de surveillance du titulaire de l'abonnement d'un accès à un service de communication du public en ligne

Le Conseil constitutionnel a considéré que le législateur n'a méconnu ni la compétence qu'il tient de l'article 34 de la Constitution, ni l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, en instituant une obligation de surveillance de l'accès à Internet à la charge du titulaire de l'abonnement énoncée par le premier alinéa de l'article L. 336-3 du code de la propriété intellectuelle ainsi rédigé : *"La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'oeuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise".*
Le non-respect de l'obligation de surveillance du titulaire de l'accès ne peut cependant être sanctionné pénalement que sous certaines conditions.

[68] décision n° 2009-580 du 10 juin 2009 relative à la loi favorisant la diffusion et la protection de la création sur Internet

[69] décision n° 2009-577 DC du 3 mars 2009

□ La limitation de l'accès d'un titulaire d'abonnement à internet : une sanction réservée à l'autorité judiciaire

En considération de la primauté de la liberté d'expression, il ne peut être confié à une autorité administrative le pouvoir de restreindre ou d'empêcher l'accès au service Internet.
Sans remettre pour autant en cause le principe même des sanctions administratives [70], le Conseil constitutionnel a déclaré non conformes à la Constitution les dispositions qui, dans le but de protéger les titulaires du droit d'auteur et des droits voisins de la contrefaçon, confiaient à la commission de protection des droits de l'HADOPI la faculté, après avoir mis en oeuvre une procédure d'avertissement, de prononcer à l'encontre du titulaire de l'abonnement une sanction administrative, consistant en une suspension de l'accès au service Internet.
Une autorité administrative, même indépendante et soumise dans son activité répressive aux exigences de l'article 6, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ne saurait restreindre la liberté d'expression ; or, la limitation de l'accès à Internet de toute personne depuis son domicile entrave *"la liberté d'expression et de communication"* qui *"est d'autant plus précieuse que son exercice est une condition de la démocratie"* [71].

Tirant les leçons de cette décision, la loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet a confié ce pouvoir de sanction à l'autorité judiciaire.

A l'occasion de l'examen de cette dernière loi, le Conseil a estimé [72] que la peine complémentaire prononcée par le juge pour réprimer les contrefaçons commises au moyen d'un service de communication en ligne, et consistant dans la suspension de l'accès à Internet pour une durée maximale d'un an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur, ne méconnaissait pas le principe de nécessité des peines. Rien ne s'oppose non plus à ce que des contraventions soient assorties d'une peine complémentaire de même nature, pour une durée de un mois, en cas de *"négligence caractérisée"* du titulaire d'un accès à Internet, dès lors que le pouvoir réglementaire définit précisément les éléments constitutifs de l'infraction.

Dans sa première décision, le Conseil avait déjà considéré [73] que le législateur ne méconnaissait pas la liberté d'expression et de communication en autorisant le tribunal de grande instance à ordonner, à l'issue d'une procédure contradictoire, les mesures nécessaires pour prévenir ou faire cesser une atteinte aux droits d'auteur ou aux droits voisins, le juge ne devant prononcer que les mesures strictement nécessaires à la préservation des droits en cause.

---

[70] Depuis sa décision relative aux pouvoirs de la Commission des opérations de bourse, le Conseil juge que : «*Le principe de la séparation des pouvoirs, non plus qu'aucun principe ou règle de valeur constitutionnelle ne fait obstacle à ce qu'une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dès lors, d'une part, que la sanction susceptible d'être infligée est exclusive de toute privation de liberté et, d'autre part, que l'exercice du pouvoir de sanction est assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis".* Dans le même sens, cf. décision n° 89-260 DC du 28 juillet 1989, cons. 6 ; n° 97-389 DC du 22 avril 1997, cons 3 ; n° 2000-433 DC du 27 juillet 2000, cons. 50.

[71] décision n° 2008-580 DC du 10 juin 2009

[72] décision 2009-590 DC du 22 octobre 2009

[73] décision n° 2009-580 DC du 10 juin 2009, cons. 38

Cependant, le Conseil n'a pas jugé contraire à la Constitution la faculté donnée par le législateur à l'autorité administrative de prendre la décision de "bloquer" un site dans le cadre de la lutte contre la pédopornographie.

□ le blocage d'un site

La Cour Européenne des droits de l'homme a jugé qu'une mesure judiciaire préventive de blocage d'un site Internet qui a eu pour effet collatéral de bloquer l'accès à tous les sites qui y étaient hébergés, constitue une violation de l'article 10 de la Convention.

L'affaire concernait la décision d'un tribunal Turc de bloquer l'accès à *"Google Sites"* au motif qu'il hébergeait un site Internet dont le propriétaire était poursuivi pour outrages à Ataturk. La mesure de blocage avait eu pour effet de verrouiller l'accès à tous les autres sites hébergés par *"Google Sites".* Ainsi, la Cour européenne a rappelé qu'une restriction d'accès à une source d'information n'est compatible avec la Convention qu'à la condition de s'inscrire dans un cadre légal strict délimitant l'interdiction et offrant la garantie d'un contrôle juridictionnel contre d'éventuels abus. Elle a jugé qu'un tribunal qui décide de bloquer totalement l'accès à *"Google sites"* en se référant seulement à l'avis d'un organe administratif, sans rechercher si une mesure moins lourde aurait pu être prise pour bloquer spécifiquement un site particulier, viole la liberté d'expression en rendant d'autres sites inaccessibles et en privant les internautes de nombreuses informations [74].

En revanche le Conseil constitutionnel [75] a, pour sa part, estimé que le dispositif législatif créé par la loi d'orientation et de programmation pour la performance de la sécurité intérieure, qui permet à l'autorité administrative de bloquer un site Internet diffusant des images pornographiques représentant des mineurs n'est pas contraire aux exigences constitutionnelles. Le Conseil a pris en considération le caractère limité de la restriction aux seuls services de communication au public diffusant des images de pornographie représentant des mineurs, et le fait que la décision de blocage de l'autorité administrative est susceptible d'être contestée, à tout moment, devant la juridiction compétente, le cas échéant par voie de référé.

Le commentaire de cette décision aux *Cahiers du Conseil constitutionnel* expose que, par rapport au dispositif de sanction de la loi HADOPI évoqué ci-dessus, il y a une triple différence : *"premièrement, il s'agit de protéger les utilisateurs d'Internet eux-mêmes ; deuxièmement, il s'agit de lutter contre l'exploitation sexuelle des mineurs, ce qui peut justifier des mesures que la préservation de la propriété intellectuelle ne peut fonder ; troisièmement, comme le rapporteur au Sénat le rappelait, 'la disposition proposée présente une portée beaucoup plus restreinte puisqu'elle tend, non à interdire l'accès à Internet, mais à empêcher l'accès à un site déterminé en raison de son caractère illicite".*

□ La responsabilité pénale personnelle du titulaire de l'abonnement

L'article 9 de la Déclaration de 1789 proclame le principe de la présomption d'innocence, dont il résulte que la loi ne saurait, en principe, instituer une présomption de culpabilité en matière répressive [76].

---

[74] décision Ahmet Yildirim c. Turquie 18 décembre 2012 req n° 3111/10 § 57/70

[75] décision n° 2011-625 DC du 10 mars 2011 *(cons 5)*

[76] Le Conseil a exceptionnellement admis une présomption de responsabilité du propriétaire du véhicule automobile en matière de contraventions routières, mais sous la triple condition *"que la présomption d'imputabilité ne revête pas de caractère irréfragable et que la preuve contraire puisse être rapportée à tout*

Le Conseil a ainsi censuré les dispositions de la loi favorisant la diffusion et la protection de la création d'Internet dont il résultait que seul le titulaire du contrat d'abonnement à Internet pouvait faire l'objet des sanctions instituées par la loi. Pour s'exonérer, le titulaire de l'abonnement devait produire des éléments de nature à établir que l'atteinte portée au droit d'auteur procédait de la fraude d'un tiers. Le Conseil a censuré ce dispositif au motif qu'il opérait un renversement des charges de la preuve et créait une présomption de culpabilité à l'encontre du titulaire de l'accès pouvant conduire à prononcer contre lui des sanctions privatives ou restrictives de droit, en méconnaissance des exigences de l'article 9 précité.

□ La responsabilité pénale de l'hébergeur :

Le principe de responsabilité personnelle fonde également la réserve d'interprétation de l'article 6 de la loi pour la confiance dans l'économie numérique qui énonce que les personnes visées au 2 *(les hébergeurs)* ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire, si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dés le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible..... Le Conseil énonce [77] que ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information notifiée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge.

□ La responsabilité pénale des animateurs de blogs :

A l'occasion d'une question prioritaire de constitutionnalité, le Conseil constitutionnel a été saisi du régime de la responsabilité pénale d'un animateur de blog. Il a considéré [78] que les dispositions de l'article 93-3 de la loi du 29 juillet 1982 ne sauraient, sans instaurer une présomption irréfragable de responsabilité pénale en méconnaissance de l'article 9 de la Déclaration de 1789, être interprétées comme permettant que le créateur ou l'animateur d'un site de communication au public en ligne mettant à la disposition du public des messages adressés par des internautes, voit sa responsabilité pénale engagée en qualité de producteur à raison du seul contenu d'un message dont il n'avait pas connaissance avant la mise en ligne.

Le Conseil a tenu compte d'une part, du régime de responsabilité spécifique dont bénéficie le directeur de la publication qui ne peut pas voir sa responsabilité pénale engagée *"s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message"* [79] et, d'autre part, des caractéristiques d'Internet qui, en l'état

---

moment, que soit assuré le respect des droits de la défense et que les faits induisent raisonnablement la vraisemblance de l'imputabilité."

[77] décision n° 2004-496 DC du 10 juin 2004 *(cons. 9)*

[78] décision 2011-164 QPC du 16 septembre 2011

[79] L'article 93-3 de la loi du 29 juillet 1982 énonce que *"lorsque l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contributions personnelles identifié comme tel, le directeur ou le codirecteur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message".*

des règles et des techniques, permettent à l'auteur d'un message ainsi diffusé de préserver son anonymat.

Réformant sa jurisprudence antérieure qui tenait le producteur d'un blog responsable des messages affichés pour en avoir permis ou facilité la diffusion, la Chambre criminelle juge désormais, au visa de l'article 93-3 de la loi du 29 juillet 1982 modifiée sur la communication audiovisuelle, qu'il s'évince de ce texte que la responsabilité pénale du producteur d'un site de communication au public en ligne mettant à la disposition du public des messages adressés par des internautes, n'est engagée, à raison du contenu de ces messages, que s'il est établi qu'il en avait connaissance avant leur mise en ligne ou que, dans le cas contraire, il s'est abstenu d'agir promptement pour les retirer dès le moment où il en a eu connaissance [80].

□ le régime de prescription des infractions de presse commises par diffusion sur Internet [81]

1) sur le point de départ du délai de prescription

La loi pour la confiance dans l'économie numérique rend applicable aux services de communication au public en ligne les dispositions pénales et de procédure pénale des chapitres IV et V de la loi du 29 juillet 1881 sur la liberté de la presse. Le législateur avait pensé différencier le régime de prescription des infractions de presse selon qu'elles sont publiées de façon classique ou exclusivement par diffusion par Internet. A cet effet, il souhaitait allonger [82] le délais de prescription des messages publiés exclusivement par voie informatique, au motif qu'une personne mise en cause par la seule voie d'un message électronique n'a pas facilement, ni naturellement connaissance de ce message.

La loi distinguait donc le message mis à disposition du public en ligne qui reproduit à l'identique le contenu d'un message publié sur un support écrit, et le message publié par la seule voie électronique. Dans le premier cas, le délai de prescription restait celui du droit commun de la presse ; dans le deuxième cas, la loi disposait que ce délai courait, non à compter de la première publication, mais à compter du jour où cesse cette mise à disposition du message au public. Le Conseil Constitutionnel [83] a déclaré cette disposition contraire à la Constitution au motif que cette différence de régime en matière de prescription dépassait manifestement ce qui était nécessaire pour prendre en compte la situation propre aux messages disponibles seulement sur un support informatique. En effet, ce régime pouvait avoir pour conséquence, en cas de maintien du message sur Internet, de fixer le point de départ du délai de prescription plusieurs années après la première publication.

---

[80] CRIM n° 11-80.010 du 31.01.2012 ; CRIM n° 10-88.825 du 30.10.2012

[81] Conseil Constitutionnel décision DC du 10 juin 2004 relative à la loi pour la confiance dans l'économie numérique *(Petites affiches 18 juin 2004 n° 122 p 10 Jean Eric SCHOTTL ; S.J, E.G. 14 juillet 2004 II 10116 ,Jean Claud ZARKA et 10117 Philippe BLANCHETIER)*

[82] La Cour de cassation juge que *"lorsque des poursuites pour l'une des infractions prévues par la loi sont engagées à raison d'une diffusion, sur le réseau Internet ,d'un message figurant sur un site, le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi du 29 juillet 1881 doit être fixé à la date du premier acte de publication qui est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs" (Cass crim 16 octobre 2001 Bull Crim n°211).*

[83] décision 2004-496 DC du 10 juin 2004

Cependant, c'est uniquement la disproportion entre les deux régimes de prescription qui est sanctionnée par le Conseil [84]. Ce dernier rappelle que le principe d'égalité ne fait pas obstacle à ce qu'à des situations différentes soient appliquées des règles différentes dès lors que cette différence de traitement est en rapport direct avec la finalité de la loi qui l'établit, et il considère que, par elle même, la prise en compte de différences dans les conditions d'accessibilité d'un message dans le temps selon qu'il est publié sur un support papier ou qu'il est disponible sur un support informatique n'est pas contraire au principe d'égalité.

2) sur l'allongement de la durée du délai de prescription de certaines infractions

Alors que l'article 65 de la loi du 29 juillet 1881 fixe le délai de prescription de l'action publique et de l'action civile à trois mois pour les infractions prévues par cette loi, l'article 65-3 prévoit que ce délai est porté à un an pour certains délits qu'il désigne à savoir : le délit de provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, les délits de diffamation et d'injure publiques commis aux mêmes fins, et le délit de contestation des crimes contre l'humanité. Les règles de la prescription applicables à ces délits ne se distinguent des règles applicables aux autres infractions prévues et réprimées par la loi du 29 juillet 1881 que par la durée de ce délai de prescription.

Saisi d'une question prioritaire de constitutionnalité, le Conseil [85] a considéré que la différence de traitement, qui résulte de la nature des infractions poursuivies, ne revêt pas un caractère disproportionné au regard de l'objectif poursuivi, qui est de faciliter les poursuites de ces infractions à caractère ethnique, national, racial, ou religieux ou contestant l'existence d'un crime contre l'humanité.

Les lois n° 2004-204 du 9.03.2004, n° 2012-1432 du 21.12.2012 et n° 2014-56 du 27.01.2014 ont ainsi, successivement, porté à 1 an les délais de prescription aux délits de provocation à la discrimination, de diffamations et injures publiques commis à raison de l'origine ou de la religion ; puis aux délits de provocation directe aux actes de terrorisme ou à leur apologie ; enfin aux délits de provocation à la discrimination, diffamation et injures publiques commis en raison du sexe, de l'orientation, de l'identité sexuelle ou du handicap.

---

[84] le commentaire aux *cahiers du Conseil* expose que ce régime aurait abouti à ce qu'un message exclusivement accessible en ligne, exposé pendant cinq ans, ne serait prescrit qu'au bout de cinq ans et trois mois, alors que le message écrit n'aurait été exposé que pendant un délai de trois mois.

[85] Décision n° 2013-302 QPC du 12 avril 2013

3.- les principes régissant les moyens d'enquête ou d'instruction

Le rapport explicatif de la Convention de Budapest exposait déjà, il y a plus d'une décennie, dans sa partie *"droits de procédure",* que la croissance ininterrompue des réseaux de communications ouvrait de nouvelles perspectives à la criminalité, qu'il s'agisse des infractions classiques ou de la nouvelle criminalité technologique ; il énonçait que le droit pénal et les techniques d'enquête ne devaient pas se laisser distancer. Il rappelait que l'un des problèmes les plus difficiles que pose la lutte contre la criminalité dans l'univers des réseaux est la difficulté d'identifier l'auteur d'une infraction et l'impact de celle-ci ; qu'un autre problème est lié à la volatilité des données électroniques qui peuvent être modifiées, déplacées ou effacées en quelques secondes. Il en concluait que le succès d'une enquête requiert rapidité et, parfois, le secret.

La Convention était ainsi présentée comme ayant pour objet de doter les pays de moyens de procédure qui permettent de recueillir efficacement les preuves des infractions pénales commises contre les systèmes informatiques ou au moyen d'un système informatique, et aussi de collecter les preuves informatiques pour toute infraction. Pour nécessaires qu'ils soient, les nouveaux moyens de procédure n'en doivent pas moins respecter les libertés fondamentales, et donc, pour la France, les principes de la Convention européenne de sauvegarde des droits de l'homme : les pouvoirs et moyens de procédure créés par le législateur et utilisés par les organes de poursuite doivent être ainsi, non seulement nécessaires mais encore proportionnels à la nature et aux circonstances de l'infraction.

La jurisprudence de la Cour Européenne des Droits de l'Homme illustre cette double exigence.

Ainsi en sa décision UZUN contre Allemagne [86], à propos de la surveillance d'une personne par le biais de son G.P.S. et l'utilisation de données recueillies par ce moyen, la Cour a-t-elle constaté que cette *"mesure de surveillance secrète"* traduit une ingérence dans l'exercice de la vie privée. Elle énonce, en conséquence, que la loi qui prévoit ce moyen de procédure doit être particulièrement précise pour indiquer à tous, de manière suffisante, en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à une telle mesure. Et la Cour indique aussi que, **pour apprécier si les mesures de cette nature bénéficient des garanties adéquates et suffisantes, il faut se référer à l'étendue et à la durée de ces mesures, aux conditions requises pour les ordonner, à la désignation des autorités compétentes pour les permettre, les mettre à exécution, et les contrôler, et au type de recours fourni par le droit interne**.

En l'espèce, pour dire qu'il n'y avait pas eu d'atteinte aux règles du procès équitable, la Cour européenne a tenu compte, principalement, de ce que l'emploi de cette méthode spéciale de surveillance était subordonnée à la nature particulièrement grave de l'infraction et au caractère subsidiaire de son utilisation lorsque d'autres méthodes ne pouvaient être utilisées, et elle a estimé que le contrôle qu'un juge pouvait exercer, a posteriori, sur le bien-fondé d'une mesure ordonnée par le parquet constituait une garantie importante.
Durant la procédure, une loi nouvelle est entrée en vigueur en Allemagne qui subordonne *"la surveillance systématique"* d'un suspect à l'autorisation d'un juge lorsqu'elle dépasse la durée d'un mois, ce que la Cour européenne a salué.

[86] CEDH Uzun c. Allemagne du 2.09.2010

De manière générale, et concernant tant le droit à la vie privée que celui de la liberté d'expression, cette même Cour a énoncé, à plusieurs occasions, que si l'Etat a pour obligation de respecter ces droits, il a aussi le devoir de protéger les utilisateurs d'Internet et, par-delà, la société toute entière, contre les atteintes de même nature utilisant ce système de communication ainsi que contre toutes activités ou contenus illicites.

Ainsi, après avoir souligné que, si l'art.8 de la Convention européenne de sauvegarde des droits de l'homme avait essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, **la Cour a souligné qu'il résulte aussi de ce texte des obligations positives pour l'Etat inhérentes au respect effectif de la vie privée et familiale, ce qui peut impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations entre les individus entre eux, sous peine**, en cas d'absence ou d'insuffisance, de condamnation sur le fondement de ce même article *(AIREY c. IRLANDE, 9.10.1979 ; X et Y x. PAYS-BAS, 26.03.1985; AUGUST c. ROYAUME-UNI, 21.01.2003 ; M.C. c. BULGARIE, n° 39272/98 ; K.U. c. FINLANDE, 2.12.2008 ; FERET c. BELGIQUE, 16.07.2009...).*

De la même façon mais au titre de l'art.10 al.2, l'effet amplificateur d'Internet a conduit la Cour à souligner que l'Etat est légitime à prendre des mesures restrictives au droit de diffuser des informations, mais cela de manière proportionnée eu égard aux intérêts concurrents ; qu'il avait même obligation de lutter contre les activités criminelles ou illégales sur Internet, y compris dans la sphère des relations des individus entre eux.

Sur ce dernier point, elle a estimé que les droits des mineurs, des jeunes et des personnes vulnérables *(cf., notamment, K.U. c. FINLANDE précité)* étaient à protéger en toutes circonstances et que **les discours incompatibles avec les valeurs proclamées et garanties par la Convention** - comme l'appel à la discrimination ou à la haine *(GUNDUNZ c. TURQUIE, 4.12.2003)*, les discours racistes et xénophobes *(FERET c. BELGIQUE précité : la Cour rappelle qu'il importe, au plus haut point, pour les Etats de lutter contre la discrimination raciale sous toutes ses formes et manifestations)*, l'intolérance religieuse, qu'elle prenne la forme de l'antisémitisme ou de l'islamophobie *(JERSILS c. DANEMARK, 23.09.1994 ; GARAUDY c. FRANCE, 65831/01, NORWOOD c. ROYAUME-UNI, 15.11.2004 ; GUNDUNZ précité*), l'apologie de la violence *(SUREK c. TURQUIE, 26682/95)* ou du terrorisme *(LEROY c. France, 2.10.2008)*, la contestation des crimes contre l'humanité , le révisionnisme et la négation de l'holocauste *(GARAUDY précité)*, et, en général, tout acte incompatible avec la démocratie et les droits de l'homme - **ne relevaient pas de la liberté d'expression et ne pouvaient prétendre bénéficier des garanties qu'elle comprend**.

Le Conseil constitutionnel applique aussi le principe de proportionnalité pour apprécier la conformité aux libertés fondamentales des règles spéciales de procédure intéressant l'enquête.

En cette matière, le Conseil se réfère principalement aux principes suivants, qui sont énoncés, par exemple, au considérant 3 de la décision 2004-492 DC du 2 mars 2004 concernant la loi portant adaptation de la justice aux évolutions de la criminalité. :

> - l'article 6 de la Déclaration des droits de l'homme et du citoyen de 1789: *"La loi est l'expression de la volonté générale... Elle doit être la même pour tous, soit qu'elle protège, soit qu'elle punisse... " ;*

- l'article 7 : *"Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la loi, et selon les formes qu'elle a prescrites... "* ;
- l'article 8 : *"La loi ne doit établir que des peines strictement et évidemment nécessaires... "* ;
- l'article 9 : *"Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi " ;*
- l'article 16 : *"Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution "* ;
- enfin, l'article 66 de la Constitution : *"Nul ne peut être arbitrairement détenu. - L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi " ;*

Le commentaire de la décision précitée [87] rappelle les principes qui régissent l'examen de constitutionnalité des moyens de procédure : Il est de jurisprudence constante qu'il incombe au législateur d'assurer la conciliation entre, d'une part, l'exercice des libertés constitutionnellement garanties, et d'autre part les besoins de la recherche des auteurs d'infractions, qui sont l'un et l'autre nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle. Et il incombe à l'autorité judiciaire d'exercer un contrôle effectif sur le respect des conditions de fond et de forme par lesquelles le législateur a entendu assurer cette conciliation[88].

En ce qui concerne les actes d'enquête et d'instruction qui peuvent affecter des droits constitutionnellement protégés *(liberté individuelle, inviolabilité du domicile et des correspondances, secret de la vie privée),* le Conseil applique le même principe de proportionnalité que celui qui régit la peine elle même. Le degré auquel ces actes affectent la liberté individuelle que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire doit être justifié par la gravité et la complexité de l'infraction suspectée. La rigueur non nécessaire est proscrite non seulement lors de la condamnation ou de l'arrestation mais au cours de toute la procédure judiciaire préalable.[89] Le Conseil a étendu les prescriptions de l'article 9 de la Déclaration de 1789, relatives à la présomption d'innocence, aux actes d'enquête et d'instruction.

Dans la décision n° 2004-492 DC du 2 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, le Conseil énonce ainsi au considérant 6 "*que, si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire, gardienne de la liberté individuelle, et que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées ; qu'il appartient à l'autorité judiciaire de veiller au respect de ces principes, rappelés à l'article préliminaire du code de procédure pénale, dans l'application des règles de procédure pénale spéciales instituées par la loi*".

C'est sur la base de ces critères que, dans la décision précitée, le Conseil a apprécie la conformité à la Constitution de nombreuses règles de procédure spéciales énoncées par la loi pour la recherche d'auteurs d'infractions graves ou complexes :

---

[87] n°16 des cahiers du Conseil Constitutionnel

[88] entre autres exemples, décision 93-223 DC du 5 août 1993, cons 5

[89] C.C. n° 2003 DC du 13 mars 2003, cons 54 ; décision n° 2004-492 DC du 2 mars 2004

- prolongation du délai de garde à vue *(cons.21 ; et décision n° 93-326 DC du 11 août 1993 cons. 6)*; pour les mineurs sous réserve de leurs règles protectrices *(cons. 37)* ;
- perquisitions, visites domiciliaires et saisies en dehors des heures légales en enquête de flagrance ou dans le cadre de l'instruction *(cons.46, 53)* ;
- perquisitions, visites domiciliaires et saisies sans consentement en enquête préliminaire *(cons. 48)* ;
- interceptions de correspondances par voie de télécommunication *(cons. 58)* ;
- sonorisations et fixations d'images de certains lieux ou véhicules *(cons. 64)* ;
- surveillance électronique des véhicules *(décision n°2005-532 DC du 19 janvier 2006 cons. 2)*

Par une motivation similaire, le Conseil constitutionnel, dans la décision 2013-679 DC du 4 décembre 2013, portant sur la loi relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière, a validé l'extension à la poursuite de délits de corruption, de trafic d'influence, de fraude fiscale aggravée ou de délits douaniers d'une certaine importance, de certains pouvoirs d'investigation et de surveillance spéciaux, tels l'infiltration, l'interception de correspondances ou encore la captation de paroles ou d'images.

Ainsi, lorsqu'il est envisagé de créer ou d'étendre des règles spéciales d'enquête, il convient de vérifier que les infractions concernées par ces actes présentent bien toutes les caractéristiques justifiant des procédures dérogatoires. **Il s'agit essentiellement de la gravité de ces infractions pour la société ainsi que de leur complexité**. Et le commentaire précité d'ajouter que l'un **ou** l'autre critère peut appeler la mise en oeuvre des moyens spéciaux d'enquête ou d'instruction. Il y est indiqué que la délinquance organisée remplit la condition de complexité en ce que ces infractions sont commises *"par des groupements ou réseaux dont le repérage, l'analyse et le démantèlement posent des problèmes complexes."*

Dans le domaine de la cybercriminalité, il semble que le critère de complexité doit être considéré comme rempli du fait des difficultés d'identification des auteurs tenant à l'anonymisation des internautes, au caractère volatile des informations sur internet et à la dispersion des acteurs dans l'espace.

C'est sur ce fondement de complexité, peut-être plus que sur le critère de gravité des infractions, que pourraient être proposées des procédures spéciales d'investigation sur Internet, sous réserve cependant de satisfaire aux critères de proportionnalité par rapport à l'objectif poursuivi, et de subsidiarité au regard des autres moyens de procédure pouvant être mis en oeuvre, et en plaçant l'usage de ces moyens, selon leur degré d'immixtion dans la vie privée et la liberté d'expression, sous le contrôle du magistrat du parquet ou du juge.

Dans la mesure où de tels moyens juridiques d'investigation et de preuve répondent à ces conditions, ils contribuent, eux aussi, à la liberté de la vie privée, de la communication et des échanges.

C'est ce qu'énonçait déjà, en droit interne, l'art. 1-IV précité de la loi de 2004 sur l'Economie numérique, en précisant, après avoir posé le principe de la liberté de communication au public par voie électronique, que

"L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui,

du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication, ainsi que par la nécessité, pour les services audiovisuels, de développer la production audiovisuelle."

La cybercriminalité : de la nécessité d'une stratégie globale

Si la France a su se doter de normes qui font autorité, si elle possède, il est vrai en trop petit nombre, des spécialistes de talent dans les administrations publiques, les autorités indépendantes et les milieux universitaires, il est temps aujourd'hui qu'elle se dote d'une stratégie globale comme le recommande l'Union européenne et comme y travaillent déjà plusieurs autres Etats.

Cette stratégie commande en premier lieu de mieux identifier la lutte contre la cybercriminalité par rapport aux concepts souvent évoqués de cybersécurité et de cyberdéfense, tout en mettant en exergue des interdépendances encore trop négligées (1).

Elle passe, d'abord et avant tout, par la prévention, l'internaute devant être l'acteur principal de la réponse à la cybercriminalité, non seulement parce que de sa sensibilisation dépendra, pour l'essentiel, la capacité de mettre en échec les menées délinquantielles, mais aussi pour des raisons tenant aux libertés fondamentales (2).

Au-delà des questions de spécialisation, la formation des acteurs constitue une deuxième exigence, car la cybercriminalité n'est pas tout à fait une délinquance comme une autre, compte-tenu de son aspect technique et de son caractère évolutif (3).

C'est cette même spécificité qui commande de développer le partenariat public-privé car, en ce domaine, l'Etat ne peut agir seul (4).

Mais la stratégie globale passe aussi par la réorganisation des services de l'Etat, afin de rendre l'action de ce dernier plus efficiente et plus cohérente (5).

Elle doit enfin s'accompagner des moyens nécessaires, notamment en ressources humaines, pour les services spécialisés (6).

II.1.- Un préalable : Sécurité des systèmes d'information, Cyberdéfense, Lutte contre la Cybercriminalité, des objectifs différents mais interdépendants

Le *livre blanc sur la sécurité et la défense nationale*, publié le 17 juin 2008, a mis en évidence le fait que le concept de défense ne pouvait plus se concevoir aujourd'hui comme la réponse à une agression classique, mais devait aussi englober d'autres formes de menaces d'importance majeure, qui appellent une approche globale et au rang desquelles il identifiait le risque d'une attaque informatique contre les infrastructures nationales, eu égard à leur dépendance de plus en plus forte à l'égard ses réseaux de communication.
Sur la base d'un tel constat, il distinguait la sécurité nationale comme devant fédérer, au plan interministériel, l'ensemble des politiques publiques destinées à répondre à ces menaces [90], et la défense du territoire et des populations qui devaient rester l'apanage du ministère du même nom [91].

A la suite de cette prise de conscience et pour faire face à ce défi désormais identifié, fut créée, en juillet 2009, ***l'Agence nationale de sécurité des systèmes d'information (ANSSI)*** [92] ; deux ans plus tard, cette agence interministérielle, relevant du Premier ministre, se voyait confier aussi une mission de défense de ces mêmes systèmes d'information.

> L'ANSSI a pour principale mission d'assurer la partie technique de la sécurité des systèmes d'information, raison pour laquelle elle est principalement composée d'ingénieurs ; elle ne s'occupe pas de la recherche du renseignement, qui relève de la responsabilité des services spécialisés de l'Etat, ni des investigations de police judiciaire pour lesquelles elle ne dispose d'aucune capacité juridique, renvoyant, à cette fin, à la D.C.R.I. ou à l'O.C.L.C.T.I.C.
>
> Au titre de la sécurité nationale, le rôle de l'ANSSI est d'ordre préventif: elle joue, à cette fin, le rôle d'expert étatique s'agissant de la sécurisation des systèmes d'information auprès des administrations comme des opérateurs sensibles. A ce titre, elle réalise des diagnostics *(sur les moyens de communication sécurisés de l'Etat ou, pour prendre des exemples intéressant le système judiciaire, les bracelets de surveillance électronique, la gestion des clés dans les établissements pénitentiaires, la future plate-forme des interceptions judiciaires...)*, fait des recommandations *(par exemple, sur les badges d'accès, la vidéo-surveillance...)* qui peuvent se traduire par la publication de véritables

---

[90] ce concept de *"sécurité nationale"* devait être introduit, peu après *(2009)*, dans le code de la Défense

[91] cf, notamment, sur l'ensemble de ce chapitre : l'entretien avec M. Patrick PAILLOUX, directeur général de l'ANSSI ; les travaux parlementaires relatifs à la récente loi de la programmation militaire ; les analyses de la DCRI ; et GUINIER (Daniel), *"les pôles cyber essentiels au cyberespace et leurs liens - approche systémique et gouvernance",* in La revue du GRASCO, n° 6, juillet 2013

[92] qui prenait toutefois la suite d'une précédente structure, *la direction centrale de la sécurité des systèmes d'information*, lointaine héritière de l'ancien service du chiffre et de cryptologie

guides à vocation générale [93], et contribue à l'habilitation de certains dispositifs *(par exemple, en matière de cartes bancaires)*. Elle assure aussi une mission d'audit et d'inspection, à la fois au plan organisationnel et s'agissant des risques d'intrusion *(centrales nucléaires, tunnel sous la Manche, application pénale Cassiopée...)*. Elle exerce encore un contrôle sur les investissements étrangers dans le domaine de la sécurité informatique, sur la base des dispositions normatives soumettant à autorisation préalable la fabrication, le commerce et l'importation de certains dispositifs *(par exemple la vente de matériel d'écoute téléphonique).* Elle entretient enfin des relations étroites avec les organismes comparables des pays étrangers.

Au titre de la cyberdéfense et en tant qu'autorité centrale de défense s'agissant des attaques portées contre les systèmes d'informations des établissements et organismes sensibles, elle dispose d'un *Centre opérationnel de la sécurité des systèmes d'information (COSSIL)*, ayant pour vocation à prendre, 24h. sur 24, les mesures d'urgence en cas de crise, centre relayé, au plan régional, par les *Observatoires régionaux de la sécurité des systèmes d'information*, dont les moyens sont toutefois limités. Alertée par les établissements, par des partenaires étrangers ou agissant d'office, l'ANSSI a alors pour tâche d'identifier l'origine de la menace ou de l'attaque et de les pallier techniquement [94].

Outre le *COSSI*, l'ANSSI dispose d'une structure d'expertise et de conseil, d'un laboratoire de développement des systèmes d'informations sécurisés ainsi que d'un centre de formation à la sécurité des systèmes d'information *(CFSSI).*

Afin d'atteindre ces objectifs, il fallait toutefois que l'Etat se dote d'une stratégie: les travaux de l'ANSSI aboutirent, en 2010, à la définition par la France d'une **stratégie nationale de défense et de sécurité des systèmes d'information** [95]**.**

Cette stratégie dite de **cybersécurité** repose sur quatre objectifs **:**

*Etre une puissance mondiale de **cyberdéfense**, afin de protéger les réseaux de communications électroniques notamment contre les risques de cyber-espionnage
*Garantir la liberté de la décision de la France par la protection de "l'information de souveraineté", qu'elle soit d'ordre diplomatique, militaire, scientifique, technologique, commerciale ou financière,
*Renforcer la **cybersécurité** des infrastructures vitales nationales, c'est-à-dire des opérateurs, tant publics que privés, qui concourent à la satisfaction des besoins indispensables à la vie des populations, à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation, et qui ont recours, pour ce faire, aux réseaux de télécommunications et singulièrement à Internet

[93] *"Guide de l'hygiène informatique"* en janvier 2013 ; *"passeport de conseils aux voyageurs se rendant à l'étranger munis de leurs appareils numériques"...*

[94] ce qui est parfois complexe et nécessite de gros moyens : lors de l'attaque sur BERCY, l'opération a nécessité 30 personnes sur deux mois car 150.000 ordinateurs étaient reliés au système d'information attaqué, sans que l'on sache, au début, lesquels se trouvaient ou non infectés ; en outre, la confidentialité est importante, notamment à l'égard du pirate qui peut encore se trouver dans le réseau, mais aussi parfois compte-tenu des exigences de l'entreprise en terme d'image.

[95] Toutefois cette stratégie ne fut rendue publique qu'en février 2011 ; cf. ANSSI, *"Défense et sécurité des systèmes d'information : stratégie de la France"*

*Assurer **la sécurité dans le cyberespace**, par la protection des systèmes d'information et des données des administrations, par l'information et la sensibilisation des entreprises et des particuliers, par enfin le renforcement de la **lutte contre la cybercriminalité** grâce à une meilleure adaptation du droit et une amélioration de l'entraide judiciaire internationale.

A cet effet, sept axes d'efforts sont associés :

- mieux anticiper et analyser l'environnement afin de prendre les décisions adaptées
- détecter les attaques et les contrer, alerter les victimes potentielles et les accompagner
- accroître et pérenniser nos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de conserver l'autonomie nécessaire
- protéger les systèmes d'information de l'Etat et des opérateurs d'infrastructures vitales
- adapter le droit afin de prendre en compte les évolutions technologiques et les nouveaux usages
- développer les collaborations internationales en matière de sécurité des systèmes d'information, **de lutte contre la cybercriminalité** et de **cyberdéfense** pour mieux protéger les systèmes d'information nationaux
- communiquer, informer et convaincre afin de permettre aux Français de prendre la mesure des enjeux liés à la sécurité des systèmes d'information.

A cette stratégie globale, est adossée **une organisation spécifique de l'Etat**, reposant sur le Premier ministre, assisté par le Secrétariat général de la défense et de la sécurité nationale - dont le responsable assure aussi la présidence du Comité stratégique de l'ANSSI -, un Haut fonctionnaire de défense et de sécurité ayant notamment pour mission d'animer un réseau de responsables en charge, dans chaque département ministériel, de la sécurité des systèmes d'information correspondants. En outre, et compte-tenu de son approche globale, elle associe, comme l'ensemble de la sécurité nationale, les autres départements ministériels, en premier lieu la Défense, mais aussi l'Intérieur *(l'ensemble des services de renseignement et au premier chef la Direction centrale du renseignement intérieur...comme les services spécialisés chargés de l'identification des auteurs),* la Justice *(s'agissant de l'évolution du droit)*, les Affaires étrangères, l'Economie numérique, l'Industrie et la recherche...., tout en développant un partenariat avec les opérateurs, publics ou privés, d'infrastructures et de réseaux vitaux pour la Nation.

Le nouveau *Livre blanc* publié le 29 avril 2013, et notamment le rapport sur la **cyberdéfense** [96], fut l'occasion de **mieux préciser la cyber-menace**, placée désormais au 3ème rang des risques, juste derrière la guerre et les attaques terroristes : l'espionnage, le plus souvent d'origine étatique mais émanant parfois d'entreprises concurrentes ; la tentative de déstabilisation à l'occasion d'un conflit international ou d'une décision controversée, qui se traduit soit par le piratage d'un site, soit par un déni de service *(blocage du site)*, soit par un détournement des informations livrées au public essentiellement à des fins de propagande ; ou encore le sabotage dont les cibles, le plus souvent vitales, peuvent être privées ou publiques *(menace qui ne semble pas s'être encore concrétisée s'agissant de la France)* [97].
De ce constat, découlait la nécessité de faire de cette **cyberdéfense** une priorité stratégique nationale, intégrant notamment une capacité de réponse graduée à la cyber-menace. En

[96] cf. *Rapport d'information n° 681 sur la cyberdéfense de M. Jean-Marie BOCKEL, fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat,* et publié le 18.07.2012

[97] cf., pour plus de détails, *le titre I, chapitre 1* et ses développements relatifs aux cyber-menaces (DCRI)

revanche, rien n'était dit d'essentiel sur la cybercriminalité, sauf la référence aux risques engendrés par le terrorisme et par la criminalité organisée dans ses formes les plus graves.

Ces nouvelles ambitions se sont traduites, récemment, dans *la loi n° 2013-1168 relative à la programmation militaire pour les années 2014 à 2019,* qui

- renforce **la cybersécurité**,

*d'abord au plan de l'organisation de l'Etat, car la responsabilité du Premier ministre dans la définition et la coordination de la mise en oeuvre de la politique en matière de défense et de sécurité des systèmes d'information est confirmée ainsi que la qualité de l'ANSSI [98] en tant qu'autorité nationale de défense de ces mêmes systèmes ;

*ensuite en ce qui concerne la sécurité de ces mêmes systèmes pour les quelques 250 *opérateurs d'importance vitale (OIV)* [99] qui se verront imposer des règles de sécurité, avec les audits et contrôles afférents, devront obligatoirement notifier tout incident et, en cas d'attaque informatique grave, suivre les prescriptions techniques de l'ANSSI ;

*aussi en reconnaissant une sorte de droit de *"légitime défense"* en cas de cyber-attaque d'importance, autorisant l'ANSSI à accéder au système d'information qui en est à l'origine, de collecter les données utiles, voire de neutraliser l'agression ;

*encore en instaurant un régime d'autorisation préalable pour la fabrication, la commercialisation, la détention et l'importation des équipements susceptibles de permettre des interceptions afin de mieux lutter contre l'espionnage ;

*enfin en augmentant, sensiblement, les moyens de renseignement s'agissant de la future *direction générale de la sécurité intérieure (actuelle DCRI)*, en hommes et, s'agissant de la prévention administrative du terrorisme, en moyens juridiques *(cf. l'art.20 de la loi, art. L.246-1 nouveau du code de la sécurité intérieure)*, qui autorise expressément les agents spécialement désignés relevant des services spécialisés de l'Etat à accéder aux données d'identité et de connexion détenues par les opérateurs, y compris en temps réel aux fins de géo-localisation, cela sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité

- renforce aussi les moyens de la **cyberdéfense**, tant en terme de ressources humaines [100], comprenant aussi un recours accru à la réserve opérationnelle et à la réserve

---

[98] qui, de simple *"agence"* devient une *"Autorité"*, dotée de nouveaux pouvoirs d'investigation auprès des opérateurs de communications électroniques *(cf. art. 25 de la loi)*, mais aussi de nouveaux moyens : disposant d'une centaine de personnes lors de sa création, l'ANSSI en a 360 actuellement mais devrait voir ses effectifs encore progresser pour atteindre 500 en fin 2015, ce qui la mettrait au niveau des instances comparables des grands pays Européens et lui permettrait de faire face à des attaques simultanées

[99] Il s'agit des opérateurs qui gèrent des établissements, ouvrages ou installations *"dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation" (art. R.1332-1 du code de la défense)* ; leur liste relève du secret confidentiel-défense mais recouvre douze secteurs d'importance vitale, qui comprend, notamment, les activités civiles et militaires de l'Etat, les activités judiciaires, l'espace et la recherche, la gestion de l'eau, l'énergie, la communication et les transports, mais aussi les grandes banques. Leur sécurité a donné lieu, récemment, à une instruction générale interministérielle en date du 7.01.2014

[100] Selon les rapports parlementaires, 350 personnels des armées supplémentaires viendront s'ajouter aux 900 déjà affectés à la cyberdéfense ; en outre, les ressources du renseignement militaire seront accrues. Cf., sur ces questions, le *Pacte Défense Cyber* récemment arrêté par le ministre de la Défense

citoyenne, qu'en ce qui concerne l'organisation *(depuis 2011, le commandement opérationnel de cyberdéfense est déjà assuré par un officier général)* et les investissements en matière de recherche et de développement (programme *"SSI-CYBER")*.

Toutefois, conformément à la stratégie précitée, la cybersécurité revêt aussi d'autres formes, comme les programmes spécifiques destinés à **protéger l'intelligence économique**, ou **le soutien au développement de l'industrie française dans le domaine de la cybersécurité** [101].

Si la **lutte contre la cybercriminalité** n'est pas appréhendée, ou de manière très partielle, voire indirecte, par la **cybersécurité** et la **cyberdéfense**, c'est que celles-ci se focalisent principalement, car c'est leur raison d'être, sur un type de menace *(portant sur les systèmes d'information)*, un niveau de gravité et des intérêts spécifiques à protéger *(les capacités de Défense de l'Etat, les O.I.V.)*, toutes questions qui relèvent, en priorité, d'autres acteurs que ceux quotidiennement concernés par la cybercriminalité.

C'est peut-être aussi car elle n'a pas fait, jusqu'ici, l'objet du même investissement que les priorités précédentes, sans doute car le besoin ne s'en faisait pas sentir et que les interrogations *(cf., par exemple, les questions parlementaires y relatives adressées au Gouvernement)* portaient, le plus souvent, sur des questions sectorielles *(l'usurpation d'identité, la vente de drogue par Internet...)*, mais, vraisemblablement aussi, car elle se prête moins, du fait de son caractère diffus et transversal *(les difficultés à la définir l'illustrent suffisamment),* à une approche globale et à la détermination d'une stratégie cohérente.

Or, même si elle est, à l'heure actuelle, mal quantifiée, l'impact de la **cybercriminalité** ne peut se limiter, malgré toute l'importance qu'il s'y attache, à la cyber-menace définie plus avant ; cet impact, il se manifeste, aussi, par la masse d'infractions qui lui est associée ; par la violation de l'intimité quotidienne déjà décrite ; par le préjudice financier qu'il représente pour les dizaines de milliers de personnes qui se font escroquer ; par l'insécurité comme le coût économique qu'il génère dans des milliers d'entreprise, bien au-delà des OIV. ; par la déstabilisation de ce qui est devenu le principal instrument de paiement bancaire ;

Mais c'est aussi du fait de l'efficacité très relative que revêt aujourd'hui la lutte contre la cybercriminalité qu'il est devenu impératif de définir de nouvelles ambitions et d'améliorer les moyens de son action.

---

[101] cf. les 34 mesures présentées par le Président de la République, le 12.09.2013, au soutien du développement de filières industrielles en France. Si la France dispose déjà d'entreprises performantes dans la cybersécurité *(CASSIDIAN, THALES, ou, dans le domaine des cartes à puce, GEMALTO, OBERTHUR...)*, il s'agit aujourd'hui de combler les carences existantes qui menacent sa souveraineté ; quant à *"l'informatique dans les nuages"*, afin de restreindre les quasi-monopoles des sociétés américaines GOOGLE et AMAZON, la solution ne peut être qu'européenne. Voir, notamment, sur ce dernier point, le rapport d'information déposé, le 20.03.2013, par Mme la sénatrice MORIN-DESAILLY, au nom de la Commission des affaires européennes du Sénat, et intitulé *"L'Union européenne, colonie du monde numérique ?"*.

Toutefois, il est nécessaire qu'une future stratégie dans la lutte contre la cybercriminalité intègre, dès le stade de sa conception, les enjeux définis par la cybersécurité, car les deux questions sont interdépendantes.

Interdépendantes, elles le sont d'abord car la menace, quelle qu'elle soit, renvoie, le plus souvent, à la notion d'infraction et donc au droit pénal : ainsi, l'auteur d'une attaque informatique contre le système de traitement automatisé d'un opérateur d'importance vitale porte atteinte au dispositif de cyberdéfense et de cybersécurité mais commet également une infraction relevant de la lutte contre cybercriminalité. En outre, toute réponse, peu importe sa nature, est bornée par les exigences tenant à la protection des libertés individuelles, dont la Justice est, en définitive, le garant.

Elles le sont aussi car l'efficacité de la lutte contre la cybercriminalité dépendra, pour une bonne part, de la réussite, tant préventive que technique et industrielle *(française ou européenne)*, de la politique de cybersécurité, et que cette dernière a besoin aussi que s'accroisse l'efficacité répressive, notamment dans le domaine des attaques contre les systèmes de traitements automatisés de données ou de l'intelligence économique.

Elles le sont encore, car la lutte contre le cyberterrorisme est au centre de toutes les préoccupations et que le monde du renseignement doit autant prévenir que fournir aux services de police et de justice spécialisés les moyens nécessaires à la répression, ce qu'il fait d'ailleurs. Il en est de même de la lutte contre la criminalité organisée [102].

Elles le sont enfin car toute stratégie face à la cyber-menace passe par une meilleure prise de conscience, l'éducation, la formation et le soutien des internautes comme des acteurs [103] ; le renforcement du partenariat public-privé ; la coopération et un meilleur encadrement de ces interlocuteurs indispensables que sont les opérateurs de communication; une meilleure organisation de l'Etat ; le renforcement tant des moyens juridiques que des ressources humaines ; la coopération internationale enfin, au plan des instruments comme de l'entraide.

Ainsi qu'y invite l'Union européenne, la détermination d'une stratégie dans le domaine de la lutte contre la cybercriminalité est donc une condition pour pouvoir disposer demain d'une approche globale du défi que constitue la cyber et favoriser une action coordonnée de l'ensemble des acteurs concernés.

A cet égard, deux points méritent, tout particulièrement, l'attention, car ils ne seront pas évoqués par la suite.

---

[102] Telle est d'ailleurs la raison pour laquelle l'ANSSI dispose d'un officier chargé de faire le lien entre son action préventive et celle tant de la DCRI que de l'OCLCTIC

[103] L'ANSSI souligne, en permanence, combien la cyber-menace est facilitée par l'insuffisante sensibilisation des décideurs, publics ou privés ; son responsable cite des exemples constatés dans le cadre de sa mission : *le recours à un mot de passe unique, partagé par plus de 200 personnes, pour l'accès à un système d'information sensible ; la pratique individuelle de l'ingénieur qui recharge son Iphone personnel non sécurisé sur un ordinateur sensible, ce qui revient à rendre celui-ci accessible sur Internet...* Il insiste aussi sur le fait que les ingénieurs ne sont aucunement sensibilisés, dans le cadre de leur formation, à ces questions de sécurité.

En France, la stratégie de lutte contre le crime est principalement axée sur l'outil juridique ; c'est normal et les développements qui suivent mettront en exergue toute son importance. Mais, plus que toute autre forme de délinquance, la cybercriminalité revêt des aspects techniques et appelle, pour sa prévention comme en terme de lutte, des innovations du même ordre [104].

Or, force est de constater que police et justice sont insuffisamment dotées des capacités nécessaires en terme de recherche et, encore davantage de développements, ce à quoi le recours au partenariat ou à l'expertise classique ne saurait remédier ; **il faut donc que l'interface entre ces départements et les pôles publics disposant de telles capacités soit, non seulement, précisée, mais aussi institutionnalisée**, en terme de remontée d'informations quant aux nouvelles techniques décelées mais aussi d'expression des besoins et de réponse. Il serait logique, ne serait-ce que pour ne pas démultiplier les structures, que l'ANSSI joue ce rôle.

La politique pénale ou de sécurité est traditionnellement tournée vers la protection de l'Etat et des victimes individuelles ; en revanche, il lui est parfois reprocher de négliger **la délinquance qui frappe l'entreprise**, peut-être par manque de connaissance mais aussi compte-tenu des réticences des entrepreneurs eux-mêmes.

Or, les entreprises, qu'elles soient grandes ou petites, sont, non seulement une cible privilégiée de la cybercriminalité organisée, mais aussi très exposées à des comportements illicites internes, avec des répercussions économiques voire sociales non négligeables ; et leurs attentes, en ce domaine, lorsqu'elles sont confrontées à une attaque, font fi des découpages institutionnels, car elles sont essentiellement globales.

En outre, la plupart de ces entreprises, qui ne sont pas vitales au sens de la sécurité nationale, ne bénéficient pas directement des dispositifs mis en oeuvre à ce titre, même si la DCRI s'y emploie, et n'ont pour solution que de se tourner vers des entreprises de sécurité, nombreuses mais d'un niveau inégal : le développement des entreprises françaises en matière de cybersécurité, le recours à une labellisation étatique des sociétés existantes, voire la création, à l'exemple de l'Allemagne ou de la Grande-Bretagne, de CERT dans les différentes branches professionnelles afin de favoriser les échanges sur les savoir-faire ainsi que l'information sur les risques et la diffusion de pratiques pertinentes, constituent autant de solutions dont l'Etat ne peut se désintéresser, même si les différentes branches professionnelles sont directement concernées.

Il est ainsi nécessaire que la thématique de l'entreprise soit spécifiquement prise en compte, raison supplémentaire pour que **l'interaction entre les différents pôles de l'Etat soit aussi efficiente que possible**, au plan national comme sur le terrain.

▬▬▬▬▬

[104] L'une des forces de la Commission nationale informatique et libertés, par rapport à toutes les autorités comparables en Europe, consiste, précisément, à disposer d'un laboratoire qui lui permet, non seulement de réaliser les diagnostics et les contrôles techniques utiles, mais aussi de discuter, d'égal à égal, avec les entreprises et opérateurs spécialisés.

II.2. - Une priorité : la prévention

La réponse judiciaire, garde-fou indispensable pour éviter qu'Internet ne devienne une zone de non droit, n'est pas la panacée, qu'elle soit civile ou pénale.

Tout un chacun, y compris les acteurs répressifs, en conviennent : Internet suppose, d'abord et avant tout, une éducation, une sensibilisation, une mobilisation qui doivent être l'oeuvre de tous.

Ce constat concerne, tout particulièrement, certaines formes de criminalité, telles les atteintes à la vie privée ou les escroqueries, qui pourraient être endiguées par une sensibilisation plus massive, mieux organisée et surtout généralisée, tant sur le plan de la *cyber-sécurité* qu'au niveau comportemental. En outre, les professionnels de l'Internet disposent des outils qui permettent d'agir au cœur du réseau, pour limiter la portée des infractions et les modes de commission des infractions.

La polysémie de la *prévention* doit être posée d'emblée pour en distinguer deux facettes : prévenir les internautes des dangers qu'ils encourent ; prévenir la commission des infractions. Mais ces actions complémentaires ne sauraient être dissociées, reposant sur les mêmes acteurs à même de cerner les risques encourus et disposant des moyens techniques d'agir au coeur du réseau pour prévenir la commission des infractions ou en limiter la portée : les opérateurs et fournisseurs de services en ligne. Il appartient aux pouvoirs publics de les engager dans de nouvelles politiques d'action.

1.- <u>Prévenir les internautes</u>

Prévenir, c'est informer les internautes des risques qu'ils encourent sur Internet et des moyens de s'en prémunir. Comme toute nouvelle technique, Internet suppose une sensibilisation, voire une éducation contre ses dangers, qu'il s'agisse du grand public - car tout un chacun, quelque son niveau d'instruction et d'éducation peut être victime de cyber-infractions, de publics ciblés - en priorité, jeunes et personnes d'un certain âge moins coutumières de ce mode de communication - ou des professionnels plus exposés.

Informer les internautes, c'est d'abord les protéger contre eux-mêmes.

L'internaute n'est pas seulement la victime d'infractions, il en est également souvent **le facilitateur involontaire**, notamment lorsqu'il livre aux réseaux sociaux des données extrêmement personnelles sans être conscient qu'elles pourront, un jour, se retourner contre lui, et l'on sait que ce risque concerne, tout particulièrement, les mineurs.
C'est aussi le cas lorsque, de manière imprudente, l'internaute ouvre un courriel inconnu susceptible d'introduire un virus dans son ordinateur, ou livre ses données bancaires à la moindre injonction présentée comme émanant d'un site officiel.
C'est toujours le cas lorsque l'entreprise ou l'un de ses salariés rendent accessibles des données susceptibles de nuire à leur confidentialité, faute d'étanchéité suffisante entre l'information et le contrôle, voire entre la vie privée et la vie économique.
C'est encore le cas lorsque des chercheurs échangent, via Internet, sur l'état d'avancement de leurs travaux scientifiques ou technologiques.

C'est toujours le cas lorsque l'internaute choisit, pour protéger ses données personnelles ou accéder à certains comptes, un mot de passe *"basique" (123456 par exemple ou sa date de naissance),* le premier que tentera de faire un cyber-délinquant, ou utilise le même mot de passe pour toutes ses applications.
C'est le cas enfin, mais la liste n'est pas close, lorsque tel fonctionnaire, tel avocat, tel magistrat se déclare, quelque peu naïvement, "ami" de tel autre, sans avoir conscience du risque ainsi porté à l'impartialité ou à la neutralité attendue...

Il faut, en résumé, **faire de chaque internaute le premier responsable de sa propre sécurité**.

Outre les campagnes de sensibilisation, la prévention suppose aussi **le développement d'espaces d'information en ligne ou par téléphone,** à l'exemple de INFO ESCROQUERIES ou de ce qui existe en matière de vente à distance ; ces espaces sont complémentaires des campagnes de sensibilisation en ce qu'ils permettent, dans la durée, de délivrer au public une information dynamique, de le conseiller de manière personnalisée et de l'orienter au sein de la multiplicité des acteurs publics et privés à même de répondre à ses attentes. Encore faut-il veiller à la cohérence des dispositifs, à ce que le champ des principales infractions commises par Internet soit effectivement couvert ; en outre, le succès de ces espaces dépend de son accessibilité, qui doit reposer sur une publicité appropriée et des ressources humaines adaptées à l'enjeu.

Les actions en matière de prévention sont légion, qu'elles soient le fait d'administrations, d'organismes professionnels ou d'associations, et, le plus souvent, d'actions menées en partenariat. Elles ne sauraient être minorées : rien qu'au niveau de l'Etat, *la Délégation aux usages de l'Internet*, le ministère de l'Intérieur, l'Education Nationale, la Concurrence et la consommation, la *Commission nationale informatique et libertés (C.N.I.L.)* et bien d'autres se sont engagés dans des actions touchant un large public.

Illustrations d'actions de prévention
mises en oeuvre par les départements ministériels
participant au groupe de travail

La Délégation aux usages de l'Internet : créée par décret du 8.12.2013, elle a pour mission de généraliser l'accès à l'Internet, notamment au bénéfice des foyers plus démunis, mais aussi de former les familles, les enfants et le grand public aux usages des nouvelles technologies.
Elle participe, en particulier, à la formation des animateurs/médiateurs des 5.000 espaces publics numériques, services de proximité déployés dans les services publics ou les espaces associatifs locaux dont la prévention des conduites à risque constitue un objectif prioritaire.
Elle coordonne aussi la mise en oeuvre du programme européen *"Safer Internet plus" (cf., sur ce point, le chapitre 4).*

La Gendarmerie Nationale intervient, de longue date, auprès des publics scolaires pour faire de la prévention. Elle a adapté récemment son dispositif à la lutte contre les cybermenaces en lançant, en décembre 2013, l'opération *"Permis Internet"* ; elle consiste à sensibiliser les élèves de classes de CM2 aux dangers de l'Internet et de leur donner des conseils pour l'utiliser en toute sécurité. A cette fin, elle prend contact avec les écoles, présente l'opération en classe et distribue un kit pédagogique, la formation étant ensuite dispensée par les enseignants *(3 à 4 séances de 45 mn).*

En interne, il faut aussi citer le *Guide du bon usage des médias sociaux au sein de la Gendarmerie Nationale,* qui est une bonne illustration d'une démarche pédagogique adaptée à un milieu professionnel.

Les policiers formateurs anti-drogue (FRAD) sont, eux aussi, de plus en plus sollicités pour parler des dangers de l'Internet et s'appuient sur des vidéos pour favoriser une prise de conscience.

L'OCLCTIC gère, quant à lui, depuis 2009, une plate-forme nationale téléphonique, dite *"Info Escroquerie"*, en prise directe avec les particuliers qui exposent au téléphone des problématiques très diversifiées *(tentative d'escroquerie sur Internet, escroqueries en cours, parfois litige commercial ou civil..)* ; ces particuliers sont orientés, par les policiers et gendarmes, dans les démarches à suivre en fonction des situations personnelles. Il s'agit d'une véritable mission de service public dans laquelle l'accueil, la prévention et l'orientation sont déterminantes.
Cette plate-forme reçoit, chaque année, plus de 42.000 appels

La BEFTI (Préfecture de police) multiplie aussi les actions de prévention, qui peuvent prendre la forme d'une participation à *La Foire de Paris,* au *salon des Seniors,* aux *Journées de la Sécurité intérieure,* ou de la diffusion de différentes brochures pédagogiques *(guide sécurité, prévention des fraudes à la carte bancaire...).*

L'ANSSI s'emploie aussi à mettre en ligne du matériel pédagogique, tel *le guide d'hygiène informatique* (avec des consignes de base pour la sécurisation des systèmes d'information) ou des conseils pratiques pour ceux qui voyagent à l'étranger.

La Protection judiciaire de la jeunesse, au-delà de l'action qu'elle mène pour lutter contre la fracture numérique, sensibilise les mineurs pris en charge aux dangers de l'utilisation de l'outil numérique à partir de trois cyber-bases justice créées dans trois régions de France.

La DGCIS contribue aussi à des campagnes de sensibilisation, notamment à destination des entreprises, par le biais de ses correspondants régionaux spécialisés dans l'intelligence économique.
….

Comment alors expliquer l'impression, largement partagée et d'ailleurs souvent exprimée au titre des attentes, qu'il reste encore beaucoup à faire en terme de prévention, en particulier de la part de l'Etat ?

D'une part, et aux risques sinon d'épuiser les acteurs comme les ressources disponibles tellement le spectre du numérique et de la délinquance qui y est associée est large, **la prévention doit répondre à une impulsion qui, reposant sur une analyse affinée des besoins mais aussi des *"cibles"* prioritaires à atteindre, permet de définir des objectifs, des moyens, des durées et de répartir l'action à entreprendre entre les différents participants.**

Cette **impulsion,** cet **accompagnement doit venir de l'Etat**, même si elle doit être conduite en partenariat avec les professionnels, les médias et le monde associatif

Or, la dernière campagne de prévention massive, relayée par de grands médias, remonte à 2009 ; encore n'était-elle pas exclusivement dédiée à l'Internet puisqu'il s'agissait d'un plan de lutte global contre les escroqueries.

Lancer une grande campagne de sensibilisation en faisant de l'éducation au numérique une *"grande cause nationale pour 2014"* répond ainsi à une nécessité ; elle compléterait aussi utilement le plan gouvernemental mis en oeuvre en 2013. La C.N.I.L. y travaille déjà avec 28 partenaires, représentants des acteurs économiques, de la société civile, du monde de l'éducation et des institutions.

Toutefois, cela ne saurait suffire pour trois raisons :

- il faut aujourd'hui **un pilotage à long terme de la prévention**, inexistant en l'état, car c'est le genre d'actions qui doivent être fédérées et pérennisées, comme l'illustrent les programmes européens en la matière. Il faut donc qu'au sein même de l'Etat une organisation, associant l'ensemble des partenaires, en ait la charge et pas simplement de manière ponctuelle.

- une campagne nationale se limite, nécessairement, à quelques cibles. Elle doit être relayée et accompagnée par **des actions plus thématiques concernant des publics prioritaires.** Là encore, il faut une organisation, car l'impact d'actions parcellaires, parfois désordonnées et souvent reposant sur des moyens dérisoires est limité.
C'est en cela que la prévention ne peut reposer que sur des **pôles de compétence**, en fonction des catégories de population concernées, de certaines formes particulières de délinquance et du savoir-faire des acteurs ; ces pôles doivent être aussi en prise directe avec la réalité sans cesse renouvelée de la technique, de la criminalité et des comportements à risques. Certaines thématiques donnent déjà lieu à action préventive, notamment la protection des mineurs, celle des oeuvres intellectuelles, ou la lutte contre les contrefaçons. Même s'il convient d'établir, secteur par secteur, un état des lieux des besoins comme de ce qui se fait, il apparaît déjà certain que les deux contentieux de masse de la cyber-criminalité **- les escroqueries** ainsi que **les fraudes de cartes bancaires** - nécessitent des campagnes ciblées, et pas simplement auprès des seuls professionnels du e-commerce.
Encore faut-il pour cela **identifier les bons acteurs de la prévention** : en amont, ceux qui sont à même de cerner les besoins des internautes, pour sélectionner l'information pertinente ; en aval, ceux qui sont à même de relayer cette information vers le public.

- le développement de la prévention butte aussi sur **le manque de financements adaptés**, ne serait-ce que pour bénéficier du concours : si l'Union européenne, si l'Etat doivent y contribuer, il est normal que soient aussi mises à contribution les secteurs professionnels de l'Internet ; le *"sponsoring"* à l'américaine n'est pas non plus à écarter.

En ce sens, la sensibilisation des mineurs aux bons usages de l'Internet [105], comme le plan d'action récemment mis en oeuvre par le ministère de l'Education Nationale, en partenariat avec l'association *e-enfance*, afin de prévenir et de répondre massivement au cyber-harcèlement en milieu scolaire, en y associant toutes les parties prenantes et en définissant des règles et des modes de traitement, constituent des exemples à suivre.

[105] programme développé par la *Délégation aux usages de l'Internet* dans le cadre du programme européen pour *un Internet plus sûr*.

"Agir contre le harcèlement à l'école"
campagne du ministère de l'Education national

Cette campagne a été lancée le 26 novembre 2013 par le ministre de l'Education nationale.

Elle résulte d'une prise de conscience récente (2011) car, si le risque pédopornographique était bien identifié, celui du harcèlement l'était moins : deux enquêtes nationales menées auprès de 30.000 élèves ont montré que la cyber-violence à l'école ne relevait pas de la sphère privée et qu'elle était moins liée à des phénomènes d'intrusion *(qui ne représentent que 5% des violences subies)* qu'à des comportements internes, le plus souvent entre élèves.

Selon une étude de victimation réalisée en 2012,
-40% des collégiens et lycéens déclarent avoir été victimes de cyberviolence au moins une fois pendant l'année scolaire
-20,3% d'entre eux ont reçu des textes humiliants, insultants ou même menaçants
-12% d'entre eux ont été victimes d'une usurpation d'identité
-11,6% d'entre eux ont été exclus d'un groupe en ligne
-et 6% des élèves se disent être agressés de manière répétée sur le net, ce qui correspond à la définition du cyber-harcèlement.

Dans un premier temps, la réponse mise en oeuvre a reposé sur une convention de partenariat signée avec l'association *e-enfance* qui mène de nombreuses actions de sensibilisation dans les collèges et travaille avec les opérateurs en communications électroniques, notamment FACEBOOK, dans le but de faire retirer les contenus illicites. L'action était essentiellement ciblée sur le public adolescent, avant que l'on ne se rende compte que les scolaires plus jeunes étaient aussi concernés et qu'il fallait aussi sensibiliser les adultes.

La loi d'orientation et de programmation pour la refondation de l'école du 8 juillet 2013, qui prévoit la généralisation à l'utilisation des outils et des ressources numériques, notamment *"une sensibilisation aux droits et aux devoirs liés à l'usage de l'Internet et des réseaux, dont la protection de la vie privée et le respect de la propriété intellectuelle" (cf. art. L.312-9 du code de l'éducation),* a intégré un plan de prévention et de prise en charge des phénomènes de harcèlement au niveau de chaque établissement. Le nouveau plan de prévention s'est traduit par la réalisation de véritables outils pédagogiques préparés en concertation avec les associations, les parents d'élèves mais aussi des victimes.

C'est dans ce cadre que s'est inscrite la campagne actuelle, qui s'appuie sur des outils diversifiés : un site Internet rénové, des clips de sensibilisation, des fiches destinées aux élèves, aux témoins, aux parents pour savoir quoi faire face à un harcèlement ; des dessins animés pour les écoliers ; un concours pour mobiliser les initiatives des élèves...

Le plan s'accompagne d'une formation étalée sur trois ans, qui concerne, dans chaque académie, des formateurs et des référents afin de pouvoir disposer de groupes interprofessionnels compétents *(200 personnes ont déjà été formées)* ; il est ensuite prévu de s'attaquer à la formation initiale des enseignants.

Mais ce qui caractérise ce plan, c'est la cible privilégiée que constituent, plus que les victimes ou les agresseurs, les témoins des harcèlements, dans le but que la classe elle-même mette hors la loi ce type de comportement ainsi que leurs auteurs, sur le modèle Finlandais qui, par ce moyen, est parvenu à diviser par trois le nombre d'harcèlements.

La prise en charge des victimes constitue une autre des priorités affichées, car il suffit d'une ou de deux semaines pour qu'un mineur-victime "décroche" soit sous la forme d'une fuite de l'école *(24% des décrochages scolaires et des absentéismes seraient dus à la peur du harcèlement, même de la part de bons élèves)*, soit en terme d'impact sur la santé mentale, voire, exceptionnellement, de tentatives de suicide ou même de suicides *(3 en 2013 suite à des harcèlements)*. En ce domaine, les difficultés tiennent d'abord au nombre des enfants-victimes *(11% des jeunes en France)*, au fait que ce sont souvent les mêmes enfants qui subissent des violences réitérées via des sms ou les réseaux sociaux, et enfin au silence que gardent la moitié des victimes.

Enfin, la prise en charge des auteurs repose sur des réponses disciplinaires ou un travail réalisé par les médiateurs de l'Education Nationale, en partenariat avec la Protection judiciaire de la jeunesse, ou, si les faits sont graves, si les auteurs ne sont pas identifiés ou si les violences émanent de l'extérieur de l'école, sur la saisine du parquet.

Ainsi que l'illustre l'exemple précédent, **la sensibilisation ne saurait se limiter à des campagnes d'information ou à des plate-forme d'information.**

Il revient aussi à l'Etat d'assurer **une prévention spéciale** en mettant à disposition des internautes les informations disponibles concernant certains types d'infractions déjà réalisées *(en matière de cyber-escroqueries notamment)*, certains sites ou même certaines sociétés à vocation purement criminelle. L'OCLCTIC étudie déjà la possibilité de mettre en ligne un moteur de recherche permettant de détecter, par mots-clés, ce type d'informations.

Afin de compléter le service offert par la plate-forme téléphonique INFO-ESCROQUERIES, l'OCTCLIC envisage de mettre en ligne une base de données, directement consultable par le public, qui lui permettrait d'obtenir des avis relatifs à des sites Internet, des adresses e-mail supportant des messages ou des petites annonces suspectées d'être constitutives d'escroqueries.

Ce projet s'inspire du site www.hoaxbuster.com qui permet de comparer un texte avec une base de données de *"hoax" (= fausses nouvelles véhiculés par Internet),* grâce à une zone de saisie permettant à l'internaute de copier/coller n'importe quel texte ou mot-clé afin d'obtenir une liste d'articles relatifs à des *"hoax"* identifiés ou, au contraire, à des faits reconnus comme étant authentiques.

Un tel outil permettrait aux internautes de tester les adresses de site Internet ou le contenu de spams pour savoir si ces éléments sont associés à des escroqueries connues. La base de données pourrait être étendue aux infractions souvent perçues par le public comme étant des escroqueries, telles les contrefaçons.

Ce moteur de recherche aurait vocation à être inclus dans un site Internet officiel dédié ou déjà existant.

Il suppose toutefois des ressources tant humaines qu'en logiciels non négligeables pour assurer la collecte de l'information et la mise à jour de la base, conditions de sa crédibilité.

Dans le même ordre d'idées, les Douanes ont déjà négocié avec Microsoft l'obtention d'un référencement prioritaire sur le moteur de recherche Google des messages d'alerte douaniers relatifs aux sites de contrefaçons, de manière à ce que ces messages soient proposés avant les sites litigieux eux-mêmes.

Au-delà, le principe devrait être posé que **toute nouvelle ouverture de services en ligne**, laquelle dépend de l'Etat dans la majorité des cas, **devrait être précédée ou accompagnée d'une véritable étude de risques**, prenant en compte les expériences étrangères et définissant les mécanismes préventifs spécifiques à mettre en oeuvre *(cf. l'exemple des jeux et des médicaments)*. Les échanges en télé-médecine, la multiplication sur les réseaux sociaux d'offres de prêts sur gage, les modes de paiement par terminal mobile, l'apparition prochaine des paiements mobiles sans contact...constituent, on l'a dit, autant de nouveaux défis qui nécessitent que l'Etat pose des règles, faute de quoi elles seront imposées par le marché.

De manière plus générale, **l'exigence de prévention doit aussi reposer sur ceux qui ouvrent des accès à Internet ou les facilitent.**

Les responsables des collectivités territoriales, des cyber-cafés, des espaces numériques publics doivent prendre toute leur part. Cela suppose un plan global cohérent, reposant sur la conscience de ce que cette éducation est aussi importante que l'accès au haut débit et doit être menée au même pas.

Quant aux **prestataires de l'Internet**, notamment les fournisseurs d'accès, ils ont, bien sur, une responsabilité toute particulière.

Il ne s'agit pas d'ignorer les efforts déjà entrepris par **le secteur privé** - hébergeurs, fournisseurs de services ou d'accès, éditeurs... appuyés par des associations actives, notamment dans le domaine de protection des mineurs -. Ainsi *l'Association des Fournisseurs d'Accès (A.F.A.)* s'engage chaque année pour relayer en France le programme européen *Safer Internet*. Mais on pourrait aussi attendre d'un fournisseur, lorsqu'il livre une « box » à un nouvel abonné, accompagnée d'un livret commercial, qu'il l'avertisse non seulement des possibilités que cet abonnement va lui procurer, mais également des risques générés par Internet. On pourrait attendre d'un site de petites annonces qu'il avertisse tout acheteur potentiel, au moment précis où il consulte une annonce, des modes opératoires correspondant au bien ou au service qu'il convoite, la prévention n'étant jamais aussi efficace que quand elle est contextuelle...

En la matière, la bonne volonté ne suffit pas car elle est trop souvent bornée, sous couvert de l'invocation des libertés fondamentales, par la priorité donnée aux intérêts économiques, raison de l'hétérogénéité des engagements constatée dans ce secteur. Aussi, la prévention doit-elle résulter également d'obligations mises à la charge des prestataires, telle, par exemple, pour les sites de vente à distance, celle consistant à faire figurer au regard de l'annonce l'adresse IP de l'annonceur ou du moins l'information selon laquelle elle est située en France, en Europe ou à l'étranger *(dispositif contournable par les escrocs, mais les obligeant à avoir des complicités en France).*

Mais les prestataires techniques sont loin d'être les seuls professionnels concernés, comme l'illustrent, par exemple, les réticences des **marchands en ligne** à sécuriser davantage les modes de paiement destinés à prévenir les fraudes à la carte bancaire malgré l'intérêt que présente ce dispositif, ou encore les réticences de nombre d'organismes bancaires à faire de la publicité concernant ce dernier [106].

---

[106] cf. le système de sécurisation des paiements sur Internet résultant de la mise à disposition d'une carte bancaire spécifique avec l'attribution de coordonnées bancaires différentes pour chaque transaction - *le code 3D-SECURE* - ; il est vrai que le e-commerce lui reproche un certain manque de fiabilité

Au regard des professionnels concernés, l'exigence de prévention devrait être adossée sur un principe de responsabilité pécuniaire en cas d'incident.

S'agissant enfin des **entreprises industrielles d'une certaine importance**, elles devraient être soumises à l'obligation de se doter d'un **plan de prévention numérique**, tant en terme de sécurité technique que de comportement interne, qui devrait être validé par des instances professionnelles adéquates.

Mais il ne faut pas non plus oublier que, par delà la délinquance organisée, **l'internaute peut être aussi auteur volontaire d'infractions**, qu'il s'agisse d'infractions aux droits d'auteurs *(piratage, téléchargement illicite, etc.),* de l'acquisition de contrefaçons, de harcèlement, de la diffusion de fausses nouvelles, d'incitation à la haine, etc. Nombre d'infractions pourraient être prévenues si certains internautes n'étaient pas désinhibés par un double sentiment : l'ignorance des limites posées par la loi, puisque tout serait permis sur Internet, du moins lorsqu'il s'agit de causé un préjudice à autrui ; la croyance en leur impunité et donc en leur irresponsabilité. Les internautes – et pas seulement les plus jeunes – doivent être informés des conséquences de leurs actes, parfois dramatiques, des limites posées par la loi commune, des peines encourues et des sanctions prononcées.

A ce titre, **la Justice doit être aussi acteur de prévention**. Les réponses judiciaires doivent encore davantage prendre en compte ce nécessaire volet pédagogique, comme le ministère public le fait déjà dans bien d'autres domaines, par exemple avec **les stages de citoyenneté, qui pourraient être utilement adaptés à la citoyenneté numérique**, surtout lorsqu'il s'agit de jeunes.

Une synergie doit être aussi recherchée entre les acteurs de la justice et les médias afin que les incidences sur les victimes et les condamnations résonnent au-delà de l'enceinte des chambres correctionnelles. Pour que les décisions de justice aient valeur pédagogique, elles doivent être commentées dans la presse. Afin de toucher au mieux le public concerné, l'idéal est de faire relayer cette information par les réseaux utilisés pour commettre les infractions, à l'instar d'expérimentations déjà mises en œuvre par la plate-forme PHAROS avec le forum français *« jeuxvideo.com ».*

22.- <u>Prévenir la commission des infractions</u>

L'information, la sensibilisation des internautes ne suffit pas, car les modes opératoires sont sans cesse renouvelés. Ainsi l'hameçonnage *(phishing)* revêt chaque année de nouveaux aspects, s'adaptant à l'actualité et à l'apparition de nouveaux services mis à la disposition des internautes. Les escrocs renouvellent leurs modes opératoires, de plus en plus agressifs *(chantage à la vidéo intime)* ou techniques *(blocage des ordinateurs par l'affichage d'une page « officielle » réclamant le paiement d'une amende)...*

La mobilisation de la recherche et de l'industrie, française ou européenne, sur la conception de logiciels, de sécurité ou autres, susceptibles de prévenir, voire de mieux répondre à ce savoir-faire technologique de la délinquance organisée est désormais reconnue comme une nécessité ; encore faut-il créer aujourd'hui une interface entre, d'une part, les services spécialisés de police judiciaire ou des administrations compétentes et, d'autre part, ces partenaires du privé, pour faire remonter les diagnostics et les besoins.

Là encore, **les professionnels de l'Internet** ont les moyens techniques, et parfois l'obligation, de participer à la prévention de la commission d'infractions, ou, à tout le moins, d'en limiter la portée.

La prévention spéciale attendue de leur part commande d'abord, comme le préconise le Contrôleur européen, une sécurisation par défaut d'un certain nombre d'accès informatiques *(anti-spam, anti-cookies, filtrages).*

Ils peuvent aussi, à l'initiative ou sur l'impulsion des pouvoirs publics, bloquer certains flux informatiques ou supprimer les outils utilisés pour commettre des infractions *(cf., sur ce point, les développements ultérieurs).*

Ces actions stratégiques reposent, pour une bonne part, sur le signalement des contenus illicites et reposent tous sur une exigence : **faire de l'internaute un acteur**. D'ores-et-déjà, sur le plan partenarial, *le Point de Contact, Signal Spam et Phishing Initiative* reçoivent des signalements en nombre ; s'y ajoutent les formulaires de signalement propres aux fournisseurs d'accès qui ne sont pas membres *de l'Association des fournisseurs d'accès (AFA).* C'est aussi le cas pour les pouvoirs publics, avec le site officiel de signalement du Gouvernement (*www.internet-signalement.gouv.fr)*, *le Centre de Surveillance du Commerce Electronique (D.G.C.C.R.F),* le point d'entrée ouvert par la brigade spécialisée de la Préfecture de police *(la B.E.F.T.I.)* et surtout la plate-forme PHAROS *(qui est passée de 1000 signalements par semaine en 2009 à plus de 2500 en 2013).* Il faut encore y ajouter les dispositifs spécifiques mis en oeuvre par des autorités administratives, indépendantes ou non.

Cependant, l'internaute devrait être encouragé dans sa démarche par des retours d'information plus systématiques afin d'être pleinement convaincu de l'intérêt de tels signalements citoyens.

Surtout, après la phase des pionniers, il faut maintenant rationaliser les points d'entrée de l'information, dont le nombre et la redondance nuisent à la lisibilité en donnant au public le sentiment d'actions parcellaires et dispersées. Il faut aujourd'hui en finir avec de tels cloisonnements, nuisibles au but recherché et inintelligibles pour la grande masse des internautes, les moins informés, en définissant, comme c'est parfois déjà le cas à l'étranger, un point d'entrée unique dédié au signalement relatif à la cybercriminalité. Cette mise en cohérence ne pourra se faire que sous l'impulsion de l'Etat mais dans un esprit de confiance, associant l'ensemble des partenaires publics comme privés.

Recommandation n° 3
relative à la prévention de la cybercriminalité

1- Impliquer davantage l'Etat en terme d'impulsion, de synergie, de définition des objectifs, de pilotage à long terme dans la politique de prévention de la cybercriminalité prise au sens large par
-des campagnes de sensibilisation destinées au grand public, sur la protection des données notamment sur les mobiles ou la vigilance contre les escroqueries
-l'organisation de campagnes-relais en direction de publics plus spécifiques, en mobilisant, voire en organisant des pôles de compétence
-la création d'un 17 de l'Internet ouvert au grand public
-la réalisation systématique d'études de risque précédant toute nouvelle ouverture de service dans les domaines réglementés.

2- Faire de l'internaute le premier acteur de sa propre sécurité et de la lutte contre les propos, images et comportements illégaux par
-l'éducation au numérique à l'école comme en mobilisant les professionnels qui opèrent dans les 5000 espaces publics numériques et assurent déjà un important effort de formation
-le développement d'espaces d'information en ligne ou par téléphone
- l'harmonisation et la généralisation des différents supports préventifs utilisés dans le cadre public
- la mise en ligne d'un moteur de recherche facilitant la détection de sites, de sociétés ou de spams associés à des cyber-infractions
-la rationalisation des points d'accès pour les signalements aux fins d'une meilleure visibilité
-la création d'un 17 de l'Internet
-une meilleure association des structures d'aide aux victimes ou de consommateurs.

3- Mobiliser les professionnels en
-assurant une meilleure cohérence des actions de sensibilisation
-instaurant un cahier des charges pour les établissements, publics ou privés, offrant l'accès à Internet - en arrêtant contractuellement ou en définissant en tant que de besoin les obligations préventives à respecter par le commerce en ligne, les opérateurs - notamment les fournisseurs d'accès mais aussi les plates-formes de téléchargement -, les vendeurs d'appareils numériques, sous peine d'une mise en cause financière
-préconisant, pour les grandes entreprises, la réalisation d'un plan de prévention numérique,
-incitant à la création de CERT et en mobilisant les correspondants régionaux spécialisés dans l'intelligence économique pour répondre aux attentes des petites et moyennes entreprises.

4- Mobiliser enfin la recherche et l'industrie françaises et européennes pour la détermination de réponses techniques et technologiques appropriées.

II.3.- Une exigence : la formation des acteurs

A l'effort de sensibilisation et de mobilisation massive, auquel le groupe de travail appelle, doit s'ajouter une préparation des acteurs étatiques à la prise en charge de la lutte contre la cybercriminalité.

Il est en effet erroné de prétendre que cette délinquance est une délinquance comme une autre car, même si elle concerne de nombreux contentieux, l'appréhension de ses manifestations et modes opératoires spécifiques comme des acteurs et partenaires constitue un préalable à une action efficace, en particulier pour les infractions strictement informatiques et les affaires complexes ou d'envergure, comme l'ont bien compris les institutions européennes. De plus, le manque de réactivité est souvent la conséquence d'un manque de savoir-faire et de maîtrise.

En ce sens, la formation concerne, certes, avant tout, les acteurs répressifs *(policiers, gendarmes, douaniers, autres agents de l'État, magistrats),* mais aussi l'ensemble des intervenants en prise directe avec les internautes, que ce soit au sein des entreprises, collectivités locales ou établissements publics, ou dans les sites d'accès (gérants de cyber-cafés, administrateurs de bornes wifi ..).

S'agissant des services répressifs - sur lesquels le groupe interministériel s'est volontairement focalisé -, le groupe interministériel entend d'abord insister sur le fait qu'**une telle formation intéresse, tout autant, les magistrats que les enquêteurs**. De nombreux acteurs auditionnés durant les travaux ont d'ailleurs souligné la nécessité d'accentuer leur formation. Or, actuellement, les magistrats sont inégalement formés puisque la formation existante repose sur le volontariat. Cette absence de formation et donc de spécialisation au niveau pénal conduit à un traitement très inégal des procédures liées à la cybercriminalité, faute de bien saisir le fonctionnement des technologies de l'information et de la communication, de savoir manier aisément les preuves numériques et de pouvoir travailler en réseau [107]. L'observation vaut aussi pour les juges civils, notamment ceux spécialisés en matière de propriété intellectuelle.

Il importe, de manière plus générale, de **ne pas se limiter à la formation de spécialistes**, qui a constitué historiquement la priorité du moins pour le ministère de l'Intérieur, mais de bien appréhender désormais l'ensemble des besoins des services d'investigation et des juridictions dans ce domaine.

Il convient, pour cela, de **définir des niveaux de formation** dans une perspective inter-services voire européenne, afin d'améliorer la lisibilité du dispositif en place mais également l'efficacité de la prise en charge des plaintes, tout en s'offrant des opportunités de mutualisation de moyens de formation.

---

[107] le constat est d'ailleurs général au plan européen *(cf., sur ce point, les prises de position des Conseils consultatifs des juges et des procureurs, et les manuels de formation spécifiques élaborés par le Conseil de l'Europe et le Réseau de Lisbonne en 2009).*

Il est opportun, à cet égard, de faire référence à la démarche entreprise par le groupe de travail européen ECTEG *(European Cybercrime Training and Education Group)* pour promouvoir le développement des capacités de lutte contre la cybercriminalité et harmoniser les référentiels des métiers et qualifications. Son action vise notamment à favoriser des démarches de formation commune entre les services répressifs et à améliorer la coopération internationale, en particulier avec les organisations internationales.

European Cybercrime Training and Education Group (ECTEG)

Né des projets Flacon et Agis et renommé ECTEG en 2009, ce projet est composé de représentants de services enquêteurs des pays membres, d'organisations internationales, d'universités et d'industriels.

Il vise, avec le soutien d'EUROPOL et en lien avec le CEPOL (Collège européen de police), à :

.encourager les initiatives nationales et internationales visant à harmoniser les formations à la lutte contre la cybercriminalité,

.partager les connaissances et les expertises dans ce domaine de formation,

.promouvoir une standardisation des méthodes et des procédures dans les programmes de formation et une coopération avec les autres organisations internationales,

.collaborer avec des partenaires académiques pour mettre en place des formations diplômantes reconnues au plan international,

.collaborer avec des partenaires industriels pour les associer aux processus de formation, mettre à disposition des supports de formation à destination des services enquêteurs.

Par-delà ces travaux européens, une première clarification des niveaux de formation s'impose au niveau national afin de pouvoir identifier les priorités d'action à conduire.

Trois niveaux devraient être envisagés, dont les contenus seraient adaptés aux différents types d'acteur *(enquêteur, magistrat*) :

- □ niveau 1 : sensibilisation de tous les acteurs répressifs à la cybercriminalité,
- □ niveau 2 : formation d'acteurs référents « cybercriminalité », ayant vocation à être répartis aux sein des services territoriaux non spécialisés dans la lutte contre la cybercriminalité,
- □ niveau 3 : formation d'acteurs spécialistes « cybercriminalité » pour les services et juridictions ayant une compétence spécifique dans ce domaine.

En outre, des compétences dépassant le niveau 3 renverraient à des niveaux d'expertise concernant des services hautement spécialisés, le plus souvent centralisés, pour lesquels l'accès à des formations spécifiques et parfois coûteuses est nécessaire *(formations diplômantes en université ou école d'ingénieur ou ponctuellement formations qualifiantes délivrées par des formateurs externes).*

Les dispositifs actuels se focalisent sur le seul niveau 3, et essentiellement, le concernant, sur la seule formation initiale, alors même que la formation continue est indispensable en cette matière.

*****

1.- La sensibilisation de tous les acteurs répressifs (niveau 1)

Un existant … inexistant

A l'heure actuelle, aucune action obligatoire de sensibilisation à la cybercriminalité n'est inscrite au programme des écoles de formation initiale de la police, de la gendarmerie, de la douane et de la magistrature.

Seule l'Ecole nationale de la magistrature (E.N.M.) avait proposé il y a deux ans un colloque exceptionnel sur ce sujet.

L'insertion obligatoire dans les formations préalables d'une action de sensibilisation à la cybercriminalité pourrait prendre différentes formes : cours magistraux, enseignement à distance, séminaire ... selon les possibilités offertes dans chacune des écoles. Il pourrait également être imaginé, s'agissant d'une sensibilisation générale, la mise à disposition d'un support de formation commun à ces différentes écoles.

Des initiatives encourageantes

C'est le sens de la démarche entreprise par le *Centre expert contre la cybercriminalité français (CECyF)*, dont la création est effective depuis janvier 2014 et qui s'inscrit dans le réseau européen né du projet 2CENTRE *(cf. les développements en 4 sur le partenariat public-privé).*

Parmi les partenaires français à ce projet, la gendarmerie, la police et l'université de technologie de Troyes (UTT) ont en effet réalisé la première version d'un support de sensibilisation à la cybercriminalité, sous la forme d'un ensemble de modules d'enseignement à distance (EAD), dont la spécification avait été réalisée lors des travaux du groupe « MITICOM » en 2010.

Ce support en ligne [108], désormais finalisé, sera mis à la disposition de tous les acteurs répressifs. Il sera notamment proposé à l'ensemble des gendarmes sur leur plate-forme de formation à distance dès janvier 2014. Son suivi pour les élèves des écoles d'officiers et de sous-officiers ou pour les candidats à la formation de niveau 2 *(acteur référent)* sera rendu obligatoire.

En vue de l'intégration d'un module « cybercriminalité » lors de la formation initiale des policiers, une mallette pédagogique est aussi en cours de conception en liaison avec la Direction des Ressources et des Compétences de la Police Nationale *(D.R.C.P.N.).*

La Direction générale de la Police national développe actuellement une plateforme de formation distancielle *(e-learning)*, dédiée à la cybercriminalité, s'appuyant sur l'expertise de la D.R.C.P.N. pour l'ergonomie et l'intégration pédagogique des contenus d'apprentissage qui eux sont fournis par le pôle de formation de l'O.C.L.C.T.I.C. La plateforme intègre également des classes virtuelles permettant de dispenser des cours théoriques à distance, en direct avec un formateur de l'Office.

La plateforme en cours de création respecte les recommandations du programme européen et offre plusieurs niveaux d'apprentissage, allant de la prise de conscience du phénomène *(niveau 1, prérequis),* aux connaissances et savoir-faire relatifs aux premiers actes juridiques et *techniques (niveau2, premier intervenant)*, pour en définitive s'axer sur la spécialité d'investigateur cybercriminalité *(niveau 3, ICC).*

[108] Contenu : définition de la cybercriminalité, visages de la cybercriminalité, dispositifs et acteurs de la lutte contre la cybercriminalité, arsenal juridique, recevoir une plainte, identifier et requérir des services et prestataires, recherche en sources ouvertes, participer à une perquisition en environnement numérique, activités d'auto-évaluation.

L'évolutivité et la modularité de la plateforme offrent une grande souplesse, permettant ainsi d'envisager dans le futur des étapes supérieures et complémentaires d'apprentissage, notamment après validation de la certification ICC *(équivalent à un niveau Bac +3/4)*. En effet, il est envisageable, en s'appuyant sur le partenariat existant avec l'école d'ingénierie informatique EPITA, que la plateforme puisse permettre l'élévation des compétences des ICC tendant vers l'expertise *(niveau 4, ingénieur).*

Les contenus de formation développés par les partenaires académiques et industriels du programme européen sont parfaitement intégrables à la plateforme de la D.G.P.N.. Ces contenus sont d'ordre très technique et intégrables en majorité à partir du niveau 3 de formation *(ICC et ICC certifiés).*

Ce support de formation initiale en ligne à la cybercriminalité [109] sera disponible au terme du 1er semestre 2014 et mis à la disposition de tous les acteurs répressifs de la D.G.P.N., notamment au sein des écoles de formation des métiers de la Police Nationale et constituera une mallette pédagogique. Cette formation de niveau 1 suscitera des vocations aux métiers de l'investigation numérique pratiqués en niveau 2 et 3. L'évaluation des formés au niveau 1 permettra de dégager un vivier et des aptitudes à la poursuite du cursus.

L'apprentissage à distance ne remplacera toutefois pas la transmission des compétences et savoir-faire d'un formateur en enseignement direct ; c'est pour cette raison que la formation pragmatique développée par la D.G.P.N. intégrera un temps d'apprentissage dédié à la pratique et à la mise en situation.

2.- La formation des référents « cybercriminalité » (niveau 2)

Un objectif de niveau intermédiaire qui fait consensus ...

La notion de référents « cybercriminalité » revêt différentes formes selon les métiers. Il s'agit toutefois principalement de personnes réparties au sein des services territoriaux non spécialisés dans la lutte contre la cybercriminalité et en charge des investigations dans ce domaine qui n'appellent pas une haute spécialisation.

Pour les magistrats, ce modèle est appliqué dans les ressorts des cours d'appel de Paris et de Versailles où un **magistrat référent en matière de cybercriminalité** est désigné. Il est l'interlocuteur privilégié de ses collègues, des services d'enquête mais également des acteurs de l'Internet. Il assure un rôle d'appui technique, de suivi, de coordination et de veille juridique des procédures diligentées dans ce domaine et peut, dans certains parquets, assurer la centralisation du traitement des procédures d'atteintes aux traitements automatisés de données.

En dehors de ces ressorts, les procédures relatives à la cybercriminalité sont généralement traités dans les services de droit commun *(mineurs, stupéfiants, presse, économiques et financiers pour les fraudes et infractions relatives aux STAD),* voire, pour les juridictions de plus petite taille, par les services de traitement en temps réel.

Les services d'investigation ont, quant à eux, des pratiques disparates mais convergentes en matière **d'enquêteurs référents**. Ces enquêteurs doivent être en mesure d'identifier et de comprendre

[109] contenu intégrant notamment le module "sensibilisation à la cybercriminalité" du Centre expert français contre la cybercriminalité : définition de la cybercriminalité, visages de la cybercriminalité, dispositifs et acteurs de la lutte contre la cybercriminalité, arsenal juridique, recevoir une plainte ou orienter le public, identifier et requérir des services et prestataires, recherche en sources ouvertes, déroulement d'une perquisition en environnement numérique, connaissances techniques basiques et minimales pour appréhender le phénomène *(l'ordinateur, les supports de stockage numérique, le réseau internet, l'email, les réseaux sociaux...), r*essources documentaires professionnelles (guides), activités d'auto-évaluation et examen.

la problématique de la cybercriminalité et d'apporter un premier niveau de réponse tant dans la prise de plainte, que dans des actes élémentaires d'enquêtes (réquisitions), mais également dans l'intervention sur des scènes de crime numériques *(identification des traces et indices numériques, mesures conservatoires en vue du recueil de la preuve, et certaines actes techniques simples).* L'objectif commun poursuivi consiste principalement à fournir un service rapide, efficace, fiable, pertinent, et fondé sur la disponibilité quotidienne auprès des enquêteurs et ce pour répondre aux besoins de support technique croissant. En effet, actuellement il est rare qu'une enquête, qu'une perquisition ou une réquisition n'ait pas un lien direct ou indirect avec les technologies de l'information et de la communication : elle nécessite alors un appui technique basé sur des connaissances et savoir-faire spécifiques au recueil de la preuve numérique. Il est donc capital que le nombre de premiers intervenants soit plus important que le nombre des spécialistes de niveau 3.

La gendarmerie et la préfecture de police de Paris dispose d'ores et déjà de ce niveau de qualification. La police nationale s'engagera sur cette voie en 2014.

⌞ La gendarmerie nationale a créé en 2008 ce niveau, appelé **C-NTECH (correspondant en technologies numériques)**, qui s'inscrit dans son dispositif global de lutte contre la cybercriminalité. Elle dispose aujourd'hui d'un millier de C-NTECH répartis dans les brigades de recherches, les brigades territoriales autonomes et les communautés de brigades. Dans chaque département, les enquêteurs NTECH *(spécialistes « cybercriminalité » du niveau 3) des* brigades départementale de renseignements et d'investigations judiciaires (B.D.R.I.J.) sont chargés d'animer le réseau des C-NTECH.

Missions des C-NTECH

(cf. circulaire n° 16000/DEF/GEND/OE/SDPJ/PJ du 16 février 2008)

.recevoir, après entente avec les victimes, les plaintes des particuliers et des entreprises pour les infractions spécifiques *(connaissance des phénomènes, qualification des infractions),*

.effectuer les actes techniques simples grâce aux outils mis à leur disposition et selon les méthodes préconisées *(perquisitions, mesures conservatoires, examens simples),*

.enquêter sur les infractions spécifiques, pour lesquelles il reçoivent systématiquement l'assistance d'un enquêteur NTECH *(réquisitions, investigations simples).*

⌞ La préfecture de police de Paris poursuit la même logique et a confié à *la brigade d'enquête sur les fraudes aux technologies de l'information* (B.E.F.T.I.) la charge de former de tels référents au sein de la direction de la sécurité publique de l'agglomération parisienne (D.S.P.A.P.) et de la direction régionale de la police judiciaire (D.R.P.J.), dans le but d'apporter une réponse active aux victimes et de procéder aux investigations simples. Toutefois, les personnels ainsi formés - au nombre de 263, dont 117 la dernière année de référence - ne relèvent pas d'un réseau structuré.

⌞ La police nationale s'engage aussi dans le même processus, par la mise en place d'une qualification de **«premier intervenant en cybercriminalité»**, intégrant les connaissances du niveau 1, mais surtout disposant de compétences et d'un réel savoir-faire technique dans l'intérêt du recueil de la preuve.

En effet, le premier intervenant au-delà de ses connaissances théoriques sera en mesure d'intervenir sur des scènes de crime numérique *(perquisitions)* en sachant identifier les traces et indices électroniques volatiles ou stockés sur des supports physiques et surtout en sachant prendre les mesures conservatoires *(copies, saisies et scellés)* adaptées et garantissant la sécurité, l'intégrité et l'inviolabilité des preuves numérique recueillies. Ainsi, son intervention technique se limitera à la copie de la mémoire vive d'un ordinateur allumé et à la duplication d'un disque dur d'un ordinateur éteint ou de tous autres supports informatiques, à l'aide d'une méthodologie et d'outils assurant la validité et la recevabilité des preuves collectées.

Le déploiement des premiers intervenants devrait se faire à un rythme de 144 spécialistes par an. Sur les 5 ans à venir, le nombre des premiers intervenants en fonction devrait atteindre 720, soit 2 fois plus que le nombre de spécialistes de niveau 3 actuellement en service. Les directions inter-régionales et les services régionaux de police judiciaire, ainsi que les directions départementales de sécurité publique et

les commissariats, enfin les directions zonales de la Police de l'Air et des Fontières seront les services principalement concernés par ce déploiement

Quant aux agents techniques de laboratoire régionaux ou locaux de la police technique et scientifique *(SRITT et SLITT),* ils sont formés à l'investigation numérique dans le cadre de leur cursus propre, mais ils pourront, au cours de leur formation initiale, avoir accès aux contenus de la plateforme, à minima au niveau 1 de celle-ci, puis aux niveaux 2 et 3 après évaluation et sélection.

Missions des futurs Premiers Intervenants de la Police Nationale

*identifier et qualifier des infractions de cybercriminalité,
*recevoir, après entente avec les victimes, les plaintes des particuliers et des entreprises pour les infractions spécifiques,
*identifier et savoir extraire les premiers éléments numériques dans une enquête
*conseiller et assister les OPJ lors de leurs enquêtes lorsque qu'ils sont confrontés à des problématiques d'identifications sur les réseaux de télécommunications ou qu'ils ont besoin de saisir un ICC
*effectuer les réquisitions d'identifications numériques,
*effectuer les actes techniques simples de collecte et préservation de preuve numérique grâce aux outils mis à leur disposition, et selon les méthodes préconisées,
*rendre un rapport détaillés et circonstancier de son intervention à toutes fins utiles pour un ICC chargé ultérieurement d'une analyse des preuves collectées,
*enquêter sur les infractions simples de cybercriminalité,
*participer et alimenter de ses expériences le réseau social d'échange professionnel des ICC.

… mais qui appelle une structuration de l'offre de formation

La formation du niveau référent est peu structurée et s'appuie principalement sur des stages de formation continue.

C'est ainsi que, pour les magistrats, différentes formations annuelles sont proposées dans le catalogue des stages de l'E.N.M.. Il s'agit de modules de formation continue, sur la base du volontariat. Elles ne rentrent dans aucun cursus obligatoire.
Un stage sur la cybercriminalité, ouvert aux magistrats (62 et 87 magistrats en ont bénéficié les deux dernières années), mais aussi aux greffiers, aux policiers, aux gendarmes et aux douaniers, et d'une durée d'une semaine, est ainsi proposé.
Par ailleurs un stage de même durée est organisée à l'attention des magistrats (8 et 10 d'entre eux en ont bénéficié les deux dernières années) par l'O.C.L.C.T.I.C.
Enfin, progressivement, l'E.N.M. introduit la dimension cybercriminalité dans des sessions sur des thématiques diverses comme par exemple la criminalité organisée, les violences sexuelles sur mineurs, le droit pénal économique et financier, le racisme ou la coopération pénale internationale.

La conception est différente pour les services enquêteurs puisque la formation continue se fait au plus près des services et unités. Elle n'existe toutefois, en l'état, qu'au niveau de la gendarmerie et de la préfecture de police.

S'agissant de la Gendarmerie, la formation des C-NTECH est dispensée au niveau des régions et durant une durée de 3 jours [110].

[110] Contenu : informatique *(notions de base, micro-ordinateur et supports),* enquête *(introduction juridique, perquisition chez un particulier, escroqueries sur Internet, recherches en sources ouvertes, contrefaçon de cartes bancaires),* GSM *(téléphone mobile, analyse de cartes SIM),*

En ce qui concerne la Préfecture de police, la formation d'une journée est assurée dans le cadre de 20 sessions annuelles ; elle est différente selon la fonction assurée par l'enquêteur .

Globalement, l'offre est ainsi assez disparate tant dans les objectifs que dans les contenus.

Concernant les enquêteurs, un référentiel commun de compétences pour les référents « cybercriminalité » pourrait être établi, à charge pour les organisations de délivrer les formations de la manière la plus adaptée à leur structure.

Concernant les magistrats et les chefs de services d'investigation dont une des composantes est dédiée à la lutte contre la cybercriminalité, le principe de formation commune, à l'instar de la session organisée par l'ENM, doit être conservé voire accentué.

Enfin, l'offre se concentre aujourd'hui sur des modules initiaux. Elle devra être complétée par des modules additionnels permettant une actualisation des connaissances, compte tenu de l'évolution permanente de la cybercriminalité et du droit attaché à cette matière.

3.- La formation des spécialistes « cybercriminalité » (niveau 3)

La formation des enquêteurs spécialistes « cybercriminalité » a fait l'objet d'efforts importants au sein de la police et de la gendarmerie depuis de nombreuses années; elle est d'ailleurs directement liée à l'effort de spécialisation mis en oeuvre sur le territoire. Elle s'avère, en revanche, inexistante au plan institutionnel en ce qui concerne la magistrature, qui ne dispose pas, en l'état, de services spécialisés, même si, à titre individuel, certains magistrats ont suivi des formations universitaires qualifiantes dans le cadre de leur formation continue *(notamment le diplôme universitaire « Cybercriminalité : droit, sécurité de l'information et informatique légale » de l'université de Montpellier (UM1), délivré à la suite d'une formation de 98 heures : 2 magistrats ont suivi cette formation en 2012, 4 en 2013* [111]*).*

Afin d'accompagner la création de pôles juridictionnels plus spécialisés *(cf. les recommandations relatives à l'organisation)*, il sera nécessaire d'assurer une formation de niveau 3 à destination des magistrats en charge de ce contentieux. Il ne s'agit aucunement d'envisager une formation techniquement lourde à l'instar de celle des enquêteurs spécialisés *(voir ce qui suit)* mais elle pourrait prendre la forme d'un module complémentaire à celui s'adressant aux magistrats référents *(cf. plus haut)*, d'une durée de quelques jours, afin d'approfondir, par exemple en collaboration avec l'université précitée, les questions de cybersécurité *(cadre juridiques, obligations des acteurs, dispositif étatique)*, l'organisation et le management des systèmes d'information des entreprises… Cette formation pourrait s'adresser également aux chefs de services d'investigation ou de composantes de services d'investigation exclusivement dédiés à la lutte contre la cybercriminalité.

---

téléphonie *(réquisitions aux opérateurs de téléphonie, interprétation des résultats),* réseaux *(Internet, investigations sur Internet, réquisitions aux opérateurs Internet),* exercices d'analyse de carte SIM, de perquisition et de synthèse.

[111] Contenu : introduction aux réseaux et à l'Internet, droit et sécurité juridique, aspects techniques de la sécurité des systèmes d'information et de la cybercriminalité, aspects juridiques et économiques de la sécurité des systèmes d'information, cybercriminalité : dispositifs juridiques et enjeux économiques et sociaux, informatique légale *(techniques d'investigation et de criminalistique numériques).*

Institutionnalisée depuis plusieurs années et liée à une qualification reconnue en interne et au regard du code de procédure pénale *(art. D.7 du C.P.P.),* la formation des enquêteurs concerne :

⌞**les enquêteurs en technologies numériques (NTECH) de la gendarmerie nationale**, institués en 2001 et au nombre de 260 actuellement.

Missions des NTECH

(cf. circulaire n° 16000/DEF/GEND/OE/SDPJ/PJ du 16 février 2008)

Elles diffèrent selon l'unité d'affectation :

□ l'institut de recherches criminelles de la gendarmerie nationale :
.réaliser des expertises et des examens techniques complexes (ou nécessitant l'utilisation d'outils de laboratoire), à la demande de l'autorité judiciaire ou des enquêteurs, en se déplaçant au besoin sur le terrain, en matière d'extraction de données à partir de supports électroniques, magnétiques ou optiques et d'analyse de systèmes et réseaux,
.animer la veille technologique et mener des actions internes ou externalisées de recherche et de développement,
.participer à la formation des NTECH (élaboration des programmes et des supports, enseignement, évaluation, stages ad-hoc) ou d'homologues étrangers,
.participer à la définition des besoins pour l'équipement des NTECH,
.définir ou valider les procédures techniques à mettre en œuvre par les NTECH et rédiger la documentation criminalistique associée.

□ le service technique de recherches judiciaires et de documentation :
.surveiller, principalement de manière pro-active, les différents espaces de l'Internet en vue de détecter et caractériser les infractions : infractions spécifiques (notamment celles liées à l'emploi de botnets ou de malwares), infractions de contenu (notamment la pédopornographie) et infractions de droit commun (notamment les autres atteintes aux mineurs et l'économie souterraine). Cette surveillance peut prendre la forme d'enquêtes sous pseudonyme,
.coordonner les enquêtes sous pseudonyme des unités territoriales de la gendarmerie,
.diriger des enquêtes ou appuyer les offices centraux de la gendarmerie et les unités territoriales en ayant la direction,
.diriger des opérations présentant une particulière envergure, gravité ou sensibilité,
.administrer la base nationale des contenus pédopornographiques issus des enquêtes de police et de gendarmerie (identification des victimes et auteurs), en lien avec INTERPOL et les homologues étrangers,
.proposer un guichet unique téléphonie et Internet (GUTI) assurant l'interface entre les opérateurs et les enquêteurs de la gendarmerie et le lien avec la plateforme nationale des interceptions judiciaires,
.animer la veille technologique et mener des actions internes ou externalisées de recherche et de développement,
.participer à la formation des NTECH et des enquêteurs sous pseudonyme (élaboration des programmes et des supports, enseignement, évaluation, stages ad-hoc), ou d'homologues étrangers,
.participer à la définition des besoins pour l'équipement des NTECH,
.définir ou valider les procédures à mettre en œuvre par les enquêteurs sous pseudonyme et rédiger la documentation associée.

□ les offices centraux de la gendarmerie :
.assister techniquement les enquêteurs de leur office,
.participer aux investigations relatives aux infractions NTECH non spécifiques traitées par leur office ou les diriger,
.assurer, dans le cadre d'une enquête judiciaire donnée, une surveillance ciblée de l'Internet (infractions relevant de l'office), voire une surveillance d'initiative (si nécessaire et si possible, en enquêtant sous pseudonyme), voire une surveillance d'initiative (si nécessaire en enquêtant sous pseudonyme),
.être en contact privilégié avec l'ensemble des enquêteurs NTECH des BDRIJ de leur zone de compétence.

□ les sections de recherches (SR) :
.assister techniquement les enquêteurs de leur unité et, ponctuellement, des autres unités de leur zone de compétence,
.participer aux investigations relatives aux infractions spécifiques NTECH traitées par leur unité ou les diriger,
.assurer , dans le cadre d'une enquête judiciaire donnée, une surveillance ciblée de l'Internet,

□ les brigades départementales de renseignements et d'investigations judiciaires (B.D.R.I.J.):
.animer le renseignement judiciaire sur l'ensemble des infractions liées aux technologies numériques,
.assister les unités de leur département pour la réalisation d'actes d'enquête ou l'examen des éléments de preuves numériques nécessitant une compétence technique ou des outils particuliers,
.assurer , dans le cadre d'une enquête judiciaire donnée, une surveillance ciblée de l'Internet, voire une surveillance d'initiative,
.assister systématiquement les C-NTECH pour toute enquête portant sur une infraction spécifique,
.animer le réseau des C-NTECH de leur département.

La formation des NTECH est assurée par la Gendarmerie en liaison avec l'Université de technologie de Troyes, dans le cadre de la formation continue. D'une durée de 14 mois, alternant scolarité et tutorat, chaque session accueille 16 à 24 stagiaires et se conclut par la validation d'une licence professionnelle [112].

⌞**les investigateurs en cybercriminalité (ICC) de la police nationale**, institués en 2005, date à laquelle ils se sont substitués aux enquêteurs spécialisés en criminalité informatique *(ESCI)* existant depuis 1999, et au nombre de 366 actuellement.

[112] Contenu : cadre et procédure (46h), technologies et architectures numériques (51h), systèmes d'exploitation (60h), Internet et réseaux (55h), recherche d'information (61h), outils forensiques pour informatique et téléphonie (88h), sécurité des systèmes d'information (16h),
partenaires industriels (12h), ouverture et soutien (8h), anglais (74h), travaux en tutorat (160h), mémoire technique (150h).

Missions des ICC

□ à l'O.C.L.C.T.I.C.
.mener des enquêtes de cybercriminalité hautement techniques et liées au crime organisé, ayant un caractère national ou transnational
.assister techniquement les enquêteurs du service et également ceux des autres offices centraux de la police judiciaire et de la sous-direction anti-terroriste
.participer aux investigations relatives aux infractions spécifiques traitées le service,
.participer aux investigations relatives aux infractions spécifiques des autres offices dès lors qu'il existe un besoin d'investigations numériques et que les ICC de ces services ne sont pas en mesure de mener ces recherches,
.assurer, dans le cadre d'une enquête judiciaire donnée, une surveillance ciblée de l'Internet, voire une surveillance d'initiative (si nécessaire en enquêtant sous pseudonyme),
.être en contact privilégié avec l'ensemble des ICC sur le territoire national et le cas échéant leur apporter une assistance technique,
.être formateur à la formation ICC,
.être formateur auprès de pays sollicitant une coopération axée sur la formation
.être formateur des magistrats dans le cadre de leur formation continue
.aider à la mise en place des interceptions et prochainement à la captation de données à distance

□ dans les services spécialisés (*DCPJ, DCRI, IGPN, BEFTI)*
.mener des enquêtes de cybercriminalité hautement techniques dans la limite de leur compétences territoriales. Concernant plus particulièrement la DCRI : prendre en compte attaques cybernétiques visant les opérateurs d'importance vitale.
.assister techniquement les enquêteurs de leur service lors de perquisition et d'analyse de la preuve numérique
.participer aux investigations relatives aux infractions spécifiques traitées par leurs services et apporter conseil et support

□ dans les services territoriaux de l'ensemble des directions *(DRPJ, DIPJ, SRPJ, PAF, DDSP, ...)*
.recevoir des plaintes et mener les premiers actes d'enquête en matière de cybercriminalité dans la limite de leurs compétences territoriales,
.participer aux investigations relatives aux infractions spécifiques traitées par leurs services,
.assister techniquement, collecter et préserver les preuves numériques lors de perquisitions et procéder à des analyses complexes de supports numériques, dans le cadre de leurs propres dossiers, ou ceux des groupes d'investigations de leurs services,
.conseiller les services d'investigations judiciaires dans les dossiers d'infractions liées ou facilitées par l'utilisation des technologies de l'information et de la communication
.être l'interlocuteur des partenaires techniques et avoir un rôle de facilitateur pour les services enquêteurs et auprès des magistrats locaux entre autres,
Maintenir un lien avec l'OCLCTIC sur le plan du renseignement judiciaire mais aussi sur le plan technique,

Leur formation, organisée par l'O.C.L.C.T.I.C., est assurée dans le cadre de 2 sessions par an, chacune d'une durée de 8 semaines sanctionnée par un examen et comprenant 18 à 20 stagiaires [113]. La certification ICC ouvre droit à la reconnaissance d'une certification professionnelle reconnue au RNCP (niveau II, Bac +3/4) à l'issue de 3 ans d'expérience de terrain, et après examen d'un mémoire par un jury de 5 experts.

[113] Contenu : la cybercriminalité et les acteurs de la lutte (2 h), notions générales et élémentaires : l'ordinateur, les systèmes de fichiers, les supports numériques (16h), procédure et arsenal juridique français en matière de cybercriminalité (6h), les réseaux (24h), le traitement des gros volumes de données, bases de données (24h), Linux (24h), distributions Live CD forensics Macintosh et produits Apple (24h),sensibilisation à la cyberpatrouille, plateforme de signalements, interceptions, groupes d'enquêtes OCLCTIC (24h), X-Ways Forensics et outils forensics, copies et exploitations de supports numériques, recouvrement de la preuve numérique (48h).

La formation de ces spécialistes s'inscrit ainsi dans des cursus de carrière distincts et comporte des différences sensibles en terme de contenu et de niveau diplômant.
Il est loisible de s'interroger sur la raison de l'existence de deux formations aussi distinctes, même s'il paraît difficile de remettre en cause des spécificités qui s'inscrivent dans des politiques de formation générale et dans des missions distinctes.
A tout le moins, un référentiel partagé des compétences pourrait être établi afin, en particulier, d'identifier des modules identiques de formation permettant une mutualisation des supports et des moyens de formation *(salle de travaux pratiques, outils d'investigation et forensiques, formateurs).*

Il est à noter que, dès 2014, la police et la gendarmerie nationales ont passé un marché commun pour l'équipement des ICC et des NTECH, piloté par le service des technologies et des systèmes d'information de la sécurité intérieure (STSISI).
De plus, depuis 2008, des formations communes ont été spécifiquement mises en oeuvre concernant l'enquête sous pseudonyme. D'une durée de 4 jours, elles ont permis de former une centaine d'enquêteurs spécialisés.

*****

Quant aux agents des Douanes et de la Concurrence, de la consommation et de la répression des fraudes, le dispositif de formation en vigueur est le suivant :

Les Douanes :

- les agents de Cybderdouane assurent, périodiquement, des actions de sensibilisation au sein des Douanes, dans le cadre des formation préalable et continue *(niveau 1).*

-Depuis 2009, afin de renforcer les compétences techniques des agents, un réseau spécifique, consacré à la cyberdélinquance douanière, a été créé dans les unités de renseignement régionales douanières par la désignation d'un référent, principal interlocuteur de Cyberdouane et formé par ce dernier *(niveau 2).*

-S'agissant enfin des fonctionnaires de Cyberdouane, leur niveau d'expertise résulte de prestations assurées par des intervenants extérieurs ou de formations organisées, sur le plan européen, dans le cadre de l'ECTEG ou du CEPOL ; au surplus, des passerelles ont été mises en place avec la Gendarmerie afin de leur permettre de suivre, le cas échéant, les formations des NTECH dispensées par l'université de Troyes *(niveau 3).*

La Concurrence, la consommation et la répression des fraudes

- l'ensemble des formations sont assurées par *le Centre de surveillance du commerce électronique* sis à Morlaix, dont les agents ont une formation de niveau 3.

- Quant aux autres agents du *Service national des enquêtes*, situés à Paris et dans les 7 antennes interrégionales, ils possèdent une formation de niveau 2, assurée par le Centre précité, et qui est suffisant pour déceler les infractions aux codes de la consommation ou de commerce sur Internet.

Recommandation n° 4
relative à la formation des acteurs pénaux

Eu égard à la spécificité de la cybercriminalité, la formation des magistrats, policiers, gendarmes, douaniers, fonctionnaires des autres administrations contribuant à la lutte contre cette délinquance répond à une impérieuse nécessité. A cet égard, il est préconisé

1.- au lieu de se limiter à la formation de spécialistes, de sensibiliser l'ensemble des acteurs à la cybercriminalité, à ses enjeux et aux modes de traitement existants *(civils comme pénaux s'agissant des magistrats)*, cela dès la formation initiale et dans les différentes écoles de formation. Une telle sensibilisation doit revêtir un caractère obligatoire.

2.- A un deuxième niveau, de systématiser et institutionnaliser la formation de référents dans les différents services territoriaux ainsi que dans les juridictions non spécialisées ; s'agissant de la police et de la gendarmerie, un référentiel commun de compétence des référents est préconisé ; en outre, l'action de ces référents doit s'inscrire dans un réseau structuré animé par des spécialistes de niveau 3.

3.- Au plan des services d'enquête spécialisés, de rapprocher les formations dispensées par la Police et la Gendarmerie, sous la forme d'un référentiel commun. S'agissant des magistrats affectés, soit au plan central, soit au niveau territorial, dans des services ou juridictions disposant d'une compétence spécifique dans la lutte contre la cybercriminalité, une formation plus approfondie doit être obligatoirement mise en oeuvre ; elle pourrait être utilement prolongée par la création d'un réseau social interne favorisant des échanges inter-actifs ainsi que l'entraide.

4.- A tous les niveaux, d'enrichir la formation continue afin d'assurer, sur la base du volontariat ou, s'agissant des spécialistes, de manière obligatoire, l'actualisation des connaissances. Les formations en ligne devraient être privilégiées à cet effet.
Elle devrait, en outre, permettre aux volontaires de poursuivre leur formation par une qualification de type universitaire.

5.- De manière générale, de développer, à l'occasion de la formation, les actions partenariales entre les différents écoles, ainsi qu'avec les acteurs privés compétents, afin de favoriser une approche pluridisciplinaire.

6.- A cette fin mais aussi pour développer l'expertise en matière de lutte contre la cybercriminalité, d'inciter les universités à accroître les formations spécialisées en la matière, sur le modèle de l'université de Troyes ou du diplôme universitaire *"cybercriminalité : droit, sécurité de l'information et informatique légale"* de l'université de Montpellier.

II.4.- Une nécessité : le partenariat public-privé

Pour lutter efficacement contre la cybercriminalité, chacun en est convaincu, l'Etat ne peut agir seul, non seulement car il n'a pas la maîtrise des outils techniques concernés, et notamment d'Internet, mais aussi parce qu'il ne possède pas toujours l'expertise suffisante.

Les enjeux de la lutte contre la cybercriminalité nécessitent donc un dialogue nourri avec l'ensemble des acteurs concernés et dans certains cas la conduite conjointe d'actions opérationnelles communes, qu'il s'agisse de l'analyse de la menace, d'échange d'informations, de recherche et de développement, ou encore, comme on l'a vu, d'actions de prévention ou même de formation.

Un tel objectif n'est en rien contradictoire avec le souhait d'un meilleur encadrement de certaines prestations privées dont il sera question plus avant.

Sans développer l'ensemble des initiatives de ce type, le présent chapitre en présente un certain nombre qui touchent à ce type de partenariats sous différentes formes, et dont certaines ont déjà été évoquées dans les commentaires précédents sur la prévention, tout en formulant de nouvelles recommandations.

1.- Dialogue institutionnel

11. L'observatoire de la sécurité des cartes de paiement (OSCP)

On l'a dit, l'Observatoire de la sécurité des cartes de paiement, créé par la loi sur la sécurité quotidienne de 2001, a été installé en 2003. Original par sa composition et son organisation, il réunit dans un cadre institutionnel les pouvoirs publics *(dont la Banque de France qui en assure la présidence et le secrétariat),* les acteurs du monde économique et social concernés par la sécurité des instruments de paiement, ainsi que des experts nommés au titre de leurs compétences individuelles.

Il a pour missions *(cf. art. L.141-4 et R.141-1 du code monétaire et financier)*

-de suivre la mise en oeuvre des mesures adoptées par les émetteurs et les commerçants pour renforcer la sécurité des cartes de paiement
- d'établir des statistiques en matière de fraude sur la base des informations que lui adressent les émetteurs de cartes de paiement
- d'assurer une veille technologique en la matière, dans le but de proposer des moyens de lutter contre les atteintes de cette nature à la sécurité des cartes de paiement.

Une telle structure permet d'échanger dans un espace de confiance *(les débats sont confidentiels).* Trois réunions plénières ont lieu chaque année, dans l'intervalle desquelles sont réunis des groupes de travail *(statistiques et veille technologique notamment, ainsi que des groupes ad hoc comme celui qui suit les difficultés de mise en place de 3D Secure).* L'OSCP produit un rapport annuel qui permet d'avoir une base statistique de référence sur quasiment l'intégralité de la fraude aux cartes de paiement en France. Le modèle de l'OSCP a été porté au niveau

européen avec le création du *Forum SecuRe Pay*, dont la vocation est toutefois plus large car il a compétence sur l'ensemble des moyens de paiement.

12. Safer Internet France

La France participe au programme européen Safer Internet financé par la Commission européenne au travers du programme *Safer Internet France* placé sous l'égide de *la Délégation aux usages de l'Internet.* Il a pour objectif de mener des actions de sensibilisation et d'accompagnement des jeunes sur Internet.

Depuis 2005, Safer Internet France est placé sous l'égide de la *Délégation aux usages de l'Internet* et s'appuie sur un comité de pilotage faisant appel à des institutionnels, à des associations, à des universitaires et à des prestataires techniques. Il fédère trois services complémentaires en matière d'éducation et de protection des mineurs :

⌞Le programme national de sensibilisation des jeunes aux risques et enjeux de l'Internet – **Internet sans crainte** http://www.internetsanscrainte.fr/ ;
Il propose un éventail complet d'informations et d'outils à destination des enfants, de leurs parents et de leurs éducateurs et intègre, depuis 2010, une plate-forme d'auto-formation en ligne destinée aux animateurs et éducateurs.

⌞Le service de signalement en ligne des contenus choquants - ***Pointdecontact***- géré par *l'Association des fournisseurs d'accès et de service sur Internet (AFA*) [114] http://www.pointdecontact.net ; ce service, mis à la disposition des internautes depuis 1998 mais qui se limitait alors à la pornographie enfantine et à la haine raciale, a été étendu, suite à la loi du 21 juin 2004 sur l'Economie numérique, aux contenus pornographiques violents ou contraires à la dignité humaine dans la mesure où ils sont accessibles aux mineurs, à l'incitation à la violence, à la discrimiantion ou à la haine, à l'apologie de crimes de guerre, de crimes contre l'humanité ou de crimes et délits de collaboration avec l'ennemi, au révisionnisme, à la provocation au terrorisme ou à la fabrication de bombes, enfin à la provocation au suicide [115].

Pointdecontact est accessible par simple clic depuis le portail de chaque prestataire et sur l'ensemble des espaces communautaires.
A la réception de tout signalement, il est procédé à une qualification juridique puis, en cas de contenu illégal, à sa localisation géographique. Si les contenus jugés illégaux sont hébergés en France ou par un membre de l'AFA, l'hébergeur en est informé aux fins de retrait, qui intervient, en principe, dans les 48 heures ; quant aux contenus pédopornographiques hébergés à l'étranger par des sociétés non membres de l'AFA, l'adresse URL du contenu est transmise au partenaire compétent du réseau INHOPE.

Selon le bilan récemment dressé pour 2013, si le nombre de signalements diminue *(5.729 contre 7.195 en 2012),* leur taux de pertinence augmente puisque 32% d'entre eux ont été considérés comme manifestement illicites *(soit 1.815).* S'agissant de ces deniers, 677 ont été transférés à l'OCLCTIC *(dont plus de la moitié ont donné lieu à dénonciation à Interpol comme concernant*

[114] l'AFA regroupe tant des hébergeurs en ligne que des fournisseurs d'accès ou de moteurs de recherche et des plates-formes du web, notamment BOUYGUES TELECOM, GOOGLE France, MICROSOFT, ORANGE et S.F.I.

[115] En revanche, l'association internationale de hotlines Internet *"INHOPE"*, qui rassemble 44 membres dans 38 pays et notamment *Pointdecontact*, membre fondateur dès 1999, lutte exclusivement contre la pédopornographie.

des sites étrangers, en grande majorité pédopornographiques), 193 transmis aux hébergeurs français et membres de l'AFA *(qui ont effectué 177 retraits)* et 325 à un partenaire étranger du réseau *INHOPE (à l'origine de 306 retraits).*Si, sur le total des signalements qualifiés, le tiers a trait à la pédopornographie, l'association constate une forte progression des contenus à connotation raciste ou violente.

Les pratiques de l'AFA reposent sur une charte, signée le 14 juin 2004, dite *"Charte contre les contenus odieux"*, qui définit les contributions des prestataires et à laquelle est associée un label *"Net+sûr".*

⌐Le numéro national d'accueil et d'assistance pour la protection des jeunes **Net Ecoute** *(0800 200 000)* ainsi que son chat en ligne sur http://www.netecoute.fr/, géré par *l'association e-Enfance*.

Cette ligne d'assistance, ouverte depuis décembre 2008, est accessible gratuitement, et des personnes spécialement formées répondent à toutes les questions concrètes que se posent les enfants, les adolescents et les parents sur Internet fixe et mobile *(aide à l'installation des logiciels de contrôle parental, conseils sur l'utilisation sécurisée d'Internet fixe et mobile pour les jeunes, aide psychologique en cas d'images choquantes, de harcèlement, de mauvaises rencontres, de pédophilie, de dépendance à internet ou aux jeux vidéos en ligne).*

En outre, chaque année, le ***"Safer Internet Day"***, organisé simultanément dans trente pays de l'Union, permet la mobilisation d'un grand nombre de partenaires autour d'un thème commun, le thème retenu pour 2014 étant *"Ensemble pour un meilleur Internet".*

13. PHAROS

Placée au sein de l'O.C.L.C.T.I.C., la plate-forme officielle PHAROS de signalement des contenus illégaux ou des activités illégales sur Internet est animée par des policiers et des gendarmes qui traitent les signalements des internautes [116].

Créée en 2009, elle présente l'intérêt de mobiliser les internautes qui souhaitent alerter les pouvoirs publics sur des contenus ou des comportements répréhensibles et dangereux recensés sur des sites Internet, des blogs, des forums... Au-delà des internautes individuels, ce site s'adresse aussi aux professionnels, actuellement une centaine qu'il s'agisse d'hébergeurs, de fournisseurs d'accès ou de service, de blogs ou de forums, de réseaux sociaux, de jeux en ligne, d'annonçeurs, d'associations... Avec certains acteurs d'ailleurs, des accès privilégiés ont été mis en place et des protocoles signés pour permettre une transmission plus efficace des informations *(dont la plateforme Pointdecontact.net de l'AFA évoquée plus haut ou certains réseaux sociaux français comme Skylogs, voire, récemment, certaines associations de consommateurs).*

Elle permet aussi aux pouvoirs publics de disposer d'une vision plus globale de la cybercriminalité et de ses tendances ainsi que des attentes des internautes..

---

[116] toutefois PHAROS n'a pas vocation à recevoir des signalements portant sur des infractions matérialisées ou révélées par des correspondances entre personnes mutuellement identifiées *(par exemple, courriels de menace)*, ni sur des infractions qui supposent un dépôt de plainte avant toute poursuite éventuelle *(injures, diffamation...)*

En 2012, PHAROS a reçu 119.788 signalements, soit une augmentation de 12% par rapport à 2011. Ces transmissions ont nécessité 321 enquêtes préliminaires ou de flagrance afin d'identifier les auteurs des faits et de déterminer les compétences territoriales, essentiellement pour des infractions concernant des mineurs. En outre, les enquêteurs habilités de PHAROS ont eu recours, en cas d'anonymisation, à la *"cyber-infiltration"* dans quelques dizaines de cas. A l'issue de ces investigations, PHAROS a effectué 7.187 transmissions - dont 1.329 aux fins d'enquête à des services de police judiciaire, 689 aux Douanes, 915 à la DGCCRF, 465 à la direction centrale du renseignement intérieur, enfin 3.970 à des services étrangers via Interpol pour des contenus pédopornographiques et des sites de *phishing.*

Il est à noter que, même si PHAROS, qui ne concerne que les infractions supposées, n'a pas vocation à se voir signaler des faits relevant de l'urgence opérationnelle*,* 484 procédures d'urgence vitale *(annonces de suicide)* ont été traitées en 2012.

La récente circulaire interministérielle du 19 juillet 2013 et l'arrêté du 3 octobre 2013 vont permettre, non seulement de rendre PHAROS accessible aux services d'enquête par le biais de personnels spécialement désignés et habilité *(Police, Gendarmerie, Douane, DGCCRF)*, mais aussi de mieux adapter les réponses juridiques et opérationnelles :

☞D'une part, la pratique de la communication d'informations à des organisation de coopération internationale en matière de police judiciaire est officialisée.

☞D'autre part, l'OCLCTIC pourra, désormais, à son initiative, communiquer des informations aux services d'enquête, dans le cadre de son travail d'orientation et de rapprochement, mais aussi aux opérateurs de communication électronique et prestataires techniques *(hébergeurs et fournisseurs d'accès),* enfin aux services de l'URSSAF*.*

Les objectifs poursuivis par la communication aux prestataires s'inscriront, pour partie, dans le processus de notification/action prévu par l'article 6 de la loi du 21 juin 2014, et, pour autre partie, dans un cadre purement partenarial : partant du constat que le cyber-escroc a recours, à un moment ou à un autre, aux courriels pour finaliser les manoeuvres frauduleuses en direction de ses victimes, courriels qui ont pour origine une même adresse e-mail quel que soit le nombre de ces dernières, l'objectif consiste, à l'instar des pratiques Canadiennes, de supprimer ces adresses pour couper les liens avec les victimes et ainsi prévenir la finalisation de nombreuses escroqueries.

Un projet de convention à cette afin a été rédigé avec les sociétés Google pour les adresses *"gmail"*, Microsoft pour les adresses *"hotmail"* et Yahoo pour les adresses du même nom, étant entendu que, sur le plan juridique, la coupure des adresses est prévu par les conditions contractuelles d'utilisation liant les clients et les fournisseurs de messages électroniques dès lors qu'elles sont utilisées à des fins frauduleuses.

Il importe toutefois que, concomitamment, PHAROS soit en mesure de systématiser le retour d'information aux auteurs de signalements, d'affiner les traitements de ces derniers ainsi que les suites données.

Il conviendrait enfin d'unifier les plates-formes publiques existantes et de fusionner le portail officiel *"internet-signalement.gouv.fr"* avec PHAROS.

2.- Dialogue partenarial

21. Signal Spam
http://www.signal-spam.fr

Créée en 2003 sous l'impulsion des services du Premier ministre, l'association *Signal Spam* rassemble des représentants des pouvoirs publics membres de droit *(dont la CNIL mais aussi la DGCCRF ou les services concernés du ministère de l'intérieur, avec une implication toute particulière de la DGGN),* des opérateurs de communications électroniques *(Orange, SFR, Google),* des routeurs de messagerie électronique et des entreprises œuvrant dans la sécurité numérique. Elle est intégralement financée sur fonds privés.

Cette association gère une plate-forme de signalement par les internautes des spams, au travers d'une interface Web ainsi que des applications intégrées directement aux principaux logiciels de courrier électronique du marché. Ces informations sont directement retransmises aux acteurs concernés : ainsi les opérateurs peuvent prendre des mesures lorsqu'un de leurs abonnés émet – à son insu ou non – des messages non sollicités, et les routeurs de messagerie électronique peuvent identifier certains de leurs clients qui commettraient des abus et bloquer les campagnes problématiques ; les services d'enquête peuvent aussi obtenir sur réquisition des informations très utiles lors de certaines investigations judiciaires. A titre d'exemple, la CNIL est destinataire chaque mois d'une liste des campagnes de courrier électronique ayant été l'objet du plus grand nombre de plaintes et l'ANSSI reçoit des informations sur différentes sources de spams dans l'administration, qui manifestent, souvent, l'existence d'ordinateurs infectés par des *botnets. Signal Spam* répond aussi aux réquisitions des services spécialisés de police judiciaire. Sa pertinence en matière de partenariat public-privé a été mise en évidence à la fois au plan de l'Union Européenne et par les institutions officielles françaises.

En 2012, selon son rapport d'activité, *Signal Spam* a reçu, en 2012, 2.454.369 signalements concernant des adresses émettrices majoritairement localisées en France, mais aussi aux Etats-Unis, en Allemagne...

Signal Spam a aussi mis en place une charte de déontologie dont la mise en œuvre s'applique à l'ensemble de ses membres mais aussi à l'ensemble des entreprises destinataires de boucles de rétroaction. Cette charte ne se contente pas de rappeler la législation existante, mais propose des mesures d'implémentation communes, conformes aux grands standards internationaux de sécurité du courrier électronique.

Des rapprochements sont envisagés entre ce dispositif et *Phising Initiative* qui suit, rapprochements qui supposent toutefois de recourir à des moteurs d'analyse capables de détecter dans les spams les contenus de type *Phishing.*

Il est à souligner que, s'agissant des spams visant les mobiles, *l'Association Française du multimédia mobile (AFMM)* - fondée par Bouygues Télécom, Orange France, S.F.R., la Fédération Française des télécoms et Mobile marketing Association (MMA) - a créé, en novembre 2008 et en réponse à une initiative gouvernementale, une plate-forme dédiée : **33.700**. Au 1er septembre 2012, elle avait reçu plus de 5 millions de signalements , dont 3,7 ont été identifiés comme des spams, auxquels s'ajoutent 350.000 autres signalements de spams oraux *(incitant, le plus souvent, à rappeler un n° surtaxé).* Après examen notamment pour distinguer les spams des promotions ou offres commerciales licites, chaque opérateur adresse aux éditeurs indélicats des rappels ou des mises en demeure, voire coupe les n°s correspondants et résilient les contrats.

22. Association Phishing Initiative
http://www.phsihing-initiative.com

Cette association, créée en 2011, regroupe MICROSOFT, PAYPAL et le Cert-Lexsi. Elle a pour but de prévenir les tentatives de hameçonnage par lesquelles les escrocs accèdent aux informations personnelles et bancaires d'une victime en usurpant l'identité d'une organisation publique ou privée digne de confiance.

> A cette fin, *Phishing Initiative* met à disposition des internautes un site en ligne, fonctionnant en permanence, afin de signaler les URL (= adresses) suspectées de rediriger vers un site de phishing. L'association vérifie chaque signalement en temps réel *(1/4 d'heure en moyenne)* et, lorsque la nature malveillante de l'adresse est confirmée, la transmet aux éditeurs des principaux logiciels de navigation sur Internet*(Firefox, Internet Explorer, Google Chrome et Safari)* aux fins de blocage des sites frauduleux dans les navigateurs. Les internautes sont avisés du résultat de l'analyse et, en cas de sites frauduleux, sont ainsi dissuadés d'y répondre.
>
> Selon le rapport 2012 de l'association, 30.000 signalements avaient été opérés la 1ère année d'ouverture du site ; leur nombre s'est élevé à 50.000 en 2012 concernant 37.000 URLs dont 24.699, soit les 2/3, se sont avérés comme hébergeant un contenu frauduleux de type *phishing.*
> Il s'y est ajouté 5.000 autres URLs. frauduleux supplémentaires identifiés par le Cert-Lexsi comme visant le public francophone. Cette croissance est due à la plus grande notoriété de la plate-forme mais aussi à la multiplication du nombre d'escrocs.

PHAROS, qui reçoit aussi des signalements sur les sites de *"phishing" (22.000 signalements recensés depuis la création du dispositif jusqu'à fin août 2013)*, étudie la possibilité de transmettre ces derniers à *Phishing Initiatives* sur la base du récent arrêté déjà cité ; une convention est en cours d'élaboration.

23. Forum international sur la cybersécurité

D'abord appelé Forum international sur la cybercriminalité et organisé à l'initiative de la gendarmerie nationale, le Forum International sur la Cybersécurité est devenu une grande conférence internationale de référence. La sixième édition a eu lieu les 21 et 22 janvier 2014 et, outre des conférences et plus de 40 ateliers ou tables rondes, elle a accueilli cette année un défi criminalistique permettant à des étudiants de tester leurs capacités dans l'investigation numérique. Cette conférence permet d'établir un dialogue riche avec l'ensemble des acteurs de la cybersécurité. Elle est coorganisée par la Gendarmerie nationale, le conseil régional du Nord-Pas-de-Calais et la société CEIS.

3.- Recherche et formation

Des relations ont été nouées entre les différents services de l'Etat et des établissements de formation ou de recherche. On peut citer le partenariat liant l'O.C.L.C.T.I.C. à l'EPITA, la licence professionnelle développée par la Gendarmerie nationale avec l'Université de technologie de Troyes ou encore l'accueil par l'Université Montpellier 1 de magistrats dans son diplôme d'université sur la cybercriminalité, qui figure désormais dans le catalogue de formation de l'Ecole nationale de la magistrature. Ponctuellement ou de façon plus prolongée des échanges ont lieu avec beaucoup d'autres entités, à l'occasion de projets de recherche et développement financés par des ressources extérieures *(Commission européenne, Agence nationale pour la recherche)* ou par les entreprises elles-mêmes, de visite et d'échanges ou d'accueil de stagiaires par les services spécialisés.

Des initiatives partenariales plus larges ont été nouées ou sont en cours de construction, par lesquelles :

31. CECyF – Centre expert Français contre la cybercriminalité

Le projet européen *2CENTRE (Cybercrime centres of excellence network for training, research and education)* est né des échanges animés par EUROPOL pour l'harmonisation de la formation à la lutte contre la cybercriminalité. Il a notamment permis en France, grâce à l'association de la Gendarmerie, de la Police, de partenaires privés *(Thalès et Microsoft France)* et d'universités *(l'Université Montpellier 1 et l'Université de Technologie de Troyes)* de développer de nouveaux outils de formation *(formation en ligne sur l'analyse de Windows 7 ou encore à destination des « premiers intervenants » donc de tous les enquêteurs),* de consolider la documentation des formations existantes ou encore de mener plusieurs études et un projet de recherche et développement appliqué. L'Irlande, mais aussi l'Allemagne, l'Angleterre, la Belgique, la Bulgarie, l'Estonie et la Roumanie poursuivent des projets similaires.

C'est dans ce cadre que le ***Centre expert contre la cybercriminalité français*** vient d'être créé en janvier 2014 sous la forme d'une association de la loi de 1901, qui vise à fédérer l'action partenariale en matière de sensibilisation, de formation et de recherche entre les acteurs privés et publics concernés par la lutte contre la cybercriminalité.

Le CECyF constitue un espace de rencontre pour la création de projets collaboratifs contre la cybercriminalité, pour donner de la visibilité à ces projets – et en particulier aider à trouver le financement de ces projets et support juridique et opérationnel de certains aspects de ces initiatives *(communication, conférences, hébergement de plateformes collaboratives de développement, etc.)* -. Cette structure a vocation à accueillir tous les services d'enquête et les administrations contribuant à la lutte contre la cybercriminalité ainsi que d'autres établissements d'enseignement *(comme l'EPITA qui a déjà un partenariat privilégié avec l'OCLCTIC, mais aussi l'Institut Mines-Télécom)* et des entreprises de différents secteurs concernées par ces questions.

Les premiers projets proposés aux membres au cours de l'année 2014 tourneront autour des thématiques suivantes dans l'optique de la lutte contre la cybercriminalité) :

.développement d'outils opensource d'investigation numérique ;
.contribution à la création de supports de sensibilisation ;
.développement de formations à distance *(pour les services d'investigation, mais aussi à destination des acteurs du secteur privé ou des collectivités locales*) ;
.partage d'information et nouvelles études sur les besoins en formation et cartographie des formations disponibles ;

.participation à des conférences pour dynamiser les échanges entre les différentes communautés sur les différents aspects de la prévention et de la lutte contre la cybercriminalité ;
.et enfin, ateliers pour l'identification et la construction de nouveaux projets.

Des sujets comme la création ou la contribution à une revue spécialisée, le soutien ou le lancement d'une conférence francophone sur la réponse à incidents pourraient être rapidement mis en œuvre.

32. AFSIN – Association francophone des spécialistes de l'investigation numérique

Créée en 2006, cette association regroupe des enquêteurs spécialisés, des experts judiciaires et des magistrats de toute la francophonie traitant de l'investigation numérique au sens large. Pour la France, toutes les administrations sont représentées. Elle organise chaque année une conférence sur trois jours : *les Journées francophones de l'investigation numérique* dont la prochaine édition se tiendra à Nancy en partenariat avec le LORIA en octobre 2014. Des tables rondes sont aussi ponctuellement organisées au cours de l'année pour réfléchir sur des sujets divers.

33. ADIJ - Association pour le développement de l'informatique juridique
http://www.adij.fr/association/

Fondée le 23 mars 1970, l'ADIJ - qui regroupe de nombreux professionels du droit, publics ou privés, mais aussi des professeurs, des chercheurs et des éditeurs - est, à la fois, un point de rencontre et d'échange interprofessionnel, un lieu d'information et de formation et un organisme de recherche interdisciplinaire en ce qui concerne les questions juridiques posées par le développement des technologies et les technologies au service de la diffusion du droit et du fonctionnement de la justice.

> Cette association mène une action dynamique et constante pour la diffusion de l'information juridique ; elle a, par exemple, réalisé, à la demande de l'Union européenne, une importante étude - *"EDIJUSTICE"* - qui portait sur les problèmes posés par les échanges informatisés en matière judiciaire tant en droit français qu'en droit comparé. Ces services d'information juridique électronique se diversifient *(banques de données télématiques, services vidéotext, sites internet, systèmes experts, réseaux neuromimétiques...)*, dans le but de permettre aux praticiens, notamment les avocats, de disposer et de pouvoir traiter de la documentation utile.
>
> Elle suit en outre l'actualité législative française et tient des conférences plénières au Parlement sur les défis juridiques de la révolution Internet ou sur la valeur probatoire des documents électroniques, notamment à l'occasion des *"mardis de l'ADIJ"* ou dans le cadre des *"ateliers de l'ADIJ".*

34. CYBERLEX
http://www.cyberlex.org/

Cette association du droit et des nouvelles technologies, créée en 2006, regroupe, à la fois, des techniciens, des juristes d'entreprise, des avocats, des magistrats, des professeurs de droit ainsi que des professionnels du marché et des technologies numériques. Elle organise des échanges réguliers sur le droit de l'Internet.

35. Le CLUSIF
http://www.clusif. asso.fr

Comme il a déjà été précisé, il s'agit d'un club professionnel constitué en association indépendante et ouvert à toute entreprise ou collectivité. Sa finalité est d'agir pour la sécurité de l'information et d'y sensibiliser tous les acteurs. Il présente, tous les ans, un panorama de la cybercriminalité en terme de tendances et de modes opératoires, et anime de nombreux groupes de réflexion sur le management des risques, l'intelligence économique...

36. Défense et stratégie
http://www.defense-et-strategie.fr

Face au développement des problèmatiques de sécurité liées aux systèmes d'information et aux enjeux fondamentaux qu'elles comportent pour la défense et la sécurité de la France, *Défense et Stratégie* a créé, en mai 2012, le *CyberCercle*, qui se veut un lieu privilégié d'échanges autour de ces problématiques ; sa vocation, outre l'avancée de la réflexion, consiste à sensibiliser les décideurs et les relais d'opinion à la problématique de sécurité des systèmes d'information, de cyberdéfense et de lutte contre la cybercriminalité.

37. Le CESIN
http://cesin.fr/

Le *Club des experts de la sécurité de l'information et du numérique (CESIN)* est une association ayant pour objet de favoriser l'échange de connaissances, le partage d'expériences et la coopération entre professionnels de la sécurité de l'information et du numérique. Il est composé d'experts occupant des postes de responsabilité dans la sécurité de l'information et du numérique au sein d'entreprises privées ou publiques, mais aussi des spécialistes du droit de la sécurité ; y sont associés les représentants des services de l'Etat .

4. Recommandations

Outre les propositions déjà faites au titre de la prévention ou de celles qui seront formulées au titre de l'organisation étatique, il est préconisé d'étendre le champ du partenariat public/privé dans deux directions.

☞ Extension du champ de compétence de l'Observatoire de la sécurité des cartes de paiement

Il est proposé d'étendre le champ de compétences de l'OSCP au moins à ce qui est maintenant inclus dans les articles répressifs du code monétaire et financier *(cf. article L133-4 du CMF),* à savoir l'ensemble des instruments de paiement autres que le chèque. L'intention étant notamment de couvrir en plus des cartes de paiement :

- la banque en ligne *(ciblée massivement par la criminalité numérique au travers de virus informatiques spécialisés*), cette question paraissant relever davantage de la compétence de *l'Autorité de contrôle prudentiel*, qui devrait alors être modifiée à cet effet ;
- les virements SEPA *(notamment lorsqu'ils sont créées par voie électronique*) ;
- les monnaies et comptes de paiement électroniques
- voire la devise numérique que constitue le bitcoin, principalement utilisée pour des transactions, légales ou illégales, sur Internet, et au sujet de laquelle les autorités monétaires ont récemment émis une mise en garde compte-tenu du caractère hautement spéculatif de cette devise et des piratages dont font souvent l'objet les portefeuilles numériques.

Il s'agit, tout à la fois, de mieux appréhender ces instruments, la place prise dans les paiements, les risques qui y sont liés en terme de cybercriminalité, et d'identifier les réponses, normatives ou partenariales, nécessaires à une meilleure protection du consommateur et de l'usager. Cette proposition est cohérente par rapport à la démarche de l'Union européenne.

Recommandation n° 5
relative à l'extension des attributions
de l'Observatoire de la sécurité des cartes de paiement

Etendre la compétence de l'Observatoire à l'ensemble des instruments de paiement autre que le chèque, afin de mieux les appréhender, d'identifier les risques en terme de cybercriminalité et de proposer les réponses de nature à mieux protéger le consommateur et l'usager.

☞ Création d'un CERT*FR *"tous publics"*

Un "CERT" *(Computer emergency response team, marque propriété de l'université Carnegie Mellon)* - parfois aussi appelé *"CSIRT" (Computer security incident response team)* est un centre d'alerte et de réaction aux attaques informatiques ; selon qu'il couvre

> tout un pays, une région, un secteur donné *(un secteur économique particulier, les membres d'un groupement d'entreprises, un opérateur...),* le CERT reçoit donc les alertes relatives aux incidents correspondants, les analyse et, le cas échéant, y apporte une réponse opérationnelle, qui peut aller de la transmission de l'information aux bons interlocuteurs jusqu'au traitement complet de l'incident. Par-delà, le CERT effectue une veille d'informations sur la sécurité et la partage avec la communauté ou le public concerné.

A ce jour, il existe en France un CERT-FR *(ancien CERTA)*, animé par l'ANSSI, pour les administrations et les opérateurs d'importance vitale *(O.I.V.)*, ainsi que quelques CERT professionnels pour les grandes entreprises ou certains types de métiers qui ont clairement identifié le risque lié à la cybercriminalité. En revanche, il n'existe pas de CERT généraliste relatif aux besoins du grand public ou au secteur des petites et moyennes entreprises en général.

Il est ainsi préconisé [117] la création – à l'instar de ce qui existe dans d'autres pays comme le Luxembourg, la Finlande ou encore la Suisse – d'une structure *(associative a priori)* jouant ce rôle. Une telle organisation aurait d'abord un rôle préventif et de sensibilisation vers ces publics et ensuite vocation à traiter l'ensemble des signalements qui n'auraient pas de CERT dédié. Il pourrait aussi servir de portail pour orienter *(comme le fait le site cert.nl aux Pays-Bas)* vers les CERT chargés des différents secteurs ou entreprises *(ou encore les services Abuse)*. Il aurait vocation enfin à accompagner l'émergence de tout CERT sectoriel en France y compris si celui-ci le déchargeait d'une partie de ses missions propres.

Dans ce contexte, ce CERT*FR pourrait être l'occasion d'**inciter à un rapprochement plus fort ou à une coordination plus forte entre les initiatives non étatiques existantes - Signal Spam, Phishing Initiative et le 33700 -** ainsi qu'avec Safer Internet, dans le but de donner davantage de visibilité aux possibilités offertes aux internautes *(cf. le chapitre 2 relatif à la prévention)*.

Les services officiels auraient une place naturelle aux côtés ou au sein de ce centre. Ce serait l'occasion d'orienter plus rapidement et plus efficacement les victimes et les partenaires étrangers vers la bonne plate-forme en fonction du problème *(l'ANSSI comme CERT des OIV et des réseaux de l'Etat, PHAROS pour les signalements de contenus illégaux, Signal Spam pour le spam, etc...).*

[117] notamment par la société MICROSOFT France

Recommandation n° 6
relative à la création d'un CERT

Créer un CERT (*centre d'alerte et de réaction aux attaques informatiques)* afin de répondre aux besoins des secteurs économiques, des populations ou des territoires non encore couverts par les CERT existants en France :
- sous la forme d'une structure associative, associant notamment des grands opérateurs français
- travaillant en coopération avec l'ensemble des CERT français et notamment le CERT-FR animé par l'ANSSI
- ayant notamment pour objectif de diffuser des informations de sensibilisation au grand publics, aux petites et moyennes entreprises et aux collectivités locales
- et de rediriger les CERTs étrangers vers les CERTs français correspondant aux secteurs visés ou en transmettant lui-même les informations provenant de l'étranger aux opérateurs et hébergeurs français ne relevant pas de l'autorité d'un CERT existant.

De manière générale, si de tels partenariats sont efficients et riches d'avenir, il convient toutefois de veiller dans le même temps, à éviter une prolifération susceptible de générer des doublons et, s'agissant des dispositifs axés sur les usagers, un manque de visibilité.

II.5.- Une condition : la réorganisation des services de l'Etat, la création d'une délégation interministérielle et d'une mission Justice

La prise de conscience de l'importance de la cybercriminalité est récente, comme le sont, par voie de conséquence, les normes en la matière et l'organisation des services de l'Etat.

Cette dernière s'est traduite par la création de services ou de bureaux spécialisés dans différents départements ministériels et par l'émergence corrélative de spécialistes motivés et de haut niveau bien qu'en petit nombre.

Parallèlement, diverses autorités indépendantes ou assimilées ont été créées au fil de l'eau à coté de la plus importante d'entre elles, *la Commission nationale de l'informatique et des libertés.*

Par delà, l'engouement pour le numérique mais aussi sa forte technicité ont généré une multiplication des *"sachants"* comme des initiatives diverses, publiques ou privées, relativement peu coordonnées et parfois concurrentes.

L'absence de toute structure de coordination oblige ainsi chaque service, voire chaque spécialiste, à tenter de compenser cette carence en multipliant les échanges inter-personnels, qui restent toutefois impuissants à arrêter une stratégie d'ensemble et à gérer les inéluctables chevauchements et conflits de compétence.

Plusieurs des auditions réalisées par le groupe interministériel ont révélé une forte attente à ce sujet, en terme de mise en cohérence et de clarification stratégique, notamment de la part des victimes individuelles comme des entreprises, mais aussi des services locaux de police et de gendarmerie comme des parquets.

Les travaux même du groupe ont aussi mis en exergue, d'une part, les liens étroits entre les questions de sécurité technique ou d'industrialisation et celles tenant à l'activité proprement répressive ; d'autre part, l'intérêt d'une démarche commune par exemple en matière de prévention, de base de connaissance ou d'échange des pratiques ; mais aussi pour ce qui a trait aux relations avec les sociétés privées participant à l'hébergement ou à la fourniture des données numérisées ; ou encore dans le domaine international, particulièrement prégnant en la matière.

Enfin, les contraintes budgétaires plaident en faveur d'une bonne gestion des rares moyens disponibles.

Les attentes sont également très fortes à l'égard de la Justice, en terme de *pilotage juridique*, mais aussi de spécialisation, de présence internationale et de politique pénale.

Elles ne sont pas non plus absentes s'agissant de l'organisation des services d'investigation.

.

Rien d'original dans un tel constat puisque l'émergence de chaque nouveau type de criminalité génère, historiquement, après les années "pionnières", un besoin accru d'organisation. Telle est d'ailleurs la démarche que poursuivent, en matière de lutte contre la cybercriminalité, plusieurs autres Etats, comme le montrent les études de droit comparé.

En résumé, **la spécificité comme le développement de cette délinquance, les enjeux qu'elle représente appellent aujourd'hui une nouvelle efficacité de l'Etat, qui passe notamment par une réforme de son organisation à trois niveaux**.

1.- la question du pilotage étatique

Si, s'agissant du développement de l'économie numérique et de la lutte contre la fracture numérique, ils sont assurés par un département ministériel spécifique, *la Délégation interministérielle à l'intelligence économique* et *la Délégation aux usages de l'Internet* ; si, s'agissant de la cyberdéfense, elle est confiée au *Secrétariat général de la Défense*, placé directement sous l'égide du Premier ministre ; si, concernant la sécurité technologique et la réponse technique aux cyber-attaques, ils relèvent, du moins pour les entreprises considérées comme sensibles, de *l'Autorité nationale de la sécurité des systèmes informatiques (ANSSI)*, elle aussi placée sous la responsabilité du Premier ministre ; il n'y a pas d'organisation comparable pour la lutte contre la cyber-criminalité, partagée entre la police et la justice et de nombreuses administrations spécialisées, tandis que les autorités administratives indépendantes existantes, dont la compétence est souvent limité à un secteur particulier *(protection des données nominatives, jeux en ligne, protection des droits d'auteur...),* n'ont pas vocation à jouer un rôle fédérateur.

Or, **chacun s'accorde à considérer qu'il est aujourd'hui nécessaire de renforcer la synergie dans la lutte contre cette forme de délinquance et de répondre à un besoin d'impulsion et de coordination qui ne saurait être satisfait que dans un cadre interministériel eu égard à la dispersion des acteurs et à la multiplicité des compétences**. Enfin, une telle organisation manifesterait , de manière tangible, l'importance qu'attachent les pouvoirs publics à cette lutte ainsi que leur volonté d'accroître son efficacité.

La question s'est d'ailleurs posée de savoir s'il ne faudrait pas préconiser, comme dans certains Etats étrangers, un pilotage interministériel unique pour le cyber-espace, rassemblant l'ensemble des trois pôles précités. Pour des raisons tenant tant au mandat reçu par le groupe, que des organisations déjà mises en place, de la spécificité de chacun de ces pôles et de la confidentialité qui s'y attache, la solution préconisée se limite à l'organisation d'un pôle interministériel consacré à la lutte contre la cybercriminalité.

Le groupe de travail entend toutefois souligner, à nouveau, l'importance que revêtent les échanges entre les différents pôles, notamment en terme de mise en cohérence sur le plan de la norme comme des actions de sensibilisation et de soutien, mais aussi concernant la recherche de solutions techniques aux questions que pose la cybercriminalité, compte-tenu des interactions évidentes mises en exergue.

A tout le moins, la création d'un niveau interministériel pour la cybercriminalité devrait favoriser des réunions de convergence entre les trois pôles.

Concrètement, **une telle création doit prendre la forme d'une délégation interministérielle spécifique, placée sous la responsabilité directe du Premier ministre et non rattachée à un département particulier**.

Certes, la prolifération de telles structures peut poser problème, notamment dans le domaine répressif compte-tenu du rôle spécifique assigné notamment par la loi à l'institution judiciaire, mais aussi au Garde des Sceaux *(cf. l'art.30 du C.P.P., modifié par la loi n° 2013-669 du 25.07.2013, qui confie à ce dernier "la conduite de la politique pénale déterminée par le Gouvernement")*, et encore au ministre de l'Intérieur *(cf. la politique de sécurité),* mais le besoin d'une stratégie globale et d'une coordination des différents services étatiques paraît devoir primer. En outre, plusieurs précédents existent en la matière, notamment en ce qui concerne *la sécurité et la circulation routière (délégation), la lutte contre la drogue et la toxicomanie (mission), la lutte contre le racisme et l'antisémitisme (délégation),* ou, plus récemment, *la prévention et la sécurité en milieu scolaire (délégation)...*

Le groupe de travail est toutefois conscient de la nécessité d'éviter certains risques inhérents à ce type de structures interministérielles ainsi que les critiques qui peuvent parfois être adressées à certaines d'entre elles, en terme de spécificité, voire d'utilité réelle ; d'autres ont tendance à s'ériger en entités autonomes, dotées souvent d'effectifs et de moyens budgétaires sans comparaison avec ceux des administrations techniques et qui ne coordonnent pas suffisamment leurs actions avec ces dernières ; d'autres sont même le théâtre de luttes d'influences entre certains départements ministériels qui nuisent à l'action.

La délégation préconisée doit être, au contraire, un lieu d'impulsion et de mise en cohérence ; elle doit oeuvrer en étroite liaison avec les administrations et services afin de leur apporter précisément ce qui manque aujourd'hui à l'action commune et dans le respect des missions spécifiques de chacun. Elle peut aussi avoir vocation à se substituer à certaines instances existantes.

Les missions de cette délégation, qui doivent être strictement définies, devraient porter sur la définition d'une stratégie d'ensemble, en synergie avec les autorités compétentes en matière de cyberdéfense et de sécurité des systèmes d'information ; en liaison avec le ministère de la Justice, sur la préparation des projets de textes relatifs à la lutte contre la cybercriminalité, en veillant à leur harmonisation et à leur mise en cohérence ; sur l'appréhension et la connaissance statistique de la cybercriminalité ; sur l'impulsion et la mise en cohérence s'agissant de la prévention ; sur un rôle de vigilance en terme de formation ; sur l'interface avec le secteur privé, en assurant, tout particulièrement, le monopole des négociations avec les prestataires techniques de l'Internet, mais aussi un rôle de médiation entre ces derniers et les internautes *(voir les développements sur les victimes titre III, chapitre 6)* et de mise à exécution des décisions de justice ayant trait à Internet ; enfin sur la représentation et la participation aux négociations internationales [118],

La délégation ne devrait, en aucune façon, interférer avec l'opérationnel.

Certains de ses points seront développés ultérieurement.

---

[118] cf., sur ce point, les précédents que constituent l'exemple de *la Mission interministérielle de lutte contre la drogue et la toxicomanie* ou la *Délégation à la lutte contre le racisme et l'antisémitisme.*

Il importe néanmoins d'insister sur la plus-value que devrait apporter cette délégation en terme de meilleure articulation des politiques administratives et des politiques strictement répressives.

Le groupe interministériel est bien conscient que chaque type de cyber-criminalité donne lieu à de fortes attentes spécifiques, comme l'illustre le chapitre consacré aux attentes. Mais il est convaincu qu'une plus grande effectivité dans la lutte contre la cybercriminalité passe, d'abord, par la recherche d'un meilleur "pilotage" et d'une plus grande cohérence, en terme de connaissance, d'instruments juridiques, de recours au partenariat...**C'est par référence à ce cadre global commun que pourront utilement prospérer des pôles spécifiques, existants ou à créer, pour tel ou tel aspect de cette délinquance.**

La problématique est similaire s'agissant du **partenariat** ; **le groupe interministériel est conscient de ce qu'on lui doit et des perspectives qu'il offre pour l'avenir. Il ne saurait, pour autant, tenir lieu de politique de l'Etat.**

Encore faut-il que la future structure préconisée sache, tout à la fois, associer ces pôles spécifiques ainsi que les principaux partenaires, tant publics que privés ; telle est la condition de sa réussite.

En terme d'architecture, outre le *délégué et le comité interministériel* qui, classiquement, regroupe les ministres concernés mais qui devrait être aussi ouvert aux responsables des principales Autorités indépendantes, cette délégation devrait comprendre une structure type *observatoire* chargée spécifiquement de l'analyse de la menace et des questions statistiques, une structure type *agence de régulation* qui aurait la haute main sur tout ce qui concerne les normes et les relations avec les prestataires techniques d'Internet, *un collège des chefs de service spécialisés dans la lutte contre la cybercriminalité* afin d'institutionnaliser, au-delà des relations inter-personnelles, les échanges/métier favorisés par le groupe de travail, mais aussi un *collège scientifique* rassemblant les principaux *sachants* tant du public que du privé.

Recommandation n° 7
relative à la création d'une Délégation interministérielle à la lutte contre la cybercriminalité

Créer une délégation interministérielle chargée de la lutte contre la cybercriminalité et placée sous la responsabilité directe du 1er Ministre. Elle aurait pour mission

1- de définir puis d'impulser une stratégie d'ensemble, en synergie avec les autorités compétentes de cyberdéfense et de sécurité des systèmes d'information

2.- d'assurer, en liaison avec le ministère de la Justice, la mise à jour des instruments normatifs dans une perspective d'harmonisation, de mise en cohérence et de plus grande efficacité

3- de définir les conditions nécessaires à une meilleure appréhension tant des menaces que de la réalité de cette délinquance, par le biais d'un **observatoire** ayant pour mission de définir les objectifs de nature statistique en y associant la recherche

4- d'impulser et de mettre en cohérence la prévention

5- de veiller à la réalisation des plans de formation par les différents départements et acteurs

6- d'assurer l'interface avec le secteur privé, en particulier les prestataires techniques d'Internet, pour ce qui relève de la lutte précitée, dans le cadre d'une **agence de régulation** chargée de veiller à la cohérence comme à la mise en oeuvre des normes applicables les concernant, disposant du monopole de négociation avec ces prestataires et du droit de les sanctionner administrativement en cas de non-respect de leurs obligations légales aux lieu et place des sanctions pénales en vigueur et sauf dans l'hypothèse d'injonctions judiciaires ; cette agence servirait en outre d'instance de médiation pour les internautes n'ayant pu faire reconnaître leurs droits lésés par les prestataires précités, et mettrait à exécution toutes les décisions de justice relatives au retrait, à l'inaccessibilité, au déréférencement, au blocage de sites ou de contenus ainsi qu'à la surveillance spécifique susceptible d'être ordonnée et au droit à l'oubli
Par souci de cohérence, le droit au recours contre les sanctions précitées devrait être exclusivement exercé devant la juridiction civile parisienne.

7- De participer à l'ensemble des discussions et négociations internationales.

Elle serait dépourvue de toute compétence opérationnelle mais comprendrait toutefois un **collège des chefs de service spécialisés dans la lutte contre la cybercriminalité**, destiné à faciliter les échanges en terme de méthodologie, de technique, d'objectifs de service, de projets comme de difficultés générées par des problématiques communes *(les réseaux TOR, les bitcoins...)*.

En outre, la Délégation comprendrait un **collège scientifique** rassemblant les principaux sachants, tant publics que privés.

2.- l'organisation judiciaire

Il y a, sur ce point, consensus, aussi bien au plan externe qu'interne, pour considérer qu'il est aujourd'hui temps de mieux structurer le système judiciaire face à la cyber-criminalité, aussi bien au plan central, qu'au plan territorial par la création de parquets et de juridictions spécialisés composés de magistrats formés à cet effet.

En effet, au-delà des quelques tentatives de la région parisienne, le bilan global révèle un déficit de sensibilisation et de connaissance à tous les niveaux, qui minore la gravité de cette nouvelle forme de délinquance et contribue au manque d'efficacité constaté globalement. En outre, l'absence de la Justice dans les organismes européens de concertation comme l'insuffisance de la politique pénale en la matière renforcent cet état de fait.

Au plan central, les attentes exprimées incitent à créer, au sein du ministère de la Justice, une structure rassemblant l'ensemble des questions relevant de la cyber-criminalité, quelle que soit la nature de l'infraction concernée, y compris la représentation et la négociation internationale. Compte-tenu de l'interférence entre le civil et le pénal, notamment pour la protection des données personnelles, il apparaît opportun qu'une telle structure ait aussi des compétences civiles, même si elle n'a pas vocation à tout traiter.

Elle devrait prendre la forme d'une mission placée directement sous l'autorité du directeur des affaires criminelles à des grâces, qui se verrait confier le soin de proposer une politique judiciaire cohérente, de veiller à l'harmonisation des normes et à l'évolution des supports statistiques Justice, de participer à l'ensemble des travaux nationaux comme internationaux, de représenter le ministère de la Justice auprès des instances interministérielles, de définir les priorités répressives, de gérer l'entraide correspondante et enfin d'animer une plate-forme de veille juridico-technique et de soutien aux autres services de l'administration centrale, comme aux juridictions et aux services d'investigation.

Parmi les missions énumérées ci-dessus, il convient d'insister sur la mise en cohérence normative, dans la mesure où chaque département, voire chaque autorité indépendante, initie actuellement des textes comportant des dispositions relatives à la cybercriminalité, tant en droit pénal qu'en procédure pénale : le rôle du ministère de la Justice en tant que ministère de la loi, garant de sa cohérence mais aussi du respect des libertés fondamentales, doit être officiellement réaffirmé et il doit pouvoir s'appuyer sur un réseau de correspondants dans les autres départements comme sur l'aide du Conseil d'Etat.

La mission de représentation et de participation aux négociations internationales relatives à la cybercriminalité est aussi vitale, dans la mesure où la Chancellerie est peu partie prenante à ces travaux, dont dépend pourtant, pour une bonne part, l'évolution des normes internes.

La détermination des priorités mais aussi des modes de traitement et des critères tenant à la répartition des affaires entre les différents parquets et donc des services de police judiciaire correspond aussi à une ardente nécessité.

L'ensemble de ces missions appellent une formation et une technicité de haut niveau.

Au plan territorial, si la gestion des plaintes produit un effet de dissémination au détriment de l'ensemble de juridictions déjà surchargées par la criminalité de droit commun, une certaine spécialisation existe soit de droit, pour les questions de cybercriminalité liées au terrorisme, voire au crime contre l'humanité *(PARIS)*, soit de fait, compte-tenu de l'implantation des services spécialisés d'enquête *(PARIS et les juridictions limitrophes s'agissant des questions traitées par la préfecture de police ; NANTERRE au regard du siège de l'Office central...)* ou des sièges sociaux des principales entreprises françaises hébergeant ou fournissant les données ou victimes d'attaques.

D'évidence, s'agissant d'une délinquance nouvelle et complexe à bien des égards, la compétence territoriale des juridictions ne saurait être davantage le fait du hasard...ou de la nécessité, mais elle doit répondre à une organisation réfléchie.

Pour autant, **l'idée, parfois avancée, d'une juridiction spécialisée unique ne saurait être opérationnelle**, puisque, pour l'essentiel, les réseaux de communications électroniques ne servent que de vecteurs à des actes de délinquance de droit commun ; il importe, en conséquence, de prendre en compte plusieurs types de facteurs :

☞ partie des infractions commises, en ce qu'elles concernent des personnes déjà identifiées ou identifiables comme se situant dans un cadre inter-personnel - notamment, de manière générale, les menaces et injures, les atteintes à la vie privée, le racisme, la xénophobie, l'homophobie, les infractions à la loi informatique et libertés, la diffusion d'images pédo-pornographiques...- ne créent pas de difficultés particulières.

☞ en revanche, les contentieux de masse que constituent les escroqueries et les fraudes aux cartes bancaires, soulèvent des problèmes spécifiques faute de recoupements centralisés permettant les regroupements nécessaires ; il convient de se reporter, sur ce point, aux recommandations figurant au *titre III, chapitre 4* du rapport.

☞ d'autres difficultés tiennent à l'insuffisance des critères classiques de compétence territoriale ; des recommandations sont faites à cet égard dans ce même *titre III, chapitre 3*.

☞ en définitive, **la spécialisation judiciaire doit concerner, au 1er chef, les attaques concernant les systèmes de traitement automatisé de données ainsi que les autres formes de délinquance les plus organisées**.

S'agissant des attaques précitées, **cette spécialisation doit reposer, d'une part, sur le parquet de PARIS**, s'agissant des attaques les plus importantes et visées au titre de la cyber-défense *(les services sensibles de l'Etat ainsi que les organismes d'importance vitale [119])*, **d'autre part, sur les juridictions inter-régionales spécialisées** lorsque les autres attaques sont le fait de bandes organisées ; telle est l'une des raisons pour lesquelles il est préconisé de créer une circonstance aggravante les concernant *(cf. les développements sur le droit pénal de fond, titre III, chapitre 1)*. En revanche, en ce qui concerne les autres infractions d'importance, ces

[119] Un tel critère de compétence suppose toutefois de définir les O.I.V., alors que leur classification relève, jusqu'ici, du Secret Défense...

mêmes juridictions inter-régionales disposent déjà, au titre de la bande organisée, de la compétence nécessaire *(cf., à titre d'exemple, les escroqueries par faux ordres de virement).*

Une telle organisation serait toutefois sans portée si elle ne s'accompagnait pas d'une formation obligatoire pour les juridictions précitées *(voir plus haut),* d'orientations précises de politique pénale quant à l'orientation des dossiers ainsi que d'un renforcement des moyens spécialisés de police judiciaire correspondants ; la carte policière doit être ainsi harmonisée avec l'organisation judiciaire.

S'agissant enfin des juridictions non spécialisées - le plus grand nombre -, leur compétence doit pouvoir s'appuyer sur un réseau de magistrats référents formés *(cf. les développements sur la formation)* et animés par la nouvelle Mission de l'administration centrale, ainsi que sur les informations, notamment juridiques, mises à disposition par cette dernière au titre de la plate-forme documentaire qu'il est proposée de créer, sans omettre le rôle primordial que l'Ecole nationale de la magistrature sera appelée à jouer.

Recommandation n° 8
relative à l'organisation judiciaire

1.- Créer, au sein du ministère de la Justice, une mission de lutte contre la cybercriminalité rattachée au directeur des affaires criminelles et des grâces, à compétence civile, pénale et internationale. Elle serait chargée de veiller à l'harmonisation des normes et à l'évolution des dispositifs statistiques judiciaires, de participer à l'ensemble des travaux nationaux et internationaux, de mettre en oeuvre la politique pénale spécifique, d'assurer une interface avec l'OCLCTIC et d'animer une plate-forme de veille juridico-technique et de soutien.

2.- Reconnaître à la juridiction parisienne une compétence concurrente sur l'ensemble du territoire national pour les atteintes aux systèmes de traitement automatisé de données visant les services de l'Etat et les opérateurs d'importance vitale.

3.- Reconnaître aux juridictions inter-régionales spécialisées une compétence similaire s'agissant de l'ensemble des autres cyber-affaires commises en bande organisée.

3.- l'organisation des services d'investigation, tant administratifs que de police judiciaire, au plan central comme territorial

Si chacun s'accorde à constater que le fait que nombre de départements ministériels, voire, pour certains d'entre eux, chaque direction, a été amené à se doter d'un service spécialisé compétent pour connaître, au titre de la police judiciaire ou de la police administrative, de la cybercriminalité, génère un certain éparpillement des ressources ainsi que des duplications inutiles, un consensus s'avère plus difficile à trouver quant aux solutions à apporter.

Au plan central, il convient de se garder de toute approche technocratique qui, méconnaissant le caractère essentiellement transversal de la cybercriminalité ainsi que la spécificité des problèmes techniques et de coopération internationale qu'elle pose, préconiserait une simple concentration des structures existantes ; il est, en effet, logique que chaque corps de contrôle entende disposer, dans son secteur de compétence, d'une structure ad hoc, d'autant plus que c'est souvent le seul moyen de disposer de personnels formés et motivés susceptibles de soutenir les services territoriaux. Pour autant, cela ne justifie sans doute pas la multiplication de services spécialisés au sein d'un même département ministériel.

Toutefois, c'est en terme de missions et de mise en cohérence et de coordination, que des solutions doivent être recherchées, compte-tenu notamment du rôle dévolu à la délégation interministérielle qu'il est proposé de créer.

Recommandation n° 9
relative à la coordination des structures administratives spécialisées dans la lutte contre la cybercriminalité

Si le caractère novateur et spécifique de la cybercriminalité a incité de nombreux départements à créer des structures spécialisées qui assurent l'assistance technique ainsi que la formation des services territoriaux, exercent une veille sur Internet et jouent un rôle opérationnel, tant pro-actif que sur saisine, pour les affaires les plus importantes, il importe

1- d'éviter leur multiplication au sein d'un même département, afin d'assurer à chacune des structures existantes, un niveau minimal en terme d'effectifs de nature à permettre l'efficience recherchée, des unités de trop petites tailles s'avérant impuissantes à réaliser notamment une veille pertinente compte-tenu de l'ampleur de la "toile".
2- Dans l'hypothèse où un même type de cybercriminalité est concerné, même sous des aspects différents *(ex. de la contrefaçon)*, de veiller, en déterminant les critères de répartition et les mécanismes d'échanges et de coopération par le biais, par exemple, de protocoles inter-administratifs, à éviter toute redondance inutile.
3- De renforcer, entre les différentes cellules de veille et services spécialisés, l'échange sur les méthodologies, les objectifs et les projets, dans le cadre de la structure ad hoc prévue à cet effet au niveau de la Délégation interministérielle projetée *(objectif de décloisonnement)*.
4- De rendre plus cohérent, tant la négociation avec les prestataires techniques de l'Internet que la production normative et l'action préventive, ce qui constitue l'une des raisons d'être de la proposition de création d'une Délégation interministérielle.

S'agissant, plus spécifiquement, de **la police judiciaire**, l'O.C.L.C.T.I.C. n'a pas de compétence opérationnelle exclusive pour les affaires les plus importantes relevant de la cybercriminalité, compte-tenu, notamment du rôle imparti à d'autres offices *(tel, s'agissant des affaires complexes intéressant la pédophilie et la protection des mineurs, l'Office central de répression des violences aux personnes).*

Toutefois, on l'a vu, il joue, en tant que gestionnaire de la base PHAROS et de la plate-forme téléphonique relative aux escroqueries, un rôle spécifique d'interface tant avec les internautes qu'avec les professionnels pour les infractions de droit commun, mais aussi de recoupements aux fins d'orientation pertinente.

Il constitue le point de contact international pour la France dans le cadre de la convention sur la cybercriminalité, raison pour laquelle il exerce un monopole dans le traitement des cybercrimes les plus graves présentant un fort aspect international.

Il exerce enfin, dans le cadre des textes réglementaires applicables, une mission de centralisation et de coordination.

En revanche, c'est le service spécialisé de la Gendarmerie qui gère la base images nécessaire à la lutte contre la pédo-pornographie.

L'un comme l'autre assurent aussi les missions communes à tout service spécialisé dans la cybercriminalité *(formation, assistance technique, rôle opérationnel pour les infractions les plus graves, soutien pour le reste...)*. L'un comme l'autre mènent encore des actions de prévention et assurent, en ordre quelque peu dispersé, des négociations avec les prestataires techniques d'Internet.

Indépendamment des recommandations relatives au traitement des contentieux de masse *(cf. titre III, chapitre IV)*, **il est préconisé, outre la mise en cohérence de certaines missions, de renforcer le rôle de coordination de l'Office et de lui donner un contenu interministériel.** En outre, son articulation avec le judiciaire doit être précisée.

Recommandation n° 10
relative à l'organisation centrale de la police judiciaire

S'agissant de l'organisation centrale de la police judiciaire, il est préconisé

1- En terme de missions, et compte-tenu de la Délégation interministérielle qu'il est proposé de créer, de décharger les services de police judiciaire des tâches de prévention et des négociations avec les prestataires techniques d'Internet ; il est, en outre, opportun d'harmoniser la formation des policiers et gendarmes spécialisés ainsi que les référentiels métiers et la doctrine d'emploi.
2- D'accroître la synergie interministérielle, l'Office central devant accueillir des fonctionnaires tant des Douanes que de la Direction générale de la consommation, de la concurrence et de la répression des fraudes ; ils auraient vocation à participer à la gestion de la plate-forme PHAROS et aux groupes d'enquête les concernant plus particulièrement.
3- De renforcer le rôle de coordination imparti à l'Office, notamment par la création d'une instance de coordination, animée par le chef de l'Office et regroupant les responsables des différents services spécialisés au plan central dans la lutte contre la cybercriminalité ; la future Mission Justice y serait représentée de droit.

Au plan territorial, il s'agit principalement de mieux articuler la carte des services de police judiciaire spécialisés dans la lutte contre la cybercriminalité avec celle des juridictions spécialisées appelées à en connaître.

Si pour PARIS, la préfecture de police, et notamment la Brigade d'enquête spécialisée dont elle dispose *(B.E.F.T.I.),* répondent à cette exigence, force est de constater qu'il n'existe aucun service spécialisé sur le reste du territoire, les fonctionnaires spécialisés *(ICC et NTECH)* étant répartis dans de nombreux services d'enquête et étant souvent utilisés en force de soutien, principalement technique *(cf., en annexe, la carte des ressources humaines existantes et leur implantation géographique)*. Or, si l'on entend que les juridictions inter-régionales spécialisées de province soient en capacité de traiter les affaires de cybercriminalité les plus graves en relevant, il est indispensable qu'elles disposent de services d'investigation spécialement formés.

Plusieurs modalités sont envisageables comme, par exemple, la création d'équipes pluridisciplinaires interministérielles spécialisées, sur le modèle des *groupements d'intervention régionaux*, qui, implantés sur le même site que les parquets et juridictions spécialisés, seraient susceptibles d'être co-saisies avec un service de police judiciaire de droit commun ; ou encore la création d'unités spécialisées directement rattachées aux directions inter-régionales de police judiciaire ; ou bien enfin, hypothèse qui a la préférence de la Police et de la Gendarmerie car elle sauvegarde le modèle organisationnel actuel, le renforcement significatif des personnels spécialisés affectés tant aux directions inter-régionales ou aux services régionaux de police judiciaire qu'aux sections de recherche sièges des J.I.R.S.

Sur le reste du territoire, la question de la formation et de l'équipement d'un plus grand nombre de policiers et de gendarmes prime, la plupart des spécialistes en fonction étant accaparés par l'exploitation des supports numériques saisis à l'occasion des enquêtes de droit commun.

Enfin, l'organisation territoriale devra prendre en compte les attentes des entreprises comme des services publics et des collectivités territoriales en terme de référents.

Recommandation n° 11
relative à l'organisation territoriale de la police judiciaire

Faire en sorte qu'au plan territorial, l'organisation de la police judiciaire prenne en compte la carte des juridictions inter-régionales spécialisées, sous la forme de la création de services pluridisciplinaires ou de la constitution d'équipes spécialisées dans la lutte contre la cybercriminalité

II.6.- Une conséquence : Des moyens pour lutter contre la cybercriminalité

Même si la formation, préalable comme permanente, des magistrats et des fonctionnaires doit mieux prendre en compte les questions de cybercriminalité, l'efficacité de la lutte contre cette dernière continuera à reposer, pour l'essentiel, sur des services et personnels hautement spécialisés.

Or, comparé à ce dont disposent les Etats étrangers voisins, la situation française, en terme de ressources humaines, est proche de l'artisanal.

Au plan judiciaire, si le parquet de PARIS dispose de 4 magistrats spécialisés, si les cours d'appel de PARIS et de VERSAILLES ont créé quelques magistrats référents, si la Chancellerie a affecté 2 magistrats au suivi de ces questions parmi bien d'autres missions, il n'existe aucune autre ressource judiciaire institutionnelle.

Au niveau de la police judiciaire, les ressources se limitent, au plan central, aux effectifs de l'Office central *(52, dont 1 ingénieur et 2 personnels administratifs)* [120] et à ceux de la Gendarmerie Nationale *(50, dont une quinzaine d'ingénieurs)*. Quant au plan territorial, outre la B.E.F.T.I. (25, dont 5 assistants techniques), un peu plus de 600 personnels spécialement formés sont disponibles *(366 I.C.C. pour la Police nationale, 260 NTECH pour la Gendarmerie nationale)*. Les services administratifs spécialisés sont encore moins bien lotis, notamment les Douanes *(10 agents à Cyberdouane ; 50 enquêteurs et 10 analystes-experts au service spécialisé de la D.G.C.C.R.F.)*.

D'évidence, la réussite des réformes organisationnelles proposées passe par l'attribution de ressources humaines supplémentaires, en priorité au parquet et au pôle d''instruction de PARIS comme dans les juridictions inter-régionales spécialisées, déjà en sous-effectifs ; il en est de même pour les futurs services spécialisés d'investigation au siège de ces juridictions, ainsi que pour les services centraux.

.

S'y ajoute, s'agissant des parquets, la nécessité de tenir compte de ce que l'on pourrait qualifier de compétence "forcée", liée à l'implantation d'un service d'enquête spécialisé dans son ressort *(l'O.C.L.C.T.I.C. à. Nanterre)* ou à la localisation du siège social d'un gestionnaire, d'un opérateur ou d'un service de vente à distance important, comme à Lognes, Roubaix ou Strasbourg.

Compte-tenu de l'état actuel des effectifs assignés à l'ensemble des tâches répressives, il paraît illusoire de procéder, autrement qu'à la marge, par redéploiement, sauf à prendre le risque de générer d'autres types de difficultés. La situation, déjà extrêmement difficile, notamment des parquets et des juridictions d'instruction spécialisés, n'y résisterait pas.

En outre, il convient de permettre à l'O.C.L.C.T.I.C. de recruter des ingénieurs et techniciens spécialisés, tellement la lutte contre les différentes formes évolutives de cybercriminalité exige des compétences dont policiers et gendarmes, malgré leur motivation,

---

[120] En outre, la sous-direction de la police technique et scientifique *(équivalent de l'IRCGN pour la Gendarmerie)* comprend une section de l'informatique des télécommunications et de l'électronique composée de 4 ingénieurs et de 10 techniciens

ne disposent pas. Quant à la Gendarmerie, il est indispensable de conserver et de renforcer l'acquis actuel résultant, en particulier, du recrutement d'officiers contractuels issus de formations universitaires spécialisées ou ayant déjà travaillé dans des administrations proches *(ANSSI, CALID, DGA...)* et souhaitant poursuivre leur carrière dans l'Arme.

A titre de comparaison internationale, la structure centrale de la *National cyber crime unit (NCCU)*, office britannique à compétence nationale pour lutter contre la cybercriminalité, soit en traitant les cas les graves soit sous la forme d'un appui aux autres services de police est composée de 150 personnes, auxquelles s'ajoutent 60 spécialistes implantés dans les structures territoriales. Aux Pays-Bas, la *National cybercrim unit* est composé de plus de 100 fonctionnaires au niveau central. En Espagne, la nouvelle sous-direction affectée à la lutte contre la cybercriminalité, qui assure des investigations technologiques ainsi que des missions relatives à la sécurité des systèmes informatiques, comporte plus d'une centaine de fonctionnaires. Quant au parquet spécialisé espagnol, il comporte plus de 70 magistrats et celui de l'Allemagne encore davantage.

Reste aussi à doter la future Délégation interministérielle qu'il est proposé de créer à la hauteur des missions qui lui sont confiées, sans affaiblir pour autant les administrations intéressées et sans omettre la Mission Justice dont la nécessité est évidente.

Toutefois, au delà des ressources humaines, il convient de prendre aussi en compte les besoins en équipement, qui se chiffrent en millions d'euros. Rien que le renouvellement, pour 2014-2018, du marché cyber relatif à l'équipement des investigateurs cyber-criminalité de la Police Nationale *(ordinateurs portables, mallettes forensic, logiciels d'exploitation complémentaires)* est évalué à 6,5 millions d'euros. Les besoins de la Gendarmerie sont proches de ceux de la Police Nationale *(5 millions d'euros sur 4 ans).* Mais ces chiffres, calculés en fonction des effectifs actuels, ne prennent pas en compte la croissance, souhaitée, du nombre de ces investigateurs. Enfin, les besoins spécifiques des services centraux spécialisés, tant de la Police que de la Gendarmerie, requièrent des investissements pour développer de nouveaux outils de lutte contre la cybercriminalité, de l'ordre d'un million d'euros sur 4 ans pour chacune.

Même si le groupe de travail est conscient des contraintes budgétaires actuelles, une politique pluri-annuelle de création de postes et de crédits d'équipements, à la hauteur de celle récemment adoptée, dans le cadre de la loi de modernisation de la Défense pour l'Autorité nationale de sécurité des systèmes d'information ou en faveur de la cyberdéfense, doit être mise en oeuvre.

Il est à craindre que sans cela, les réformes organisationnelles, juridiques et stratégiques préconisées restent sans effet.

Recommandation n° 12
relative au renforcement des moyens affectés
à la lutte contre la cybercriminalité

Une stratégie globale destinée à renforcer l'effectivité de la lutte contre la cybercriminalité, compte-tenu des préjudices dont elle est à l'origine et des enjeux qu'elle représente, doit s'accompagner d'un renforcement significatif, en ressources humaines et en crédits d'investissement, des services spécialisés de police judiciaire, et, pour la Justice, de son administration centrale, comme des parquets et juridictions d'instruction de PARIS, de NANTERRE et des juridictions inter-régionales spécialisées.

La cybercriminalité : Des réponses répressives plus effectives et davantage protectrices

Lorsque la prévention, la sensibilisation, la formation ne suffisent pas à répondre à la cybercriminalité, vient le temps de la répression.

L'objet des recommandations qui suivent poursuit un seul objectif - renforcer l'effectivité d'une répression encore très lacunaire - tout en assurant une mise en cohérence parfois perdue de vue et en veillant au respect des libertés fondamentales comme à une meilleure protection des victimes.

Cette recherche d'effectivité ne requiert pas des modifications du droit pénal de fond, sauf à la marge pour répondre à certaines questions non encore résolues ou insuffisamment prises en compte (1).

En revanche, elle suppose d'abord une clarification de la coopération attendue des prestataires de service, notamment étrangers, dans la mesure où leur rôle est fondamental en terme d'accès, de stockage et de commerce sur Internet, et, partant, pour l'identification des mis en cause comme pour le recueil de certains éléments de preuve. L'encadrement normatif existant doit être mis à jour et précisé (2).

Anonymisation, rapidité des transferts et des flux, extranéité, autant de caractéristiques de cette délinquance qui explique, tout à la fois, sa croissance et les difficultés spécifiques rencontrées par les services d'enquête : la toute première des priorités passe donc par le renforcement des moyens d'investigation (3).

Mais, s'agissant des contentieux de masse que recouvre, pour partie, la cybercriminalité, ces moyens ne suffisent pas : il faut encore changer de modèles organisationnels si l'on entend être efficace et préserver les capacités des services locaux tout en rendant plus pertinent la gestion des noms de domaine (4).

La coopération pénale internationale reste incontournable, même si les instruments dont on dispose actuellement ne sont pas encore à la hauteur des enjeux (5).

L'intérêt des victimes doit être au centre des préoccupations avec le souci de mieux répondre à leurs préoccupations (6).

Enfin, la politique pénale doit être réaffirmée afin de donner une cohérence à l'ensemble de l'action répressive (7).

III.1.- Des incriminations suffisantes pour l'essentiel

1 - A **quelques exceptions près, le droit pénal français permet de saisir l'ensemble des agissements répréhensibles relevant de la cybercriminalité, soit par le biais d'incriminations spécifiques, soit en ayant recours à des incriminations plus générales**, d'autant plus que l'on a beaucoup légiféré depuis 15 ans en ce domaine et que partie des nouveaux textes est encore sous-utilisée.

En outre, comme l'a rappelé le Conseil d'Etat dans un avis rendu en 2011 [121], la jurisprudence de la Cour de cassation va dans le sens d'une *"dématérialisation"* des éléments constitutifs de certains délits, par exemple lorsqu'elle admet que le délit de vol soit constitué par le simple fait de s'approprier, à l'insu de son propriétaire, un document, quel qu'en soit le support, pour la seule durée nécessaire pour le copier [122], ou celui d'abus de confiance par le détournement d'un bien *"quelconque"* pour d'autres usages que ceux pour lesquels il a été confié, ou encore celui d'escroquerie par l'utilisation d'un code de carte bancaire.

Plus avant, il doit être noté que, s'agissant des attaques contre les systèmes d'information, la législation française paraît déjà répondre aux obligations résultant de la récente *Directive 2013/40 de l'Union européenne du 12.08.2013.*

Pourtant, en ce domaine, nombreuses sont les propositions sectorielles ayant pour objet la création de nouvelles incriminations. Elles sont principalement motivées par la volonté de dénoncer certains comportements préoccupants et d'afficher la détermination de l'Etat à les réprimer. Or, l'on doit constater que, bien souvent, notre législation contient déjà des dispositions plus générales permettant une telle répression.

En fait, ces préconisations en faveur de l'adoption de dispositions spécifiques renvoient, pour partie, à un phénomène, plus général, de parcellarisation du droit pénal, chaque administration technique, autorité indépendante ou association spécialisée dans la défense de certaines catégories ayant par trop tendance à prétendre à l'adoption de dispositions particulières, ce qui n'est pas sans conséquence en terme de cohérence mais aussi de mise en oeuvre pour des services de police et de justice essentiellement généralistes.

Par delà, est indirectement mise en cause la méthode traditionnelle de législation à la française en matière pénale, sur laquelle veillent le ministère de la Justice et celui des Affaires étrangères comme le Conseil d'Etat, qui consiste à toujours privilégier le recours à des infractions de droit commun et à ne recourir à des incriminations spécifiques que si les premières s'avèrent véritablement impuissantes à saisir les nouveaux comportements à réprimer, même lorsque les directives internationales paraissent préconiser plutôt la démarche inverse.

Si une telle méthodologie requiert parfois du temps pour que la jurisprudence fasse son oeuvre, elle présente l'avantage de limiter l'inflation pénale, d'éviter l'obsolescence

---

[121] avis n° 384.892 du 31.03.2011 *(section des finances)*

[122] la Chambre criminelle, en son arrêt n° 07-84.002 du 4.03.2008, assimile au vol *"le fait de copier sur des supports matériels des données et fichiers informatiques appartenant à une société afin de se les approprier"*.

qui menace des textes trop spécifiques notamment lorsque la criminalité s'avère particulièrement évolutive, et surtout d'atteindre une plus grande effectivité dans la mesure où les infractions courantes sont mieux connues et mieux appliquées par des enquêteurs et magistrats qui sont, on l'a dit, pour l'essentiel, des généralistes.

Il n'en reste pas moins que de telles propositions soulignent, à juste raison, le manque de lisibilité du corpus pénal existant en matière de cybercriminalité, mais les réponses à y apporter relèvent davantage de la pédagogie *(voir plus loin)* que de l'adoption de textes nouveaux.

En résumé, l'efficacité de la répression passe moins par la création de nouvelles infractions que par l'adoption de moyens destinés à renforcer l'effectivité de la mise en oeuvre des dispositions déjà existantes, généralement suffisantes, compte-tenu des obstacles rencontrés par les services d'enquête et de Justice.

Recommandation n° 13
relative au droit pénal général et au droit pénal spécial
en matière de cybercriminalité

Eu égard au caractère quasi-exhaustif du droit pénal de fond existant et au risque de générer des incohérences tant en ce qui concerne les éléments constitutifs des infractions que les peines qui leur sont applicables, il est recommandé de limiter l'adoption de nouvelles incriminations dans le domaine de la cybercriminalité aux seules hypothèses où les infractions de droit commun s'avèrent impuissantes à saisir certains nouveaux comportements répréhensibles. Il appartient au ministère du droit que constitue le ministère de la Justice d'y veiller.

Néanmoins, et compte-tenu des différentes réflexions en cours dont le groupe de travail a été saisi, outre la transposition obligatoire en droit interne des plus récentes directives européennes, certaines réformes ponctuelles s'avèrent opportunes.

*** l'usurpation d'identité en ligne**

L'usurpation d'identité concerne plus de 300.000 personnes chaque année *(source : CREDOC)* et elle est, le plus souvent, commise en ligne. Elle est incriminée soit lorsqu'elle est l'occasion de commettre une infraction *(art. 434-23 du code pénal),* soit, depuis mars 2011, lorsqu'il en est fait usage, notamment sur un réseau de communication au public en ligne, dans le but de nuire à la tranquillité d'une personne ou de porter atteinte à son honneur *(art. 226-4-1 du code pénal).*

Incontestablement, Internet a accru, dans des proportions considérables, le risque d'une telle usurpation, notamment par le biais de la création de faux profils sur les réseaux sociaux.

Si l'incrimination créée par la loi du 14.03.2011, en ce qu'elle vise *"l'usage d'une ou de plusieurs données de toute nature permettant d'identifier (un tiers)",* est suffisamment large pour réprimer toute usurpation d'identité numérique, y compris au préjudice des personnes morales et donc des entreprises, les peines prévues ne paraissent pas à la hauteur des conséquences subies par les

victimes, en terme d'immixtion dans leur vie privée, de préjudice financier et d'atteinte à la réputation. De plus, *la note d'orientation n°4 du Comité de suivi de la Convention cybercriminalité* en date du 5 juin 2013 souligne combien l'appropriation frauduleuse d'informations relatives à l'identité sert à la préparation de nouveaux agissements criminels sous la forme de fraudes et assimilées.

Telle est la raison pour laquelle deux propositions de loi ont été déposées, respectivement le 24.07.2013 par M. Le FUR, député, et le 10 octobre suivant, par M. LAZARO, aussi député ; la première vise à ériger en circonstance aggravante le fait de commettre l'usurpation d'identité par un réseau de communication électronique, la seconde propose une aggravation sensible des peines encourues.

Recommandation n° 14
relative à l'usurpation d'identité

Compte-tenu de l'importance et de la gravité de cette délinquance, ériger en circonstance aggravante le fait que l'usurpation d'identité intervienne sur un réseau de communication électronique..

*** les délits d'atteintes aux systèmes de traitement automatisé de données** *(art. 323-1 s. du C.P.).*

Si les incriminations sont exhaustives, les dispositions relatives à la pénologie ne prennent pas suffisamment en compte l'importance que peuvent revêtir certaines de ces attaques, notamment lorsqu'elles sont commises en bande organisée ou portent sur des opérateurs d'importance vitale.

Recommandation n° 15
relative aux atteintes aux S.T.A.D.

Eu égard à la gravité particulière que peuvent revêtir les atteintes aux systèmes de traitement automatisé de données *(art. 323-1 s. du C.P.)* et par souci de cohérence avec les priorités affichées en matière de cyberdéfense, il est préconisé
1- d'accroître le quantum des peines applicables, notamment sous la forme de la création d'une circonstance aggravante de commission en bande organisée, punie de peines aggravées, le délit de l'art. 323-4 relatif à l'association de malfaiteurs paraissant insuffisant ; au surplus, cette incrimination est cohérente avec les propositions organisationnelles tendant à reconnaître une compétence spécifique aux juridictions inter-régionales spécialisées.
2- de mettre en cohérence la circonstance aggravante tenant au type de système de traitement automatique de données visé, actuellement limitée aux systèmes mis en oeuvre par l'Etat, en l'étendant, en harmonie avec les dispositions du code de la Défense, à l'ensemble des opérateurs d'importance vitale, qu'ils soient publics ou privés, dans la mesure où les intérêts fondamentaux de la Nation sont en cause.

*** l'envoi de spams massifs affectant la capacité des utilisateurs à se servir d'Internet**

Il est d'abord à noter que le Conseil de l'Europe incite à incriminer un tel comportement.

Si la Cour européenne des droits de l'homme n'a pas eu à se prononcer sur de tels envois massifs, elle a toutefois estimé, dans l'arrêt MUSCIO c. ITALIE du 13.11.2007, à propos d'un spam pornographique reçu par un internaute qui soulevait la responsabilité de l'Etat sur le fondement de l'art. 8 pour défaut d'obligations positives, que *"la réception de communications indésirables peut s'analyser comme une ingérence dans la vie privée; toutefois, les utilisateurs du courrier électronique, une fois connectés à Internet, ne peuvent plus jouir d'une protection effective de leur vie privée, et s'exposent à la réception de messages indésirables, qu'ils peuvent réguler par l'exploitation de filtres informatiques".*

Si, incontestablement, dans pareille circonstance, l'obligation positive de l'Etat n'est que relative, il serait toutefois opportun de pouvoir incriminer les envois massifs qui, non seulement constituent des entraves à la liberté de communication par les effets techniques qu'ils produisent, mais aussi constituent de véritables pratiques d'harcèlement, le plus souvent pour conduire à la faute partie des dizaines de milliers de personnes qui en sont souvent destinataires et réaliser, à leur préjudice, de nombreuses escroqueries..

Cette modification serait d'autant plus opportune que l'envoi de ces courriels violent la règle du consentement préalable instauré par la loi du 21 juin 2004 et posée par l'article L.121-20-5 du code de la consommation.

Le projet de loi sur la consommation *(cf. art. L.34-5 du code des postes et communications électroniques et le projet d'art. L.121-22 du code de la consommation)* constitue une première réponse, en prévoyant des sanctions administratives s'agissant des spams constitutifs de publicités commerciales intempestives.

Toutefois les autres pratiques ne sont actuellement aucunement réprimées, même si le projet de loi pour l'égalité entre les hommes et les femmes - non définitivement adopté à ce jour - paraît vouloir combler cette carence.

Il conviendra toutefois de définir les contours à donner à cette incrimination *(nombre minimum de spams, nature du message...).*

Recommandation n° 16
relative aux spams

Il est recommandé d'incriminer spécifiquement la pratique de l'envoi de spams massifs, conformément aux préconisations internationales et aux souhaits exprimés par les associations de victimes et de consommateurs.

*** le cyber-harcèlement, notamment entre adolescents**

Dans le cadre de l'examen du projet de loi pour l'égalité entre les hommes et les femmes, un amendement a été déposé ayant pour objet d'instaurer, à coté des délits de harcèlement moral et de harcèlement sexuel, un délit général d'harcèlement commis par le biais des *"nouvelles technologies d'information et de communication, en vue d'humilier ou d'intimider une personne".* Voté par le Sénat en 1ère lecture, le nouvel article projeté incrimine *"le fait, par tout moyen, de soumettre une personne à des humiliations ou à des intimidations répétées, ou de porter atteinte de façon répétée à sa vie privée"*, et prévoit plusieurs circonstances aggravantes.

Si, en cours de débats, la référence à la notion, contestable sur le plan juridique, d'humiliation a été écartée, il n'en reste pas moins qu'au regard tant de la jurisprudence du Conseil constitutionnel qu'à la difficulté rencontrée déjà par les praticiens pour cerner le harcèlement moral de l'article 222-33-2 du code pénal, alors même qu'il fait référence à un élément matériel précis *(la dégradation des conditions de travail)*, l'incrimination projetée peut soulever des réserves.

Au regard toutefois de l'importance et parfois de la gravité des pratiques dénoncées, mais qui concernent, il faut le rappeler, majoritairement des mineurs entre eux *(cf., sur ce point, les enquêtes réalisées par l'Education nationale),* il convient d'abord de noter que la Cour de cassation juge déjà que l'incrimination des appels téléphoniques malveillants réitérés en vue de troubler la tranquillité d'autrui *(cf. art. 222-16 du code pénal)* s'applique à des SMS. Par ailleurs, l'enregistrement et la diffusion d'images de violence sont déjà incriminés en tant que tels *(cf. art. 222-33-3 du code pénal).* Les délits de menaces sont aussi applicables sous certaines conditions *(art. 222-17 et 18 du code pénal).* Enfin et surtout, au regard tant de la jurisprudence que, depuis 2010, de la loi *(cf. art. 222-14-3, modifié par la loi du 9.07.2010)*, le comportement en question doit s'analyser comme une violence psychologique, déjà punissable.

Si l'on entend toutefois sanctionner plus sévèrement ce type de harcèlement, la solution la plus simple consisterait alors, s'agissant des infractions de violences ayant entraîné ou non une incapacité d'une durée supérieure à 8 jours *(art. 222-11 et 13 du code pénal),* à prévoir une circonstance aggravante tenant à leur commission par le biais d'un réseau de communication électronique.

Recommandation n° 17
relative au cyber-harcèlement

L'incrimination spécifique du harcèlement par le biais d'un réseau de communication électronique ne paraît pas répondre à une évidente nécessité eu égard aux incriminations déjà existantes, notamment en matière de violences.

Toutefois, si l'on souhaite pouvoir sanctionner plus sévèrement ce type de comportements, compte-tenu du préjudice et parfois des drames qu'il peut engendrer, il est proposé de prévoir une circonstance aggravante en matière de violences.

Il est à noter que, dans la mesure où de tels comportements répréhensibles sont majoritairement le fait de mineurs sur des mineurs, la démarche préventive et pédagogique mise en oeuvre, par exemple, par l'Education nationale doit être privilégiée.

*** la violation du secret des affaires**

Les réseaux de communication électronique, notamment Internet, exposent davantage les entreprises à des risques d'espionnage industriel ou à des attaques visant à récupérer des données sensibles, alors même que le patrimoine social est de plus en plus composé de biens immatériels qui vont des fichiers de clients aux procédés de fabrication et aux méthodes de commercialisation, et dont la valeur économique est élevée. Selon la Commission européenne, 25% des entreprises de l'Union s'estimeraient avoir été victimes de vol d'informations confidentielles en 2012.

La jurisprudence a, tour à tour, fait usage d'infractions de droit commun *(vol, recel, abus de confiance, violation du secret professionnel, espionnage)* ou d'incriminations plus spécifiques *(violation du secret de fabrication, intrusion dans un système de traitement automatisé de données)* pour réprimer cette réalité, mais pas toujours avec succès eu égard aux conditions posées par certains de ces textes.

L'intérêt accru porté à la question de l'intelligence économique et les fortes demandes émanant des milieux professionnels ont incité l'Assemblée Nationale à adopter, le 23.01.2012 en première lecture, une proposition de loi destinée à créer un délit sui generis d'atteinte au secret des affaires d'une entreprise, texte qui n'a toutefois pas prospéré.

La question a connu une nouvelle actualité avec le *projet de directive sur la protection des savoir-faire et des informations commerciales non divulguées (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites,* présenté le 28.11.2013 par la Commission européenne.

Au plan interne, la nouvelle *Délégation interministérielle à l'intelligence économique* propose une réforme d'ensemble du code de commerce, du code de procédure civile, du code pénal, du code de procédure pénale et de la loi du 29.07.1881 sur la liberté de la presse, et préconise notamment des mesures spécifiques, tant civiles que pénales, pour protéger, faire cesser ou réprimer les atteintes au secret des affaires.

Recommandation n° 18
relative au secret des affaires

Même si figurent déjà dans le droit positif des incriminations susceptibles d'assurer, pour partie, le secret des affaires, la création d'une incrimination particulière semble opportune, compte-tenu tant des prescriptions résultant de la directive sur le commerce en ligne que des attentes des professionnels.

Une solution simple et directement opérationnelle consisterait à incriminer spécifiquement, au même titre que le vol d'électricité *(cf. art. 311-2 du code pénal),* le vol de biens immatériels que la Cour de cassation a commencé à consacrer.

*** la peine de suspension du droit d'accès à Internet**

Prévue par la loi HADOPI pour la protection du droit d'auteur *(cf., notamment, les art. L. 335-7 s. du code de la propriété intellectuelle),* le principe même d'une telle peine a donné lieu à de vifs débats.

Comme l'avait pourtant implicitement suggéré le Conseil constitutionnel, une telle peine paraît tout à fait pertinente lorsque des crimes ou délits graves sont commis au moyen d'un réseau de communications électroniques.

Il est ainsi préconisé de l'ériger en peine complémentaire pour les infractions commises par un tel moyen et mettant en péril un mineur soit sous la forme de propositions sexuelles *(art. 227-22-1 du code pénal)*, soit par le biais de la pédopornographie *(art. 227-23),* soit au titre des atteintes sexuelles dans l'hypothèse prévue par l'article 227-26 al. 4 du même code.

Naturellement, l'effectivité d'une telle peine commande d'en assurer la notification à l'ensemble des fournisseurs d'accès.

Recommandation n° 10
relative à la peine complémentaire de suspension du droit d'accès à Internet

Créer, pour les infractions mettant en péril un mineur commises au moyen d'un réseau de communications électroniques, une peine complémentaire de suspension temporaire de l'accès à Internet, assortie de l'interdiction de souscrire, pendant la même période, un autre contrat portant sur un service de même nature auprès de tout opérateur.

12 - Le constat des praticiens, en ce qui concerne le droit pénal de fond, est assez paradoxal puisque, si la richesse de ce droit est généralement saluée, **il est unanimement jugé peu accessible à la fois compte-tenu de l'éparpillement des textes [123] et d'un manque d'homogénéité, voire de cohérence, dans leur conception et leur rédaction, constat qui renvoie, lui-même, à l'hétérogénéité de l'impulsion législative en la matière.**

S'ajoutant aux difficultés relatives à l'identification des mis en cause et au droit de la preuve, ce manque d'accessibilité contribue à une insuffisante effectivité du droit qu'attestent les statistiques de condamnations puisque certaines incriminations ne paraissent guère avoir fait l'objet d'application pratique.

Si partie de ces dispositions méritent d'être réécrites - notamment l'art.6 de la loi n° 2004-575 du 21.06.2004 pour la confiance dans l'Economie numérique -, sur un plan général différentes solutions peuvent être envisagées pour remédier à ces difficultés.

▬ quant au <u>support normatif</u>,

*si la solution de créer un code spécifique à la cybercriminalité ne peut être que rejetée au regard de la transversalité de cette dernière et du nombre considérable d'infractions de droit commun qu'elle recouvre, **il serait nécessaire de redonner au code pénal l'exclusivité qui était naturellement la sienne, conformément à l'esprit ayant présidé à son adoption en 1992**, exclusivité qui pourrait prendre deux formes :

☞faire figurer les incriminations dans ce seul code ;

☞ dupliquer à l'identique dans ce code les incriminations prévues par d'autres textes *(cf., les précédents en matière routière ou s'agissant des infractions à la législation sur les stupéfiants)*, ce qui présente l'avantage de ne pas démembrer les textes en question tout en assurant une source unique pour les praticiens du droit et en facilitant au ministère de la Justice le suivi de l'évolution des incriminations dans le temps [124].

Si la *Commission supérieure de codification* est réservée sur ce principe du code pilote-code suiveur, le guide de légistique préconisant de faire un renvoi sans citation à un titre, un chapitre ou à des articles d'un autre code, le groupe interministériel estime que tant le principe d'accessibilité et de lisibilité de la loi par les justiciables que la recherche d'une meilleure application par les praticiens du droit commandent d'apporter remède à l'éparpillement existant.

---

[123] En l'état, même les gestionnaires de la table NATINF, qui disposent de la vision la plus précise du droit pénal français, ne sont pas assurés du caractère exhaustif de l'inventaire réalisé par leurs soins puisque, en sus des incriminations existant dans le code pénal, le code monétaire et financier *(contrefaçon des moyens de paiement)*, le code de la propriété intellectuelle, le code des postes et des communications électroniques, le code de la consommation *(cf. altération de marquage sur les produits, technique de la boule de neige...),* la loi sur la liberté de la presse, la loi du 21.06.2004 pour la confiance dans l'économie numérique...et d'autres encore comportent des incriminations relatives à la cybercriminalité, sans compter leurs textes réglementaires d'application.

[124] Une telle duplication, même si elle oblige à renvoyer dans le code pénal à des dispositions qui lui sont extérieures, apparaît particulièrement utile pour les incriminations figurant dans des textes non codifiés.

*dans l'immédiat, il est préconisé de **réaliser une nomenclature unifiée de l'ensemble des incriminations existantes.**

Si, a priori, une nomenclature distinguant, d'une part, les infractions relatives aux technologies de l'information et de la communication *(infractions par nature)* et celles de droit commun commises par la voie électronique *(infractions de contenu)* apparaît séduisante, elle présente le défaut d'être difficilement accessible pour les non-initiés.

Par cohérence avec la suggestion précédente, il est préconisé d'avoir recours à la nomenclature du code pénal et de mettre en exergue les infractions spécifiques, tant déjà incluses dans ce code que dépendant de textes extérieurs. L'ébauche d'une telle nomenclature, renseignée à partir du texte même des incriminations et comportant les visas de la table NATINF, figure en annexe du rapport ; elle a été réalisée, à la demande du groupe interministériel, par la direction des affaires criminelles et des grâces**.**

Outre une meilleure appréhension des incriminations existantes, elle serait susceptible de favoriser un plus grand recours aux peines complémentaires spécifiques déjà applicables, notamment pour mieux répondre aux attentes des victimes [125].

*dans un second temps, il est préconisé de **réaliser**, sur la base de la nomenclature précitée, **un corpus exhaustif**, ayant vocation à servir de base à la formation et largement diffusé à l'ensemble des praticiens du droit.

Un tel corpus aurait vocation à regrouper

- les dispositions du droit international applicables,

- l'interprétation faite par les Affaires Etrangères du droit français au regard des directives internationales : lorsque la France considère que la création de certaines incriminations préconisées par des textes internationaux n'est pas utile au regard des textes déjà existants, l'interprétation officielle faite doit donner lieu à publicité *(à l'exemple de ce que réalise le comité de suivi de la Convention dite de Budapest).*

- Mais aussi, au regard de chaque incrimination - **y compris et peut-être surtout de droit commun non spécifiquement visée par la loi au titre de la cybercriminalité -**, la jurisprudence, tant internationale *(Cour européenne des droits de l'homme, Cour de justice de l'Union européenne)* que française, compte-tenu du rôle primordial qu'elle est conduite à jouer dans l'interprétation, tant des nouvelles incriminations, que des infractions générales.

[125] ainsi, pour prendre l'exemple des atteintes aux systèmes de traitement automatisée de données, l'art. 323-5 du C.P. comporte de nombreuses dispositions spécifiques, étant entendu que, s'agissant de la peine d'affichage, la modification de l'art. 131-35 par la loi du 21.06.2004 autorise l'affichage par un service de communication au public par voie électronique.

A titre d'exemple, il peut être fait référence aux interrogations de la doctrine quant à l'application de l'incrimination de vol à l'hypothèse de la soustraction de données informatiques par recopiage, doctrine qui fait souvent référence au jugement du tribunal de grande instance de CLERMONT-FERRAND, en date du 26.09.2011, en omettant de viser l'arrêt précité rendu en 2008 par la Cour de cassation...

▬ quant au manque d'homogénéité, il est symptomatique, tout à la fois, d'une conception éclatée des textes concernés dans l'espace - entre divers départements mais aussi avec une forte initiative parlementaire - comme dans le temps, de la rapidité avec laquelle ces textes sont conçus et examinés, et d'une insuffisante reconnaissance du pilotage du ministère de la loi que constitue la Chancellerie.

Le libellé des circonstances qualifiantes ou aggravantes visant la cybercriminalité mais aussi de certaines dispositions procédurales spécifiques illustre ce phénomène, puisque, selon les textes en vigueur, l'on vise tantôt *"la voie électronique" (cf. art. 226-15 du code pénal),* tantôt un *"moyen de communication électronique" (art. 227-22-1 du code pénal, art. 706-25-2, 706-35-1, 707-47-3 du C.P.P.)* ou un *"réseau de communications électroniques"* limité parfois à *"un public non déterminé" (cf. art. 227-23 sur la pédo-pornographie, art. 222-24 8˚, 225-7 10˚, 227-11 al.1, 227-23 al.3, 227-26 4˚ du code pénal) ,* tantôt un *"réseau de communications" (art. 225-12-2 du code pénal)* ou un *"réseau de communication au public en ligne" (cf. la contrefaçon aggravée résultant de la loi de mars 2011, l'art. 226-4-1 du code pénal)*, tantôt un *"service de communication au public en ligne" (art. L.335-7 et autres du code de la propriété intellectuelle)*...
Une pareille hétérogénéité suscite des interrogations chez les praticiens quant aux intentions exactes du législateur, puisque ces différents concepts ont des contenus plus ou moins larges.

Il mériterait une mise en harmonie, opérée par ordonnance, autour d'un concept suffisamment large pour inclure Internet, mais aussi la téléphonie et l'ensemble des technologies numériques en évolution rapide, tel que celui de *"communications électroniques"* et de *"réseau de communications électroniques"*, déjà définis par le code des postes et des communications électronique *(cf. art. L.32),* définitions auxquelles le code pénal pourrait explicitement renvoyer, sauf dans l'hypothèse où l'on voudrait spécifiquement viser Internet *(mais il serait alors plus simple d'en faire directement mention).*

Il n'en reste pas moins que, pour garantir, à l'avenir, une meilleure cohérence des textes relatifs à la cybercriminalité, il importe de confier à la Chancellerie, en tant que ministère de la loi pénale et civile, un rôle de pilotage dans leur rédaction, en lien avec les administrations et partenaires concernés : c'est l'un des buts poursuivis par la recommandation précédente ayant pour objet la création d'une mission spécifique au sein du ministère de la Justice. La Délégation interministérielle dont la création est aussi préconisée devrait également favoriser une meilleure cohérence des initiatives en la matière et assurer un pilotage en amont.

Recommandation n° 20
relative à l'amélioration de la lisibilité et de la cohérence du droit pénal de fond

1.- afin d'assurer la cohérence des incriminations tout en renforçant leur accessibilité, insérer l'ensemble de ces dispositions dans le code pénal, conformément à leur vocation. Cet objectif peut être atteint soit en rapatriant dans ce code les dispositions éparses dans les autres codes ou les textes non codifiés, soit en les dupliquant systématiquement.

2.- Concomitamment, veiller à une mise en cohérence terminologique, notamment s'agissant tant de l'extension de certaines incriminations à la cybercriminalité que des circonstances aggravantes intéressant cette dernière.

3.- Dans l'immédiat, et afin de favoriser une meilleure effectivité de la loi en renforçant son accessibilité, dresser et rendre accessible en ligne un corpus exhaustif de l'ensemble des dispositions en question, avec, au regard, les principales décisions jurisprudentielles, internes comme internationales.

4.- Dans l'avenir,
*Faire assurer, par la délégation interministérielle dont la création est préconisée, la mise en cohérence des initiatives normatives relatives à la cybercriminalité émanant des différents départements ministériels, ainsi qu'un dispositif de veille, tant sur le plan interne qu'au niveau international.
*Réaffirmer, à l'occasion de la constitution d'une mission spécifique au sein du ministère de la Justice, le pilotage du ministère de la loi, qui devrait pouvoir s'appuyer sur un réseau de référents au sein des autres départements ministériels.

III.2.- de la coopération attendue des hébergeurs, fournisseurs, d'accès et autres prestataires de l'Internet et de son nécessaire encadrement

La coopération avec les professionnels de l'Internet est au coeur de la lutte contre la cybercriminalité, puisqu'ils détiennent les données susceptibles de permettre d'identifier les auteurs d'infractions et de réunir partie des éléments de preuve et disposent des moyens techniques de prévenir ces mêmes infractions comme d'y mettre un terme.

Elle est aussi au coeur des difficultés que rencontrent, quotidiennement, les praticiens.

Si cette coopération s'est renforcée ces dernières années, bien que de manière inégale, selon que le prestataire est français ou étranger, selon aussi l'origine de la demande *(simple utilisateur, service d'investigation déconcentré à vocation généraliste ou service spécialisé au plan central),* **elle appelle aujourd'hui une clarification, de nature normative**.

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, a constitué une étape décisive en adaptant au droit interne *la directive 2000/31/CE du 8 juin 2000 de l'Union Européenne relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique.*

Néanmoins, dix ans plus tard, les difficultés d'interprétation que génèrent ce texte fondateur dans son application ne sont toujours pas surmontées, d'autant plus que les techniques ont évolué et que les prestataires se sont diversifiés. Par ailleurs, la croissance de la cybercriminalité a accru les attentes à l'égard des différents prestataires oeuvrant sur Internet et commande aujourd'hui une clarification du rôle qui leur est assigné, afin que l'Etat puisse jouer pleinement le rôle qui lui est dévolu et que les victimes soient mieux protégées, comme le recommande d'ailleurs la directive précitée.

Il est aujourd'hui temps de redéfinir un cadre global adapté aux obligations de ces prestataires.

C'est, d'ailleurs, une démarche identique que mènent le Conseil de l'Europe et l'Union Européenne et c'est en tenant compte de leurs réflexions actuelles que les préconisations qui suivent sont émises, même si les difficultés rencontrées par les praticiens en ont été le fil directeur.

L'irresponsabilité de principe des prestataires techniques n'est pas en cause (1), même s'il convient de préciser les hypothèses dans lesquelles elle doit s'effacer, ne serait-ce que pour ramener à leurs justes proportions les réserves émises par les plus grandes sociétés du marché (2).

Le même souci conduit le groupe interministériel à souligner que les formes de la coopération attendue de ces prestataires ne sauraient relever du seul partenariat, malgré l'intérêt évident qu'il représente, la protection de l'intérêt général comme le principe de libre concurrence nécessitant que la loi définisse et précise les principes applicables (3).

L'état des lieux dressé par le groupe interministériel, à la lumière tant des observations des praticiens que de l'audition des principaux opérateurs, a mis en exergue deux difficultés principales ; l'une tient au fait qu'une partie de ces professionnels ne sont pas saisis par le droit actuel ; l'autre a trait au positionnement particulier des grands prestataires américains qui s'estiment non soumis au droit français. Le groupe interministériel fait des préconisations pour y mettre un terme, tout en proposant d'étendre le rôle de la future *Plate-forme nationale des interceptions judiciaires* (4).

Il faut aussi préciser, sur le plan normatif, le type de mesures aujourd'hui exigibles de ces prestataires afin que les autorités, tant administratives que judiciaires, puissent disposer d'un cadre cohérent et stable ; pour définir ce cadre, le groupe interministériel a pris en compte les quelques exemples offerts par le droit ou reposant sur le partenariat ainsi que la nécessité d'atteindre une plus grande effectivité dans l'application de la loi et des décisions de justice (5).

Des développements spécifiques concernent quelques mesures particulières relatives à la géo-localisation ou au blocage des sites (6).

Enfin, les difficultés relatives à certains autres opérateurs sont abordées in fine de ce chapitre (7).

1 - <u>Le principe selon lequel l'auteur du contenu, le directeur de publication ou l'éditeur sont les responsables, civilement comme pénalement, de ce contenu - avec, en corollaire, l'irresponsabilité de principe des prestataires techniques - doit être réaffirmé</u> comme l'exigent le droit de la responsabilité en matière civile comme pénale, celui de la liberté d'information ainsi que les règles internationales [126].

S'agissant des prestataires, ce principe est énoncé en droit international, notamment par la directive 2000 précitée, qui fixe des règles précises d'irresponsabilité du fait du contenu s'agissant

- du fournisseur d'accès à Internet (le *"transporteur", art.12)*, défini par l'art. 6.I 1 de la loi de 2004 comme la personne *"dont l'activité est d'offrir un accès à des services de communication en ligne",* à la condition qu'il ne soit pas à l'origine de la transmission, ne sélectionne pas le destinataire de la transmission, et ne sélectionne ni ne modifie les informations faisant l'objet de la transmission

- du transmetteur d'information (*art. 13),* - c'est-à-dire, en droit interne *(cf. art. L.32-15° du code des postes et communications électroniques, résultant de la loi de 2004) "l'opérateur ou l'exploitant d'un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications"* - à la condition qu'il ne modifie pas l'information et qu'il se conforme aux conditions d'accès à l'information et aux règles de mise à jour de cette dernière ;

- de l'hébergeur *(art.14),* défini par l'art. 6.I.2.1 de la loi de 2004 comme la personne physique ou morale qui assure *"même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services..."*

Une telle irresponsabilité de principe repose sur un double constat : le rôle essentiel que jouent ces prestataires dans la transmission, la circulation, l'acheminement et enfin l'accès par l'utilisateur des textes, images, sons et autres données circulant sur Internet ; et le caractère purement technique d'un tel rôle, dans la mesure où il n'implique aucune intervention à quelque stade que ce soit sur les contenus ; elle a donc pour finalité d'assurer la neutralité et donc la crédibilité de l'Internet *(cf., notamment, la communication de la Commission européenne "l'Internet ouvert et la neutralité de l'Internet en Europe" (19.04.2011)*

L'art.6 de la loi de 2004 intègre dans le droit national ces principes d'irresponsabilité pénale et civile, en particulier pour l'hébergeur *(cf. art.6-I,2 et 3)*, mais aussi implicitement pour le fournisseur d'accés ainsi que, à titre de conséquence, le fait que ces deux catégories de prestataires *"ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites" (cf. art 6-I.7), cette dernière disposition reprenant littéralement les termes de l'art.15 de la directive.*

.

Il appartient aux juridictions, nationales comme internationales, d'y veiller. La Cour de Justice de l'Union européenne a ainsi rappelé, dans une affaire qui opposait la société Belge des auteurs compositeurs et éditeurs à un fournisseur d'accès internet, qu'imposer un filtrage systématique et sans limitation de durée dans l'intérêt de la protection des droits d'auteur à un tel fournisseur

[126] cf. la décision 496 DC du 10.06.2004 du Conseil constitutionnel relative à la loi du 21.06.2004

contrevenait à l'absence de devoir de surveillance générale pesant sur ceux-ci [127].

[127] cf. *arrêt Scarlet Extended contre SABAM n° C-70/10 du 24 novembre 2011, §§35 et 36 ;* cf. aussi, sur l'équilibre à assurer entre le droit de propriété et notamment les droits d'auteur et les autres droits fondamentaux, *l'arrêt Promusicae CJUE C-275/06 du 29 janvier 2008*

2.- <u>Toutefois, une telle irresponsabilité de principe s'efface lorsque, par leur action ou leur inaction, ces prestataires agissent sur le contenu des informations ou refusent de coopérer à la mise en oeuvre des normes destinées à protéger les droits d'autrui</u>.

21 - **Tel est, naturellement, le cas lorsque ces prestataires jouent, de fait, un rôle actif, en contravention avec les règles précitées qui l'interdisent.**

A cet égard, les autorités chargées de veiller à la protection des données nominatives émettent quelques doutes s'agissant du rôle purement passif de ces prestataires compte-tenu des capacités de filtrage qu'ils développent notamment à des fins économiques *(cf., par exemple, l' avis du Contrôleur européen de la protection des données du 7.10.2011 sur la communication qui suit)* [128].

Un tel contrôle revient, en premier lieu, aux juridictions, qui peinent toutefois à l'assumer compte-tenu et de la technicité requise, et de l'absence de transparence de certains prestataires.

Toutefois, la jurisprudence a tendance aujourd'hui à interpréter largement les obligations générales qui pèsent sur les prestataires, en retenant ainsi leur responsabilité, à tout le moins au plan civil [129]. Un récent arrêt de la Cour européenne des droits de l'homme [130] illustre aussi, en matière de presse, cette évolution, puisque la responsabilité civile d'un site d'information exploitant un blog a été retenue pour des raisons tenant à la fourniture de moyens par l'hébergeur : même en l'absence de connaissance du contenu litigieux, la responsabilité du chef de diffamation est motivée par l'absence d'un filtrage suffisant et de modérateur efficace.

Mais, au-delà même du respect, par ces prestataires, de leur obligation d'impartialité, les normes peuvent leur imposer certaines obligations positives, et cela pour trois raisons.

---

[128] cf. aussi, à titre d'illustration, les polémiques ayant suivi l'arrêt rendu, le 15.01.2014, par la cour d'appel du district de COLUMBIA (U.S.A.) déniant au *"gendarme"* américain des télécommunications - la Fédéral communications commission -, la possibilité d'imposer aux fournisseurs d'accès des règles pour assurer la neutralité d'Internet, les fournisseurs américains désirant surtaxer les plus grands utilisateurs de bande passante pour continuer à les faire bénéficier d'une vitesse de connexion maximale sur leurs sites ou services *(cf. Le Monde, 24.01.2014)*.

[129] la jurisprudence a parfois décidé d'étendre la qualité d'éditeur à des sociétés qui se présentaient comme de simples hébergeurs : ainsi, en son arrêt n° 06-18.855 du 14.01.2010, la 1ère chambre civile de la Cour de cassation a procédé à une telle extension dans une affaire d'atteinte aux droits de propriété intellectuelle par un site accessible via TISCALI, qui s'est vue assimilée à l'éditeur pour avoir fourni des services excédant les simples fonctions technique de recherche. Cette décision a été toutefois critiquée. C'est sans doute la raison pour laquelle cette même chambre, en son arrêt n° 09-13.202 est revenue à une position plus orthodoxe en jugeant que relevait du seul régime applicable aux hébergeurs la société qui, ayant créé un site Internet, se borne à structurer et à classifier les informations mises à la disposition du public pour faciliter l'usage de son service mais sans être l'auteur des titres et liens hypertextes et sans déterminer, ni vérifier les contenus du site, en résumé sans avoir jouer un rôle actif de connaissance ou de contrôle des données stockées. Mais c'est au niveau des juridictions du fond, notamment parisiennes, que cette interprétation extensive est la plus forte.

[130] arrêt DELFI c. ESTONIE du 10.10.2013 ; une telle décision rappelle la jurisprudence antérieure de la Chambre criminelle et que cette dernière a dû abandonner suite à la décision du Conseil constitutionnel 2011-164 QPC du 16.09.2011

22 - **Le premier fondement est évident puisque, maniant des données personnelles, ces prestataires doivent respecter les normes qui leur sont applicables pour la protection de la vie privée.**

La récente condamnation de GOOGLE par la CNIL, ainsi que la mise en cause de cette même société par d'autres autorités de régulation similaires illustrent de telles exigences comme l'importance qui s'attache à un tel contrôle, appelé à s'accroître dans le futur.

23 - **le deuxième fondement tient au rôle joué par ces prestataires qui, bien que de manière non-intentionnelle, participent matériellement à l'accessibilité des contenus contraires aux lois ou le favorisent.**

Telle est la raison pour laquelle la directive 2000 précitée fixe deux premières conditions supplémentaires à l'irresponsabilité des prestataires :

- s'agissant du transmetteur d'informations : il engage sa responsabilité s'il n'agit pas *"promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retenir l'information ou d'en rendre l'accès impossible" (cf. art.13)*

- s'agissant de l'hébergeur, l'irresponsabilité tombe s'il a *"effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, () de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente"* et si, *"dès le moment où il a de telles connaissances",* il n'agit pas *"promptement pour retirer les informations ou rendre l'accès à celles-ci impossible" (cf. art. 14).*

La loi de 2004 en a tiré des conséquences en terme de suites à donner par l'hébergeur, voire par le fournisseur d'accés, aux signalements qui leur sont faits *(art.6)*.

24 - **Il existe toutefois un dernier fondement aux limites de l'irresponsabilité des prestataires, qui tient à ce que l'Etat, au titre de ses obligations positives pour la défense de la vie privée et de la liberté d'expression, doit pouvoir les mobiliser et leur assigner certains objectifs exigés par la prévention ou la répression des infractions commises via ou sur Internet**, dans la mesure où ils constituent un moyen souvent obligé pour faire obstacle à la poursuite d'une violation du droit d'autrui légalement garanti, et pour identifier ou même localiser l'auteur de ces atteintes ou encore réunir des preuves à son encontre.

Une telle exigence relève de **l'intérêt général,** qui doit primer sur les intérêts particuliers, y compris ceux des prestataires.

C'est ce que rappelle, s'agissant des conditions et sauvegardes de nature procédurale *(cf. art. 15 de la Convention),* le rapport explicatif de la Convention sur la cybercriminalité, adopté le 8.11.2001, en soulignant, sans négliger pour autant les contraintes des prestataires, qu'une *"grande importance doit être accordée à 'l'intérêt public', et notamment une 'bonne administration de la justice'... Dans la mesure où cela reste compatible avec l'intérêt public, les*

Parties devraient examiner d'autres facteurs, tels que l'impact du pouvoir ou de la procédure sur 'les droits, responsabilités et intérêts légitimes de tiers', y compris les fournisseurs de service, qui découle des mesures de coercition, et les moyens pouvant être mis en oeuvre pour réduire cet impact. En résumé, il faut d'abord prendre en compte la bonne administration de la justice et autres intérêts publics (comme par exemple la sécurité et la santé publiques, et d'autres intérêts, y compris les intérêts des victimes et le respect de la vie privée)..."

25 - **Pour autant, l'action de l'Etat n'est pas sans limites sur ce dernier point :**.

✓ les unes, générales, relèvent du principe de proportionnalité qui doit guider toute ingèrence dans la vie privée ou la liberté de communication des internautes, ainsi que des garanties qui doivent l'accompagner *(cf., sur ce point, le titre I, chapitre 6).*

✓ les autres, particulières, résultent de l'irresponsabilité première des prestataires et du principe de subsidiarité qui en résulte.

Les textes internationaux comme les textes internes établissent un principe de subsidiarité, les mesures susceptibles d'être prises, notamment en terme de filtrage ou de blocage, devant concerner, au 1er chef, les auteurs du contenu illicite et les éditeurs, ou, à défaut, les fournisseurs d'hébergement et enfin les fournisseurs d'accès à distance.

Cela n'entraîne nullement l'obligation de mettre en cause systématiquement le niveau précédent, comme l'a déjà jugé la Cour de cassation [131], mais signifie simplement que la coopération des prestataires techniques ne doit être sollicitée que si celle de l'auteur du contenu ou de l'éditeur s'avère, selon toutes vraisemblances, impossible ou vaine. En pratique, c'est l'absence d'identification de l'auteur ou son extranéité rendant impossible sa mise en cause, qui incitent l'Etat à se tourner d'abord, de préférence, vers l'hébergeur, et, lorsque ce dernier est à l'étranger, vers le fournisseur d'accès. Mais la mobilisation des prestataires peut aussi être motivée par l'urgence à faire cesser la diffusion illégale.

[131] CIV 1ère n° 07-12.244 du 19.06.2008 : l'obligation faite à un fournisseur d'accès, à défaut de l'hébergeur, de rendre inaccessible un site n'est pas subordonnée à la mise en cause préalable du prestataire d'hébergement.

3.- <u>les formes que doit revêtir la coopération des prestataires techniques et leur encadrement</u>

(31) - Le Conseil de l'Europe recommande qu'au premier chef la coopération entre, d'une part, l'administration ou les services d'enquête, et, d'autre part, les prestataires de service que sont les hébergeurs et les fournisseurs d'accès, s'effectue sur **des bases partenariales**, compte-tenu de l'intérêt commun de créer un environnement informatique plus sûr, plus fiable et mieux protégé.

> *Les lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet contre la cybercriminalité* adoptées en avril 2008 par la Conférence Octopus - qui n'ont pas valeur juridique mais doivent aider à appliquer les normes, notamment de procédure, - préconisent, de préférence à *"une culture de confrontation"*, des échanges d'information, des partenariats formels reposant sur des procédures de coopération écrites et standardisées et la désignation de points de contact *(cf. aussi les lignes directrices visant à aider les fournisseurs de services Internet, développées en coopération avec l'Association européenne des fournisseurs, 2008)*.
> A titre d'illustration, le Conseil de l'Europe a récemment signé avec MICROSOFT un accord sur la contribution de cette société au projet Octopus (3.12.2013).

Au plan interne, des lignes directrices semblables inspirent, depuis près de dix ans, la démarche des pouvoirs publics et des partenaires privés, sans se limiter aux seuls prestataires nationaux :

> - charte de l'A.F.A. en matière de lutte contre la pédo-pornographie, le racisme et la violence *(juin 2004)*
> - charte des fournisseurs d'accès dans la lutte contre le piratage de la musique *(Juillet 2004)*
> - charte des fournisseurs d'accès en faveur du contrôle parental sur l'accès à Internet *(novembre 2005)*
> - charte des plate formes de commerce en matière de commerce électronique *(juin 2006)*
> - accords dits de l'Elysée en matière de lutte contre le piratage de la propriété intellectuelle et artistique sur Internet *(novembre 2007)*
> - charte déontologique des sites comparateurs de prix *(juin 2008)*
> - charte de lutte contre la contrefaçon sur internet *(décembre 2009)*
> - charte sur la publicité ciblée et la protection des internautes *(30.09.2010)*

(32) - **Si une telle contractualisation** - qui relève du partenariat public/privé déjà abordé - **a le mérite de mieux motiver l'ensemble des parties prenantes, grâce à une meilleure prise en compte des contraintes de chacun, elle ne saurait être fondée que sur l'édiction de normes claires, établissant les obligations pesant sur les prestataires techniques.**

Procéder autrement, c'est prendre le risque d'être confronté, comme c'est d'ailleurs le cas actuellement, à des situations très hétérogènes susceptibles d'entamer l'effectivité recherchée dans le respect des droits des internautes et de porter atteinte à la concurrence.

Sans nier l'évolution positive enregistrée ces dernières années, le constat opéré par le groupe interministériel a ainsi démontré, en matière pénale, l'hétérogénéité des pratiques des différents prestataires, leur appétence plus ou moins forte, particulièrement s'ils sont étrangers, à conclure les engagements

nécessaires à la mise en oeuvre de la loi pénale française [132] ainsi que les conséquences néfastes qui en résultent pour les victimes, les administrations techniques, les services de police judiciaire et l'autorité judiciaire s'agissant du respect de la loi.

Il a aussi mis en exergue le fait que, si certains prestataires respectent parfaitement les obligations légales, d'autres s'en affranchissent pour partie, ce qui porte, incontestablement, atteinte à la concurrence.

Au surplus, il y a quelque paradoxe à voir les plus grandes sociétés invoquer le principe de neutralité qui les régit pour refuser l'application de la norme française et européenne, et estimer que les atteintes à cette même neutralité sont admissibles au titre du partenariat. Seul un cadre normatif est de nature à éviter aux prestataires la mise en cause éventuelle de leur responsabilité par les auteurs de contenus lorsqu'ils portent atteinte à ces derniers, sauf lorsque leur action se fonde sur des dispositions contractuelles prévoyant des sanctions en cas de commission d'infraction, auquel cas les réticences de ces sociétés ne sont pas davantage acceptables.

Telle est la raison pour laquelle le droit international incite les Etats à légiférer en cas de besoin.

> Ainsi, la directive précitée du 8 juin 2000 préserve-t-elle, pour chaque type de prestataire, *"la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des Etats membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation"*, voire, s'agissant de l'hébergeur, *"la possibilité, pour les Etats membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible" (cf. art. 12, 13 et 14 in fine).*
>
> Le même texte, après avoir posé l'interdiction d'imposer aux prestataires *"une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites"*, précise aussitôt que *"les Etats membres peuvent instaurer, pour les prestataires de service de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement" (cf. art. 15).*
>
> En outre, l'exposé des motifs précise que sont autorisées les obligations de surveillance applicables à un cas spécifique résultant de la législation nationale *(cf. § 47)* ainsi que les obligations de prudence susceptibles d'être imparties aux hébergeurs *"et ce afin de détecter et d'empêcher certains types d'activités illicites (cf. § 48).*
>
> C'est d'ailleurs à cette unique fin que la Directive 2006/24/CE de l'Union du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au

[132] Afin de mieux identifier les politiques suivies par chaque opérateur et prestataire important, le groupe interministériel a tenu à entendre leurs représentants mais les a saisi d'un questionnaire précis, qui figure en annexe. Si tous ont accepté de répondre, **les réponses des sociétés américaines n'étaient pas encore parvenues lors de la clôture du présent rapport.**

public ou de réseaux publics de communications, a fixé le principe d'une durée de conservation obligatoire comprise entre 6 et 24 mois.

Quant au groupe dit *"de l'art.29"*, il a souligné, dans son avis 1/2008, que la directive 95/46/CE du 24 octobre 1995 relative à la protection des données personnelles ne faisait aucunement obstacle à ce que l'Etat prévoit une obligation de retirer ou de bloquer des données à caractère personnel.

Enfin, à la cohérence juridique recherchée, doit s'ajouter une cohérence institutionnelle.

La détermination des obligations des prestataires techniques comme les relations que l'Etat doit entretenir avec eux doivent répondre à davantage de cohérence puisque, actuellement, chaque administration, voire chaque service spécialisé est, sinon à l'origine de normes spécifiques, du moins de *"négociations"* avec ces interlocuteurs de manière non-coordonnée.

Cette *"parcellarisation"* de l'action publique, encore aggravée par un recours parfois désordonné au partenariat, est source d'hétérogénéité, voire de contradiction tant dans l'application de la norme que dans les pratiques ; elle laisse aussi un large champ de manoeuvre aux interlocuteurs privés, confrontés à une pluralité d'interlocuteurs ; elle génère, en outre, pour ces mêmes prestataires, beaucoup d'incertitudes si les attentes sont contradictoires ou du moins non homogénes.

Elle introduit enfin une césure entre le droit administratif spécial et la procédure pénale, dans la mesure où les services d'enquête comme l'autorité judiciaire n'ont pas qualité pour négocier les modalités d'application de la loi pénale.

Aussi est-il préconisé, sous réserve des pouvoirs déjà impartis à certaines Autorités administratives indépendantes, de confier à la future Délégation interministérielle, par le biais d'une agence consacrée à cet unique objet, le soin d'assurer la cohérence des projets normatifs relatifs aux obligations des partenaires techniques en la matière, de négocier ou de superviser les conventions de partenariat utiles à la mise en oeuvre de l'application de la loi, d'en contrôler l'application, voire d'en sanctionner la violation aux lieu et place des sanctions pénales en vigueur.

Recommandation n° 21
relative à la clarification du droit relatif aux prestataires techniques

Clarifier et préciser les normes en vigueur relatives aux prestataires dits techniques et aux obligations que la loi peut leur imposer, en.

1- réaffirmant l'irresponsabilité de principe des prestataires techniques au regard du contenu des données figurant sur Internet, dans la mesure où ils ont un rôle passif vis-à-vis de ces derniers et respectent les obligations qui leur sont fixées par la norme en terme de protection des données personnelles, ou ayant pour finalité l'identification des auteurs des contenus illicites, la réunion des preuves à leur égard et, dans les limites imparties par la directive européenne, la prévention ou la mise d'un terme à ces activités illicites.

2- Posant expressément le principe que le non-respect de telles obligations est de nature à engager la responsabilité des prestataires, soit au titre de l'action civile entreprise par la personne lésée, soit sous la forme de sanctions administratives ou pénales.

3- Enonçant que, lorsque l'intérêt public et la nature de l'obligation ne s'y opposent pas, la mise en oeuvre des obligations mises par la loi à la charge des prestataires techniques peut prendre la forme de conventions conclues avec ces derniers.

4- Confiant, pour des raisons de cohérence et sous réserve des pouvoirs propres de l'Autorité judiciaire et des prérogatives déjà reconnues par la loi aux Autorités administratives indépendantes, à la future délégation interministérielle, par le biais d'une agence spécifique de régulation, le rôle de veiller à la mise en cohérence des projets de norme créant de telles obligations, de négocier ou de superviser les éventuelles conventions de partenariat, de surveiller l'application, par les prestataires, de ces obligations et conventions, de servir de médiateur aux internautes qui n'ont pu faire reconnaître leurs droits par les prestataires et, sauf en cas d'injonction pénale, de sanctionner administrativement le non-respect de la loi par ces derniers.

4.- L'état des lieux de la coopération entre les services de police et de justice et les prestataires techniques

Les difficultés rencontrées sont de deux natures.

41 - **la première tient au fait que la norme actuelle ne régit pas l'ensemble des prestataires techniques**

> La dichotomie sur laquelle reposent les instruments juridiques actuels - les hébergeurs et les fournisseurs d'accès s'agissant des données de connexion, les seuls fournisseurs en ce qui concerne les interceptions de flux - est de plus en plus battue en brèche par l'apparition, ces dernières années, de prestataires de service de plus en plus variés et hybrides. Outre les fournisseurs de recherche et le positionnement particulier de Google, des réseaux sociaux *(comme Skyrock)*, des forums *(comme Doctissimo)*, des plates-formes de publication participative *(telle Dailymotion [133])* cumulent le statut d'éditeur et d'hébergeur mais en ne fournissant que le cadre de la création de contenus par les internautes eux-mêmes. Quant aux flux de communication en temps réel, ils ne sont plus désormais l'apanage des seuls fournisseurs d'accès mais obéissent à des protocoles variés, même s'ils restent dominés par de grands prestataires étrangers *(Skype notamment)*.
>
> S'il n'est pas de la compétence du groupe de se prononcer sur la question générale tenant à la prise en compte de nouveaux types de prestataires dans les instruments internationaux actuels, question qui fait l'objet, actuellement, de diverses réflexions au titre de la protection de la vie privée [134], il lui revient de s'interroger sur l'opportunité de soumettre certains d'entre eux à partie des obligations positives actuellement applicables aux hébergeurs et aux fournisseurs en ce qui concerne l'application de la loi interne.

Si **les éditeurs de logiciels pour les navigateurs ou pour les messageries** *(cf. Internet Explorer, Firefox, Safari...)* intéressent moins directement l'objet du présent rapport puisque les objectifs qui pourraient utilement leur être impartis relèvent de la sécurité informatique et de la prévention générale *(filtrages anti-virus, blocages de tentatives d'hameçonnage...sur la base notamment des listes qui pourraient être produites à cet effet)*, il n'en est pas de même des fournisseurs de moteurs de recherche.

---

[133] S'agissant de Dailymotion, voir TGI Paris 3ème chambre civile 1ère section 15.04.2008 ; CASS 1ère CIV. 17.02.2011, bull. I n°30 : le réencodage comme la structuration du site en rubriques permettant le classement et donc la recherche des vidéos ne transforment pas l'activité d'hébergeur de cette société en celle d'éditeur dans la mesure où il n'y a pas de choix éditorial.

[134] Sur ce point, il est à noter que, de manière générale, l'Union européenne paraît estimer actuellement que le statut d'hébergeur tel que défini par la Directive sur le commerce électronique ne justifie pas d'être révisé *(cf. Communication de la Commission, janvier 2013)*, aux motifs que devaient être privilégiés des engagements volontaires pris par les différents prestataires ainsi que les procédures de *"Notice and Take down"*.
Il n'est toutefois pas sûr que la jurisprudence suffise, à elle seule, à faire évoluer suffisamment la notion d'hébergeur, bien qu'elle ait commencé à le faire pour les sites de partage ou les plates-formes d'enchère électronique et les réseaux sociaux *(cf. les décisions rendues, en mars 2010 et juillet 2011, par la C.J.U.E., dans les affaires GOOGLE et eBAY ; et celles rendues par la Cour de cassation, le 17.02.2011 Dailymotion et le 3.05.2012 eBAY)*.
Toutefois, et comme le souligne le ministère de l'Economie numérique, il n'est pas certain que l'approche consistant à sérier, un par un, et de façon analytique, les nombreux types de services numériques existants, puisse prospérer au regard du caractère protéiforme, multifonctionnel et mouvant de l'offre de service en ligne.

En l'état, **les fournisseurs de moteurs de recherche** ne sont aucunement réglementés par le droit national.

Il en est de même au regard de la Convention sur la cybercriminalité du Conseil de l'Europe, dans la mesure où cette dernière n'évoque explicitement que les hébergeurs et fournisseurs d'accès *(cf. art.1)*.

Toutefois, ils ne sont pas totalement absents de la directive européenne précitée dont l'exposé des motifs rappelle que la définition des services de la société de l'information, telle que figurant dans les directives 98/34/CE et 98/84/CE, qui couvre *"tout service fourni, normalement contre rémunération, à distance au moyen d'équipements électroniques de traitement et de stockage des données, à la demande individuelle d'un destinataire de services",* concerne aussi, dans la mesure où ils représentent une activité économique*, "des services qui ne sont pas rémunérés par ceux qui les reçoivent"*, tels que *"les services...qui fournissent des outils permettant la recherche, l'accès et la récupération des données" (§ 18)...*

Et une telle intégration est logique puisque, ainsi que le souligne l'avocat général de la Cour de Justice de l'Union Européenne dans ses conclusions en date du 25.06.2013 dans l'affaire *GOOGLE c. Agencia Espanola de proteccion de Datos,* l'accessibilité universelle des informations sur Internet dépend, en réalité des moteurs de recherche, qui jouent ainsi un rôle crucial pour la société de l'information mais renforcent aussi, de manière non intentionnelle, la portée des contenus illicites.

S'il ne crée pas, en principe, de contenu, le moteur de recherche constitue un intermédiaire entre le fournisseur du contenu et l'internaute en extrayant des sites web des contenus qu'il indexe sur ses propres machines, ce qui lui permet, de fournir à l'utilisateur un hyperlien vers les sites qui comportent les termes recherchés par ce dernier. Ainsi, le service d'un moteur de recherche consiste en *"la fourniture d'outils, à la demande individuelle d'un destinataire de services, permettant de rechercher des informations, d'y accéder ou de les extraire".* Le fournisseur est rémunéré, non par l'utilisateur, mais par la publicité qu'il associe, sous forme de contenu additionnel, en marge des résultats de recherche, suite à des contrats passés avec des annonceurs qui, à cette fin, se portent acquéreurs de certains thèmes de recherche en tant que mots-clés.

En l'espèce, l'Agence espagnole de protection des données nominatives avait enjoint à GOOGLE de retirer certaines données personnelles de l'index de son moteur. Si, au regard de la Directive 95/46/UE du 24.10.1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, l'avocat général, après avoir souligné le caractère inadapté de cet instrument au regard du défi actuel que constitue Internet, a émis l'avis que l'injonction en question n'était pas, en général, juridiquement fondée, **il ajoute qu'une procédure de notification ou de retrait concernant les liens vers les pages web sources comportant des contenus illicites relève, par contre, de la responsabilité du droit national.**

A défaut de texte normatif interne, la jurisprudence a tendance, s'agissant du droit de la responsabilité, à appliquer les mêmes critères généraux qu'aux autres prestataires en vérifiant si le fournisseur du moteur de recherches a eu un rôle passif et impartial, ou, au contraire, un rôle actif dans la diffusion du contenu, par exemple, dans la sélection des mots-clés et dans la rédaction des messages publicitaires

Ainsi, la 1ère chambre civile de la Cour de cassation, en son arrêt n° 11-20.358 du 12.07.2012, a-t-elle cassé la décision d'une cour d'appel qui avait refusé la mise en cause du moteur de recherche GOOGLE, via la fonctionnalité Google Suggestion, par une société de défense des droits d'auteur, laquelle invoquait le fait que GOOGLE proposait automatiquement d'associer à la requête initiale des termes de recherche portant sur des noms d'artistes ou d'oeuvre, d'autres termes supplémentaires correspondant à des systèmes de téléchargement illicites ; la Cour de cassation a considéré que, par une telle association, fut-elle automatique, GOOGLE contribuait au téléchargement illégal, le requérant étant alors fondé à en demander la suppression afin de rendre plus difficile la recherche de tels sites [135].

Au-delà de cette question générale de responsabilité, **rien ne justifie que les moteurs de recherche soient exclus des obligations pesant sur les hébergeurs et les fournisseurs d'accès ayant pour objet la prévention et la sanction des contenus illicites figurant sur Internet.**

Telle paraît être aussi l'interprétation du Groupe de l'Union dit de *"l'article 29"* qui, dans son avis 1/2008, précise que l'Etat membre peut prévoir une obligation de retirer ou de bloquer des données à caractère personnel, en fonction du droit de la responsabilité civile délictuelle, et, s'agissant des fournisseurs de moteurs de recherche, un droit de notification et une obligation de retrait, que ces sociétés doivent exécuter.

Il est à noter que certains de ces fournisseurs contribuent déjà, volontairement, à la surveillance du net, soit sous la forme de leur participation à l'A.F.A. dans le cadre de la surveillance spécifique déjà citée prévue par l'art. 6-I.7 *(alors que les moteurs de recherche ne sont pas concernés par ce texte)*, soit dans le cadre de la Charte contre la contrefaçon, soit même par le biais d'un filtrage préalable des résultats de recherche ; ainsi, selon les informations en provenance de la Cour de justice de l'Union européenne, GOOGLE France filtrerait déjà, sans l'énoncer publiquement, *"les objets de collection nazis, les négationnistes de l'holocauste, les partisans de la suprématie blanche et les sites faisant de la propagande à l'encontre de l'ordre constitutionnel démocratique"*, ce qui ne saurait s'expliquer, compte-tenu du principe de neutralité qui s'impose aux prestataires techniques et qui conditionne leur irresponsabilité, que par le fait que ce fournisseur considère, à juste raison, qu'il ne fait en cela qu'appliquer les normes qui s'imposent implicitement à lui.

En outre, tous ces fournisseurs recourrent déjà à des *"listes noires"* s'agissant des sites qu'ils veulent exclus de leur indexation comme mettant en place des techniques frauduleuses en vue d'augmenter leur position de classement dans le moteur de recherche.

Enfin, la loi n° 2010-476 du 12 mai 2010 relative aux jeux d'argent et de hasard en ligne a ouvert la voie puisque l'ARGEL peut solliciter du juge des référés parisien *"toute mesure destinée à faire cesser le référencement du site d'un opérateur...par un moteur de recherche ou un annuaire" (art. 61)*.

[135] Au plan international, l'on pourrait aussi citer, s'agissant de la responsabilité d'un moteur de recherches en ce qui concerne une marque protégée, l'arrêt C.J.C.E. C-236-08 à C-238/08, Google France SARL, Google INC c. Louis Vuitton Malletier SA, Viaticum SA, le Centre national de recherche en relations humaines SARL, Pierre Alexis THONET et autres, du 23.03.2010.

Si l'efficacité d'une mesure de désindexation ou de déréfencement est sujette à caution dans certaines hypothèses *(ex. des spams),* elle est adéquate de manière générale pour les raisons déjà exposées et, tout particulièrement, pour les sites commerciaux. Au surplus, elle est simple et peu coûteuse à mettre en oeuvre pour le prestataire requis et fait l'économie du risque pour les tiers que peut générer un blocage. *La Commission nationale de l'informatique et des libertés* paraît d'ailleurs préconiser des mesures similaires afin de protéger un nouveau droit à l'oubli [136] ; il en est de même du *Conseil supérieur de la propriété littéraire ou artistique* par référence aux actuelles dispositions de l'art. L.336-2 du code de la propriété intellectuelle telle qu'interprétée par le tribunal de Paris. Aussi, **il est temps d'en poser le principe dans la loi.**

Recommandation n° 22
relative aux obligations des fournisseurs de moteurs de recherche

Prévoir qu'au même titre que les hébergeurs et les fournisseurs d'accès, les fournisseurs de moteurs de recherche doivent contribuer, lorsqu'ils en sont requis par la loi, à la prévention ou à la sanction des contenus illicites.

42 - **la seconde difficulté tient à l'extranéité juridique revendiquée par certains prestataires techniques.**

Le constat dressé par l'O.C.L.C.T.I.C. et le S.T.R.J.D. montre que, pour l'essentiel, l'obtention de données de connexion comme les interceptions de flux ne rencontrent pas de difficultés de principe s'agissant des **opérateurs de communications électroniques français** *(Orange, SFR, FREEE, Bouygues Télécom, Numéricable...).*

De manière générale, la France peut d'ailleurs se réjouir de disposer d'acteurs majeurs de l'économie numérique *(0VH, Skyrock, Dailymotion...).*

Dans l'avenir, un enjeu stratégique pour la lutte contre la cybercriminalité est que l'Etat puisse garantir les conditions du maintien de ces sociétés sur son sol, au triple plan économique, fiscal et juridique, et favoriser l'essor de nouveaux acteurs français ou européens.

En revanche, **la coopération avec les entreprises étrangères**, en majorité américaines *(Google, Facebook, Twitter, Microsoft, Yahoo...)*, butte sur le refus de ces sociétés de reconnaître et donc de se soumettre à tout ou partie du droit français, tant pour des raisons d'organisation, que de culture ou pour des motifs juridiques. Par voie de conséquence, cette coopération repose, au principal, sur le principe du consensualisme, que les représentants de ces sociétés ne manquent pas d'invoquer dans le cadre des discussions...

La conséquence, c'est que, si le niveau de coopération va en s'améliorant du fait des relations quotidiennes entretenues par l'O.C.L.C.T.I.C., le S.T.R.J.D., CyberDouanes et d'autres services spécialisés, les prestations restent trop hétérogènes comme dépendant, pour une bonne part, de la politique définie par

[136] cf. rapport d'activité 2012

chaque société, dans la mesure où le droit américain ne joue pas de rôle d'harmonisation et que les intérêts économiques de chacune prédominent.

Les principales difficultés recensées s'agissant des sociétés américaines ont trait à :

- **l'absence de représentation française mandatée pour les obligations légales,** ce qui pose, d'évidence, des difficultés en terme d'échanges et de réactivité *(Facebook, Twitter)* ; en outre, celles de ces sociétés qui disposent d'une délégation en France [137], la limitent à un objet commercial et refusent qu'elles puissent être juridiquement saisies de demandes qui doivent obligatoirement viser la société-mère américaine, sous peine d'être rejetées.

Il est à noter, sur ce point, que la loi du 12.05.2010 sur l'autorisation des jeux en ligne a déjà imposé que les sociétés concernées aient une représentation en France. Il serait des plus utiles que les fournisseurs d'accès étrangers les plus importants s'y résignent, ne serait-ce que pour donner tout son sens au partenariat auquel elles sont attachées, dans la mesure où il n'est pas simple de devoir négocier avec les responsables des services juridiques des filiales irlandaises de sociétés américaines...

- l'absence de politique homogène concernant **la conservation des données.** Alors que le droit français prévoit une durée d'un an, s'agissant des données techniques ou de connexion, comme, sous réserve de l'autorisation d'un juge, pour les données de contenu *(voir le chapitre suivant)*, les sociétés américaines paraissent avoir des pratiques très diverses, qu'elles se refusent, pour l'instant, à afficher [138], ce qui est de nature à faire obstacle tant au gel des données *(sur la base d'une directive européenne que, pourtant, les U.S.A. ont ratifié)* qu'aux réquisitions.

- **le refus de réquisitions** : c'est la question la plus préoccupante.

Les sociétés américaines se fondent, non seulement sur le droit américain compte-tenu du lieu supposé de stockage des données, mais aussi sur l'art.5 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui ne soumet à la loi française que les traitements de données à caractère personnel dont le responsable est établi sur le territoire français ou qui, sans être établi sur ce territoire ou celui d'un Etat membre de l'Union, recourt à des moyens de traitement situés sur le territoire français, ainsi que sur le fait que la loi du 21 juin 2004 est taisante s'agissant du champ de compétence française en ce qui concerne les prestataires techniques [139].

---

[137] et qui n'envisagent pas de la supprimer pour des raisons fiscales...

[138] Google efface les données des comptes devenus inactifs après une durée indéterminée ; Twitter semble les conserver pendant 2 ou 3 mois, même s'il invoque une durée maximale légale de 18 mois ; Facebook paraît donner la priorité à la conservation des données de création de compte, au détriment des données de connexion...

[139] Cette même stratégie est défendue devant les juridictions civiles, ce qui a conduit certaines juridictions *(cf., notamment, le jugement en référé rendu par le T.G.I. de Paris le 24.01.2013 dans une affaire mettant en cause Twitter)* à faire application des dispositions de l'article 145 du code code de procédure civile qui, compte-tenu de la jurisprudence de la Cour de cassation, autorise la juridiction civile à faire application de la loi française pour ordonner toutes mesures d'instruction utiles : c'est dans ce cadre que la juridiction a ordonné

Afin d'y pallier, les services d'enquête ne procèdent pas sous la forme de véritables réquisitions mais sous celle de *"demandes de renseignements"* ; la Chambre criminelle a, récemment, validé de telles pratiques sur le fondement du principe de la libre remise, aux motifs que la limitation de la compétence territoriale d'un officier de police judiciaire ne lui interdisait nullement de solliciter des renseignements à l'extérieur de sa zone de compétence, y compris à l'étranger *(CRIM, plénière, 6.11.2003).*

Toutefois, même si elles visent les textes du code de procédure pénale applicables aux réquisitions, ces demandes n'ont pas de force coercitive et s'exposent, par voie de conséquence, à des refus.

Effectivement, même si elles ne sont pas indifférentes aux exigences françaises, les réponses de ces sociétés sont fonction et des capacités de traitement dévolues par ces entreprises à leurs services juridiques, et de critères inconnus qu'elles déterminent elles-mêmes, tenant soit à la nature des infractions concernées *(Twitter limite ses réponses aux "serious crimes", étant entendu que l'ensemble des sociétés américaines sont aussi réticentes à donner suite aux demandes visant une infraction dite de presse, eu égard à la conception américaine de la liberté d'expression),* soit à des conditions de territorialité.

Ainsi Google et Facebook ne répondent-elles aux demandes que lorsque les utilisateurs concernés sont Européens *(pour le premier)* ou Français *(pour le second)*, par référence au seul critère de l'adresse IP ; en cas contraire, Google fait mention du pays concerné, afin de permettre aux enquêteurs français de se retourner vers celui-ci, Facebook avisant, quant à elle, les autorités du pays concerné, mais sans dévoiler ce dernier aux enquêteurs français.

Autant dire que de nombreuses enquêtes, y compris relatives à la délinquance organisée, se heurtent à l'absence de coopération de ces sociétés, qui font bénéficier ainsi les délinquants concernés, qu'ils agissent depuis la Chine, de pays Africains ou de cyber-paradis, d'une véritable impunité qu'elles sont, à l'évidence, incapables de justifier qu'on on les invite à le faire.

- **le non-respect des conditions de confidentialité** : à l'exception de Google, la majeure partie des autres sociétés américaines *(notamment Twitter et Facebook)* portent à la connaissance des titulaires de comptes les demandes de gel comme les réquisitions qui les concernent, sauf si l'enquêteur précise expressément, dans sa demande, que les investigations ne doivent pas être divulguées. De telles pratiques de notification, d'ailleurs expressément contraires à la procédure pénale française, sont de nature à ôter toute efficacité aux investigations.

Il résulte de tout ce qui précède que les administrations techniques comme les services de police judiciaire, sont souvent voués à l'impuissance, tant en ce qui concerne l'identification des auteurs de

---

la communication aux requérants des données d'identification de gestionnaires de sites à connotation raciste, raison pour laquelle certains services d'investigation conseillent, parfois, en désespoir de cause, aux victimes de recourir à la voie civile.

contenu et le recueil des éléments de preuve, que pour les mesures destinées à mettre un terme à l'infraction. Une partie des classements sans suite décidés par les parquets, qui signent l'impossibilité de l'Etat de protéger les cyber-victimes, s'expliquent aussi par une telle difficulté. Quant aux tribunaux, ils se heurtent à de véritables obstacles pour faire valoir les droits individuels et l'application de la loi, tant civile que pénale.

☞**Le groupe interministériel estime qu'un tel positionnement de sociétés étrangères qui, tout en ayant des millions d'abonnés ou d'utilisateurs sur le territoire français et en engrangeant des bénéfices substantiels tirés de l'exploitation des données personnelles des ressortissants français à des fins publicitaires, refusent délibèrement d'appliquer certaines obligations légales internes ayant pour objet la lutte contre la cybercriminalité et soumettent l'effectivité de cette dernière à leur appréciation, n'est plus admissible.**

Si l'outil Internet facilite l'anonymat et l'irresponsabilité, s'il ne faut pas espérer une collaboration de la part de délinquants qui se rattachent à la criminalité organisée, au moins peut-on attendre des professionnels que sont les prestataires techniques concernés exerçant leur activité sur le territoire français une autre attitude. Mais il y va aussi, comme il a déjà été dit, d'une concurrence équilibrée entre les sociétés françaises et étrangères, comme au sein même de ces dernières.

> Au plan international, si tout un chacun s'accorde à reconnaître que l'état actuel n'est pas satisfaisant et qu'il ne saurait y être remédié, s'agissant de l'obtention des données d'identité et de connexion, par l'entraide pénale ou civile internationale, deux moyens sont préconisés pour y pallier.
>
> *les autorités américaines incitent ainsi leurs interlocuteurs étrangers à saisir directement de leurs demandes, lorsqu'elles portent sur de telles données, les fournisseurs d'Internet. Ce processus public/privé, que préconisent aussi - on l'a vu - les sociétés de droit américain, revient à légitimer le statu quo avec toutes ses effets néfastes ; en outre, les autorités françaises sont plus que réticentes à accorder la réciprocité aux autorités américaines s'agissant des prestataires français - qui, eux, joueraient pleinement le jeu -, pour des raisons que l'actualité récente conforte sans nul doute.
>
> *Sur le plan Européen, si l'Union apparaît réticente à effectuer un distinguo selon la nature des données, alors même que toutes ne sont pas de même nature, y compris au regard des libertés individuelles, *le Comité de suivi* institué par le Conseil de l'Europe au titre de la Convention sur la cybercriminalité y réfléchit actuellement ; mettant en exergue le fait que 80% des demandes de gel portent sur l'adresse IP, il envisage, pour les infractions les plus graves, de faciliter l'échange sur le premier type de données, hors le système d'entraide pénale, sous la forme d'une réquisition policière qui pourrait alors donner lieu à validation judiciaire.
>
> Le Comité souligne, à cet égard, qu'un tel dispositif répondrait à l'esprit de la Convention, qui, en son art.30, souligne la nécessité que le gel rapide des données soit suivi d'une divulgation aussi rapide des données ainsi conservées.

*Quant au Groupe *"de l'article 29"*, s'agissant de la protection des données personnelles [140], il a proposé, soutenu en cela par la Commission, une interprétation plus large du principe de compétence territoriale destinée à viser des opérateurs non établis en Europe ; ce dernier reposerait sur le ciblage du public visé, ou, en d'autres termes, l'offre de biens ou de services aux personnes résidant dans l'Etat considéré [141]. Cette approche est jugée aussi compatible avec la jurisprudence de la Cour de justice de l'Union européenne. Le projet de règlement européen sur les données personnelles officialise une telle approche en appliquant la norme européenne à des opérateurs non établis en Europe mais ciblant des données de résidents européens *(cf. art.3.2, exposé des motifs § 20 et 21).*

La Cour de Justice de l'Union européenne s'intéresse aussi à cet état de fait ; après avoir réuni des éléments d'information intéressants sur la stratégie poursuivie par GOOGLE [142], elle vient de rendre une décision qui va aussi dans le sens d'une extension de compétence. En effet, dans l'arrêt rendu le 3 octobre 2013 *(C-170/12 - Pinckney/KDG Mediatech AG)*, la Cour de Justice énonce, sur une question préjudicielle de la Cour de cassation française et contrairement à l'avis de l'avocat général, qu'est compétente pour connaître d'une violation alléguée d'un droit patrimonial d'auteur la juridiction de l'Etat membre qui protège les droits patrimoniaux dont le demandeur se prévaut et dans le ressort de laquelle le dommage allégué risque de se matérialiser, dès lors que cette violation a été commise *"par l'intermédiaire d'un site Internet accessible dans le ressort de la juridiction saisie".*

Toutefois, l'évolution des normes internationales sur ces différents points demandera encore plusieurs années.

Telle est la raison pour laquelle le Groupe interministériel a choisi une autre solution, relevant de l'action souveraine de la France, consistant à

---

[140] Au plan civil, la compétence de chaque Etat membre s'agissant du traitement des données nominatives est actuellement régie par l'art.4 de la directive 95/46/CE, rédigé avant l'ère d'Internet : il faut que le traitement soit effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat-membre ou, si le responsable n'est pas établi sur le territoire de l'Union, qu'il soit fait recours, à des fins de traitement, à des moyens situés sur le territoire de cet Etat.

[141] art. 3.2. du projet de réglement européen sur la protection des données personnelles : *"Le présent règlement s'applique au traitement des données à caractère personnel appartenant à des personnes concernées ayant leur résidence sur le territoire de l'Union par un responsable du traitement qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union ; ou b) à l'observation de leur comportement".*

[142] les conclusions précitées en date du 25.06.2013 dans l'affaire *GOOGLE c. Agencia Espanola de proteccion de Datos* sont riches d'enseignements s'agissant de GOOGLE. La société Californienne GOOGLE Inc. dispose de filiales dans plusieurs Etats membres de l'Union *(BELGIQUE, FINLANDE...),* dont les activités sont coordonnées par sa filiale Irlandaise ; en l'espèce, la filiale GOOGLE SPAIN est présentée comme une simple représentation commerciale, ne gérant aucun traitement de données à caractère personnel sauf à l'égard des annonceurs espagnols. GOOGLE se refuse, dans le même temps, à situer exactement au plan géographique les traitements de données afférentes aux personnes résidant dans l'Union pour le fonctionnement de son moteur de recherche. Privilégiant, à l'instar du Groupe des 29, une approche économique, l'avocat général estime que chacun des établissements joue un rôle significatif dans le traitement des données *(vente de publicités ciblées en fonction de l'Etat considéré, fourniture de noms de domaines Internet nationaux, activité du moteur de recherche tenant compte de la diversification nationale dans l'affichage des résultats de recherche...).*

soumettre l'ensemble des prestataires oeuvrant sur le territoire national, qu'ils soient français ou étrangers, à un corpus commun d'obligations fondé sur la loi et relatif tant à la fourniture des données d'identité et de trafic qu'à des mesures de coopération destinées à prévenir ou à mettre un terme à des agissements ou contenus illicites, cela dans le strict respect de l'exigence de confidentialité [143].

Recommandation n° 23
relative aux obligations des prestataires techniques étrangers à l'égard de la loi française

Prévoir que les obligations normatives, tant civiles, que pénales ou administratives, imposées aux prestataires concernent non seulement les prestataires français ou installés en France, mais aussi les prestataires étrangers exerçant une activité économique sur le territoire secondaire, fut-elle accessoire, par exemple sous la forme d'abonnements ou de contrats publicitaires, ou offrant des biens ou des services, même à titre gratuit, à des personnes de nationalité française ou domiciliées sur le territoire national, et cela indépendamment du lieu d'implantation de leur siège social et du lieu de stockage de leurs données.

43 - la troisième et dernière difficulté rencontrée par les services d'investigation, essentiellement territoriaux et non spécialisés, tient à **la formalisation des demandes.**

Ils rencontrent, en effet, des difficultés pour mettre en forme les demandes en fonction des modalités, d'ailleurs hétérogènes, imposées par les prestataires, mais aussi en ce qui concerne la célérité des réponses souhaitées du fait d'un recours trop systématique à la notion d'urgence ou d'un manque de diligence des destinataires.

Outre l'effort de formation déjà évoqué, il s'agit ici de faciliter et d'accélérer les réquisitions adressées aux opérateurs, hébergeurs et fournisseurs d'accès, en les formatant davantage ainsi que les circuits d'acheminement.

Déjà, le ministère de l'Intérieur, par la création de *guichets unique téléphonie et internet (G.U.T.I.)* - dont dispose chaque direction centrale *(à l'O.C.L.C.T.I.C. pour la direction de la police judiciaire, au S.T.R.J.D. pour la gendarmerie...)* - a créé une fonction d'assistance au bénéfice des services et même de résolution des difficultés remontées du terrain grâce à des contacts périodiques avec chaque prestataire. En outre, une telle centralisation partielle permet de prioriser les dossiers importants et d'aider à l'exploitation des résultats techniques les plus complexes.

[143] A noter que l'actuel projet de loi sur la consommation ouvre d'ailleurs la voie puisque le futur art. L. 139-1 du code du même nom s'apprête à définir ce qu'il faut entendre par *"lien étroit avec le territoire d'un Etat-membre"* par référence, entre autres, au fait que *"le professionnel dirige son activité vers le territoire de l'Etat membre où réside le consommateur"* ou que *"le contrat a été précédé dans cet Etat d'une offre...ou d'une publicité..."*.

Toutefois, une telle assistance n'a pas résolu tous les problèmes : faute d'interphase centralisée unique entre les services de police et de justice et ces prestataires, chaque service territorial reste contraint de procéder, par ses propres moyens, à des investigations, souvent lourdes et auxquelles il est mal formé, s'il n'a pas la chance d'être doté d'un enquêteur spécialisé ; une partie non négligeable des réquisitions *(entre 15 et 25% selon les opérateurs)* est toujours rejetée pour des questions de forme ou reste sans réponse ; même si une récente tarification mise en oeuvre par le ministère de la Justice va produire un effet positif, les frais de justice sont exhorbitants et conduisent les parquets à définir une politique malthusienne, faute de crédits suffisants...Autant d'obstacles qui s'ajoutent aux difficultés générées par l'anonymat...Quant aux prestataires, ils restent confrontés à des demandes par trop hétérogènes, tant dans leur présentation que dans leur formulation, ce qui ne facilite pas leur tâche.

Pourtant, l'outil existe et sera opérationnel dans quelques mois s'agissant des réquisitions adressées aux opérateurs téléphoniques, tant fixes que mobiles : la future **plate-forme des interceptions judiciaires (PNIJ)**, conçue par le ministère de la Justice.

Tout en préservant la responsabilité de la décision policière et judiciaire, elle devrait décharger les services enquêteurs d'une partie de leurs charges ; diminuer les temps de réponse ; favoriser la substitution aux réquisitions individuelles de demandes multiples transmises en ligne ou sur support numérique ; contribuer à une baisse très sensible des frais de justice grâce à la passation de marchés globaux ; et assurer un meilleur contrôle des prestataires.

Dès lors, la solution consiste à confier à cette plate-forme la responsabilité du transit des réquisitions adressées aux prestataires pour les besoins de la lutte contre la cybercriminalité, du moins pour les principaux fournisseurs d'accès Internet, car la multiplicité des interlocuteurs, notamment des réseaux sociaux, commande, pour le reste, de maintenir le rôle des *guichets* existants, qui ont montré leur pertinence et leur souplesse. Ainsi, les services territoriaux seraient-ils déchargés de partie des tâches administratives qui leur incombe actuellement, les policiers et les gendarmes affectés à la PNIJ jouant d'ailleurs, pour les demandes qui transiteront par là, un rôle assimilable à celui des guichets en question.

Recommandation n° 24
relative à l'extension du rôle assigné à la future plate-forme des interceptions judiciaires

Elargir, par le biais d'une modification réglementaire, les missions dévolues à la plate-forme des interceptions judiciaires au traitement des réquisitions adressées aux principaux fournisseurs d'Internet.

5.- Les mesures exigibles au titre de la coopération des prestataires techniques

Si les prestataires ne sauraient être astreints à une obligation de surveillance générale, tant les instruments internationaux que la loi du 21 juin 2004 prévoient la possibilité de les soumettre à des obligations spécifiques de surveillance spéciale.

Elles nécessitent aujourd'hui et un cadrage normatif plus précis et une mise en cohérence.

51 - **les obligations dites préventives**

En l'état, l'art.6.I.1 de la loi sur l'économie numérique fait obligation aux fournisseurs d'accès Internet de mettre à disposition de leurs abonnés un logiciel de filtrage afin de leur permettre de restreindre l'accès à certains services ou de les sélectionner.

Ces mêmes fournisseurs doivent aussi informer leurs abonnés des moyens de sécurisation leur permettant de prévenir un manquement aux obligations de l'article L.336-3 du code de la propriété intellectuelle en terme d'utilisation de leur accès à Internet *(art.6.I. al.2)*.

S'agissant enfin des seuls jeux en ligne, les opérateurs doivent informer *"leurs abonnés des risques encourus par eux du fait d'actes de jeux réalisés en violation de la loi".*

La future Agence dont la création est préconisée devra contrôler le respect des deux premières obligations, l'A.R.J.E.L. étant déjà compétente pour la troisième.

Mais les obligations préventives doivent aller plus loin en ce qui concerne

☞ **la détection d'infractions d'une gravité certaine et se prêtant à une appréhension technique** [144], telles que celles faisant consensus au niveau international ou visées par les instruments européens ou faisant déjà l'objet, pour partie, d'une mesure de filtrage de la part de certains prestataires [145]. Pourquoi faire peser ce type de détection, comme actuellement le fait la loi, sur les seuls internautes alors que les prestataires sont en mesure de le faire de manière beaucoup plus efficace ?

---

[144] Il est à noter que le droit pénal comporte déjà implicitement de telles exigences, par exemple l'art. 227-24 qui incrimine le fait de *"...transporter, de diffuser...un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger..."*, même si le législateur a pris la précaution de renvoyer, en ce qui concerne la détermination des personnes responsables aux *"dispositions particulières des lois qui régissent ces matières" (?)* ; cf. aussi la loi du 16.07.1949 relative aux publications destinées à la jeunesse....

[145] cf., dans le cadre de la lutte contre la contrefaçon sur Internet, la charte signée en décembre 2009 par les titulaires de grandes marques et plusieurs plates-formes de e-commerce, et dans laquelle ces dernières s'engagent à mettre en oeuvre des mesures de filtrage par mots-clés des annonces et des profils des vendeurs afin d'identifier les annonces manifestement illicites ; en février 2012, cette opération a été étendue aux sites de petits annonces entre particuliers ainsi qu'aux opérateurs postaux.

Recommandation n° 25
relative à la détection, par les hébergeurs et fournisseurs, d'infractions graves

Fixer par la loi aux prestataires, en particulier les hébergeurs, les fournisseurs de moteurs de recherche et les fournisseurs d'accès, une obligation de surveillance préventive s'agissant de la détection des contenus illicites présentant un degré de gravité particulier et se prêtant techniquement à une telle détection. Il est recommandé, à cette fin, de viser les infractions déjà énumérées à l'art. 6-I.7 de la loi du 21.06.2004 ou susceptibles de l'être. Ce contrôle devrait donner lieu, ainsi que le prévoit déjà l'article en question, à l'information de l'autorité publique par le biais d'un point central - l'O.C.L.C.T.I.C.

52[146] - Les obligations relevant de la technique dite de la notification/action

En l'état, la loi sur l'économie numérique du 21 juin 2004 prévoit deux types de signalements :

-l'un, qui relève de la responsabilité limitée des hébergeurs, résulte de la directive européenne sur le commerce électronique et de sa transposition dans l'art. 6.I.2 et 6.I.3 : le mécanisme mis en oeuvre permet à toute personne, y compris la personne publique, de dénoncer à l'hébergeur un contenu illicite quelconque ; à la condition que cette dénonciation soit spécialement justifiée dans les conditions prévues par l'art. 6.I.5 de la loi du 21 juin 2004 et que le caractère illicite soit manifeste[147], l'hébergeur doit retirer l'information ou en rendre l'accès impossible, sous peine de voir sa responsabilité civile et pénale retenue.
En fait, ce dispositif s'avère, en l'état, peu efficace s'agissant des personnes privées, d'autant plus que les sanctions prévues par la loi ne sont pas appliquées.
En revanche, il a été investi par l'autorité publique ; de telles demandes, qui relèvent alors de la police administrative, peuvent viser aussi bien des hébergeurs étrangers que français ; elles sont généralement satisfaites à l'heure actuelle lorsque l'infraction visée concerne le racisme, la pédopornographie ou l'escroquerie. Il s'agit toutefois d'une simple obligation de moyens, dans la mesure où l'hébergeur peut s'exonérer de toute responsabilité s'il justifie que l'auteur ou l'éditeur de la page concernée a été inviter à retirer ou à modifier le contenu faisant grief [148].

- l'autre, qui relève de la surveillance spéciale mise à la charge tant des hébergeurs que des fournisseurs d'accès *(art. 6.I.7),* qui doivent apporter leurs concours *"à la lutte contre* (certaines) *activités illicites"* ; en fait, faute de précision, cette obligation se limite, en droit,

---

[146] *procédure dite de "Notice and Stay-down"*

[147] cf., sur ce point, la réserve d'interprétation du Conseil constitutionnel dans sa décision 2004-496 DC du 10 juin 2004 relative à la loi en question

[148] En effet, la manière dont l'hébergeur va répondre à la demande est indifférente : il est fréquent qu'il prenne contact, préalablement à la fermeture de tout un site, avec l'éditeur concerné.

* à la mise en place d'un dispositif *"facilement accessible et visible"* permettant aux abonnés de signaler aux opérateurs techniques les contenus illicites dans le domaine de la pornographie enfantine, de l'incitation à la discrimination ou à la haine, de l'apologie de crimes contre l'humanité ; son champ d'application vient d'être étendu, par la loi pour l'égalité entre les hommes et les femmes, à la provocation à la discrimination ou à la haine ou à la violence à raison du sexe, de l'orientation ou de l'identité sexuelle ou de l'handicap *(art. 24, al.9, de la loi sur la presse)* ainsi qu'à l'enregistrement ou à la diffusion des atteintes volontaires à l'intégrité humaine *(art. 222-1 à 222-14-1, 222-23 à 222-31 et 222-33 du code pénal)*.
Ce texte, comme la proposition de loi renforçant la lutte contre le système prostitutionnel *(qui souhaite étendre cette même surveillance à la traite d'êtres humains et au proxénétisme et assimilé - art. 225-4-1, 225-5 et 225-6 du code pénal),* illustre la tendance actuelle à élargir le dispositif.

*à l'information prompte des autorités publiques compétentes, via l'O.C.L.C.T.I.C.

*à la publicité faite aux moyens consacrés à la lutte contre ces activités illicites.

Ce *"flou du droit"* a généré, comme il fallait s'y attendre, des pratiques hétérogènes selon les prestataires.

Ainsi les prestataires membres de l'Association des fournisseurs d'accès à Internet *(A.F.A.)* [149] ont-ils mobilisé leur service de signalement *"Pointdecontact" (cf., sur ce point, le titre II, chapitre 4)*. Les mécanismes déjà décrits montrent, en fait, que les fournisseurs d'accès n'ont jamais recours à la technique dite du blocage à laquelle ils sont pourtant astreints par la loi, car c'est principalement l'hébergeur qui est sollicite pour mettre un terme à l'infraction.

Les pratiques des prestataires non membres de l'AFA varient : si FACEBOOK comme TWITTER ont mis en place un dispositif de base suite aux pressions ministérielles, en revanche, d'autres prestataires, notamment français tels que FREE, refusent toujours de se soumettre à une telle obligation. Enfin, l'accessibilité et la visibilité du dispositif sont souvent sujettes à caution [150].

Cet état de fait illustre les propos antérieurs sur les limites du recours au partenariat lorsqu'il s'agit de lutter contre la cybercriminalité et les atteintes à la concurrence que représentent une telle diversité, atteintes d'ailleurs fort justement dénoncées par l'A.F.A. qui a souvent exprimé le souhait que les pouvoirs publics fassent respecter l'art. 6.1.7 précité par les grandes entreprises françaises qui s'en affranchissent toujours alors qu'il s'agit d'une obligation pénalement sanctionnée. Et le constat s'avère encore davantage négatif en ce qui concerne les entreprises étrangères non affiliées à l'A.F.A....

Il démontre l'absolue nécessité tant de préciser les obligations normatives que d'instituer cette autorité de régulation déjà évoquée, afin de s'assurer du respect de leurs obligations par l'ensemble des prestataires et de sanctionner les manquements

[149] L'AFA regroupe tant des hébergeurs en ligne que des fournisseurs d'accès ou de moteurs de recherche, et notamment BOUYGUES TELECOM, GOOGLE France, MICROSOFT, ORANGE et S.F.R.

[150] notamment lorsque l'information figure sur le portail d'un opérateur, que personne ne consulte...

constatés, étant entendu que les sanctions pénales prévues par la loi du 21 juin 2004 ne sont jamais appliquées.

Depuis 2004, ces deux dispositifs généraux ont été enrichis par des mesures thématiques, tel le protocole européen signé en mai 2011 avec des plate-formes commerciales sur la vente en ligne des produits contrefaits, qui prévoit déjà, outre une action envers les infractions répétées et des mesures préventives ou proactives, un système de notification et retrait.

En ce qui concerne ces *"procédures de notification et action"* - visant les procédures suivies par les prestataires intermédiaires de l'Internet pour agir contre des contenus illicites suite à la réception d'une notification -, l'Union européenne souhaite, tout à la fois, inciter à les généraliser, mais aussi unifier les pratiques existantes ; ainsi la communication de la Commission 2011 (942), relative à *"un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne"* annonçait la mise en place d'un cadre européen plus global. Les préconisations qui suivent sont ainsi faites sous réserve d'un tel cadre, étant toutefois souligné qu'il n'aura rien d'exclusif et ne devrait être qu'incitatif..

Si, de manière générale, la technique du signalement contribue à la vigilance des internautes et à une manifestation de civisme qu'il convient d'encourager, il convient toutefois de préciser quel doit en être le destinataire compte-tenu de la nature de l'intérêt en cause, tout en donnant davantage de cohérence aux dispositifs existants.

□ **S'agissant des droits de la personne à la protection de sa vie privée comme, par exemple, de ses droits de consommateur** - et de manière générale lorsqu'est en cause le droit particulier d'une personne -, il est cohérent qu'ils s'expriment, en premier lieu, si la personne qui s'estime lésée le souhaite, sous la forme d'un demande de retrait adressée à l'auteur du contenu ou, à défaut, sous celle d'une demande de retrait ou d'inaccessibilité adressée à l'hébergeur. A cet égard, obligation devrait être faite aux prestataires de mettre en place un dispositif facilement accessible en ligne et visible[151] .Il serait d'ailleurs opportun de recommander qu'un tel dispositif soit utilisé préalablement au dépôt de plainte ou à la saisine du juge [152].

Cette demande devra continuer à être spécialement motivée afin de permettre au prestataire d'apprécier *"le caractère manifestement illicite"* du contenu ou du comportement dénoncé [153].

---

[151] curieusement, seul l'art.6.I.7 fixe une telle obligation

[152] à noter aussi le droit de réponse ouvert à toute personne nommée ou désignée dans un service de communication au public en ligne, qui, en cas d'anonymat de l'éditeur, peut être exercé via l'hébergeur *(cf. art. 6-VI de la loi du 21.06.2004, décret n° 22007-1527 du 24.10.2007) ;* comme l'a rappelé la Cour de cassation, il appartient à la juridiction civile de déterminer si le refus d'insertion d'un droit de réponse constitue ou non un trouble manifestement illicite, en fonction de l'existence ou non du préjudice allégué, le plus souvent une diffamation. L'efficacité d'une telle disposition reste à prouver.

[153] la liste des données devant accompagner la demande est souvent jugée trop importante *(cf. art. 6.I.5 de la loi de 2004) ;* elle revêt toutefois un caractère impératif au regard de la décision du Conseil constitutionnel et constitue la nécessaire contrepartie de l'absence de procédure contradictoire *(cf. CIV 1ère n°s 09-67.896 et 09-15.857 du 17.02.2011).*

Toute demande devra donner lieu à réponse de la part de l'hébergeur, le rejet devant être succinctement motivé *(tel est déjà le cas dans la Charte relative à la contrefaçon)*.

Dans l'hypothèse où le demandeur entend contester les motifs du rejet, **il aura l'obligation d'en saisir l'agence de régulation relevant de la Délégation interministérielle préconisée - ou, en matière de droit de consommation, un dispositif équivalent que l'actuel projet de loi semble envisager - qui devra, en fonction de l'analyse à laquelle elle se livrera, offrir sa médiation en ligne** *(cf. les recommandations relatives aux victimes, chapitre 6).* Tout refus considéré comme abusif de la part d'un prestataire continuera de pouvoir donner lieu à sanction, mais par le biais de l'agence en question, la sanction pénale existante *(art. 6.I.4. de la loi du 21.06.2004)* s'étant révélée peu effective.

Ce n'est qu'en cas d'échec de cette médiation, que le demandeur aura la possibilité d'agir en justice, s'il le souhaite.

S'il est généralement souhaité que la procédure civile soit rendue, à cet égard, plus effective et plus rapide, il n'est pas apparu possible de préconiser la procédure de saisine sur simple requête, dans la mesure où le contradictoire doit être assuré à l'égard du prestataire concerné.
Toutefois, le juge civil, qui bénéficiera de l'application du droit français à l'ensemble des prestataires étrangers, se verrait aussi explicitement reconnu le droit d'ordonner au moteur de recherche le déférencement du site concerné, droit qui ne résulte pas, en l'état, des dispositions de l'art. 6-I.8 de la loi du 21.06.2004, en ce qu'elles ne visent que les hébergeurs et les fournisseurs d'accès.

□ **S'agissant, en revanche, des infractions relevant de la protection de l'ordre public pris au sens large**, et de manière générale lorsque la personne qui se prétend lésée n'est pas à l'initiative de l'action, l'application de la loi ne saurait reposer sur le signalement d'internautes-tiers adressé directement aux hébergeurs [154], le destinataire devant en être l'autorité publique et sur la base d'un point d'accès unique. Tel est déjà notamment le cas s'agissant de la plate-forme PHAROS.

Il reviendra à l'autorité d'accuser réception du signalement et d'aviser l'intéressé, au besoin par des procédés automatisés, des suites données.

Par voie de conséquence, en pareille hypothèse, **le dispositif de *"notification/action"* à l'égard de l'hébergeur, voire du fournisseur d'accès, serait le fait de l'autorité publique s'agissant des contenus manifestement illicites, et cela quelle que soit la nature de l'infraction.** Sauf à contester ce caractère devant l'autorité judiciaire civile - et non administrative -, le prestataire serait tenu, comme actuellement, de rendre l'information inaccessible.

Si une telle distinction devrait contribuer à clarifier les dispositifs existants, **elle n'a toutefois pas vocation première à remettre en cause les dispositifs de signalements partenariaux actuels**. Néanmoins, pour faciliter l'information

[154] En outre, l'effectivité de tels signalements paraît assez réduite

comme les droits de l'utilisateur-consommateur, il serait opportun, là aussi et comme il a déjà été dit, d'unifier autant que faire se peut les points d'accès. Tel pourrait être aussi le rôle de l'agence de régulation précitée.

□ **Toutefois, le dispositif de notation/action ne saurait se limiter au signalement des contenus manifestement illicites.**

Le droit français connaît déjà de deux autres types de dispositions, qui relèvent aussi de la surveillance spéciale imposée aux hébergeurs et fournisseurs d'accès.

> - s'agissant des jeux d'argent et de hasard en ligne, les hébergeurs et fournisseurs d'accès doivent aviser leurs abonnés des services de jeux en ligne qui sont considérés comme répréhensibles par les autorités publiques en la matière *(cf. art. 6.I.7 et 6-VI.1 de la loi du 21.06.2004 modifiée)*.
>
> - le même article 6.I.7 prévoit, de manière sybilline, la possibilité, pour l'autorité judiciaire, de demander une *"surveillance ciblée et temporaire"* aux hébergeurs comme aux fournisseurs d'accès ; faute de précision, une telle disposition est restée lettre morte.

Il appartient à l'Etat de préciser, au regard de l'intérêt public, des capacités des prestataires et des initiatives déjà prises à cet effet, les obligations en la matière, même s'il importe aussi de laisser la marge à l'évolution souhaitable et au partenariat.

Sans prétendre à l'exhaustivité, quatre types de mesures pourraient être requises de ces prestataires ainsi que des fournisseurs des moteurs de recherche :

☞ **la notification, par l'autorité administrative compétente sur la base des décisions administratives prises à cet effet, des noms de domaines interdits ou confisqués** *(voir, supra, le chapitre 4),* **ainsi que des sites illégaux, marques contrefaites et autres aux fins de retrait d'accès ou de déréfencement** *(pratique dite des "listes noires")* ; encore faut-il s'assurer du respect de ces mesures par les fraudeurs et de la non-réapparition des contenus illicites.

☞**la notification aux mêmes fins - mais aussi, le cas échéant aux fins de blocage par les fournisseurs d'accès - par la police judiciaire, agissant d'office ou sur plainte de la victime, des données manifestement illégales relatives à la pédopornographie** : si, de manière générale, la police judiciaire ne saurait être dotée d'un pouvoir de sanction qui relève exclusivement de l'autorité judiciaire, il n'est pas nécessaire, compte tenu du caractère manifestement illicite de telles images et des instruments internationaux existants, de soumettre une telle action à l'appréciation préalable d'une autorité judiciaire. Afin de préserver toutefois les possibilités d'enquête et de poursuite, la conservation éventuelle des données pourrait être, concomitamment, ordonnée *(pour les blocages, voir les développements in fine)*.

Ces deux types de notifications revêtiraient un caractère obligatoire pour les prestataires, qui pourrait toutefois saisir le juge en cas de contestation.

Il est proposé, par souci de cohérence, de soumettre l'ensemble des recours des prestataires au seul juge judiciaire.

☞ **l'injonction, par l'autorité judiciaire, civile comme pénale, consistant en la notification des mesures, provisoires ou définitives, tendant à la suppression ou à la limitation d'accès d'activités ou de contenus illicites, mais aussi de celles destinées à éviter leur réitération pendant une durée déterminée, si leur nature le permet techniquement** [155]. En résumé, il s'agit de davantage mobiliser les prestataires en vue d'une meilleure effectivité des décisions de justice [156]

Actuellement, seul le juge civil a la capacité de décider de mesures provisoires.

Afin de mieux préserver les droits des victimes et de rendre plus effective l'action pénale, il est préconisé, s'il y a **urgence** de mettre fin à l'infraction, de **créer une procédure pénale comparable à celle du référé civil, consistant, pour le procureur de la République à saisir, sur simple requête [157], le juge des libertés et de la détention ou le juge d'instruction aux fins de retrait ou, à défaut, de déréférencement, voire, dans les conditions prévues in fine, de blocage, avec conservation concomitante des données nécessaires à la poursuite.**

En outre, le juge pénal compétent sur le fond pourrait ordonner, au même titre que le juge civil, les mesures précitées.

☞ **toujours au titre judiciaire, l'injonction aux fins de mise à exécution du droit à l'oubli qu'il est proposé de reconnaître au bénéfice du mineur ou du jeune majeur, sous contrôle du juge** *(cf., supra, la recommandation n°).*

---

[155] Il convient d'éviter, toutefois, certaines pratiques qui s'apparentent à de la surveillance générale ; cf. CIV 1ère n° 11-15.165 et 188, qui a jugé contraire aux dispositions de l'art. 6-I le fait d'ordonner à un hébergeur et à un gestionnaire des services de référencement de prendre toutes mesures utiles pour prévenir toutes nouvelles mises en ligne d'une photographie litigieuse, mesure assimilable à une obligation générale de surveillance et à la mise en place d'un dispositif de blocage sans limitation dans le temps ; elle a ainsi jugé la fonction GOOGLE Image non responsable d'une remise en ligne. Cf. aussi, s'agissant de GOOGLE Vidéo pour une remise en ligne d'un film CIV 1ère n° 11-13.669 du 12.07.2012 et n° 11-13.166 du 21.07.2012.
Pour autant, on ne saurait admettre que certaines décisions de justice relatives à la fermeture de sites soient systématiquement coutournées par l'ouverture, dès le lendemain de leur rendu, de sites autrement dénommés mais poursuivant un objet identique

[156] Il est à noter qu'une telle possibilité intéresse aussi les autorités administratives ; ainsi, dans le cadre des réflexions poursuivies par Mme. IMBERT-QUARETTA sur la contrefaçon en ligne des oeuvres protégées au titre de la propriété intellectuelle, il serait envisagé de passer des accords cadre avec les professionnels de la société de l'information afin d'inciter à la généralisation des pratiques de retrait durable volontaires grâce à l'utilisation des technologies de reconnaissance des contenus, pendant une certaine période *(cf. la Charte de 2009)*.

[157] cf., à titre de comparaison, les pouvoirs déjà dévolus au J.L.D. afin d'autoriser une visite domiciliaire en enquête préliminaire ; de manière générale, dans le cadre d'une procédure pénale, il est plus aisé pour le parquet de saisir le J.L.D. que de recourir au juge des référés, raison pour laquelle l'art. 50-1 de la loi du 29.07.1881 sur la presse n'est quasiment pas appliqué.

Il serait vraisemblablement opportun que, à tout le moins pour les injonctions judiciaires, ces décisions puissent être ramenées à exécution par une autorité centralisée, qui, le cas échéant, pourrait aussi faire bénéficier les autorités concernées de conseils, voire d'une aide sur le plan technique, et, sur un plan plus général, négocier avec les prestataires les modalités techniques afférentes à ces différentes mesures ; ce devrait être le rôle de l'agence spécialisée au sein de la délégation interministérielle dont il est proposé la création.

Recommandation n° 26
relative à la procédure dite de notification/action à l'égard des hébergeurs et fournisseurs

1 - Maintenir le droit reconnu à toute personne qui s'estime personnellement lésée par une activité ou un contenu publié sur Internet, le droit, à défaut de pouvoir s'adresser directement à l'auteur du contenu, à l'éditeur ou au directeur de publication, de le signaler en ligne à l'hébergeur, via un dispositif approprié mis en oeuvre par ce dernier de manière simple et accessible.
Ce signalement devra continuer à être motivé conformément aux dispositions de l'art. 6-I.5 de la loi du 21.06.2004.
Obligation sera faite à l'hébergeur, comme actuellement, d'effectuer le retrait ou de rendre le contenu inaccessible en cas d'illégalité manifeste ; en cas d'absence de réponse ou de rejet, succinctement motivé, le demandeur devrait pouvoir saisir l'agence de régulation précitée aux fins de médiation ; ce n'est qu'au terme de ce processus, qu'une action civile ou pénale serait susceptible d'être engagée.

2.- Reconnaître à toute personne non individuellement lésée par une activité ou un contenu accessible sur le net et qui lui paraît illicite ou dangereux, le droit de le signaler à l'autorité publique, et cela en ligne et via un point d'accès unique qui pourrait être la plate-forme PHAROS.
Cette dernière devra l'aviser des suites données.

3.- Reconnaître le droit de l'autorité publique de notifier, dans le respect du principe de subsidiarité,
- à l'hébergeur les contenus manifestement illicites aux fins de retrait ou d'inaccessibilité, comme c'est déjà le cas aujourd'hui
- à l'hébergeur, au fournisseur de moteur de recherche, voire au fournisseur d'accès, aux fins de retrait, d'inaccessibilité, de déférencement, voire, dans des conditions précisées plus avant, de blocage,
*les décisions administratives relatives aux noms de domaine interdits ou confisqués et aux sites ou contenus illégaux,
*les signalements de la police judiciaire relatifs à la pédopornographie
*les décisions judiciaires civiles relatives à la reconnaissance du droit à l'oubli
*les décisions judiciaires, civiles ou pénales, provisoires ou définitives, ordonnant de telles mesures aux fins de mise à exécution ou/et de prévention de la réitération des infractions pendant une période limitée dans le temps.

4.- A cette fin, habiliter le juge des libertés et de la détention et le juge d'instruction à prendre, en cours de procédure pénale, des mesures provisoires comparables à celles du juge des référés.

5.- Prévoir que, sous réserve de la saisine par leurs soins du juge judiciaire, l'inaction et le refus des prestataires feront l'objet de sanctions, soit de nature pénale lorsque l'injonction est judiciaire, soit de nature administrative dans les autres cas.

6.- Préciser que les obligations ainsi mises à la charge des prestataires constituent des obligations de moyens dont le contrôle devrait relever de la Délégation interministérielle future, leur responsabilité, administrative ou pénale, ne pouvant être engagée s'ils justifient avoir mis en oeuvre tous les moyens nécessaires à l'accomplissement des missions ainsi imparties.

✓ les propositions qui suivent n'épuisent toutefois pas le sujet car il convient aussi d'encadrer plus strictement **les prestataires de paiement** comme **les régies publicitaires**, ainsi que le principe en est déjà acquis pour les jeux en ligne.

Par-delà, il est aujourd'hui acquis que certains sites et contenus illicites ne prospèrent que grâce à certains flux financiers mal identifiés. Les Etats-Unis ont su, par exemple, mobiliser les opérateurs de paiement comme *Pay Pal, MasterCard, Visa ou American Express* pour bloquer ces flux financiers à destination des sites de jeux illicites ou des sites de piratage *(programme "follow the money" = "frapper au portefeuille").*

En interne, ces mêmes prestataires ont déja développé en France des dispositifs internes du même ordre en cas de pédophilie, ce qui montre leur capacité à procéder à de l'auto-régulation qui pourrait aussi être mobilisée à d'autres fins.

La réflexion publique semble plus avancée dans le secteur marchand, notamment sur les contrefaçons.

Le groupe interministériel n'a toutefois pas poussé sa réflexion sur ce point jusqu'à son terme, qui aurait nécessité d'entendre les principaux prestataires concernés.

✓ Enfin, s'agissant de l'action pénale, les réquisitions et autres mesures destinées à permettre l'identification et la localisation de l'auteur présumé ainsi que le recueil des preuves de l'infraction, il convient de se référer aux dispositions prévues par le code de procédure pénale ou les textes spécifiques.

6. - De quelques obligations particulières

La géo-localisation

Il s'agit d'une technique permettant aux opérateurs de communication électronique de déterminer, en temps réel ou de manière différée, la localisation d'une personne, d'un véhicule ou de tout autre objet doté d'un terminal de communication.Elles étaient ordonnées jusqu'à ces derniers temps, indifféremment par le procureur de la République ou le juge d'instruction, sur le fondement des pouvoirs généraux qui leur étaient reconnus par la loi comme par la jurisprudence *(cf. en ce sens, les arrêts CRIM. n° 11-84.315 du 9.11.2011 et n° 11-84.308 du 22.11.2011).*

Les deux arrêts rendus par la Chambre criminelle le 22.10.2013 *(n°s 13-81.945 et 13-81.949),* en énonçant que de telles mesures constituaient *"une ingérence dans la vie privée nécessitant d'être ordonnée sous le contrôle d'un juge"*, ont contraint le Gouvernement à préparer en urgence un projet de loi, actuellement en cours de discussion parlementaire.

Compte-tenu de cet examen, le groupe interministériel a entendu se borner à souligner l'importance que revêt le recours à une telle technique ; les difficultés que suscitent de tels revirements de jurisprudence ; l'urgence qui s'attache à ce qu'il soit remédié, dans les meilleurs délais, à la vacuité actuelle ; la nécessité que les garanties du futur dispositif prennent en compte et la réactivité indispensable à certains types d'enquête, et les enseignements de l'arrêt de la Cour européenne des droits de l'homme du *2.09.2010 (Uzun c. Allemagne)* ; et enfin la différence sensible, en terme d'ingérence et même de couverture juridique, selon que l'investigation est menée en temps réel ou de manière différée.

Toutefois, de manière plus générale et eu égard à l'importance qui s'attache aux investigations techniques pour la lutte contre la cybercriminalité, **il est préconisé, afin d'éviter de devoir légiférer en urgence, d'une part, de mieux anticiper les réformes et, d'autre part, que des dispositions législatives couvrent, de manière générale et, à l'instar de ce qui est, par exemple, mis en oeuvre en Allemagne, l'ensemble des mesures techniques susceptibles d'être mises en oeuvre par les services de police et de justice**.

Le blocage d'un site internet

Compte-tenu des interrogations qu'elle suscite, cette mesure appelle des développements particuliers.

Un double constat préalable s'impose :

□ **le blocage des sites fait l'objet de recommandations réitérées dans les instruments internationaux et se trouve être appliqué, depuis de nombreuses années, dans la majorité des Etats européens et de manière parfois massive**.

En ce sens, l'analyse comparative montre que, dans un premier temps, le blocage résultait, pour l'essentiel, d'une démarche partenariale encouragée parfois par la menace de légiférer et s'inscrivait généralement dans le cadre de la technique dite de *"notification action"*. Toutefois, l'évolution des directives européennes, fondée tant sur le caractère hétérogène des situations que sur l'importance que revêt une telle mesure, comme celle de la jurisprudence [158] , incite aujourd'hui l'ensemble des Etats-membres à définir un cadre légal.

Au plan international, les textes sont nombreux à préconiser le blocage dans le cadre de la lutte contre la cybercriminalité.
Le plus important est *la Directive du 4.11.2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, qui prévoit, en son art. 25 intitulé "mesures contre les sites internet contenant ou diffusant de la pédopornographie :*
1.- Les Etats membres prennent les mesures nécessaires pour faire rapidement supprimer les pages internet contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et s'efforcent d'obtenir la suppression des pages hébergées en-dehors de celui-ci
2.- Les Etats membres peuvent prendre des mesures pour bloquer l'accès par les internautes sur leur territoire aux pages internet contenant ou diffusant de la pédopornographie. Ces mesures doivent être établies par le biais de procédures transparentes et fournir des garanties suffisantes, en particulier pour veiller à ce que les restrictions soient limitées à ce qui est nécessaire et proportionné, et que les utilisateurs soient informés de la raison de ces restrictions. Ces garanties incluent aussi la possibilité d'un recours judiciaire".

□ Si la France a beaucoup légiféré sur cette question, le blocage reste peu usité compte-tenu des difficultés à définir, réglementairement, les modalités d'application de cette mesure, et d'un manque de consensus.

(1) Le débat législatif sur le blocage a débuté lors de l'examen de la loi relative à la confiance dans l'économie numérique du 21 juin 2004. La solution alors retenue fut d'ordre civil.

Si la personne lésée s'est vue reconnaître par l'art. 6.I.5 le droit de requérir de l'hébergeur implanté en France le retrait de données *"manifestement"* illicites, une telle disposition s'avérait sans portée lorsque l'hébergeur était implanté à l'étranger.

Telle fut la raison pour laquelle l'art. 6.I.8 de cette même loi a reconnu, implicitement, au juge civil la possibilité d'ordonner notamment le blocage d'un site : *"L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1 (les fournisseurs d'accès), toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne".*

La personne ainsi lésée, afin de voir prononcer en urgence le blocage du contenu incriminé, peut ainsi faire une action en référé, sur la base des dispositions de l'article 809 du code de procédure civile, qui dispose que *"le*

[158] l'un des exemples les plus récents à pour origine la Cour de cassation Belge qui, en son arrêt du 22-10-2013 The Pirae Bay, vient de valider la possibilité pour la Justice de bloquer un site, en notifiant son url aux fournisseurs d'accés, et d'obliger ces derniers à surveiller toute réapparition sous un autre item.

.

président (du tribunal de grande instance) peut toujours, même en présence d'une contestation sérieuse, prescrire en référé les mesures conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite...".

Toutefois, le refus des fournisseurs d'accès étrangers de se voir appliquer la loi française a contraint les juges civils à faire, de préférence, application du référé conservatoire de l'article 145 du même code, dans la mesure où, de jurisprudence constante, la loi française est alors applicable au litige, texte qui prévoit que *"s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé sur requête ou en référé".*

Des difficultés identiques sont survenues en ce qui concerne la mise en oeuvre du référé spécial prévu à l'article 50-1 de la loi du 29 juillet 1881 sur la liberté de la presse, selon lequel *"...lorsque les faits visés par les articles 24 et 24 bis résultent de messages ou informations mis à la disposition du public par un service de communication au public en ligne et qu'ils constituent un trouble manifestement illicite, l'arrêt de ce service peut être prononcé par le juge des référés, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir."*

Le débat a rebondi à l'occasion du vote de la loi HADOPI de 2009, même si la solution retenue en définitive fut de même nature. C'est ainsi que l'article L.336-2 du code de la propriété industrielle dispose que *"En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de grande instance, statuant le cas échéant en la forme des référés, peut ordonner à la demande des titulaires de droits sur les oeuvres et objets protégés, de leurs ayants droit, des sociétés de perception et de répartition des droits visées à l'article L. 321-1 ou des organismes de défense professionnelle visés à l'article L. 331-1, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier".*

La loi relative aux jeux en ligne du 12 mai 2010 a été l'occasion de traiter, une nouvelle fois, de cette question, même si, en définitive, son article 61 a fait le choix, lui aussi, d'une procédure civile, en prévoyant que *"A l'issue de ce délai, en cas d'inexécution par l'opérateur intéressé de l'injonction de cesser son activité d'offre de paris ou de jeux d'argent et de hasard, le président de l'Autorité de régulation des jeux en ligne peut saisir le président du tribunal de grande instance de Paris aux fins d'ordonner, en la forme des référés, l'arrêt de l'accès à ce service aux personnes mentionnées au 2 du I et, le cas échéant, au 1 du 1 (les fournisseurs d'accès) de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique".*

Un tel dispositif est effectivement utilisé par l'A.R.J.E.L. qui l'a mis en oeuvre à 49 reprises, preuve qu'un tel dispositif peut s'avérer opérationnel; en outre, par décisions en date des 12 juillet 2013 et 21 janvier 2014, la Chambre commerciale de la Cour de cassation a refusé de saisir le Conseil constitutionnel de la question prioritaire de constitutionnalité dont elle était saisie par l'un des fournisseurs d'accès, avant de rejeter le pourvoi formé par ce dernier.

(2) Le caractère parfois tardif de l'intervention judiciaire, son efficacité relative ont toutefois incité le législateur à instituer des mesures de blocage dits administratifs, en s'inspirant de l'art.3 de la directive 2000/31/CE du 8 juin 2000 dite du commerce électronique.

Telle fut l'origine de l'article 18 de la loi du 21 juin 2004, modifiée sur ce point par la loi du 5 mars 2007 relative à la prévention de la délinquance, qui autorisa l'administration à prendre des *"mesures restreignant, au cas par cas, le libre exercice (d'une activité de commerce électronique)...lorsqu'il est porté atteinte ou qu'il existe un risque sérieux et grave d'atteinte au maintien de l'ordre et de la sécurité publique, à la protection des mineurs, à la protection de la santé publique, à la préservation des intérêts de la défense nationale ou à la protection des personnes physiques que sont les consommateurs ou des investisseurs autres que les investisseurs appartenant à un cercle restreint définis à l'article L.411-2 du code monétaire et financier".*

L'avant-projet de décret du ministre en charge de l'Economie numérique, élaboré en 2011, soit sept ans après la loi, prévoit un mécanisme de mise en demeure puis d'injonction de faire *(allant de l'obligation d'informer les usagers des risques encourus jusqu'au retrait ou à la cession de la diffusion du contenu litigieux)* pénalement sanctionné, visant, en premier lieu, l'éditeur du site, à défaut et en cas de démarches infructueuses, l'hébergeur de données, à défaut encore et seulement en cas d'extrême urgence, le fournisseur d'accès à Internet.

Les autorités administratives énumérées dans l'avant-projet sont nombreuses: le ministre de la Défense *(atteintes aux intérêts de la Défense nationale)*, celui de la Justice *(atteintes à la protection des mineurs)*, celui de l'Intérieur *(ordre et sécurité publics),* les ministres de l'Economie et de l'Economie numérique *(protection des consommateurs et des investisseurs)*, le ministre de la santé *(protection de la santé publique)*, l'Autorité nationale de défense des systèmes d'information *(ANSSI en cas d'attaques informatiques).*

Si, selon cet avant-projet, cette procédure a vocation à être appliquée à l'ensemble des opérateurs, quel que soit le pays où il se trouve être établi, il est toutefois prévu et cela conformément à la Directive, lorsque cet établissement concerne un autre Etat de l'Union Européenne, que la France devrait solliciter de l'Etat-membre concerné qu'il prenne les mesures propres à prévenir ou à faire cesser le trouble ; ce n'est qu'en cas de carence ou d'extrême urgence qu'une mise en demeure ou qu'une injonction pourrait être adressée directement à l'éditeur, après information de la Commission européenne et de l'Etat étranger.

Ces mesures de police administrative doivent être motivées, les personnes concernées étant mises à même, sauf cas d'urgence, de prononcer des observations préalables.

Toutefois, toujours selon ce projet, la méconnaissance d'une injonction n'exposerait son auteur qu'au prononcé d'une contravention de 5ème classe avec possibilité de confiscation, sanction peu dissuasive pour les éditeurs étrangers et, en général, pour les fournisseurs d'accès d'importance.

Enfin, le projet de décret reconnaît un droit à compensation pour les fournisseurs d'accès, dont les modalités étaient toutefois renvoyées à une autre disposition réglementaire.

Consulté sur l'avant-projet de décret, *le Conseil national du numérique* rendait, en urgence *(juin 2011)* un avis mitigé en recommandant que le projet soit notifié pour avis à la Commission Européenne ; que son champ d'application soit clarifié en visant, en premier lieu, *"l'auteur du contenu"* aux lieu et place de *"l'éditeur de site"*, concept non défini ; que le pouvoir d'injonction auprès des hébergeurs soit modifié comme contraire à la procédure de notification exclusive de l'art. 6.I.5 de la loi sur l'économie numérique, seule l'absence du retrait d'un contenu *"manifestement illicite"* pouvant entraîner sa responsabilité ; que toute mesure de blocage imposée aux fournisseurs d'accès ne puisse être instituée que par voie législative et n'intervenir que par la voie judiciaire.

(3).- Telle fut encore la solution adoptée en ce qui concerne **les contenus pédo-pornographiques par la loi du 14 mars 2011.**

Partant du constat que, la grande majorité des images en question sont diffusées par des sites hébergés à l'étranger, ce qui voue à l'inefficacité le dispositif conçu en 2004 par l'art. 6.I de la loi sur l'économie numérique, le législateur décidait de faire peser, non plus sur les hébergeurs, mais sur les fournisseurs d'accès, l'obligation de faire obstacle aux contenus illicites pédopornographiques dont les adresses électroniques seraient désignées par le ministre de l'Intérieur, et cela sous peine de sanctions pénales.

L'art. 6-I.7 modifié de la loi de 2004 prévoit ainsi qu'en ce qui concerne *"la diffusion des images ou des représentations de mineurs relevant de l'art. 227-23 du C.P.P."*, l'autorité administrative peut notifier aux fournisseurs d'accès les adresses électroniques des services de communication au public en ligne contrevenant à ces dispositions afin qu'ils en empêchent *"l'accès sans délai"*.

En sa décision n° 3011-625 DC du 10.03.2011, le Conseil constitutionnel a estimé non contraire à la Constitution une telle procédure administrative de blocage compte-tenu de son caractère proportionné et de la nature de son objet. Interprétant cette décision, *le Conseil national du numérique*, dans son avis précité, a considéré que l'on ne pouvait déroger au principe du recours préalable au juge qu'à trois conditions :
- la mesure doit protéger les utilisateurs d'internet eux-mêmes
- la nature des contenus doit justifier les mesures prises
- la mesure doit viser à restreindre l'accès à un site déterminé en raison de son caractère illicite.

Depuis lors, ce dispositif de blocage - qui devait rentrer en application au plus tard en mars 2012 - se trouve être en attente d'un décret d'application, préparé par le ministre de l'Intérieur, lequel prévoit de confier la charge de l'établissement et de la transmission des listes d'adresses électroniques dont l'accès doit être interdit à l'O.C.L.C.T.I.C., un magistrat se voyant confier une mission de contrôle [159].

En fait, ce décret a été retardé car les négociations entre l'administration et les fournisseurs d'accès n'ont pas encore abouti. s'agissant des modalités de compensation financière qui, prévues en leur principe par l'art. 3 du futur décret [160], doivent faire l'objet d'une convention passée entre les parties prenantes. Entamées depuis le 2ème semestre 2011 par le ministre de l'Intérieur, le ministre de l'Economie et la ministre déléguée à l'Economie numérique sur la base d'une évaluation réalisée dès 2009 par le *Conseil général de l'Economie, de l'industrie, de l'énergie et des technologies (C.G.I.E.T.),* ces négociations - menées avec la Fédération française des télécommunications, l'Association française des fournisseurs d'accès, les sociétés Orange, SFR et Free -, se sont révélées complexes, à la fois sur le plan technique et financier, compte-tenu des positions hétérogènes et parfois exorbitantes des opérateurs.

---

[159] On peut s'interroger sur la raison d'être d'un contrôle judiciaire, qui serait purement formel puisqu'il devra porter sur la régularité de la communication des listes d'adresse aux FAI, alors même que le Conseil constitutionnel a rappelé que la décision de l'autorité administrative était susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, si besoin selon la procédure du référé

[160] cf. les décisions 2000-441 du 28.12.2000 et 2011-625 du 10.03.2011 du Conseil constitutionnel, selon lesquelles le concours apporté par des tiers à la sauvegarde de l'ordre public, lorsqu'ils ne sont pas à l'origine du trouble et que ce concours est étranger à leur objet, ouvre droit à leur profit à une compensation pour les surcoûts occasionnés

Les principaux départements ministériels concernés, suivant en cela une proposition formulée en 2009 par le C.G.I.E.T. s'interrogent aussi sur l'opportunité de déterminer un dispositif général de blocage et de compensation qui serait applicable, non seulement aux sites pédo-pornographiques, mais encore à tous autres sites illégaux en fonction de l'évolution de la loi.

(4) dans le cadre du **projet de loi renforçant les droits, la protection et l'information des consommateurs** - en cours d'examen -, le projet initial prévoyait, en son art. 10, de revenir au principe de l'autorisation judiciaire en reconnaissant le droit à la direction générale de la concurrence, de la consommation et de la répression des fraudesle droit de *"demander à l'autorité judiciaire d'ordonner les mesures mentionnées au 8 du I de l'art. 6 de la loi du 21.06.2004 pour la confiance en l'économie numérique"*, notamment le blocage d'un site.

Toutefois, à l'occasion de l'examen de ce projet de loi *(cf. art. 25 bis en l'état)*, **les deux chambres du Parlement ont voté, de manière conforme, une disposition abrogeant l'art. 18 précité de la loi du 21 juin 2004** ainsi que le principe du dépôt, par le Gouvernement et dans le délai d'un an, d'un rapport sur *"les effets et la justification des mesures de blocage du contenu d'un service de communication au public en ligne".*

Les motifs avancés sont les suivants :
-le constat selon lequel le décret d'application n'a pas été publié depuis 2004
-la nécessité de soumettre la décision de blocage à une décision de justice
-le caractère attentatoire de la mesure à la liberté d'expression et de communication, d'autant plus qu'elle est susceptible de produire des effets pervers par le blocage de sites de renommée mondiale [161]
-l'efficacité contestable de la mesure, puisqu'elle serait contournable par des éditeurs malveillants ainsi que par les internautes
-enfin le coût de la mesure, compte-tenu du principe du désintéressement posé par le Conseil constitutionnel.

Même si cela ne concerne que la disposition précitée et que les partisans du blocage administratif ne désarment pas *(cf., à titre d'exemple, le rapport d'une commission d'enquête du Sénat, déposé en octobre 2013, proposant de modifier la loi de 2004 afin d'obliger les fournisseurs d'accès et les hébergeurs à bloquer les sites internet faisant la promotion de l'évasion fiscale)*, **il est à penser que la prise de position du Parlement revêt une portée générale**.

L'on en veut pour preuve les débats parlementaires relatifs à une **proposition de loi renforçant la lutte contre le système prostitutionnel,** en cours de discussion au Parlement. Son article 1er prévoyait la modification de l'art. 6-I.7 de la loi de 2004 afin d'autoriser l'autorité administrative, pour les nécessités de la lutte contre le proxénétisme et la traite des êtres humains aux fins d'exploitation sexuelle relevant des art. 225-4-1, 225-5 et 225-6 du code pénal, de notifier aux fournisseurs d'accès à l'Internet *"les adresses électroniques des services de*

[161] Sur ce point, les parlementaires font sans doute allusion à l'arrêt AHMET YILDIRIM c. TURQUIE rendu le 18.12.2012 par la C.E.D.H. Dans cette affaire, un tribunal Turc avait ordonné le blocage d'un site litigieux ; l'autorité chargée d'exécuter cette décision, après avoir constaté que ce site ne pouvait être bloqué puisque son propriétaire n'était pas titulaire d'un certificat d'hébergement et se trouvait à l'étranger, avait décidé de bloquer tout le contenu du domaine Internet sur lequel il se trouvait, en l'espèce GOOGLE SITES, rendant l'accès à ce dernier impossible. Le propriétaire d'un site qui se trouvait ainsi dans l'impossibilité d'y accéder saisissait la Cour qui condamnait l'Etat sur le fondement de l'art. 10. A noter que l'arrêt, outre des éléments de droit comparé sur les restrictions au droit d'accès, fait état d'une décision de la Cour de Justice de l'Union européenne en date du 24.11.2011, qui a prohibé toute injonction générale de filtrage imposée à un fournisseur d'accès.

communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai. Les décisions de l'autorité administrative peuvent être contestées devant le juge administratif, dans les conditions du droit commun".

Selon l'exposé des motifs, il s'agissait clairement de faire obstacle à l'accès du public à des sites hébergés à l'étranger.

Le *Conseil national du numérique* a fait part de son désaccord avec ce nouveau dispositif de blocage aux motifs que *"l'absence d'autorisation judiciaire constitue une atteinte disproportionnée à la liberté d'expression et de communication"* et que *"les dispositifs de blocage sont facilement contournables par les usagers".* Il rappelle enfin que le Gouvernement a pris l'engagement, en février 2013, de garantir un contrôle indépendant pour les mesures administratives de coupure et de filtrage

Quant à *l'Association des fournisseurs d'accès et de services Internet (A.F.A.)*, elle considère aussi que cette proposition porte atteinte à la liberté d'expression et de communication en attribuant à l'administration un rôle qui relève du seul juge, lequel doit apprécier si le contenu est illicite et si le blocage est nécessaire, proportionné et adapté.

Fin novembre, le Gouvernement a déposé un amendement de suppression de cette disposition aux motifs que *"le partage entre les responsabilités respectives du juge et de l'autorité administrative dans ces décisions est un sujet qui mérite une réflexion plus approfondie, dans le respect des droits fondamentaux en termes de libertés d'expression et de communication".*

✓ **les difficultés normatives ont incité certaines parties prenantes à mettre en oeuvre le blocage sur des bases partenariales**, telle la convention conclue entre l'association *Phishing initiatives* et les sociétés Google et Microsoft s'agissant des sites diffusant des virus ou pratiquant le hameçonnage.

Au plan des principes, il est préoccupant de voir que le recours au partenariat est motivé par l'impossibilité de définir une norme consensuelle et applicable.

✓ **La fin d'un tel imbroglio suppose, en premier lieu, de mieux cerner les avantages comme les inconvénients de cette technique dite de blocage, sans minimiser l'obligation juridique à laquelle est confrontée la France de se mettre en conformité par rapport aux instruments internationaux, notamment pour ce qui a trait à la pédopornographie envers laquelle elle est manifestement à la traîne par rapport aux Etats comparables.**

Ainsi que le répètent à l'envie l'ensemble des services de police judiciaire, la principale raison d'être du recours au blocage tient au fait que si, pour la majorité des infractions, les dispositifs de retrait suffisent, ces derniers se révèlent totalement inefficaces s'agissant de la délinquance organisée, qui procède à des stockages de données dans les cyber-paradis.

Pour autant, il s'agit moins de sanctionner compte-tenu des possibilités de contournement existantes - même si le blocage d'un site est de nature à compliquer la poursuite des activités criminelles - que de diminuer l'impact de l'action criminelle en prévenant l'accès involontaire du plus grand nombre.

Elle constitue de plus une mesure adéquate vis-à-vis des victimes, notamment, s'agissant de la pédo-pornographie, des mineurs victimes de viols dont l'image est reproduite sur les sites concernés.

Elle contribue aussi à la prévention de la délinquance, notamment sexuelle.
Elle assure enfin aux décisions de justice, tant civiles que pénales, une certaine efficacité dont elles seraient parfois totalement privées.

En résumé, si la technique du blocage n'est pas la panacée - mais celle-ci n'existe que rarement dans le domaine de la lutte contre la cybercriminalité -, elle constitue un outil, parmi d'autres, dont on aurait tort de se priver à condition de le cantonner strictement.

✓ Les inconvénients tiennent, d'une part, au **risque de surblocage**, qui porte directement atteinte à la liberté de communication de tiers, et, d'autre part, à l'existence de **pratiques de contournement**. L'un comme l'autre renvoie, en fait, au choix de **la technique de blocage** [162], question technique qui n'entre pas dans les compétences du groupe interministériel, sauf à constater que la Directive précitée interdit un blocage simple de l'adresse IP compte-tenu des risques qu'il comporte, que certains Etats ont recours à la solution DNS essentiellement pour des raisons de simplicité de mise en oeuvre *(Allemagne, Italie...),* mais que la plupart laissent la technique au choix de chaque fournisseur d'accès. Il semble, en fait, que le critère du nom de domaine soit généralement reconnu comme le plus précis.

En outre, la question du **coût** s'avère particulièrement prégnante en France, dans la mesure où le Conseil constitutionnel a posé le principe de l'indemnisation de l'opérateur dès lors que le concours qu'il apporte à la sauvegarde de l'ordre public est étranger à sa mission. [163]

Toutefois, si la loi du 14 mars 2011 a prévu une surcompensation des surcoûts ainsi générés aux opérateurs par le blocage *(art. 4)*, si la loi du 12 mai 2010 en fait autant en ce qui concerne les sites de jeux ou de paris en ligne *(art. 61)* selon des modalités qui ont été fixées par décret, deux autres lois, qui confèrent au juge, le pouvoir de blocage, ne fixent aucune obligation de cette nature [164].

✓ Reste une question primordiale, tenant à **la qualité de l'autorité susceptible d'ordonner le blocage** : l'administration ou l'Autorité administrative indépendante qui permet une plus grande réactivité dans le respect des principes constitutionnels compte-tenu du recours possible de l'opérateur devant le juge *(cf. la décision du Conseil constitutionnel précité)* ou le juge, garant constitutionnel des libertés individuelles.

---

[162] les spécialistes distinguent le blocage d'adresses IP, le blocage par redirection utilisant le protocole BGP, le blocage par nom de domaine (DNS), le filtrage par inspection de contenu (DPI), le blocage d'url, le blocage hybride...

[163] cf. décision n° 2000-441 DC du 28.12.2000 ; cf. aussi la décision n° 2011-625 DC du 10.03.2011 relative à la loi d'orientation et de programmation pour la performance de la sécurité intérieure : s'agissant du blocage des images pédo-pornographiques, le Conseil observe que *"en prévoyant que les surcoûts résultant des obligations mises à la charge des opérateurs seraient, s'il y a lieu, compensés,* (le législateur) *n'a pas méconnu l'exigence constitutionnelle du bon usage des deniers publics" ;* cf. enfin, l'avis rendu le 6.03.2012 par le Conseil d'Etat à la demande du ministre de l'Intérieur sur la possibilité d'imposer aux opérateurs de téléphonie mobile le financement de l'acheminement de communications de pouvoirs publics destinées au public pour l'avertir de dangers imminents et atténuer les effets de catastrophes majeures et des investissements y afférents

[164] loi du 12.06.2009 dite HADOPI, loi du 28.10.2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet

<u>Les préconisations du groupe interministériel</u> sont les suivantes :

☞ ① il ne peut être recouru à un dispositif de blocage, visant d'ailleurs tant le fournisseur d'accès français que le fournisseur étranger dans les conditions déjà définies - qu'à titre **subsidiaire** par rapport au retrait ordonné à l'auteur du contenu ou à l'hébergeur, mais aussi, conformément à la *recommandation n° 22*, **par rapport au déférencement ou au retrait d'indexation ordonné au fournisseur du moteur de recherche**, dans la mesure où cette dernière technique, plus aisée à mettre en oeuvre et ne faisant pas courir le même degré de risque que le blocage, a un impact similaire par rapport à l'objectif recherché.

<u>Plus précisément, il est recommandé de recourir largement au déférencement, y compris au plan administratif, de préférence qu'au blocage</u><u>, ce qui devrait rendre, le plus souvent, inutile le recours à cette dernière technique</u>.

☞ ② Compte-tenu de ce qui précède et dans la droite ligne de la décision du Conseil de 2011, le blocage devrait concerner des **infractions graves, se prêtant techniquement à une telle mesure et aux seules fins de protéger les utilisateurs d'internet en restreignant l'accès à un site déterminé.**

Tel est déjà le cas pour les infractions déjà énumérées dans l'art. 6-I.7 de la loi de 2004, soit
**l'apologie des crimes contre l'humanité,*
**l'incitation à la haine raciale,*
**l'incitation à la pornographie enfantine,*
**l'incitation à la violence,*
**les atteintes à la dignité humaine*,
- visées aux art. 24 (al. 5 et 8) de la loi du 29.07.1881 ou 227-23 et 227-24 du C.P.
**les activités de jeux illicites,*
**la pédopornographie*
** ainsi que, suite à la loi pour l'égalité entre les hommes et les femmes, la provocation à la discrimination, la haine ou la violence, à raison du sexe, de l'orientation ou de l'identité sexuelle ou du handicap, et l'enregistrement ou la diffusion des atteintes volontaires à l'intégrité humaine*
étant souligné que certaines d'entre elles font l'objet de recommandations européennes ou de décisions de conformité constitutionnelles,

Toutefois, outre ces hypothèses de droit liées à la nature de l'infraction, la future loi-cadre devrait prévoir aussi la possibilité, **pour le juge, civil** *(qui en dispose déjà)* **comme pénal, dans le cadre des mesures provisoires ou des décisions au fond, d'ordonner, au cas d'espèce, un tel blocage lorsqu'il paraît constituer la seule possibilité de mettre un terme à l'infraction et au préjudice subi par la victime.** Un tel pouvoir devrait être encadré par la loi qui, outre les conditions générales précitées, fixerait le critère de gravité en fonction du quantum de peine applicable.

☞ ③ Eu égard aux effets sur les libertés individuelles, **la décision de blocage devrait nécessairement être judiciaire et relever, soit d'un juge civil, saisi en référé ou sur le fond, soit du juge des libertés et de la détention, du juge d'instruction ou de la juridiction pénale de jugement.**

Toutefois, comme il a déjà été dit, **une exception est préconisée pour la pédo-pornographie**, dans la mesure où l'infraction est avérée par nature et où le dispositif légal existe et a été validé par le Conseil constitutionnel [165] et que les textes internationaux n'exigent à cet égard qu'une possibilité de recours judiciaire; **il est néanmoins nécessaire, compte-tenu de la nature de ce contentieux et pour des raisons de cohérence, que les recours éventuels soient portés devant le juge judiciaire et non devant le juge administratif**.

☞ ④ La décision judiciaire de blocage pourrait s'accompagner, si le juge en décide ainsi et si elle s'y prête techniquement, **d'une obligation de surveillance spécifique** mise à la charge de l'opérateur et limitée dans le temps, destinée à prévenir, dans la mesure du possible, un procédé de contournement.

☞ ⑤ La décision de blocage devrait **préserver les droits des tiers** et proscrire toute mesure assimilable à un sur-blocage [166].

☞⑥ **La mise à exécution de ces décisions serait déléguée à l'agence de la future Délégation interministérielle**, qui se verrait conférée la possibilité de saisir le juge en difficulté d'exécution si, pour des raisons techniques avérées, le blocage risquait de léser de tels droits ou si la surveillance ordonnée s'avère techniquement impossible.

☞ ⑦ tout blocage devrait s'accompagner de **la publication d'un message automatisé sur le site ou le domaine concerné** faisant état de la mesure judiciaire ainsi que des poursuites auxquelles s'exposeraient les personnes qui réitéreraient ou référenceraient le contenu prohibé [167].

☞ ⑧ **Le fournisseur d'accès pourrait échapper à l'obligation qui lui est faite**, dans l'hypothèse où il obtiendrait de l'éditeur ou de l'hébergeur la suppression du contenu illicite ou de son accés et en apporterait la preuve

☞ ⑨ S'agissant de **la compensation financière** due aux opérateurs,il importe de prendre en compte le fait que certains d'entre eux ont déjà recours à cette technique de blocage, soit de leur propre initiative, soit dans le cadre d'accords

---

[165] cf. la décision n° 2011-625 DC du 10.03.2011

[166] cf. la décision C.E.D.H. *Ahmet YILDIRIM c. Turquie, 18.12.2012 (déjà citée)*. S'agissant des risques sur les droits des tiers consécutivement à une mesure de blocage, il pourrait être utilement référé à l'exemple tiré du code monétaire et financier et, plus précisément à l'art. L.563-4 qui prévoit, en ce qui concerne les établissements bancaires, *"L'Etat est responsable des conséquences dommageables de la mise en oeuvre de bonne foi, par les organismes, institutions et services régis par le titre 1er du présent livre, leurs dirigeants ou leurs préposés, des mesures d'interdiction mentionnées à l'article L. 562-2. Aucune sanction professionnelle ne peut être prononcée à l'encontre de ces organismes, institutions ou services, leurs dirigeants ou leurs préposés"*.

[167] La Cour européenne des droits de l'homme. a jugé que l'insertion obligatoire d'un avertissement adéquat dans les archives Internet indiquant qu'un article faisait l'objet d'une procédure en diffamation et ne devait ni être utilisé, ni reproduit, ne constitue pas une ingérence disproportionnée dans le droit à la liberté d'expression *(Times Newspaper Ltd c. Royaume-Uni, 10.03.2009)*

partenariaux, et donc qu'ils disposent des capacités logicielles pour ce faire ; en tout état de cause, il conviendrait d'instaurer une tarification réglementaire pour en terminer avec les palinodies actuelles.

☞⑩ en ce qui concerne enfin **le probléme technique**, il est suggéré de privilégier une approche européenne, non seulement pour bénéficier de l'expérience déjà acquise par certains Etats mais aussi pour harmoniser les pratiques dans la mesure où elles sont susceptibles de concerner les mêmes opérateurs. Le nouveau *Centre européen de lutte contre la cybercriminalité* pourrait utilement en être saisi.

Recommandation n° 27
relative au blocage des sites et des noms de domaine

Le cadre général suivant est préconisé s'agissant du blocage susceptible d'être imposé sur Interne :

1.- Fixer le principe que le recours au blocage, qui n'a pour finalité que de protéger les internautes en restreignant l'accés à un site ou à un nom de domaine illégal et qui ne peut intervenir que de manière subsidiaire aux mesures susceptibles d'être requises des hébergeurs ou des fournisseurs des moteurs de recherche, doit être limitée aux infractions graves qui s'y prêtent techniquement.

2.- Sauf en ce qui concerne la pédopornographie, reconnaître au juge seul, qu'il soit civil ou pénal, d'ordonner, de manière provisoire ou dans le cadre du jugement au fond, le recours au blocage d'un site.

3.- Autoriser le juge, afin de limiter les risques de contournement, d'assortir sa décision de blocage d'une obligation de surveillance spécifique et limitée dans le temps à la charge du prestataire.

4.- Prévoir que la mise à exécution de l'ensemble de ces décisions est assurée par l'agence de régulation relevant de la future délégation interministérielle, laquelle pourra saisir le juge en difficulté d'exécution en cas de risque de sur-blocage.

5.- Prévoir que toute décision de blocage devra s'accompagner, à l'initiative de l'agence en question, de la publication d'un message explicatif sur le site concerné.

6.- Autoriser le fournisseur d'accès à échapper à l'obligation de blocage s'il apporte la preuve du retrait du contenu ou de l'impossibilité d'y accéder.

7.-Recourir à une tarification complémentaire s'agissant de la compensation financière des prestataires.

8.- Saisir les instances européennes compétentes des questions afférentes au processus technique à utiliser pour le blocage.

7. - De quelques "opérateurs" particuliers

L'évolution numérique permet aujourd'hui de se connecter à Internet quasiment partout et en tout lieu. Toutefois, certains dispositifs, qui ont précisément pour ambition de faciliter un tel accès afin d'en faire bénéficier le plus grand nombre, rencontrent des difficultés à s'insérer dans le cadre légal.

Il en est d'abord ainsi des **opérateurs non commerciaux** *(collectivités territoriales, établissements hospitaliers, scolaires ou universitaires...)* qui négligent souvent les obligations légales qui pèsent pourtant sur eux en terme de conservation des données pendant la période réglementaire. **Une campagne de sensibilisation pédagogique devrait être mise en oeuvre à leur bénéfice** afin de leur **r**appeler ces obligations et surtout les moyens à mettre en oeuvre pour les respecter.

La question s'avère moins aisée pour **les points d'accès publics** que constituent **les *"cyber-cafés"*** et les ***"offreurs de hot-spots wi-fi publics"***, ces derniers implantés dans les aéroports, gares, restaurants, entreprises, salons..., qui offrent, gratuitement, la possibilité au public de se connecter sur internet.

L'ensemble de ces opérateurs particuliers sont soumis en tant que tels aux obligations prescrites par le code des postes et des télécommunications, s'agissant, notamment, de la conservation et de la communication des données permettant d'identifier, à des fins judiciaires, toute personne ayant contribué à la création d'un contenu mis en ligne [168], ainsi que, en cas de non-respect, aux sanctions prévues par la loi.

Or, les professionnels qui gèrent les *"cyber-cafés"* ne s'assurent pas de l'identité des utilisateurs et omettent de stocker les données requises [169].Quant aux *"hot-spots"* libres d'accès, l'on voit mal comment, techniquement, il pourrait être procédé.

Ceci n'aurait qu'une importance limitée si des délinquants professionnels, y compris en matière de terrorisme, connaissant les failles de ces dispositifs de nature à renforcer leur impunité, n'y avaient pas recours.

La réponse doit relever, avant tout, là encore, de la sensibilisation de l'ensemble des responsables concernés car, sans doute, l'effort en la matière a-il trop privilégié l'accés du plus grand nombre en négligeant les questions de sécurité.

Pour les *"cyber-cafés",* l'identification ne saurait résulter que de la production d'un document d'identité préalablement à toute utilisation, voire de la traçabilité des moyens de paiement utilisés. Quant au stockage, il nécessite que le professionnel se dote des moyens matériels nécessaires.

---

[168] cf. la décision de l'A.R.C.E.P. en date du 26 avril 2007 s'agissant des opérateurs de réseaux utilisant la technologie RLAN *(radio local area network)* sans fil *(wi-fi)* et l'art. L.34-1 du code précité modifié par la loi n° 2013-1168 du 18.12.2013

[169] compte-tenu de ces défaillances, la méthode classique d'identification de l'adresse IP n'identifie que le *"cyber-café",* tandis que l'absence de sctockage empêche les enquêteurs de remonter dans le temps.

Dans un deuxième temps, des contrôles inopinés, réalisés sur réquisition du procureur de la République par des enquêteurs spécialisés, permettraient de s'assurer du respect effectif des normes.

Quant aux *"hot-spots"*, ils nécessitent des solutions techniques.

Recommandation n° 28
relative aux *"cyber-cafés"* et aux *"hots-spot wi-fi"*

1.- réaliser une grande campagne de sensibilisation, à destination des professionnels concernés, quant aux risques liés à l'utilisation de ces points d'accès, à la réglementation à respecter et aux moyens d'y parvenir

2.- réaliser des contrôles inopinés des *"cyber-cafés"* afin de vérifier le respect de la réglementation

3.- concevoir les solutions techniques nécessaires à la gestion des *"hot-spots"*.

III.3.- des moyens d'investigation à renforcer

La cyber-infraction se caractérise, généralement, par sa rapidité et souvent son instantanéité ; par le fait qu'elle est commise à distance, le plus souvent de l'étranger où sont détenus les avoirs criminels, par des auteurs en général anonymes via l'utilisation de pseudo et les relations numériques [170] ; par la volatilité de la preuve numérique, qui rend obsolètes les moyens de droit commun et le temps policier ou judiciaire ; enfin par le recours fréquent au cryptage ou au chiffrement, qui constitue un défi supplémentaire à surmonter.

De telles caractéristiques posent, à l'évidence, de redoutables défis s'agissant de l'identification des auteurs d'infraction et des modes de preuve, comme en attestent les difficultés d'élucidation et l'importance des classements sans suite. Les attentes des services de police et de justice, qui ont parfois le sentiment d'être confrontés à une mission impossible, sont, en conséquence, fortes en terme d'adaptation des moyens procéduraux.

Si la production normative de cette dernière décennie est riche en la matière, force est de constater qu'elle n'a pas répondu à l'ensemble des besoins, faute de clarification des attentes à l'égard des prestataires techniques d'Internet ou compte-tenu des difficultés tant à traduire au plan réglementaire certains concepts posés par la loi qu'à mettre en oeuvre, au plan pratique, partie de ces dispositions.

Par-delà, la stratégie de l'Etat hésite parfois entre une réponse de nature administrative, d'ailleurs encouragée par les administrations techniques ainsi que par le monde du renseignement préoccupés par le manque d'efficacité ou le formalisme de l'action pénale, et une réponse de nature judiciaire, débat qui est souvent à l'origine, non seulement de redondances, mais aussi d'un manque de cohérence, ne serait-ce qu'en terme de garanties pour les libertés individuelles [171].

Concernant ces dernières, le débat actuel souffre aussi d'un manque de consensus global s'agissant de la traduction concrète à donner au principe de proportionnalité lorsqu'il s'agit de trouver un point d'équilibre entre les principes conventionnels et constitutionnels énoncés *(principe de légalité, respect de la liberté d'information, de la vie privée et de la protection des données)* et les ingérences justifiées par les nécessités répressives. Les débats encore récents sur la garde à vue ou ceux à venir s'agissant de la traduction en procédure pénale des récentes Directives européennes l'illustrent au même titre que l'évolution amorcée par la Cour de cassation sur la répartition des compétences entre le pouvoir d'initiative de l'enquêteur, le rôle du parquet et celui du juge.

De plus, et comme en attestent les auditions tant des responsables de la *Commission nationale consultative des droits de l'homme* et de *la Commission nationale informatique et*

---

[170] Il est parfois difficile de faire comprendre aux non spécialistes que, sur Internet, l'anonymat est la règle et l'identité l'exception, car la fourniture de cette dernière n'est jamais un préalable à l'accès ; la seule identité est celle du support utilisé pour communiquer ; encore cette adresse IP est-elle essentiellement dynamique, changeant en permanence de titulaire et souvent masquée. Comme le résume M. Michel QUILLE, directeur adjoint d'EUROPOL, *"la délinquance par Internet peut être aujourd'hui le fait de n'importe qui, mais elle peut aussi provenir de n'importe où".*

[171] Telle est d'ailleurs la raison pour laquelle le groupe interministérielle a voulu proposer un cadre d'ensemble cohérent s'agissant des prestataires techniques d'Internet

libertés que de la précédente Bâtonnière de Paris, mais aussi les débats parlementaires, récents ou actuels, sur le blocage des sites ou la géo-localisation, l'équilibre paraît parfois encore plus difficile à trouver lorsque l'on traite d'Internet eu égard notamment au caractère contradictoire des attentes et à une forte exigence de transparence.

En outre, comme pour le droit pénal de fond, les dispositions procédurales se trouvent dispersées entre différents supports normatifs, ce qui, ajouté à la complexité ou au caractère général et non spécifique de certaines de ces dispositions, ne facilite pas le travail des praticiens comme le positionnement des victimes.

En conséquence, le groupe interministériel s'est attaché à examiner l'ensemble des seules questions de procédure posant débat, en privilégiant une approche concrète des difficultés et en préconisant des éléments de réponse qui se veulent, tout à la fois, efficaces et respectueux des libertés fondamentales.

Si, comme pour le droit pénal de fond, la première question abordée tient à la lisibilité des dispositions normatives (31), le groupe interministériel s'est ensuite penché sur la question de la compétence territoriale (32) puis sur celle de la prescription de l'action publique (33).

Précédés d'une analyse du régime de la preuve numérique (34), sont ensuite successivement abordés les modes d'investigation posant difficulté : les réquisitions (35), l'accès aux données informatiques, leur saisie et leur analyse (36), l'enquête sous pseudonyme (37), la captation des données à distance (38), enfin le recours aux moyens de lutte contre la délinquance organisée (39).

Les recommandations du groupe de travail sont guidées par le souci d'adapter ces différents modes en fonction des difficultés inventoriées par les praticiens.

Il n'est toutefois pas certain qu'à terme cette adaptation suffise, à elle seule, à atteindre une efficacité maximale.

Toutefois, combinées avec les réformes préconisées s'agissant des prestataires techniques, aux réformes organisationnelles et à la croissance de ressources humaines mieux formées, ces préconisations devraient être de nature à apporter une amélioration sensible.

Il conviendra toutefois, si elles sont suivies d'effet, d'en mesurer l'impact dans les années qui suivent.

*****

③① - La lisibilité du dispositif procédural

Ainsi qu'il vient d'être dit, les dispositions procédurales souffrent d'un manque de lisibilité et de cohérence semblable à celui déjà souligné pour le droit pénal de fond. Aussi, les recommandations susceptibles d'être faites sont similaires et n'appellent pas de plus amples commentaires.

Recommandation n° 29
relative à l'amélioration de la lisibilité et de la cohérence du droit procédural

1.- afin d'assurer la cohérence des dispositions procédurales et des moyens d'investigation relatifs à la cybercriminalité, tout en renforçant leur accessibilité, insérer dans le code de procédure pénale l'ensemble de ces dispositions, conformément à leur vocation et au rôle imparti à l'Autorité judiciaire. Cet objectif peut être atteint soit en rapatriant dans ce code les dispositions éparses dans les autres codes ou les textes non codifiés, soit en les dupliquant systématiquement.

2.- Concomitamment, unifier les dispositions procédurales ainsi que les moyens d'investigation poursuivant le même objet, afin de mettre un terme aux doubles-emploi constatés.

3.- Dans l'immédiat, et afin de favoriser une meilleure effectivité de la loi en renforçant son accessibilité, dresser et rendre accessible en ligne un corpus exhaustif de l'ensemble des dispositions en question, avec, en regard, les principales décisions jurisprudentielles, internes comme internationales, et cela en suivant le plan du code de procédure pénale.

4.- dans l'avenir,
*la délégation interministérielle, dont la création est préconisée, devrait permettre de mieux coordonner les initiatives normatives relatives à la cybercriminalité émanant des différents départements ministériels, tout en créant un dispositif de veille, tant sur le plan interne qu'au niveau international.
*la constitution d'une mission spécifique au sein du ministère de la Justice serait l'occasion de réaffirmer le pilotage du ministère de la loi, qui devrait pouvoir s'appuyer sur un réseau de référents au sein des autres départements ministériels.
*il importe enfin, en matière de cybercriminalité, de mieux articuler le droit administratif et le droit pénal, lorsqu'ils portent sur le même comportement, s'agissant des modes d'investigation ; l'intégration, d'une manière ou d'une autre, dans le code de procédure pénale, des pouvoirs ainsi reconnus aux fonctionnaires ou agents chargés de certaines fonctions de police judiciaire visés aux art. 22 à 29-1 dudit code faciliterait cette mise en cohérence.

*****

③②.- La compétence territoriale

Bien qu'aux confins du droit pénal de fond et de la procédure pénale, il a été estimé opportun de traiter de cette question dans le cadre des moyens d'investigation tant elle commande l'action des parquets comme des services d'enquête.

La première question concerne la compétence des juridictions françaises à connaître des infractions afférentes à la cybercriminalité, compte-tenu de ce qu'elles sont souvent commises de l'étranger et par des étrangers.

La seconde a trait aux critères de compétence des juridictions entre elles, qui commandent, le plus souvent, celle des services d'enquête.

La compétence française en matière de cybercriminalité

A première analyse, les dispositions du code pénal relatives à l'application de la loi pénale dans l'espace, complétées par les art. 689 s. du code de procédure pénale et par certains instruments internationaux, paraissent de nature à justifier la compétence française pour la quasi-totalité des crimes et délits relatifs à la cybercriminalité, puisque, en particulier,

*son article 113-2 donne compétence aux juridictions françaises pour les infractions commises sur le territoire national, étant entendu qu'est réputée commise sur ce territoire toute infraction dont l'un des faits constitutifs a lieu sur ce dernier
*son article 113-6 fixe le principe d'une compétence similaire s'agissant des crimes et délits commis par un français à l'étranger, sous certaines conditions tenant notamment à l'existence d'une plainte préalable
*son article 113-7 procède de même en cas de crime ou de délit puni d'emprisonnement commis hors du territoire sur une personne de nationalité française, sous certaines conditions tenant notamment à l'existence d'une plainte préalable.

En conséquence, si l'on se place au plan de la victime, dès lors qu'il y a plainte d'une personne de nationalité française pour un crime ou un délit puni d'emprisonnement et cela même si le lieu de commission de l'infraction est extérieur au territoire français - ce qui n'est pas une hypothèse d'école en matière de cybercriminalité -, la loi française est applicable.

Toutefois, la plainte préalable est rare dans certains types d'affaires.

Or, et sauf exception tenant à la nature de la cyber-infraction, il est le plus souvent peu aisé de déterminer son lieu de commission, compte-tenu des difficultés tenant à l'identification de la personne ou de la société en cause, notamment lorsque l'auteur utilise des ordinateurs "rebonds" *(VPN ou proxy)* donnant dans un premier temps une fausse indication quant à l'adresse IP de l'ordinateur responsable de l'attaque ; quant à la localisation du serveur informatique utilisé par l'auteur, il est difficile dans les premiers temps d'une enquête de déterminer, avec exactitude, sa localisation, d'autant plus qu'elle s'avère souvent évolutive.

En outre, il n'est pas toujours possible de trouver un élément constitutif commis en France pour fonder la compétence de la loi nationale.

Dès lors, les praticiens se heurtent à des difficultés d'interprétation et leurs interrogations sont nombreuses [172].

Même si la jurisprudence adopte, généralement, une conception extensive, en retenant ordinairement la compétence des juridictions françaises dès lors que les contenus illicites diffusés via Internet sont accessibles en France, des doutes subsistent encore pour d'autres infractions, notamment la contrefaçon.

Telle est la raison pour laquelle il est estimé opportun, eu égard à la spécificité de cette criminalité, de lever toute équivoque en préconisant un nouveau critère de compétence.

Recommandation n° 30
relative à la compétence des juridictions françaises

Créer, eu égard à la spécificité de la cybercriminalité et aux difficultés rencontrées par les praticiens, un nouveau cas de compétence des juridictions pénales françaises, en énonçant que toute infraction commise par le biais d'un réseau de communication électronique, de nature criminelle ou de nature correctionnelle mais punissable d'un emprisonnement, lorsqu'elle est tentée ou commise au préjudice d'une personne, physique ou morale, de nationalité française au moment de sa commission, est réputée avoir été commise en France.

Une fois que la compétence de la loi française est établie, se pose la question de savoir quel parquet est territorialement compétent.

Les critères de compétence entre juridictions

cette 2ème interrogation relève tant du droit interne que de la politique pénale *(cf., sur ce dernier point, le chapitre VII).*

Concrètement, dans la grande majorité des cas, le parquet est saisi d'une cyber-infraction soit par plainte, soit par dénonciation *(par ex. d'un professionnel)*, sans que l'on connaisse ordinairement l'identité de l'auteur supposé et, a fortiori, son lieu de résidence.

Dès lors, en droit et par référence aux dispositions de l'art. 43 du code de procédure pénale, seul le critère du lieu de commission de l'infraction peut fonder la compétence judiciaire.

Or, si les infractions dites de presse peuvent être souvent considérées comme

[172] cf. le rapport de l'I.N.H.E.S.J. sur *"l'impact des nouvelles technologies sur les enquêtes judiciaires"*, 2012-2013, II-7 relatif à *"la problématique de la compétence territoriale dans les enquêtes judiciaires"*, qui concerne, spécifiquement, les infractions cybercriminelles et dont est tirée une partie du constat précité

étant commises sur l'ensemble du territoire *(lieu de diffusion d'internet)*, si, selon la nature de certaines infractions, partie des éléments constitutifs sont commis dans un lieu donné *(par exemple au siège de l'entreprise victime, ou le lieu de livraison en matière de vente à distance)*, si la compétence spéciale reconnue, pour certaines infractions, à la juridiction parisienne ou aux juridictions inter-régionales spécialisées est aussi attributive de compétence, le critère de compétence de droit commun lié au lieu de commission peut s'avérer impuissant à saisir la cyber-infraction.

Les difficultés qui en résultent, notamment lorsque l'infraction est commise de l'étranger ou encore en terme de dessaisissements obligatoires alors même qu'un premier service d'enquête est parvenu à récupérer l'adresse IP et à identifier l'auteur supposé mais qu'il apparaît que ce dernier est domicilié dans un autre ressort [173], a entraîné le parquet et la cour d'appel de Paris à retenir le critère du trouble social [174].

Il est préconisé, là encore, de tenir compte de la spécificité de la cybercriminalité, en créant un nouveau critère de compétence territoriale relatif à la victime, de nature à renforcer la sécurité des procédures et à faciliter le travail des services d'enquête et des parquets.

Recommandation n° 31
relative à l'extension des critères de compétence territoriale

Modifier le code de procédure pénale afin de reconnaître, s'agissant des infractions commises contre ou via un réseau de communications électroniques, la compétence du parquet et de la juridiction du lieu de domicile ou de résidence de la victime, personne physique, ainsi que du lieu du siège social, lorsqu'il s'agit d'une personne morale.

*****

[173] Curieusement, l'identification positive se traduira ainsi par un dessaisissement, d'où un investissement jugé peu valorisant par les premiers services d'investigation, sauf à recourir, de manière intensive, à des autorisations d'extension de compétence territoriale sur le fondement de l'art. 18-4 du C.P.P. comme le pratique le parquet de PARIS ; quant au service et au parquet nouvellement saisi, ils devront prendre connaissance d'une affaire dont ils ignoraient tout

[174] cf. C.A. Paris 9.05.2008

③③.- la prescription de l'action publique

Si la prescription de droit commun ne soulève pas de difficulté, il n'en est pas de même de celle des infractions dites de presse, compte-tenu des dispositions de l'art. 65 de la loi du 29.07.1881 relatives au délai de 3 mois et à l'obligation, pour les réquisitions d'enquête, d'articuler et de qualifier précisément l'infraction..

Certes, la loi du 9.03.2004 puis celle du 21.12.2012 ont porté le délai de prescription de 3 mois à 1 an, s'agissant des infractions de

- provocation directe ou apologie du terrorisme
- contestation de crime contre l'humanité
- provocation à la discrimination, à la haine ou à la violence, en raisons de l'origine, de l'ethnie, de la nation, de la race
- diffamation et injures pour les mêmes raisons,

L'ensemble de ces modifications sont, en fait, motivées par les difficultés spécifiques aux enquêtes relatives aux cyber-infractions et souvent par l'incapacité dans laquelle se trouvent les victimes de réagir à temps, faute d'avoir eu connaissance des propos diffusés sur Internet les concernant. Et les conséquences d'une possible inaction sont lourdes en la matière car, contrairement à la presse-papier, audio ou télévisuelle, les propos restent inscrits dans le marbre de l'Internet *ad vitam aeternam.*

Le législateur, en mettant sur le même plan tous les types de supports dits de presse, quitte à allonger l'ensemble des délais afférents, a tenu compte des exigences de la jurisprudence constitutionnelle - notamment de la censure partielle de la loi pour la confiance dans l'économie numérique qui prévoyait le report du point de départ du délai de prescription pour les seules infractions commises sur Internet *(cf. 2004-496 DC du 10.06.2004),* qui privilégie *(cf. aussi la décision du 12.04.2013),* comme d'ailleurs la Cour de cassation, l'unité de régime de la loi de 1881 -.

Pour autant, les retouches successives apportées à la loi de 1881 ne règlent pas entièrement la question, d'autant plus que l'extension de la durée de la prescription fait peser une responsabilité beaucoup plus importante sur les organes de presse traditionnels et l'on peut s'interroger sur son opportunité.

Deux solutions sont envisageables :

☞ une solution, radicale, consisterait à proposer d'inscrire dans le code pénal l'ensemble des infractions relevant de la cybercriminalité, aux motifs que tant la prescription, que les conditions de poursuite de la loi de 1881 sont inadaptées à cette délinquance et que l'assimilation des messages électroniques à la presse écrite ou audio-visuelle apparaît quelque peu artificielle.
Même si la cohérence de la loi de 1881 se trouve être peu à peu entamée par la création de délits d'expression publique dans d'autres textes *(cf., par exemple, les propos racistes proférés dans des stades)*, cette proposition n'a pas les faveurs du groupe interministériel, d'abord car elle serait dénoncée comme un facteur de rupture d'égalité, ensuite parce qu'elle s'avérerait contraire au véritable but poursuivi par la loi de 1881 qui, malgré son titre et son manque de lisibilité, entend protéger la liberté

d'expression au sens de l'art. 10 de la Convention européenne des droits de l'homme

☞Telle est la raison pour laquelle une autre solution a été choisie, de nature à éviter des modifications incessantes de ce texte et respectueuse de la jurisprudence du Conseil constitutionnel - lequel a admis la possibilité de décider de délais de prescription plus longs en fonction de la nature et de la gravité des infractions et donc du concept d'ordre public-.

La distinction proposée s'avère, sur ce point, justifiée par des éléments objectifs tirés de la spécificité des cyber-infractions dans la mesure où ni l'atteinte, ni le préjudice ne disparaissent, et que leur portée *(en nombre de "lecteurs")* est sans commune mesure avec celle des infractions de même nature mais commises par d'autres modes. Elle permettrait enfin de maintenir ou de restaurer le court délai de prescription pour la presse écrite ou audio-visuelle.

Recommandation n° 32
relative au délai de prescription des infractions dites de presse commises sur Internet

Compléter l'art. 65-3 précité en rajoutant un alinéa supplémentaire énonçant que *"En outre, ce même délai d'un an est applicable à toute infraction prévue par la présente loi lorsqu'elle est commise au moyen d'une réseau de communication électronique" .*

Toutefois, cette recommandation, formulée en cours des débats de ce qui devait devenir la loi du 27.01.2014, qui a étendu le délai d'un an aux infractions commises en raison du sexe, de l'orientation et de l'identité sexuelle ou du handicap, a perdu une bonne partie de sa raison d'être, même si la formule préconisée paraît toujours pertinente.

Pour autant, le groupe interministériel est conscient qu'une telle proposition ne résout par toutes les difficultés car les réquisitions spécifiquement qualifiées de l'art. 65 précité sont difficilement applicables par des parquets non spécialisés, alors même qu'Internet, ne serait-ce qu'eu égard à la masse des données qu'il concerne mais aussi à sa nature *(blogs),* génère des infractions de presse d'un volume sans précédent. **Il est douteux que si les propos haineux continuent à se répandre à cette vitesse sur le web, les parquets et les juridictions soient en mesure d'y faire face compte-tenu des conditions formelles auxquels ils sont contraints.** Il convient donc de réfléchir sur l'opportunité de limiter le formalisme des réquisitions qui, en définitive, se retournent contre les victimes que la loi est censée protéger. C'est, vraisemblablement, à ce prix que la loi de 1881 pourra continuer à régir Internet.

*****

③④ - le régime de la preuve numérique

La preuve résultant de l'exploitation de données contenues dans un système ou un réseau de communications électroniques prend une importance de plus en plus cruciale dans le procès, compte-tenu du développement de tels outils.

La preuve numérique exige aussi, pour être recherchée et réunie, de nouveaux modes d'investigation, extraordinaires par rapport au droit commun.

Or, les garanties traditionnelles de procédure pénale ne sont pas toujours adaptées à ces modes spécifiques d'investigation.

Ainsi, lorsqu'il y a lieu à intervenir sur un serveur soit pour copier les données qu'il contient, soit pour les exploiter, même à distance, les garanties ordinaires, tenant, par exemple, à la présence ou au consentement du propriétaire ou de l'utilisateur des lieux dans lesquels ce serveur est entreposé, voire des deux témoins requis pour la perquisition, se révèlent, d'abord, impraticables compte-tenu de la durée de telles opérations ou lorsque la saisie intervient dans un autre cadre qu'une perquisition. En outre, elles apparaissent particulièrement formelles en terme de protection contre éventuelles manipulations ; il en serait d'ailleurs de même de l'autorisation préalable d'un magistrat, dans la mesure où il serait incapable de procéder à un quelconque contrôle.

Telle est la raison pour laquelle la preuve numérique fait parfois l'objet d'interrogations, voire de contestations.

Dès lors, il s'agit, pour poursuivre sur l'exemple précédent, de définir de nouvelles garanties permettant de s'assurer de l'intégrité et de la sincérité du support saisi comme de l'exploitation qui en a été faite, voire des captures d'écrans réalisés ou des extractions opérées, afin tant de sécuriser les opérations de police judiciaire que de favoriser un réel débat contradictoire sur la preuve numérique et de permettre au juge, saisi de contestations, de trancher ces dernières.

Certes, l'une des garanties fondamentales procède de la qualité d'officier ou d'agent de police judiciaire, de la qualité de magistrat du procureur de la République, de l'indépendance du juge d'instruction, et, en règle générale, de leurs formations, éthiques et déontologies.

Mais, face à une question d'ordre essentiellement technique, la sécurité ne peut résulter que de réponses d'ordre méthodologique [175] et... technique - en terme de matériels et de logiciels notamment -, avec un processus de labellisation et de certification externe, à l'exemple de la démarche réalisée pour les laboratoires de police scientifique ou technique, pour les laboratoires d'analyse de l'A.D.N., c'est-à-dire par référence à des normes, si possible

[175] par exemple, la saisie d'un ordinateur doit respecter des modalités différentes selon qu'il est ouvert ou fermé ; ou encore, l'analyse de données contenues dans un support saisi doit respecter un protocole strict d'examen des supports, notamment en ce qui concerne le blocage en écritures, afin de s'assurer qu'aucune donnée n'est ajoutée.

européennes ; le protocole interministériel en matière de médecine légale pourrait aussi servir d'exemple. L'article 19c) de la Convention de Budapest, relatif à la nécessité de préserver l'intégrité des données informatiques stockées, ainsi que *le mémento de recueil des preuves* diffusé par le Conseil de l'Europe confortent une telle démarche.

La certification technique devrait concerner les matériels destinés à réaliser une copie du support numérique en cause *(bloqueurs en écriture et copieurs de supports numériques)* ainsi que les logiciels dédiés à l'investigation numérique proprement dite *("forensic)* qui explorent le support numérique copié afin de mettre en évidence des preuves, y compris des données effacées, des traces de navigation interne...

Le processus de certification lui-même devrait concerner prioritairement les fonctionnalités de préservation de l'intégrité du support-source.

La solution technique, aux dires des experts, serait de recourir à une certification de sécurité dite de premier niveau qui devrait pouvoir être assurée - au titre de la coopération entre la sécurité des systèmes d'information et la lutte contre la cybercriminalité - par un centre d'évaluation agréé par l'ANSSI et selon des critères, une méthodologie et un processus définis par cette autorité et son *Centre de certification national (CNN).*

C'est une démarche ambitieuse, qui se veut pionnière en Europe, et qui ne sera pas aisée à mettre en oeuvre eu égard notamment aux réticences des praticiens, au caractère artisanal que revêt, trop souvent, l'investigation, à la diversité des matériels et logiciels utilisés, et enfin au coût et à la lourdeur des processus de certification, en particulier pour les mises à jour.

Mais c'est une démarche nécessaire afin que la confiance soit au rendez-vous.

Recommandation n° 33
relative à la preuve numérique

Adapter le droit de la preuve à la matière numérique en

1.- fixant le principe, par la voie réglementaire, d'une modélisation de la méthodologie devant être mise en oeuvre par l'agent pour la saisie des supports comme pour toute intervention sur ces supports dans des conditions assurant l'intégrité du matériel saisi aux fins d'éventuelles exploitations ultérieures et garantissant le respect effectif des droits de la défense ; cette méthodologie aurait aussi pour vocation de traiter du recours aux principaux types de logiciels utilisés pour les copies et les exploitations, de la transcription en procédure des éléments intéressant l'enquête, de la suppression corrélative de tous autres éléments temporairement mémorisés et enfin de la traçabilité de l'ensemble

3.- Prévoyant un mode de certification externe de cette modélisation ainsi que des principaux matériels et logiciels utilisés,

4.- formant les praticiens à cette méthodologie et les aidant à la mettre en oeuvre par la diffusion d'un guide méthodologique aux praticiens.

Certaines recommandations qui suivent, notamment en terme de saisie, s'inscrivent dans ce devenir.

*****

③⑤ - les réquisitions

S'agissant de la lutte contre la cybercriminalité, le législateur a fait le choix d'apporter les modifications nécessaires aux articles régissant le droit commun des réquisitions *(cf. art. 60-1, 77-1-1 et 99-3 du C.P.P.)*, tout en y ajoutant des dispositions spécifiques *(cf. articles 60-2, 77-1-2 et 99-4 du C.P.P.).*

Même si partie de ces modification sont récentes, les praticiens se heurtent à certaines difficultés eu égard au caractère particulier de l'outil de communication que constitue Internet.

Toutefois, l'essentiel des difficultés, lourdes de conséquence pour la sécurité des procédures et l'effectivité des enquêtes, a trait aux prestataires techniques et a déjà été examiné au titre du chapitre précédent.

□ la conservation des données

Comme il a été dit, la conservation des données par les prestataires techniques est essentielle pour l'effectivité du droit de réquisition, du droit de *"gel"* de données résultant de la Convention de Budapest, et du droit de saisie.

L'article 6 de la Directive 2006/24 de l'Union européenne du 15.03.2006 dispose ainsi, sous le titre *"durée de conservation"*, que *"les Etats membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une durée minimale de 6 mois et maximale de 2 ans à compter de la date de communication".*

En application de cette disposition, la législation française comporte trois séries de dispositions :

⌞ s'agissant des opérateurs de communication électronique, le code des postes et des télécommunications électroniques prévoit, en son article L.34-1 (III) que

"Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales....et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire...,il peut être différé pour une durée maximale d'un an aux opérations tenant à effacer ou à rendre anonymes certaines catégories de données techniques".

Les articles R.10-12 et R.10-13, pris en application des dispositions précédentes, précisent les catégories de données, intéressant tant l'identification des utilisateurs que les informations de nature technique, relatives aux communications et à la localisation des équipements terminaux..

⌞ s'agissant des hébergeurs et des fournisseurs d'accès, l'article 6-II de la loi du 21.06.2004 prévoit que

"Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elle est prestataire.

...L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés au 1 et 2 du I les données mentionnées au premier alinéa."

Le décret du 25.02.2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, prévoit, au titre des réquisitions judiciaires fondées sur l'article précité, une liste extrêmement détaillée des données d'identité et techniques en question *(art. 1er),* la durée de conservation de ces dernières, fixée à 1 an *(art.3),* et précise enfin que *"les conditions de la conservation doivent permettre une extraction dans les meilleurs délais pour répondre à une demande des autorités judiciaires" (art.4 in fine).*

⌞ Enfin, les articles 60-2 (al.2), 77-1-2 (al.2) et 99-4 *(al.2)* du code de procédure pénale prévoient la possibilité pour l'officier de police judiciaire, sur réquisition du procureur et après autorisation du juge des libertés et de la détention ou du juge d'instruction, de requérir des opérateurs de télécommunications et des fournisseurs d'accès à des services de communication en ligne, de *"prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs".*

Cette dernière disposition, qui ne paraît pas avoir été précisée par l'autorité réglementaire ni avoir fait l'objet d'application pratique, soulève des interrogations quant à l'objet exact poursuivi par le législateur puisque, par son caractère général, elle se rapproche du dispositif de gel des données prévu par la Convention de Budapest tout en concernant, non pas les données techniques, mais les données de contenu.
Toutefois, la procédure retenue semble privilégier une approche individuelle en référence à un dossier précis, afin, par exemple, de préserver la possibilité de réquisition ou d'interception ultérieures.

Si, outre la précision que requiert l'alinéa 2 de l'art. 60-2, la principale difficulté en la matière - relative au refus des prestataires étrangers de se soumettre au droit français - a déjà fait l'objet d'une recommandation au titre de la coopération attendue des prestataires techniques, il reste le fait que l'ensemble des dispositions précitées, qui concernent directement les services de police judiciaire et de justice, sont peu accessibles à ces derniers comme figurant, pour l'essentiel, dans un code spécifique et dans des textes non codifiés, et ne sont pas cohérentes au regard du niveau normatif fixant le délai d'un an et de la précision des éléments devant être stockés, l'un visant des catégories de données, un autre des données précises, le troisième ne comportant aucune définition...

Recommandation n° 34
relative à la conservation des données numérisées

Harmoniser, au sein d'un même corpus qui pourrait utilement être inséré dans le code de procédure pénale comme intéressant principalement cette dernière, les différents textes faisant obligation aux prestataires techniques de conserver, soit de plein droit, soit à la demande d'un juge, les données nécessaires aux enquêtes de justice, en veillant à inscrire le délai d'un an dans la loi et à mettre en cohérence le niveau de détail des données en question.

□ **les réquisitions dites informatiques**

Certaines prescriptions légales ne paraissent pas répondre à une évidente nécessité et n'ont pas d'ailleurs reçu d'application effective, alors même qu'elles autorisent une ingérence particulière.

C'est ainsi que le premier alinéa de l'art. 60-2 du C.P.P. prévoit que

> *"Sur demande de l'officier de police judiciaire, intervenant par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa du 3° du II de l'article 8 et au 2° de l'article 67 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent."*

Les art. 77-1-1 et 99-4 du même code rendent applicables ces dispositions à l'enquête préliminaire et à l'information judiciaire, sous réserve de l'autorisation préalable du procureur de la République ou du juge d'instruction.

L'ensemble de ces dispositions, difficiles à interpréter notamment par référence au droit commun des réquisitions au fin de communication de documents, n'a pas reçu d'application depuis leur entrée en vigueur en 2007.

L'intention du législateur était vraisemblablement, en cas d'enquête judiciaire vaste et importante *(terrorisme notamment)*, de mettre à la disposition des enquêteurs une mesure d'investigation de plus grande ampleur que le seul accès à certaines données spécifiques. Il s'agissait, en fait, de leur permettre de pouvoir accéder à tout ou partie d'un système d'informations, d'y travailler, directement et en temps réel, et cela sans risque d'endommager les traitements et en interprétant correctement les données. Les art. R.15-33-67 et s. du même code en ont défini les conditions qui supposaient, essentiellement, la conclusion de protocoles avec les sociétés concernées, protocoles qui n'ont jamais été élaborés.

Au surplus, le système anglais, auquel le législateur s'était sans doute référé, repose, non pas sur une pénétration ponctuelle d'un système d'informations inconnu et dont il ne connaît rien, mais sur l'immersion, à demeure, de policiers chez les opérateurs.

Compte-tenu de ce constat, comme du caractère très intrusif de telles dispositions, il est préconisé de les abroger, purement et simplement.

Recommandation n° 35
relative à l'abrogation des dispositions autorisant l'intrusion dans les systèmes informatiques

Abroger l'alinéa 1er de l'art. 60-2 et modifier, par voie de conséquence, les art. 77-1-2 et 99-4 du C.P.P.

□ la légalité des réquisitions adressées à des prestataires étrangers

La question est citée pour mémoire, comme ayant été traitée au chapitre précédent.

□ l'objet des réquisitions numériques

Il suscite deux interrogations.

L'une a trait à la terminologie des articles 60-1 et 77-1-1 précités, dans la mesure où la réquisition numérique vise, exclusivement, la remise de *"documents"*, alors que l'alinéa 1er des articles 60-2 et 77-1-2 - dont il est préconisé l'abrogation pour les raisons déjà évoquées - privilégie la notion *"d'informations utiles à la manifestation de la vérité"*.

Si la Cour de cassation privilégie une interprétation large du concept de *"documents"* numériques [176], une telle évolution n'est pas propre à cette matière puisqu'elle intéresse aussi nombre de réquisitions de droit commun[177] .

Il apparaît aujourd'hui nécessaire de modifier les articles régissant le droit de réquisition pour tenir compte de ces réalités, comme cela a déjà été fait pour les dispositions procédurales relatives aux saisies *(cf. les art. 56, 94 et 97 modifiés par la loi de 2004)*.

Recommandation n° 36
relative à l'objet de la réquisition

Modifier les articles 60-1 et 77-1-1 du code de procédure pénale afin de substituer à la notion de *"documents"* celle *"d'informations"*.

[176] cf., notamment, CRIM n° 11-84.308 du 22.11.2011

[177] à titre d'exemple, la réquisition de droit commun faite dans le but de connaître l'identité ou la domiciliation d'une personne ne vise pas à l'obtention de *"documents"* particuliers

L'autre concerne la protection de la vie privée.

Les dispositions précitées du code de procédure pénale ne tiennent pas compte de l'objet de la réquisition, selon la nature de l'ingérence qu'elle constitue, mais font reposer la garantie des libertés individuelles sur le type d'enquête conduite, l'enquête de flagrance, l'enquête préliminaire ou la commission rogatoire consacrant le pouvoir d'initiative de l'officier de police judiciaire -sauf exceptions destinées à protéger certaines professions ou lieux particuliers - ou le soumettant à l'autorisation préalable d'un magistrat, du parquet ou du siège.

La *Cour européenne des droits de l'homme* privilégie, pour sa part, une hypothèse différente, en prenant en compte tant le type d'ingérence et son caractère intrusif - étant entendu que la réquisition est, par exemple, considérée comme beaucoup moins intrusive que la perquisition ou l'interception des communications - que l'objet même de la réquisition. Une telle approche explique la raison pour laquelle, par exemple, la réquisition aux fins de géo-localisation, assimilée à une ingérence de gravité moyenne, appelle des garanties supplémentaires. Il est toutefois aussi tenu compte, dans l'approche *in concreto* de la Cour, du degré d'atteinte à l'ordre public en fonction de la gravité, plus ou moins grande, de l'infraction.

Si, de manière générale et au regard de l'évolution de ces dernières années, induite par la jurisprudence de Strasbourg, la distinction française traditionnellement faite entre l'enquête de flagrance et l'enquête préliminaire se trouve ainsi, pour une bonne part, frappée de désuétude, le groupe interministériel s'est interrogé sur la nécessité de mieux encadrer les réquisitions en matière de cybercriminalité en fonction de leur objet.

Au-delà des préconisations destinées à assurer une plus grande sécurité juridique s'agissant des réquisitions dites techniques *(cf. les commentaires sur la géo-localisation)*, il est un fait que les grandes possibilités de stockage numérique font courir à la vie privée des risques plus importants. Faut-il pour autant soumettre les réquisitions numériques à un régime particulier lorsqu'elles portent sur la vie privée ?

La question ne se pose pas, comme l'a rappelé implicitement la Cour de cassation lorsque la remise est volontaire, que cette remise intervienne ou non à la demande de l'enquêteur et qu'elle soit le fait du *"propriétaire"* des données concernées ou de leur simple *"détenteur"* [178]. Elle ne se pose pas davantage lorsque l'enquêteur s'est vu reconnaître, explicitement, le droit d'accès à certains fichiers.

S'agissant des réquisitions proprement dites, le concept tenant à la vie privée n'est pas véritablement opérationnel puisque la plupart d'entre elles sont, au regard des impératifs d'ordre public qui les motivent, attentatoires, peu ou prou, à la vie privée. Quant à faire un sort particulier aux réquisitions numériques, alors même que de telles données concernent tous les aspects de la vie sociale et la

[178] cf. *CRIM 6.11.2013* s'agissant des réquisitions prises sur le fondement de l'art. 77-1-1 : *"la réception d'informations ou de documents remis de plein gré par leurs destinataires"* ne nécessite pas que l'O.P.J. ait reçu l'autorisation préalable du procureur de la République ; dans le même sens, CRIM n° 06-80.351 du 28.03.2006 ; n° 07-88.604 du 12.03.2008 ; 08-81.443 du 20.05.2008...

quasi-totalité des types de criminalité, c'est prendre un risque sérieux en terme d'effectivité du travail d'investigation.

En fait, une meilleure protection de la vie privée dans le domaine numérique passe par l'encadrement des réquisitions adressées aux gestionnaires de stockage numérique de masse *(les opérateurs de communications électroniques ou les prestataires techniques d'Internet)*.

Dés lors, la solution, déjà esquissée par les instruments normatifs comme par la Cour de cassation [179], consiste à différencier, s'agissant des réquisitions destinées à de tels gestionnaires, celles portant sur les données de connexion et de trafic, et celles relatives au contenu des communications.

Recommandation n° 37
relative aux réquisitions adressées aux opérateurs et prestataires visant le contenu des échanges

Soumettre légalement à l'autorisation préalable du juge des libertés et de la détention ou du juge d'instruction la réquisition, destinée à un opérateur de communications électroniques, notamment aux prestataires techniques d'Internet, ayant pour objet la communication des échanges entre deux personnes privées.

□ les délits obstacles relatifs au respect du droit de communication

En matière de cybercriminalité, le respect, par la personne requise, de la confidentialité des réquisitions revêt une importance toute particulière. Par ailleurs, le refus de réponse ou la simple abstention des professionnels, notamment lorsqu'il s'agit d'identifier une personne sur Internet, réduisent, souvent de manière définitive, à l'impuissance les services de police et de justice. Il s'agit, en conséquence, de renforcer les dispositions actuelles.

☞ la violation des règles de confidentialité

L'audition, par le groupe interministériel, des représentants des sociétés gestionnaires de réseaux sociaux a montré combien l'obligation de confidentialité à l'égard des demandes qui leur sont faites n'était pas systématiquement respectée par l'ensemble de ces sociétés.

[179] cf. CRIM n° 13-81.945 du 22.10.2013 ; CRIM 6.11.2013 ; dans ces deux espèces, la Cour a jugé, implicitement puis explicitement, que la réquisition fondée sur l'art. 77-1-1 et autorisée par le procureur de la République était fondée à solliciter, d'un opérateur de communications électroniques, la remise des données d'identification et de trafic afférentes à des échanges, mais non le contenu de la correspondance, lequel suppose l'intervention d'un juge. En revanche, la saisie, par exemple d'un boîte de messagerie électronique détenue par une personne ou une entreprise donnée, est licite *(CRIM n°s 08-87.415 et 08-87.416 du 8.04.2010 ; CRIM n°s 10-81.748 et 10-81.749 du 30.11.2011 ; CRIM n° 12-85.645 du 27.11.2012 ; CRIM n°s 12-80.331 et s. du 24.04.2013)*.

Or, si l'on se réfère au plus récent modèle de normes minimales internationales en matière de lutte contre la cybercriminalité élaboré avec le soutien de l'Union Européenne *(cf. "Cybercriminalité. Modèles de lignes directrices politiques et de textes législatifs - HIPCAR - UIT 2012"),* il comprend une incrimination de *"divulgation des détails d'une enquête",* ainsi rédigée :

> *"Un fournisseur de service Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime, divulgue de manière intentionnelle*
> *- le fait qu'une injonction ait été émise*
> *- toute action réalisée aux termes de l'injonction*
> *- ou toute donnée collectée ou enregistrée aux termes de l'injonction, commet (un infraction punissable)..".*

Une telle incrimination se fonde directement sur les articles 20.3 et 21.3 de la Convention de BUDAPEST qui prévoit, dans l'hypothèse de *"collecte en temps réel des données relatives au trafic"* et *"d'interceptions de données relatives au contenu"* que *"Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus par le présent article a été exécuté ainsi que toute information à ce sujet".*

Etant entendu que si l'art. 11 du code de procédure pénale pose le principe du secret de l'enquête et de l'instruction, une telle obligation ainsi que l'incrimination de l'art. 226-3 du code pénal qui sanctionne l'atteinte au secret professionnel ne pèsent que sur les personnes qui concourent à la procédure et qui sont tenues au secret soit en raison de leur état, soit en raison de leur profession ; il n'existe donc, semble-t-il, aucune disposition normative instituant une obligation de confidentialité pour les autres tiers qui sont requis par un officier de police judiciaire ; dès lors, ils ne s'exposent à aucune sanction s'ils violent ladite obligation.

Recommandation n° 38
relative au respect de la confidentialité par les tiers requis

Compléter les dispositions relatives aux réquisitions afin de prévoir que les tiers requis, s'ils ne sont pas parties à la procédure, sont soumis à une obligation de confidentialité et ne peuvent, sous peine de sanctions pénales, divulguer à quiconque une demande ou une réquisition, quel qu'en soit l'objet, provenant d'un officier de police judiciaire. ou d'une autorité judiciaire, ou le contenu de cette dernière, sauf dans l'hypothèse où l'exécution même de cette réquisition l'exige.

Les peines doivent être dissuasives, notamment à l'encontre des professionnels et des personnes morales.

☞ **l'abstention et le refus de réponse par la personne requise**

Les art. 60-1 (al.2), 60-2 (al.4)...précités prévoient que *"le fait de s'abstenir de répondre dans les meilleurs délais"* ou *"le fait de refuser de répondre sans motif légitime"* aux réquisitions précitées expose la personne publique ou privée à des poursuites correctionnelles ; toutefois, le montant de l'amende *(3.750 €)* n'est

aucunement dissuasif notamment pour une personne morale, à supposer d'ailleurs qu'elle soit effectivement poursuivie.

Même si cette peine est identique à celle prévue par l'art. 434-15-1 du code pénal s'agissant du témoin qui refuse de comparaître ou de déposer, elle devrait être substantiellement aggravée, notamment à l'égard des professionnels et des personnes morales, si l'on entend que les réquisitions soient suivies d'effet, en se référant, par exemple, aux dispositions de l'art. L.39-4 du code des postes et des communications électroniques qui punit de 3 mois d'emprisonnement et de 30.000 € d'amende le fait, pour un utilisateur de réseaux ou un service de communications électroniques, de refuser de fournir des informations ou documents légaux.

A noter, dans le même sens, que l'art. 6.VI loi du 21.06.2004 réprime d'un an d'emprisonnement et de 75.000 € d'amende le fait, pour un prestataire de service, de ne pas avoir conservé les données d'identification ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication de ces éléments.

Recommandation n° 39
relative à la sanction de l'inaction ou du refus de réponse du tiers requis

Renforcer substantiellement la peine encourue au titre des articles 60-1 et 60-2 s'agissant des professionnels et des personnes morales.

③⑥ - l'accès aux données informatiques, leurs saisies et leur analyse

Ces questions sont actuellement régies, s'agissant de l'enquête de flagrance, par les articles 56, 57, 57-1 et 60 du code de procédure pénale, ainsi que par les articles 76, 76-3, 77-1 du même code en ce qui concerne l'enquête préliminaire, l'information judiciaire faisant l'objet de dispositions similaires.

Dans leur application pratique, ces textes posent de nombreuses difficultés aux services de police et de justice en terme, notamment, de sécurité juridique et d'adaptation à la lutte contre la cybercriminalité, auxquelles il convient d'apporter réponse pour accroître l'efficacité de l'action répressive. Par ailleurs, la garantie effective des libertés commande de sortir du flou actuel.

Il est à noter que **partie de ces difficultés trouve leur origine dans un manque de reconnaissance de la spécificité de la cybercriminalité, résultant, techniquement, du mode de rédaction législatif retenu.**

A titre de comparaison, il est fait mention ci-après des plus récentes normes minimales internationales en matière de cybercriminalité érigées avec le soutien de l'Union européenne *(cf. "Cybercriminalité - Modèles de lignes directrices politiques et de textes législatifs - HIPACAR - UIT 2012")*, lesquelles paraissent plus claires et plus opérationnelles que les textes internes, à vocation trop générale :

perquisition et saisie :

1 - *"Si un juge/magistrat est convaincu qu'il existe de bonnes raisons de soupçonner/croire qu'il peut exister **dans un lieu** un objet ou des données informatiques*
- pouvant être considérés comme importants pour servir de preuve à une infraction
- ou ayant été obtenus par une personne suite à une infraction
*il peut émettre un mandat autorisant un agent, avec toute l'assistance pouvant être nécessaire, **d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question**, notamment perquisitionner ou accéder de manière similaire à*
- un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées
- un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays.

2 - Si un agent qui entreprend une perquisition sur la base de l'article précédent a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur le territoire national, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, il sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système.

3 - Un agent qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des articles précédents."

Assistance :

*"**Toute personne** non suspectée de crime mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition au terme des articles*

précédents doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à
- fournir des informations permettant de prendre les mesures mentionnées aux articles précités
- accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système
- obtenir et copier ces données informatiques
- utiliser l'équipement pour faire des copies
- et obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédure légales".

Ce droit d'assistance a pour fondement l'article 19.4 de la Convention de BUDAPEST relatif aux perquisitions et saisie de données informatiques stockées, qui dispose que *"Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les données raisonnablement nécessaires, pour permettre* (les perquisitions et saisies)".

1.- Le champ des saisies et des perquisitions

les textes actuels, qui constituaient, en 2003, une avancée certaine, sont aujourd'hui pour partie obsolètes, comme partant du principe que les données sont entreposées dans un ordinateur fixe ou dans des supports de stockage informatique *(cf. art. 57-1 in fine)***, saisis dans le cadre de la perquisition d'un domicile, voire sur les lieux du crime ou du délit** *(cf. art. 54)*.

Or, la diversification des supports de stockage numérique *(cédéroms, clefs USB),* la multiplication des terminaux mobiles *(smartphones, tablettes)* comme le recours fréquent à des supports appartenant à des tiers ou leur partage par plusieurs utilisateurs, rend une telle conception par trop restrictive, même si la notion de *"domicile"* a été élargie par la jurisprudence.

Il est ainsi préconisé de mieux distinguer la notion de saisie d'objets numériques de celle de perquisition.

Recommandation n° 40
relative à l'extension du droit de perquisition et de saisie des terminaux et supports informatiques

1 - Etendre le droit de perquisition à tout lieu privatif où se trouvent des objets ou données informatiques utiles à la manifestation de la vérité.

2 - Autoriser explicitement la saisie des terminaux et des supports indépendamment de tout transport sur les lieux de l'infraction et de toute perquisition.

2.- **L'accès aux systèmes informatiques et l'analyse des données informatiques.**

Les services d'investigation se heurtent à des difficultés de différente nature.

21 - **la première difficulté concerne les modalités relatives à l'analyse des données informatiques saisies et à l'interrogation des autres systèmes informatiques accessibles à partir du système initial et visés à l'art. 57-1.**

En l'état actuel, les textes *(cf. art. 56 du C.P.P.)* prévoient soit une analyse sur les lieux de la perquisition, soit, en présence des personnes assistant à cette perquisition, la constitution d'un scellé provisoire - la mise ultérieure sous scellés définitifs devant être alors aussi réalisée en la même présence - ou la réalisation d'une copie sur un support numérique, afin de permettre implicitement une exploitation ultérieure [180].

L'analyse sur place, qui demande un environnement technique, notamment la présence sur les lieux d'un technicien, s'accorde mal avec les possibilités des services territoriaux et avec un travail en urgence sur les lieux de la perquisition. Il y a, en effet, des différences sensibles entre la prise de connaissance de documents-papier ou la reconnaissance d'objets, et l'analyse de données informatiques qui peuvent être volumineuses.

En cas de recours à des scellés provisoires, la présence des personnes ayant assisté à la perquisition aux fins de constitution des scellés définitifs s'avère souvent impossible en pratique, compte-tenu de la durée que requiert leur exploitation.

Si la possibilité reconnue aux services d'enquête de procéder à une copie des données numériques afin d'exploiter plus aisément ces dernières constitue une avancée indéniable, la grande capacité de certains supports requiert un temps de copie souvent important, qui s'avère incompatible avec la durée de la perquisition ainsi que, en cas d'interpellation d'une personne, avec celle de la garde à vue.

Les services de police judiciaire sont aujourd'hui contraints, dans de telles situations, de profiter de la présence du mis en cause ou des tiers concernés, pour placer le support informatique sous scellé définitif puis de faire appel à un de leurs collègues techniciens en le requérant sur le fondement de l'art. 60 du C. P.P. , puisque la loi autorise cette personne requise à briser le scellé aux fins d'analyse et à le reconstituer, hors la présence de la personne, compte-tenu de son indépendance par rapport à l'enquête...La complexité de la démarche est évidente pour un surcroît de garantie limitée par rapport à celle qu'offre tout officier de police judiciaire.

Enfin, la loi est muette s'agissant de l'exploitation des supports saisis en dehors d'une perquisition, par exemple sur la personne suspecte ou sur un tiers, ou de la possibilité de réaliser, en pareille hypothèse, une copie.

---

[180] Une telle assimilation de l'accès à un système informatique à la perquisition d'un domicile est d'ailleurs à l'origine du concept, évocateur mais mal défini, de *"perquisition informatique"*, traduction approximative du terme anglais de *"search"* qui a un contenu beaucoup plus large, raison pour laquelle il est préconisé de retenir le terme *"d'accès"* aussi usité dans la Convention de Budapest.

L'accès à un serveur distant pose les mêmes types de difficultés.

Indépendamment de la question des garanties qui doivent accompagner l'analyse *(voir les recommandations sur la preuve numérique*), il s'agit moins d'une difficulté de nature juridique que d'une insuffisance tenant à la conduite à tenir en matière d'accès, selon que l'on procède à des scellés fermés provisoires du support physique des données informatiques ou à la réalisation de copies, selon que la personne en cause peut être ou non présente, insuffisance à l'origine d'une véritable insécurité juridique, en premier lieu pour les enquêteurs.

Il est aujourd'hui nécessaire d'adapter la procédure aux spécificités du support informatique.

Recommandation n° 41
relative à l'analyse des données saisies

1 - Prévoir explicitement que l'accessibilité, à partir du système initial ou du scellé provisoire, aux données stockées dans ce système ou dans un autre système visé à l'art. 57-1 peut être réalisée soit sur les lieux de sa saisie, soit dans les locaux du service d'enquête ou dans les locaux des techniciens saisis en application de l'art. 60.

2 - Autoriser explicitement la réalisation d'une copie sur les lieux de la saisie du support numérique ainsi que dans les locaux d'enquête sur la base du scellé provisoire et hors la présence de la personne.

3.- Autoriser l'enquêteur, en cas de réalisation différée de la copie ou dans l'hypothèse d'une exploitation différée du scellé provisoire, de mettre le support saisi sous scellés définitifs hors la présence de la personne, mais en présence d'un responsable hiérarchique.

Ces trois dispositions doivent s'accompagner de garanties spécifiques *(voir les recommandations sur la preuve numérique).*

4 - Doter les services d'enquête, compte-tenu des besoins croissants à cet égard et de l'exigence de rapidité qui prévaut en cas d'interpellation du mis en cause, du matériel technique leur permettant de réaliser ces copies dans les meilleurs délais.

22. - **la seconde de ces difficultés tient à la méconnaissance des codes d'accès verrouillant l'accès au contenu informatique, dans la mesure où leur détenteur** *(suspect ou tiers)* **est soit absent, soit refuse de les fournir.**

Dans la mesure où l'art. 56 al.2 lui permet de prendre connaissance sur place des données informatiques avant saisie, l'officier de police judiciaire se trouve confronté à une impossibilité difficilement surmontable.

En outre, il importe de répondre à l'hypothèse de la découverte des codes d'accès sur place et de leur utilisation, soit en l'absence de l'intéressé, soit après refus de sa part de les fournir. Dans l'espèce ayant donné lieu à l'arrêt de la Chambre criminelle en date du 6.11.2013, cette utilisation par les

enquêteurs ne soulevait pas de difficultés dans la mesure où l'identifiant avait été obtenu dans le cadre d'une perquisition autorisée par le juge des libertés et de la détention ; toutefois, d'une part, la perquisition ne requiert pas nécessairement une autorisation d'un juge ; d'autre part, une telle saisie peut être opérée en tous lieux.

Enfin, le droit à l'assistance doit être spécialement reconnu, au-delà de la possibilité de rétention prévue in fine par l'art. 56 du C.P.P. ou de faire appel à une personne qualifiée. Une telle disposition compléterait harmonieusement les dispositions de l'art. 434-15-2 du code pénal réprimant la personne qui, ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé dans le cadre d'un crime ou d'un délit, refuse de prêter son concours alors qu'il en est requis.

Recommandations n° 42
relative aux codes d'accès

1.- Prévoir explicitement que la saisie peut porter tant sur les terminaux et supports de stockage que sur les éléments permettant l'accessibilité aux différents systèmes informatiques *(identifiants, méthodes de chiffrement...)* et que ces éléments peuvent être utilisés par l'officier de police judiciaire pour avoir accès aux données informatiques, à condition d'en faire mention dans la procédure.

2.- Inscrire dans le code de procédure pénale le droit, pour l'officier de police judiciaire, de requérir tout tiers ayant connaissance du système informatique, dans la mesure où il ne saurait être assimilé à une personne qualifiée,

3.- reconnaître explicitement le droit, déjà largement mis en oeuvre en pratique, pour l'officier de police judiciaire de casser lui-même le code d'accès ou de faire appel à une personne qualifiée pour ce faire, à condition d'assurer l'intégrité du système et d'en faire mention dans la procédure.

23.- **La troisième difficulté tient au recours de plus en plus fréquent à des logiciels de chiffrement.**

Quant aux **données cryptées ou chiffrées**, les dispositions des art. 230-1 et s. du code de procédure pénale permettent, aux seuls magistrats, de requérir toute personne physique ou morale ainsi que l'organisme technique interministériel habilité secret défense - *le Centre technique d'assistance (DCRI)* -. Si, s'agissant des données émanant des opérateurs de communication électronique, la future *Plate-forme nationale des interceptions judiciaires* devrait apporter des solutions, dans le cadre de la convention conclue avec le centre précité, la difficulté reste entière pour l'accès aux autres données informatiques.

Recommandation n° 43
relative au cryptage et au chiffrement des données

1 - Autoriser l'officier de police judiciaire, s'agissant des données chiffrées et lorsque la convention de chiffrement ne peut être obtenue du maître du système ou du tiers dont l'assistance est requis, à requérir toute personne qualifiée, y compris, par le biais de l'O.C.L.C.T.I.C. ou de l'I.R.C.G.N., *le Centre technique d'assistance.*

2 - Compte-tenu des compétences de ce *Centre* et de l'assistance précieuse qu'il peut fournir, gratuitement, aux autorités judiciaires, mieux faire connaître ce service, en accroître les capacités afin d'accélérer son expertise et en faciliter l'accès en prévoyant la possibilité pour les magistrats de le saisir directement, sans devoir passer par l'intermédiaire de l'O.C.L.C.T.I.C,

3 - Rechercher et poursuivre effectivement les personnes, physiques ou morales, qui se livrent au commerce, à l'importation et à l'exportation des logiciels de chiffrement et de cryptologie, en violation de la réglementation française existante, sans exclure, s'agissant des utilisateurs, l'application de la circonstance aggravante prévue par l'art. 132-79 du code pénal.

3 - **<u>les droits d'accès à un système informatique second sis à l'étranger</u>.**

Le temps où les données intéressant l'enquête étaient toutes stockées dans l'ordinateur du mis en cause est désormais révolu ; d'une part, l'évolution de la technique favorise leur externalisation ; d'autre part, les liens informatiques qu'a pu entretenir un suspect avec d'autres bases de données intéressent aujourd'hui autant la lutte contre la cybercriminalité que les données stockées.

La Convention du Conseil de l'Europe sur la cybercriminalité en a tiré les conséquences en prévoyant, en son article 32, que, sauf pour celles qui sont accessibles au public, l'accès transfrontalier à des données stockées sur le territoire d'un autre Etat est conditionné par *"le consentement légal et volontaire de la personne autorisée légalement à divulguer ces données".*

Le législateur français a ainsi modifié les deux premiers alinéas de l'art. 57-1 [181]. Quant à la Chambre criminelle, elle a elle-même, en son arrêt du 6 novembre 2013, donné l'interprétation la plus large possible au texte existant en privilégiant le doute quant à la localisation des données.

[181] art. 57-1 du C.P.P. :
"Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.
S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en-dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur".

Il en résulte que, pour les données non publiques, s'il n'est pas *"préalablement avéré"* que ces données sont stockées dans un système informatique situé en dehors du territoire national, l'officier de police judiciaire est autorisé à les consulter, implicitement selon la loi, explicitement selon la Cour de cassation.

En revanche, lorsqu'il est avéré que le système informatique en cause est situé en-dehors du territoire national, le principe est aussi celui de la consultation, sous réserve du *"consentement légal et volontaire de la personne autorisée légalement à divulguer ces données",* qui suppose de disposer d'informations le plus souvent inexistantes quant à la domiciliation légale du serveur ou du site concerné, et a fortiori, quant à l'identification du pays dans lequel les données sont stockées.

Les spécialistes se perdent aussi en conjecture pour déterminer exactement *"la personne autorisée légalement"* dont fait état la Convention, d'autant plus qu'une telle définition renvoie à des réalités propres à chaque système juridique.

A défaut, la seule solution juridique consiste en l'ouverture d'une information judiciaire aux fins de délivrance d'une commission rogatoire internationale, solution qui n'est pas envisageable dans les affaires de masse et de moindre gravité et s'avère inadaptée compte-tenu de la célérité qui s'impose et du risque de déplacement ou d'altération des données.

Si l'accès à un site ouvert au public ne soulève pas de difficultés *(à la condition de s'entendre sur ce que recouvre exactement un tel concept, notamment pour les réseaux sociaux : cf. La notion "d'amis" sur Facebook...)*, la difficulté est entière s'agissant des espaces privatifs situés à l'étranger, qui, à l'instar du coffre bancaire ou de la boîte à lettres, requièrent, en terme d'accès, des garanties tenant, à la fois, à la personne et à l'Etat, voire à la personne seule dans le cadre de la Convention précitée.

D'évidence, une telle limitation favorise l'impunité des délinquants, compte-tenu du recours de plus en plus fréquent à la localisation des données à l'étranger, au besoin dans des *"cyber-paradis"*, voire dans les *"nuages".* Elle constitue, pour les praticiens, l'une des difficultés majeures rencontrées dans les enquêtes ou les instructions préparatoires portant sur la cybercriminalité.

Le groupe interministériel a pris acte des réflexions du Conseil de l'Europe susceptibles de déboucher, à terme, sur un protocole additionnel destiné à autoriser à distance, pour les données d'identité et de trafic, ce type de consultations dans la mesure où les données intéressant l'enquête sont accessibles à partir du système initial. Il conviendra toutefois de bien examiner les effets directs d'une telle évolution s'agissant des sociétés françaises ainsi que le temps que va requérir une telle évolution.

Le Groupe est d'avis, vu l'urgence et à l'instar de nombre autres Etats européens [182], de procéder sur le plan de la législation interne.

Deux solutions ont été explorées.

[182] cf. le code d'instruction criminelle belge, le code de procédure pénale portugais...

En premier lieu, il pourrait être envisagé de procéder de manière similaire à ce qui est recommandé pour les réquisitions et d'instituer un *"droit de suite"* en énonçant que tout système informatique accessible à partir d'un système initial présent sur le territoire français et en possession ou utilisé par une personne paraissant avoir participé à un crime ou à un délit grave est présumé ne faire qu'un avec le système initial et soumis aux mêmes modalités de consultation que ce dernier, en bornant ou non cette possibilité d'accès aux seules données personnelles de l'intéressé.

Une telle solution, conforme semble-t-il aux dispositions déjà existantes au bénéfice de l'administration fiscale et à la décision prise par la cour d'appel de PARIS en son arrêt du 31 août.2012, serait logique dans la mesure où, si des agents ont autorité pour accéder à un ordinateur, ils doivent être à même de consulter l'ensemble des données créées par le suspect ou accessibles par lui.

Toutefois, c'est une autre solution qui est préconisée, comme plus protectrice et plus cohérente avec les dispositions internationales existantes : recourir à l'autorisation préalable d'un magistrat lorsque le consentement de la personne habilitée à autoriser l'accès n'a pu être recueilli.
Cette proposition se situe dans la droite ligne des dispositions de la Convention précitée tout en leur donnant leur pleine effectivité, en positionnant en quelque sorte le magistrat comme une autorité de substitution lorsque, notamment, la personne légale autorisée à consentir à la divulgation n'est pas déterminée, se trouve être empêchée ou a pris la fuite.

Recommandation n° 44
relative à l'accès en ligne
aux données informatiques stockées à l'étranger

Prévoir, dans la loi française, que, lorsqu'il avéré que le stockage des données informatiques a lieu à l'étranger et que le consentement de la personne habilitée à autoriser l'accès n'a pu être recueilli, leur consultation puisse être autorisée par un magistrat.

.

4.- **le recours à des techniciens et experts qualifiés**

La technicité requise par les analyses numériques suppose le concours de spécialistes formés à cet effet. Les praticiens rencontrent plusieurs difficultés concrètes à cet égard.

41 - **La première difficulté, rencontrée par les enquêteurs, a trait au rôle respectif des officiers de police judiciaire habilités à procéder à l'enquête, et des policiers ou gendarmes requis en tant que personnes qualifiées sur le fondement des dispositions de l'art. 60 du code de procédure pénale, notamment les ICC et les NTECH.**

Pour des raisons pratiques et afin d'éviter une césure dans les investigations nécessaires en cours d'analyse et d'exploitation des matériels, les services enquêteurs souhaiteraient que les policiers et gendarmes requis puissent exercer, à la fois, leur qualité de technicien et leur qualité d'officier de police judiciaire.

En l'état de la jurisprudence, il n'existe aucune incompatibilité entre les deux qualités lorsque le technicien appartient au service chargé de procéder à l'enquête. Ainsi, dans l'arrêt n° 10-84.389 rendu le 4.11.2010 par la Chambre criminelle, le fait que des fonctionnaires du service local d'identité judiciaire aient effectué des constatations et examens, mêmes techniques, pour le compte d'un officier de police judiciaire relevant du même service régional de police judiciaire saisi de l'enquête par instructions du procureur de la République, ne relevait pas des dispositions de l'art. 60 ; vraisemblablement, la Cour de cassation a ainsi voulu éviter qu'il soit procédé à des réquisitions internes à un même service et à des prestations de serment, qui revêtiraient un aspect purement formel au regard du principe de l'autorité hiérarchique. Par-delà, il y a la volonté d'assurer le respect de la désignation du service d'enquête compétent par le procureur de la République comme par le juge d'instruction.

En revanche, lorsque le technicien relève d'un autre service ou d'une autre unité que celui ou celle saisi de l'enquête, le recours à l'art. 60 s'impose avec, comme corollaire, l'impossibilité, pour le technicien, de procéder à des actes d'enquête. Toutefois, l'interprétation de l'arrêt précité tendrait à permettre de faire l'économie d'un tel recours si le service ou l'unité dont fait partie le technicien - à la condition qu'il s'agisse d'un service ou d'une unité de police judiciaire et que le technicien ait lui-même la qualité d'officier ou d'agent de police judiciaire -, est co-saisi par le magistrat.

En conséquence, ce n'est que dans l'hypothèse d'une saisine d'office, par l'enquêteur, d'un technicien relevant d'un autre service que le sien, qu'il devrait être fait recours aux dispositions de l'art.60 avec les conséquences qu'il implique.

Le groupe interministériel a estimé ne pas devoir revenir sur cette dichotomie dans la mesure où les examens techniques et scientifiques effectués dans le cadre de l'art.60 requièrent, de manière générale, sinon une certaine indépendance institutionnelle, du moins une impartialité fonctionnelle consacrée par la prestation de serment. C'est d'ailleurs, compte-tenu de cette spécificité que la personne qualifiée de l'art. 60 peut, comme un expert dans le cours d'une information, briser les scellés et les reconstituer.

Bien entendu, plus la compétence des O.P.J. sera élevée s'agissant des constatations opérées en cette matière, plus les services et unités seront dotés de NTEC ou d'ICC, moins ils auront besoin de requérir les techniciens spécialisés en provenance d'autres services.

42 - la seconde difficulté, propre aux juges d'instruction, a trait à la compétence comme d'ailleurs au coût des experts en matière numérique.[183]

Si une partie des experts dispose d'une véritable compétence, une des difficultés que rencontre la Justice, qui n'est d'ailleurs pas propre à la cybercriminalité, concerne l'instruction des demandes d'inscription sur les listes des experts judiciaires.
Elle doit pouvoir bénéficier d'un avis technique autorisé provenant soit de la profession, soit, si celle-ci n'est pas suffisamment organisée, d'une autorité externe qualifiée.

Une autre difficulté tient au recours même à l'expertise. S'il s'agit simplement de procéder à des constatations sur le fondement de l'al. 4 de l'art. 81 *(consultation et analyse des données existantes sur les supports saisis, y compris avec la mise en oeuvre de logiciels forensiques)*, un tel recours ne s'avère pas nécessaire et les enquêteurs spécialisés peuvent y procéder, à la condition que leur nombre s'accroisse.
Il convient toutefois de déterminer plus précisément où s'arrêtent les constatations et où débutent les investigations véritablement techniques *(recherche ou reconstitution de données illisibles ou effacées, mise à jour de données cachées, recherche de mots clés, d'images, de logiciels illégaux...)*.

La formation comme le soutien apportés aux juges d'instruction doit aussi prendre en compte la nécessité de déterminer de manière précise les missions expertales et de veiller à ce que les experts ainsi commis aillent bien à l'essentiel et présentent leurs travaux de manière dynamique, sans se limiter à une transcription et à une mise à plat des données recueillies.

Enfin, reste le coût des expertises, souvent démesuré par rapport aux attentes du juge, et qui nécessiterait d'être mieux encadré, sous peine de peser lourdement dans le futur sur la dotation allouée aux juridictions.

Si les futures juridictions spécialisées seront en mesure de disposer du savoir-faire nécessaire, il serait opportun que l'administration centrale apporte un soutien institutionnel sur ces différents points.

[183] A noter sur ce point qu'il existe, depuis 1989, une *Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA)*, qui regroupe environ 110 experts.

Recommandation n° 45
relative aux recours aux personnes qualifiées et aux experts

1 - prévoir une aide institutionnelle de *l'Autorité nationale sur la sécurité des systèmes d'information* en ce qui concerne l'inscription des experts en cybercriminalité sur les listes des cours d'appel, soit sous la forme d'avis, soit sous celle de labellisations d'organismes ou de laboratoires

2 - préconiser, de préférence à l'expertise, le recours aux techniciens de la Police ou de la Gendarmerie s'il s'agit de procéder à de simples constatations.

3.- apporter, au plan de l'administration centrale de la Justice avec le concours de l'Ecole nationale de la Magistrature, un soutien aux magistrats instructeurs dans la détermination des missions d'expertise *(diffusion de missions-type...)*.

4 - poursuivre la tarification des analyses en matière informatique et examiner la possibilité de passation de marchés publics.
.

---

③⑦.- l'enquête sous pseudonyme

Elle est prévue, pour des infractions strictement délimitées *(provocation directe aux actes de terrorisme, apologie du terrorisme, traite des êtres humains, proxénétisme assimilé, recours à la prostitution de mineurs ou de personnes particulièrement vulnérables, mise en péril des mineurs)* par les art. 706-25-2, 706-35-1 et 706-47-3 du code de procédure pénale ainsi que par l'art. 59 de la loi du 12.05.2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, et, s'agissant de plusieurs délits douaniers *(l'importation, l'exportation ou la détention de produits stupéfiants, de tabac manufacturé et de marchandises contrefaites),* par le 3˚ de l'art. 67 bis-1 du code des douanes.

Même si leurs formulations diffèrent, ces dispositions ont pour but d'autoriser certains fonctionnaires nommément désignés à participer sous un pseudonyme à des échanges électroniques, à être en contact, par ce moyen, avec les personnes susceptibles d'être les auteurs des infractions visées, et d'extraire ou d'acquérir les données d'identification ainsi que les éléments de preuve nécessaires à l'enquête, sans que de tels actes puissent, en aucun cas, être constitutifs d'une provocation à commettre une infraction.

Si une telle interdiction comme la possibilité d'acquérir des éléments de preuve [184] constituent des points de similitude avec la procédure dite d'infiltration, prévue en droit commun par les art. 706-32, 706-81 s. du C.P.P. et l'art. 67 bis du code des Douanes, parler de cyber-infiltration pour cette technique d'enquête menée sous pseudonyme relève d'un abus de langage, juridiquement erroné et de nature à susciter des réserves quant à son utilisation.

En effet, les pouvoirs dévolus aux enquêteurs sont bien en-deçà de ceux dont disposent les agents infiltrés qui peuvent, eux, *"acquérir, détenir, transporter, livrer ou détenir des substances, biens produits, documents ou informations tirés de la commission des infractions ou servant à la commission de ces infractions"* et surtout *"utiliser ou mettre à disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication"*, c'est-à-dire commettre des infractions pour la bonne cause.

Telle est d'ailleurs la raison pour laquelle les conditions de l'infiltration sont plus rigoureuses que celle de l'enquête sous pseudonyme.

Paradoxalement, le champ de l'infiltration est bien plus large *(cf. l'ensemble des infractions visées à l'art. 706-73 du C.P.P.)* **que celui de l'enquête sous pseudonyme.**

En outre, par comparaison avec les exemples étrangers, la législation française paraît bien restrictive, puisque, dans plusieurs pays, il est recouru à cette technique dans le cadre des pouvoirs généraux d'enquête *(Canada, USA, Luxembourg)* ; que d'autres distinguent les investigations passives qualifiées d'observations, des investigations actives *(Suisse) ;* enfin, au Royaume-Uni, qui dispose d'une législation spécifique, les conditions tiennent à la formation particulière des enquêteurs et à l'autorisation de leurs chefs de service, la technique étant par ailleurs autorisée pour toute infraction si la mesure est nécessaire et proportionnée.

En l'état, l'objectif recherché par le législateur - faciliter les enquêtes pro-actives des services spécialisés sur Internet - n'est pas véritablement atteint pour deux raisons.

---

[184] qui se distingue toutefois de la technique dite *"du coup d'achat"*, prévue par le même art. 67-I du code des Douanes, et utilisée par Cyberdouane pour lutter contre les infractions supposant des transferts d'argent ou de marchandises, notamment dans le domaine de la contrefaçon

□ **une confusion entre la *veille policière* sur Internet et *l'enquête sous pseudonyme***

La *"veille"* consiste à accéder aux espaces ouverts au public sur Internet afin de déceler l'existence d'éventuelles infractions. C'est l'application à ce système de communication du vieux principe de surveillance préventive que doivent exercer policiers et gendarmes en tous lieux ouverts au public, qui ne nécessite pas une autorisation légale autre que celle qui résulte des art. 12 et 41 du C.P.P., sauf a contrario, s'agissant de la surveillance des personnes, les dispositions de l'art. 706-80 du C.P.P.

Cette veille se réalise sans moyens d'investigation particuliers autres que le recours à un accès Internet non rattaché au réseau Police [185] ainsi qu'à des moteurs de recherche et ne donne lieu à aucun acte d'enquête.

Elle suppose toutefois, ne serait-ce que pour pouvoir accéder aux réseaux sociaux, forums de discussions, blogs... d'avoir recours, comme tout un chacun, à un pseudonyme. Un tel recours procède aussi d'une nécessaire égalité des armes, compte-tenu de l'usage généralisé de pseudonymes sur Internet, mais aussi d'une sécurité minimale pour les agents.

Une telle veille était de pratique courante ; elle se trouve aujourd'hui fragilisée, s'agissant des seuls officiers et agents de police judiciaire comme des douaniers [186], par la rédaction même des articles précités qui paraissent soumettre aux mêmes conditions l'usage d'un pseudonyme qu'il soit ou non accompagné d'investigations.
En liant ainsi le recours à un pseudonyme avec la prise de contact et l'acquisition ou l'extraction de preuve, la veille est limitée à quelques agents et pour quelques infractions graves, alors même que, par nature, elle doit revêtir une portée générale et ne requiert pas un encadrement normatif au sens des alinéas 2 des art.8 et 10 de *la Convention européenne des droits de l'homme*, car elle ne saurait être assimilée à une ingérence dans le droit au respect de la vie privée des personnes ou dans la liberté d'expression.

.

Sauf à remettre en cause cet objectif général de veille, il importe de modifier les articles en question afin de lever les interrogations existantes et de permettre aux membres de la police judiciaire ainsi qu'aux douaniers de recourir librement à un pseudonyme.

[185] une telle veille *"en mode caché"* répond à des raisons évidentes : le recours à l'adresse IP du ministère de l'Intérieur préviendrait d'éventuels délinquants...Encore faudrait-il que l'ensemble des services d'enquête en soient dotés.

[186] nombreux sont les services administratifs, autorités administratives indépendantes, associations, groupements professionnels qui réalisent de telle veille sur Internet

Recommandation n° 46
relative à la veille sur Internet
pratiquée par la police judiciaire

Autoriser, de manière générale, le simple usage d'un pseudonyme sur Internet par les officiers et agents de police judiciaire, lorsqu'il ne s'accompagne pas d'investigations particulières.

□ **le champ d'application trop restreint de *l'enquête sous patronyme***

Parfois la veille ne suffit pas et il faut passer à une phase active d'identification de l'auteur d'une infraction et à la réunion d'éléments de preuve.

Les services enquêteurs, qu'ils soient spécialisés ou non, sont tous unanimes pour souligner combien la phase d'identification d'un cyber-délinquant devient de plus en plus difficile. La méthode reine d'investigation - l'identification d'une personne par une adresse IP - devient de plus en plus hypothétique et pour plusieurs raisons mises en évidence notamment par l'O.C.L.C.T.I.C. qui ont déjà été mentionnées mais qui méritent d'être précisées :

⌙ les internautes malveillants ont recours fréquemment à des techniques, gratuites et simples, garantissant leur anonymat ; certains sites fournissent ainsi un service consistant à masquer l'adresse IP ; d'autres serveurs permettent l'envoi d'e-mails anonymes ; les réseaux décentralisés aléatoires *(comme TOR)* et les serveurs mandataires *(proxies)* allouent des adresses IP d'emprunt ; des navigateurs gratuits *(tel que Firefox)* permettent le téléchargement d'options d'anonymisation *(plugins)...*

⌙ les mêmes bénéficient du développement de l'Internet nomade, qui leur permet de se connecter, de préférence, à des bornes *"wifi"* publiques et gratuites, dans les gares, les mairies, les aéroports...Lorsqu'ils ont recours à des connexions en *"3G" (Internet mobile)*, les flux échangés passent par des serveurs intermédiaires des fournisseurs d'accès, qui reçoivent des milliers de connexion par seconde, rendant l'identification d'un abonné particulièrement complexe.

⌙ quant aux délinquants les plus organisés, ils placent leurs traces informatiques hors de portée des enquêteurs français en jouant sur le particularisme des législations internes : les forums dédiés à la consommation et à l'échange de produits stupéfiants sont hébergés à l'étranger, dans des *cyber-paradis* ; les sites incitant à la haine raciale sont hébergés sur des serveurs de sociétés américaines...

Dés lors, l'enquête sous pseudonyme, malgré l'absence de contrainte qui la caractérise au regard de l'infiltration, s'avère parfois la seule possibilité encore offerte à un service spécialisé pour identifier un délinquant.

Certes, les praticiens s'accordent à reconnaître qu'une telle technique d'enquête n'est pas la panacée, puisqu'elle suppose une certaine disponibilité de l'enquêteur et une formation préalable et qu'elle n'est pas adaptée à toutes les formes de cybercriminalité. Toutefois, de manière générale, l'efficacité de telles enquêtes est avérée.

Telle est d'ailleurs la raison pour laquelle elle est largement pratiquée, sous une forme ou sous une autre, tant par CYBERDOUANE que par des enquêteurs de nombreux pays d'Europe *(Belgique, Bulgarie, Lettonie, Pays-Bas, Royaume-Uni...)*.

En France, le caractère extrêmement restrictif de son champ d'application pose problème.

Deux possibilités d'évolution sont envisageables : soit l'autoriser pour un plus grand nombre d'infractions, spécialement visées par la loi, selon une méthode souvent mise en oeuvre depuis 15 ans en matière de procédure pénale, mais l'on voit mal quel serait le critère d'inclusion ; soit la généraliser mais en la bornant, c'est-à-dire en l'érigeant en réponse spécifique aux difficultés d'identification d'une personne mise en cause, et en l'accompagnant de garanties supplémentaires au regard des art.8 et 10 déjà cités de la Convention européenne des droits de l'homme. C'est la solution préconisée.

Recommandation n° 47
relative à la généralisation de l'enquête sous pseudonyme

Généraliser la possibilité de réaliser des enquêtes sous pseudonyme à tous les crimes et délits punis d'une peine d'emprisonnement commis par le biais d'un réseau de communications électroniques, lorsque l'enquêteur est confronté à une difficulté d'identification de la personne susceptible d'en être l'auteur, et à la triple condition que
- l'officier ou agent de police judiciaire appartienne à un service spécialisé désigné et soit spécialement habilité à cette fin
- l'enquête soit limitée à une certaine durée, avec une possibilité de renouvellement soumise à l'autorisation préalable du procureur de la République
- la traçabilité des opérations soit assurée.

*****

③⑧ - la captation des données à distance

La loi du 14.03.2011 a reconnu au juge d'instruction la possibilité de décider de la captation à distance des données informatiques, dans le cadre des dispositions spécifiques relatives à la criminalité et à la délinquance organisée *(cf. art. 706-102-1 à 706-102-8 du code de procédure pénale).*

Ce texte a manifestement été inspiré tant par les dispositions relatives à la sonorisation des domiciles que par les législations étrangères comparables.

A cet égard et à titre d'exemple, on peut souligner que le plus récent modèle législatif de lutte contre la cybercriminalité édité en 2012 avec le soutien de l'Union européenne prévoit un dispositif similaire *(cf. "Cybercriminalité - Modèles de lignes directrices politiques et de textes législatifs - HIPACAR - UIT 2012" - Logiciel de criminalistique),* la disposition - présentée comme une norme minimale -, étant ainsi rédigée :

> *"Si un juge/magistrat est convaincu qu'il existe, dans une enquête relative à une infraction énumérée au par. 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres moyens, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut autoriser un agent à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. ...*
> *La durée de l'autorisation est limitée à 3 mois...*
> *L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect...".*

Deux ans et demi après le vote législatif et alors même que les dispositions réglementaires sont intervenues *(décret 3.11.2011, arrêté 4.07.2012)*, la loi n'est toujours pas en application, ce qui distingue la France des autres Etats comparables qui mettent déjà en oeuvre, souvent depuis des années, cette technique de la captation.

En fait, les raisons du retard sont exclusivement techniques, le vote de la loi étant intervenu alors que les solutions techniques n'avaient pas été suffisamment expertisées, sans doute pour rassurer les sociétés françaises concernées quant aux investissements requis.

Si les dispositions précitées prévoient deux moyens de captation - l'un par introduction physique au domicile, l'autre à distance, permettant soit d'enregistrer les frappes du clavier, soit les données figurant à l'écran -, il s'est avéré nécessaire de faire développer les outils utiles par des sociétés françaises, tant pour des raisons de sécurité que pour des raisons de souveraineté, et de répondre aux impératifs de miniaturisation et de contingentement de la captation par rapport aux données autorisées par la loi. Cette question technique, dans laquelle s'est impliquée l'A.N.S.S.I., devrait être définitivement réglée pour le début de 2014.

Reste à régler l'épineuse question du coût de l'investissement et de la commercialisation de ces produits, l'Exécutif ayant le choix entre le dégagement d'une enveloppe budgétaire conséquente ou le paiement à l'acte sur les frais de justice, lequel pose, à son tour, le problème d'une éventuelle tarification.
Cette question est actuellement examinée par le ministère de l'Intérieur et celui de la Justice *(Délégation aux interceptions judiciaires).*

Recommandation n° 48
relative à la captation à distance de données informatiques

Le Groupe de travail réaffirme l'intérêt que revêt le recours, pour combattre les formes les plus graves et les plus organisées de la cybercriminalité, à la technique de la captation à distance - équivalent de la sonorisation pour les infractions de droit commun -, ainsi que la nécessité de donner rapidement aux praticiens la possibilité d'utiliser cette technique légalisée dès 2011.

*****

③⑨ - le recours aux moyens de lutte contre la délinquance organisée

Le code de procédure pénale *(art. 706-73 s.)* prévoit, s'agissant de crimes et délits graves spécialement visés relevant de la délinquance organisée, des moyens procéduraux exceptionnels, notamment les interceptions et les gardes à vue prolongées.

Compte-tenu des difficultés, déjà soulignées, pour lutter contre la cybercriminalité, le groupe interministériel s'est interrogé sur l'opportunité d'étendre le dispositif en question aux infractions les plus significatives commises par l'intermédiaire ou au moyen d'un système de communications électroniques.

Dans sa réflexion, il a tenu compte des réserves d'ordre général émises quant à l'opportunité d'accroître encore le recours à une procédure pénale spécifique et dérogatoire aux règles communes ; du fait que la plupart des infractions visées à l'art. 706-73 sont réprimées d'une peine au moins égale à 10 ans d'emprisonnement, alors que les infractions incriminant spécifiquement des infractions relevant de la cybercriminalité sont punies de peines maximales inférieures ; du revirement de jurisprudence résultant de la décision du Conseil constitutionnel du 4.12.2013 portant sur la loi relative à la fraude fiscale et à la grande délinquance économique et financière [187].

Toutefois, eu égard à la gravité exceptionnelle que peut revêtir une atteinte aux systèmes de traitements automatisés de données *(S.T.A.D.),* le groupe de travail a déjà été conduit à recommander, d'une part, des modifications du droit pénal, aux fins notamment de la création d'une circonstance aggravante tenant à l'existence d'une bande organisée, d'autre part, la reconnaissance d'une compétence spécifique aux juridictions inter-régionales spécialisées les concernant [188] et d'une compétence spéciale pour Paris s'agissant des atteintes portées à des sites vitaux.

Par voie de conséquence, les atteintes aux S.T.A.D. ainsi aggravées, compte-tenu et de leur gravité et des difficultés tenant à l'identification et à l'appréhension de leurs auteurs, devraient relever des dispositions procédurales exceptionnelles susvisées.

---

[187] En son considérant 75, le Conseil a validé l'extension à certains délits économiques et financiers de divers pouvoirs de surveillance et d'investigation propres à la délinquance organisée *(surveillance étendue de l'art. 706-80 du C.P.P., infiltration de l'art. 706-81s., interception de correspondances de l'art. 706-95, sonorisation et captation de données informatiques des art. 706-96s.)*, en considération de la gravité des infractions concernées et de *"la difficulté d'appréhender les auteurs de ces infractions* (tenant) *à des éléments d'extranéité ou à l'existence d'un groupement ou d'un réseau dont l'identification, la connaissance et le démantèlement posent des problèmes complexes".*
En revanche, en son considérant 77, il a jugé comme contraire au principe de proportionnalité le fait de prévoir, pour ces mêmes délits, la possibilité de prolonger la garde à vue, sur le fondement de l'art. 706-88, de deux prolongations supplémentaires de 24h. venant s'ajouter au délai de droit commun, aux motifs que les infractions énumérées *"constituent des délits qui ne sont pas susceptibles de porter atteinte en eux-mêmes à la sécurité, à la dignité ou à la vie des personnes".* Il est à noter qu'un tel revirement de jurisprudence fragilise, pour l'avenir, les atteintes aux biens commises en bande organisée visées au titre de la délinquance organisée - et notamment les escroqueries qui intéressent directement la lutte contre la cybercriminalité -, bien que la loi de 2004 ait été validée par ce même Conseil.

[188] les J.I.R.S. ont été créées, principalement, pour connaître de l'ensemble de la criminalité organisée *(cf. art. 706-75 s. du C.P.P.).*

Néanmoins, et afin de prendre en compte la décision constitutionnelle précitée, il est proposé de n'autoriser le recours à la garde à vue prolongée que dans l'hypothèse où l'atteinte précitée porterait sur un service de l'Etat ou un opérateur d'importance vitale, induisant alors la compétence Parisienne ; en effet, dans un tel cas de figure, la durée de la garde à vue de droit commun apparaît insuffisante pour répondre à une délinquance qui, au-delà des difficultés générales tenant à la lutte contre la cybercriminalité, y ajoute la complexité tenant à la bande organisée et celle tenant au but recherché. **Certes, un tel critère va au-delà de celui récemment fixé par le Conseil, mais la défense des intérêts fondamentaux de la Nation paraît mériter autant d'attention que les atteintes à la dignité de la personne.**

Recommandation n° 49
relative à l'extension à certaines formes de cybercriminalité des moyens relevant de la lutte contre la délinquance organisée

1 - Autoriser le recours aux moyens de procédure exceptionnels relevant de la lutte contre la délinquance organisée s'agissant des atteintes aux systèmes de traitements automatisés de données, aux motifs que de telles atteintes peuvent revêtir un degré de gravité particulièrement important dans certaines circonstances et que, par nature, la complexité des enquêtes à mener en ce domaine nécessite de pouvoir disposer de l'ensemble des moyens d'investigation existants.

2.- Limiter toutefois la possibilité de recourir à la garde à vue exceptionnelle de 96h. à l'hypothèse où l'atteinte en question porte sur un service de l'Etat ou un opérateur d'importance vitale et menace ainsi les intérêts fondamentaux de la Nation.

IIII.4.- De la réponse aux contentieux de masse et de la police des noms de domaine

La cybercriminalité donne lieu à deux types de contentieux de masse qui, pour des raisons différentes, ne sont pas traités de manière satisfaisante et appellent, dès lors, des modes de traitement spécifiques et totalement novateurs.

1.- **L'escroquerie** constitue l'infraction la plus répandue, celle qui fait le plus grand nombre de victimes, qu'elle prenne la forme d'une fraude sur la vente à distance, constitutive d'un véritable marché parallèle qui recourt à des intermédiaires plus ou moins complices *("les mules" dans le jargon policier)*, de l'escroquerie dite *"à la nigériane"*, qui exploite la crédulité humaine sous la forme de mails *(faux appels aux dons, fausses loteries, faux héritages, fausses annonces, voire escroqueries sentimentales)* et fait transiter les fonds par l'intermédiaire de sociétés de transfert d'argent incontrôlées, ou encore de vastes escroqueries soigneusement préparées visant exclusivement les entreprises *(cf. les escroqueries par faux ordres de virement, apparues en France il y a deux ans, et qui font actuellement l'objet d'informations judiciaires ouvertes à Paris, Bordeaux, Lille, Lyon, Rennes...)*. C'est aussi celle qui est la plus mal élucidée et pour laquelle les services de police et les parquets rencontrent les plus grandes difficultés.

L'origine de cet état de fait doit être recherchée dans le mode de traitement mis en oeuvre.

Par nature, l'escroquerie, qui ne peut en l'état faire l'objet d'investigations pro-actives car la cyber-infiltration n'est pas actuellement autorisée pour ce type d'infractions, est portée, comme n'importe quelle infraction, à la connaissance d'un service enquêteur par la plainte de la victime, en fonction de son domicile ou de son siège social.

Cette plainte, qui n'est pas souvent accompagnée des éléments nécessaires à l'enquête - notamment le courriel qui en est à l'origine, voire les rares éléments d'identification disponibles -, n'est pas non plus toujours recueillie de manière utile, faute de sensibilisation suffisante des agents concernés.

En outre, dès l'abord, l'enquête se heurte à l'anonymisation des données personnelles, ce qui nécessite de requérir le fournisseur d'accès aux fins d'obtention de l'adresse IP.

A ce stade, l'enquêteur et, a fortiori, le parquet sur le ressort duquel il opère ne disposent d'aucune donnée pour apprécier si l'escroquerie dont il est saisi relève d'un acte isolé ou d'une délinquance plus organisée, puisqu'aucun rapprochement ne peut être opéré entre plaintes similaires, sauf pour celles déposées auprès de la même sûreté ou de la même brigade.

Sauf l'existence d'un modus operandi révélateur d'une délinquance organisée, le parquet apprécie alors la suite à donner en fonction du seul préjudice individuel subi par chaque victime, souvent de peu d'importance ; dès lors, pour des raisons tant de priorités que d'économies - les dotations en frais de justice étant particulièrement contraintes - il a tendance, en fonction de seuils divers qu'il a lui-même fixés, de ne pas requérir le fournisseur, ce qui entraîne le classement sans suite de la plainte.

Même dans l'hypothèse où l'adresse IP est requise et obtenue - ce qui n'est pas toujours le cas, faute parfois de réquisitions pertinentes ou du fait de l'absence ou du refus de réponse de certains fournisseurs -, les services locaux se heurtent à une autre difficulté tenant au fait que, **le plus souvent, l'adresse renvoie à une domiciliation étrangère, parfois éloignée de l'Union européenne**. **Le parquet se livre alors à une nouvelle appréciation, tenant à l'opportunité d'avoir recours à l'entraide pénale internationale pour aller plus loin, voire d'ouvrir une information judiciaire**. Là encore à ce stade de nombreuses plaintes sont classées sans suite pour des raisons similaires aux précédentes.

Enfin, **lorsque l'adresse IP renvoie à une domiciliation sur le territoire national, la plainte est, le plus souvent, transmise au parquet territorialement compétent,** ce qui nécessite la saisine d'un nouveau service d'enquête, avec la déperdition de temps et d'énergie que l'on imagine.

En fait, les services d'investigation territoriaux comme les parquets manquent d'une donnée essentielle d'appréciation, tenant à l'existence de faits similaires commis selon le même *modus operandi* au-delà du territoire dans lequel ils opèrent, car les différents fichiers existants ne sont pas en mesure, en l'état, de jouer ce rôle.

Or, la spécificité de l'escroquerie commise par Internet tient à ce que l'escroc opère, concomitamment, en direction de milliers ou de dizaines de milliers de victimes potentielles sur le territoire national.

Policiers, gendarmes et magistrats du parquet sont bien conscients d'une telle carence mais n'ont aucun moyen d'y pallier, raison pour laquelle tous ceux qui ont été entendus par le groupe de travail sollicitent une réforme.

Quant aux services spécialisés à l'échelle nationale, faute de remontée d'informations, ils ne peuvent que réaliser des recoupements partiels, fondés sur les seuls signalements des internautes via la base PHAROS *(cette base exclut les plaintes)* et des partenariats mis en oeuvre avec les entreprises privées impactées par la fraude, partenariats certes importants mais insuffisants ; il est vrai que les 5 à 6 policiers ou gendarmes dont dispose le groupe "escroqueries" de l'O.C.L.C.T.I.C. sont déjà au maximum de leurs capacités.

En résumé, les modes classiques de saisine et de traitement, en ce qu'ils reposent sur le traitement individualisé et local de chaque plainte, outre qu'ils pèsent lourdement sur des services territoriaux impuissants, s'avèrent totalement inadaptés pour les escroqueries commises via Internet.

Il est aujourd'hui temps de substituer au traitement local actuel un traitement centralisé, de nature à permettre, à l'issue de la phase d'identification opérée par le futur service central à créer, d'effectuer les regroupements nécessaires entre les différents faits dénoncés et de saisir ensuite, de manière utile, le parquet le plus compétent pour en connaître.

> **Ainsi serait-il mis un terme à un traitement différencié, guère compréhensible, entre les signalements qui sont traités à un niveau centralisé, et les plaintes dépendantes encore du niveau local, alors que les uns et les autres renvoient à une même réalité criminelle, qui appelle des recoupements.**

En outre, la réforme préconisée aurait valeur de test avant d'éventuelles extensions.

Recommandation n° 50
relative à la création d'une plate-forme centralisée
pour le traitement des cyber-escroqueries

Compte-tenu de l'inefficacité du traitement de ces infractions en fonction du lieu du dépôt de plainte, il est préconisé

1.- de substituer au système actuel un traitement centralisé par une plate-forme nationale de l'ensemble des escroqueries réalisées via Intranet, les usurpations de carte bancaire relevant toutefois d'un traitement spécifique.

2.- D'alimenter cette plate-forme par des plaintes formulées en ligne selon des menus déroulants destinés à s'assurer de l'exhaustivité des informations utiles, plaintes qui, contrairement à l'expérimentation actuelle, feraient l'économie d'une convocation et d'une audition de la victime par le service d'enquête, et donneraient lieu à la délivrance d'un accusé de réception automatisé.
Cette nouvelle modalité sera de nature à simplifier et à favoriser les démarches des victimes.
Toutefois, s'agissant des victimes qui souhaiteraient pouvoir continuer à déposer plainte localement, les applications informatiques relatives au traitement des procédures de la Police et de la Gendarmerie devront intégrer des imprimés et conduites-type, afin de s'assurer, là encore, de l'exhaustivité des informations recueillies.

3.- Donner pour mission à cette plate-forme nationale - qui devrait être gérée par l'O.C.L.C.T.I.C. ou travailler en synergie avec lui, puisque cet Office assure déjà la responsabilité de la base PHAROS qui reçoit les signalements des internautes ainsi que du dispositif "INFO-ESCROQUERIE", mais qui devrait, en tout état de cause, favoriser une approche interministérielle - de

□ procéder à une analyse des plaintes, particulièrement du modus operandi, grâce à un logiciel performant de rapprochement de nature à mettre en évidence les escroqueries relevant d'une même action criminelle
□ délivrer les réquisitions nécessaires aux prestataires afin d'obtenir les éléments d'identification et de domiciliation disponibles
□ puis, sur la base de critères pré-déterminés par l'autorité judiciaire et avec son aval, saisir les parquets compétents des affaires ainsi regroupées avec les éléments recueillis par ses soins, tout en en informant les victimes. Ainsi, chaque parquet et chaque service d'enquête, tout en faisant l'économie de la phase d'identification, disposera d'informations plus directement exploitables.

4.- Rendre, comme PHAROS depuis peu, cette plate-forme accessible aux services d'enquête, tant pour son alimentation qu'à des fins de consultation.

5.- Doter cette même plate-forme des moyens en personnels nécessaires à son action, notamment en analystes, ainsi que des moyens en logiciels utiles.

2.- L'autre contentieux de masse concerne **le détournement des moyens de paiement** que constituent **les captations des données de cartes bancaires et les fraudes associées**, qui sont commises, pour partie, via Internet, et à l'origine de partie des escroqueries précitées. S'étant substituées aux chèques sans provision, elles sont en constante augmentation depuis plusieurs années *(cf. le titre I, chapitre 1).*

Ainsi que le souligne l'O.C.L.C.T.I.C., le principal mode de captation est le *skimming (copie des données numériques de la carte bancaire)*, qui permet aux réseaux criminels organisés de monétiser ces données captées frauduleusement soit en les encodant sur des nouvelles cartes à partir desquelles sont réalisées des retraits dans les distributeurs de billets ou des achats chez les commerçants, soit par leur revente sur des forums internet dédiés et difficiles d'accès *(forums de carding)*, véritables commerces virtuels de coordonnées bancaires et personnelles.

Toutefois, les techniques de ces réseaux, qui intègrent désormais des techniciens de haut niveau exploitant les carences du système bancaire comme l'ensemble des possibilités d'Internet, évoluent très rapidement ; perfectionnant sans cesse les dispositifs de captation, ces réseaux sont aussi à l'origine de sociétés commerciales fictives dont l'objet consiste exclusivement en l'obtention d'un terminal de paiement électronique destiné à alimenter un compte bancaire par le passage en masse de cartes bancaires réencodées, les sommes ainsi acquises étant immédiatement blanchies par exemple par l'achat de véhicules ou des retraits en espèces servant à l'alimentation de cartes bancaires prépayées assurant l'anonymat.

En cette matière, le droit comme la politique pénale ont évolué.

Au plan juridique, la priorité s'est portée sur l'indemnisation du titulaire de la carte bancaire par le prestataire de services de paiement *(cf. art. L. 133-18 et L.133-19 du code monétaire et financier).*

Quant à la politique pénale, elle a évolué, puisque le ministère de la Justice, après avoir rappelé, dans un premier temps *(cf. circulaire du 17.02.2010, Direction des affaires criminelles et des grâces)*, que la couverture financière par les banques ne saurait se traduire par un refus d'enregistrer les plaintes de la part des services d'enquête, soulignait, dans un second temps *(cf. circulaire du 2.08.2011, id.)*, la nécessité, pour ces mêmes services, de différer l'enregistrement des plaintes.

Ce différé devait s'accompagner de la recommandation faite à la victime de solliciter son remboursement auprès de sa banque aux motifs que le régime d'indemnisation restait encore trop méconnu des utilisateurs de carte bancaire et qu'une plainte préalable ne conditionnait pas cette dernière.

D'autres motifs, tenant à la volonté du ministère de l'Intérieur de maîtriser les statistiques de la délinquance économique et financière, expliquaient aussi un tel revirement.

Toutefois, la même instruction suggérait que les banques, seules en mesure de fournir les éléments utiles aux investigations, déposent plainte aux lieu et place des titulaires.

Cette évolution a, certes, permis de libérer les services de police de plaintes extrêmement nombreuses qui, faute de possibilités de recoupements centralisés, parvenaient rarement à leur terme *(cf. titre I, chapitre 1 : seuls un peu moins de la moitié des victimes déposeraient plainte)*.

Mais elle a entraîné, dans le même temps, une méconnaissance par ces mêmes services tant des cartes bancaires piratées que de la réalité de cette criminalité, le plus souvent

organisée, qui a d'autant plus prospéré qu'elle n'était guère réprimée, les organismes bancaires ne s'étant pas substitués aux détenteurs pour déposer plainte à leur place.

En outre, il est à craindre que l'abandon total du recours à la plainte déresponsabilise une minorité des titulaires de cartes, voire incitent un petit nombre d'entre eux à effectuer des fausses déclarations à leurs banques.

Enfin, les véritables victimes que sont les commerçants ou prestataires de service, qui supportent in fine l'essentiel du préjudice, se sont retrouvées sans protection effective et conduites, à leur tour, à déposer plainte du chef d'escroquerie. C'est par ce biais que, tardivement, les services d'enquête connaissent d'une partie des captations réalisées, alors que la réactivité est une donnée essentielle en face d'équipes criminelles très mobiles au plan international ; ils sont ainsi contraints d'adresser des réquisitions à différents opérateurs techniques ou bancaires

Si certains ont préconisé d'abroger la circulaire de 2011 et d'en revenir, purement et simplement, au principe du dépôt de plaintes individuelles par les détenteurs préalablement à la demande d'indemnisation, le groupe interministériel a considéré qu'un tel mode ne serait pas opératoire et se heurterait aux mêmes difficultés que celles rencontrées en matière de cyber-escroqueries, d'autant plus que le détenteur ignore, le plus souvent, le moment et les circonstances dans lesquelles les éléments d'identification leur ont été soustraits, même s'il a tendance à en rendre responsables les paiements sur Internet.

Considérant, au contraire, que la circulaire en question n'était pas allée jusqu'au bout de sa logique, il recommande d'ériger en obligation le fait pour les organismes bancaires de dénoncer à la future plate-forme compétente pour les escroqueries les fraudes dont il a connaissance ainsi que les éléments dont il dispose en terme d'identification et de rapprochement. Il est à noter que c'est aussi l'intérêt du système bancaire d'accroître l'effectivité de la lutte contre ce type de délinquance, qui génère des incertitudes, parmi les consommateurs, sur la sécurisation du dispositif des cartes bancaires et les règlements associés.

Recommandation n° 51
relative à la centralisation du traitement des captations des cartes bancaires et des fraudes qui leur sont associées

Eu égard à la déperdition des informations actuelles par rapport à une délinquance, le plus souvent organisée et en forte progression, il est préconisé,

1.- de faire obligation au système bancaire de dénoncer les captations illicites et fraudes associées dont ils ont connaissance ainsi que les éléments utiles dont il dispose via ses processus et enquêtes internes tenant notamment à l'identité des titulaires des comptes destinataires de fonds, aux victimes directes ou indirectes, ainsi qu'au rapprochement des escroqueries commises selon le même mode opératoire.
2.- de solliciter le G.I.E. cartes bancaires et les autres opérateurs de moyens de paiement de produire les points de compromission dont il a connaissance *(commerces principalement visés par les transactions frauduleuses)*
3.- d'opérer de telles dénonciations en ligne et en direction d'un point d'entrée unique, qui pourrait être la plate-forme préconisée en matière de cyber-escroqueries, cela afin de favoriser une synergie entre deux natures d'infractions souvent associées.

Faut-il aller plus loin et généraliser une 1ère phase de centralisation pour l'ensemble des infractions relevant de la cybercriminalité ?

Cela ne paraît, en l'état, ni souhaitable, ni d'ailleurs réalisable.

En effet, d'une part, une telle centralisation n'apporterait rien s'agissant de certaines infractions, compte-tenu de leur nature, notamment lorsqu'elles s'inscrivent dans des conflits entre personnes identifiées ou identifiables ; d'autre part, et s'agissant des infractions les plus graves, les recommandations relatives à la spécialisation de certains tribunaux comme le fait que l'enquête soit, le plus souvent, confiée à des services d'enquête spécialisés facilitent, par nature, les recoupements ; enfin, pour les autres infractions, moins importantes quantitativement, d'autres procédés techniques devraient permettre de favoriser les rapprochements nécessaires.

En effet, *le futur fichier de traitement d'antécédents judiciaires (TAJ)*, dès lors que les traitements de rédaction des procédures de la Police et de la Gendarmerie, qui l'alimentent, prendraient effectivement en compte les données intéressant spécifiquement la cybercriminalité [189] *(cf. la recommandation)*, devrait être en mesure, à terme, d'effectuer des rapprochements automatisés de données, notamment quant au mode opératoire, favorisant ainsi les rapprochements nécessaires.

*****

[189] identités virtuelles ou pseudos utilisés par les mis en cause, sites ou forums utilisés, adresses électroniques, adresses de livraisons...

3.- Ces deux réformes organisationnelles devraient être combinées à une troisième**,** visant, spécifiquement, **les fraudes commises par le biais d'entreprises commerciales sur Internet**, par le biais du **renforcement de la police des noms de domaine**.

Si les adresses IP constituent les identifiants fondamentaux des ordinateurs proposant des services sur Internet, elles ne peuvent être aisément mémorisées. Le nom de domaine est un système permettant à l'internaute de retenir et de communiquer facilement ces adresses IP, puisqu'il suffit de taper ce nom, obtenu le plus souvent par le biais d'un moteur de recherche, pour que le navigateur interroge une base de référence et permette l'accès direct de l'utilisateur au site concerné.

L'attribution d'un nom de domaine revêt ainsi une importance toute particulière pour les sites commerciaux sur Internet, ce nom jouant à leur égard le rôle de véritables enseignes.

Le système d'adressage Internet (D.N.S.) est composé de deux types de domaines :

- les domaines nationaux, en *fr. (France)*, *re. (La Réunion)...*, dont les règles sont définies par la France *(2,6 millions de noms de domaine en fr., intitulés ordinairement "nomdesociété.fr")*
- les domaines génériques en *com., org.* et *net.*, dont les règles sont définies, au plan international, par l'ICANN.

Sur le plan français, l'encadrement juridique des noms de domaine résulte de la loi du 21.06.2004 modifiée par celle du 22.03.2011 *(cf. art. L.45 à L.45-7, art. R.20-44-38 à R.20-44-46 du code des postes et télécommunications électroniques)*. Toutefois, faute d'inscription dans un cadre européen, une remise à plat doit intervenir courant 2014.

L'Association française pour le nommage internet en coopération (A.F.N.I.C.), personne de droit privé chargée d'une mission de service public, assure l'attribution des noms des domaines nationaux via les 480 bureaux d'enregistrement qu'elle accrédite *(pour l'essentiel, des hébergeurs)* ; elle établit les règles de nommage qui doivent garantir, selon la convention qui la lie à l'Etat, la liberté de communication, celle d'entreprendre et les droits de propriété intellectuelle.

Même si pour certains noms de domaine, l'A.F.N.I.C. doit procéder à un examen préalable, le principe est que l'enregistrement s'effectue sous la seule responsabilité du demandeur et sous la forme d'une simple location pluri-annuelle. Par voie de conséquence, l'A.F.N.I.C. ne procède pas à un contrôle préalable et n'est pas en mesure de refuser un enregistrement.

Toutefois, l'A.F.N.I.C., outre la diffusion quotidienne des noms de domaine enregistrés, a pour mission de collecter auprès des bureaux d'enregistrement les données nécessaires à l'identification des personnes titulaires de noms de domaines, qui sont intégrées dans la base de données *Whois.*

Elle contribue aussi à la lutte contre la fraude de plusieurs manières :

*la communication aux organismes d'Etat qui en font la demande de la liste des noms de domaine en *fr.*, voire d'extractions réalisées à partir d'un certain nombre de mots clefs.

*la levée d'anonymat d'un titulaire de nom de domaine *(identité et coordonnées des personnes, historique des noms de domaine, portefeuille des noms de domaine du titulaire visé...)* au bénéfice des services de l'Etat disposant d'un droit de réquisition ou de communication *(autorité judiciaire, Police, Gendarmerie, Douanes, D.G.C.C.R.F., Finances Publiques, C.N.I.L.)*

* la procédure de vérification des coordonnées d'un titulaire de nom de domaine, l'A.F.N.I.C. étant habilitée à procéder à des vérifications d'éligibilité d'un titulaire, soit d'office *(chaque année, un contrôle de qualité est effectué sur un échantillon de 25.000 titulaires)*, soit suite à la demande motivée d'un tiers *(D.G.C.C.R.F. et Finances Publiques notamment)* ; un courrier recommandé est adressé à l'adresse déclarée et le titulaire doit fournir les éléments justificatifs dans un délai de 30 jours, à défaut de quoi le nom de domaine peut être supprimé si les règles d'éligibilité n'ont pas été respectées.

* le système de résolution des litiges (SYRELI), entré en vigueur en novembre 2011, permet à tout intéressé d'obtenir la suppression ou la transmission d'un nom de domaine dans un délai de 3 mois s'il justifie que ce nom est soit susceptible de porter atteinte à l'ordre public, aux bonnes moeurs, à des droits garantis par la Constitution, aux droits de propriété intellectuelle ou de la personnalité, soit semblable à celui d'un nom public.
Sur les 317 décisions rendues depuis un an et demi, 10% des requérants sont des personnes publiques, étant entendu que la prestation est gratuite pour certaines d'entre elles selon la Convention précitée *(D.G.C.C.R.F., Douanes, Finances publiques, O.C.L.C.T.I.C...)*.

Ce dispositif s'avère toutefois insuffisant, comme le montre le constat dressé notamment par CYBERDOUANE :

⌞ les noms de domaines en *fr.* constituent un label de qualité. Toute tromperie en la matière induit en erreur le consommateur quant à certaines qualités attendues du prestataire *(société française ou domiciliée en France...)*.

⌞ Or, partie des contrefacteurs parviennent à obtenir un tel nom de domaine, en arguant de fausse identité ou de l'identité d'un tiers *(fausse domiciliation, domiciliation fictive ou simple boîte aux lettres...)*, le règlement intérieur de l'AFNIC exigeant simplement de justifier d'une activité en France.

⌞ De telles pratiques sont aussi motivées par le souci de fraude fiscale.

⌞ Les conditions de suppression du nom de domaine sont lacunaires, dans la mesure où il ne peut intervenir que dans trois circonstances limitatives [190] qui sont appréciées par l'A.F.N.I.C., sauf à agir en justice devant le juge des référés sur le fondement de l'art. 6-1-8 de la loi du 21.06.2004, selon une procédure souvent peu compatible avec la célérité que requiert la réaction sociale.

⌞ Une fois qu'un nom de domaine est interdit à une entreprise, ce nom est remis sur le marché aux risques de voir les mêmes individus le redéposer à nouveau quelques instants après le prononcé de l'interdiction ; en outre, rien n'interdit à une personne convaincue de fraude ou de contrefaçon d'obtenir un nouveau nom de domaine.

[190] cf. art. L.45-2 du C.P.E. : l'atteinte à l'ordre public ou aux bonnes moeurs ou à des droits garantis par la Constitution ou par la loi, mais l'A.F.N.I.C. a tendance à interpréter restrictivement certains de ces concepts ; l'atteinte illégitime et de mauvaise foi à un droit de propriété intellectuelle ou de la personnalité ; l'utilisation illégitime et de mauvaise foi d'un nom apparenté à un service public ou à une entité publique.

L'Europe a bien compris l'enjeu que représentait la police des noms de domaine *(un projet de recommandation est en cours d'examen)*.

Quant aux U.S.A., ils autorisent, depuis 2010, la saisie des noms de domaines par l'Etat dans le cadre de la protection de la propriété intellectuelle sur Internet ou en cas de fraude douanière. Cette saisie s'accompagne d'un renvoi vers une page d'information officielle. C'est ainsi qu'en 2012, une vaste opération a été menée dans le domaine des contrefaçons, en association avec EUROPOL Les juridictions américaines ont jugé récemment que de telles saisies étaient compatibles avec la liberté d'expression.

En liaison étroite avec l'A.F.N.I.C. qui a émis certaines suggestions en ce sens, le groupe interministériel s'est attaché à définir les conditions dans lesquelles cette police des noms de domaine devrait être sensiblement renforcée, y compris en cours de procédure pénale, afin de prévenir et de mettre un terme aux activités pénalement sanctionnées, telles que les contrefaçons ou les escroqueries.

Recommandation n° 52
relative au renforcement de
la police des noms de domaine

Dans le souci de rendre le nom de domaine en fr et assimilés plus sûr et donc plus attractif, il est préconisé de

1.- Renforcer le contrôle a priori dans le processus d'attribution, en ce qui concerne l'identité et la domiciliation, et prévoir une obligation de mise à jour de cette dernière.

2.- Faciliter aux services de l'Etat concernés la surveillance des enregistrements grâce à la production gratuite de la liste des noms de domaine correspondant à certains mots clés.

3.- Faciliter aux services de l'Etat concernés la levée de l'anonymat.

4.- Permettre à l'ensemble des services de l'Etat concernés de solliciter gratuitement de l'A.F.N.I.C., la suppression du nom de domaine en cas de fausse déclaration relative à l'identité ou à la domiciliation, ou, dans le cadre du dispositif SYRELLI, en cas de violation de la loi par le titulaire du nom ou autres motifs déjà visés par la législation actuelle.

5.- Reconnaître aux services de l'Etat concernés, en cas de suppression pour l'un des motifs visés en 4, d'exiger le transfert de titularité du nom de domaine à l'Etat, afin d'éviter tout nouveau dépôt ; cela suppose la création d'un bureau d'enregistrement propre à l'Etat.

6.- Prévoir la possibilité pour les services d'enquête, avec l'accord du procureur de la République et l'autorisation préalable du juge des libertés, ou celle du juge d'instruction, de saisir en cours d'enquête et en cas d'urgence tout nom de domaine en cas d'activité contraire à la loi, et cela dès l'interpellation de son titulaire et la saisie du serveur.

7.- Reconnaître la faculté au juge d'instruction ou au tribunal saisi au fond de confisquer le nom de domaine saisi, emportant transfert à l'Etat

8.- Au titre des peines complémentaires obligatoires et sauf décision contraire du tribunal, interdire à la personne reconnue coupable d'une infraction commise au moyen d'un site ainsi dénommé de pouvoir solliciter tout autre nom de domaine de 1ère catégorie pendant une certaine durée.

9.- Dans tous les cas de suppression et de saisie d'un nom de domaine, prévoir l'inscription d'un message d'information sur le site concerné pour l'information du public

III.5.- de la coopération pénale internationale

Bien plus que les autres formes de délinquance, c'est l'extranéité qui caractérise la cybercriminalité, d'abord parce que l'essentiel des prestataires techniques détenteurs des informations nécessaires à l'enquête sont eux-mêmes étrangers et avec eux les principales bases de données, ensuite du fait que les auteurs, du moins ceux relevant de bandes organisées, agissent, pour partie, depuis l'étranger, et que les fonds détournés sont, pour l'essentiel, aussi destinés à l'étranger.

En outre et compte-tenu de la volatilité de certaines informations *(cf. l'exemple de l'adresse IP)* comme des éléments de preuve, la célérité de l'action s'avère essentielle, ce qui n'est pas toujours compatible avec le formalisme juridique.

Ces spécificités sont, pour partie, à l'origine de l'efficacité réduite de l'action répressive.

Certes, la Convention du Conseil de l'Europe sur la cybercriminalité adoptée, à BUDAPEST, le 23.11.2001, a permis une avancée essentielle, notamment *(cf. son art. 29)* en organisant, en préalable d'une demande d'entraide judiciaire, le gel provisoire des données informatiques stockées dans les Etats-parties qui est opéré en urgence comme reposant sur des points de contact nationaux, disponibles 24 heures sur 24, le plus souvent policiers *(O.C.L.C.T.I.C. en ce qui concerne la France)* [191].Le protocole additionnel adopté le 7.11.2002 a étendu ce dispositif en matière de racisme et de xénophobie sur Internet [192]. Il en a été de même de la Directive adoptée par l'Union européenne en juillet 2013 s'agissant des attaques contre les systèmes d'information, non encore en vigueur.

Encore faut-il que l'entraide judiciaire internationale puisse suivre pour que les données ainsi gelées puissent être récupérées et exploitées.

Or cette entraide rencontre des difficultés jusqu'ici non surmontées.

Elles tiennent, d'une part, à la lourdeur du processus, qui fait en sorte qu'il n'y est pas fait recours pour les infractions de masse à faible préjudice, chaque parquet définissant des seuils en fonction de son plan de charge et de ses priorités. Les recommandations qui précèdent sur ces types de contentieux sont de nature, en substituant à l'approche individuelle de chaque plainte un recoupement effectué au plan central, à lever cet obstacle en mettant en évidence le caractère organisé des escroqueries.

Même lorsqu'il est décidé d'y recourir, la simple préparation de la demande d'entraide puis, le plus souvent, sa traduction, génèrent des délais parfois incompatibles avec le maintien à disposition des données gelées. Ces contraintes de formalisation se doublent de difficultés organisationnelles car, à l'exception des grands parquets, le ministère public peine à spécialiser des magistrats à cet égard ; sans doute, le rôle de soutien des parquets généraux est-il appelé à s'étendre sur ce point..

---

[191] Entrée en vigueur le 1er juillet 2004, cette Convention a été signée et ratifiée par 39 Etats, dont certains non européens, tels les U.S.A. ; pour les Etats non parties, l'entraide est régie par des conventions bilatérales ou multilatérales qui ne comportent aucune disposition spécifique à la lutte contre la cybercriminalité.

[192] Toutefois, l'ensemble des Etats parties à la Convention n'ont pas signé ce protocole, notamment les U.S.A.

Une autre contrainte tient à l'hétérogénéité des conditions fixées à l'entraide, en fonction des traités applicables, qui, malgré l'incitation de la Convention précitée, ne prennent guère en compte les contraintes de la lutte contre la cybercriminalité, sauf pour certains types d'infractions qui font, en général, l'unanimité *(tels la pédo-pornographie, le terrorisme ou la protection des droits d'auteur).* Les contraintes sont d'autant plus fortes lorsque la demande concerne un Etat étranger extérieur à l'Union européenne. Or, ce sont précisément de tels Etats qui, soit sont supposés détenir sur leur territoire, par le biais des prestataires techniques, les informations nécessaires à l'action judiciaire, soit sont utilisés par la criminalité organisée comme point de départ de l'attaque.

Si l'on ne dispose pas de données quantitatives quant aux demandes d'entraide transmises directement par la voie judiciaire locale, les 136 dossiers qu'a eu à traiter depuis 2009, hors Europe et concernant les seules infractions qualifiées par la loi de cybercriminalité, *le Bureau de l'entraide pénale internationale (B.E.P.I., Direction des affaires criminelles et des grâces, ministère de la Justice)* concernent principalement les U.S.A., siège des principaux gestionnaires de données ; or, les autorités américaines ont tendance à considérer que le traité bilatéral qui lie cet Etat et la France n'est ni coercitif, ni exclusif. Au surplus, s'agissant des données de contenu, et tout spécialement concernant la liberté d'expression protégée par le 1er amendement de la Constitution américaine, le système juridique américain s'avère très restrictif et très formaliste lorsqu'il s'agit d'analyser les demandes dont il est saisi, alors qu'il est lui-même très demandeur des données étrangères [193]...

Cette hétérogénéité se retrouve aussi dans la durée légale de conservation, extraordinairement variable selon les Etats, même si, là encore, l'Europe a fait oeuvre utile en fixant par directive une durée minimale ; mais nombreux sont encore , y compris en Europe, les systèmes juridiques qui se sont refusés, jusqu'ici, à fixer des durées de conservation quelles qu'elles soient.

En outre, et par nature, le cybercriminel est essentiellement mobile, mettant en échec le concept territorial, en évoluant, en un espace de temps, d'un état à l'autre, en fonction des opportunités comme des couvertures juridiques. Nombreux d'ailleurs sont les cas où les services d'enquête ne savent pas précisément où se trouvent les données utiles.

Un dernier obstacle tient à l'incapacité de bon nombre des états requis à faire face, en urgence, aux demandes d'entraide pénale qui leur sont adressées, compte-tenu de l'inflation générale qu'une telle entraide connaît.

Il y a consensus en France comme dans bon nombre d'autres états pour considérer que, si l'on ne remédie pas à de telles difficultés, la lutte contre la cybercriminalité continuera à générer une débauche d'énergie pour des résultats limités. Faut-il encore pouvoir traduire un tel consensus dans les faits. Si les solutions sont généralement à rechercher dans l'évolution des instruments internationaux, quelques pistes peuvent être préconisées à cet égard.

☞La première consiste à **différencier les modes de traitement selon qu'ils portent sur des données d'identité et de trafic ou sur des données de contenu** *(pour mémoire, cf. la recommandation n° 44).*

[193] cf., sur ce point, le guide en ligne sur l'entraide avec les U.S.A. mis en ligne sur le site du B.E.P.I.

☞ au plan européen, l'obligation, faite aux prestataires techniques, de **stockage des données** durant une certaine durée est, eu égard au temps policier et judiciaire, une condition sine qua non de l'efficacité de l'action, tant d'ailleurs au plan civil que pénal. A cet égard, les réticences, voire les souhaits de remise en cause exprimés par certains Etats-membres sont des plus préoccupants. Il importe, non seulement de maintenir les instruments existants, mais aussi de les étendre au plan international.

☞ au plan européen encore, il est préconisé de s'inspirer des exemples existants en instituant **un dispositif *"Schengen"* de coopération simplifiée** en matière de cybercriminalité, s'agissant, notamment, de la saisie des données de contenu mais aussi des moyens de mettre fin à des contenus ou comportements illégaux, pour une liste d'infractions graves précisément énumérées.

Si un tel processus a pu être mis en oeuvre, et de manière satisfaisante, s'agissant de l'arrestation des personnes, s'il a pu être étendu à une partie de l'exécution des peines notamment s'agissant du recouvrement des amendes, a fortiori on doit pouvoir aisément s'en inspirer pour saisir des éléments de preuve, mettre un terme à des infractions et contribuer à la mise à exécution des condamnations prononcées en matière de cybercriminalité en ce qu'elles ont de spécifique.

Il est aujourd'hui peu compréhensible que *la décision-cadre 2008/798/JAI du Conseil du 18 décembre 2008 relative au mandat européen d'obtention de preuves visant à recueillir des objets, des documents et des données en vue de leur utilisation dans le cadre de procédure pénale* exclut délibérément, par exemple, les données de communication conservées par les fournisseurs de service *(cf. art.4 §3e).* Il faut espérer que la future directive relative à la décision d'enquête européenne qui va la remplacer lèvera ce genre d'exceptions.

☞ hors Europe, outre les actions classiques de coopération policière et judiciaire notamment à l'égard de certains pays africains, il est aujourd'hui temps d'avoir une action résolue s'agissant des Etats constitutifs de **véritables cyber-paradis** qui refusent toute coopération et qui n'adhéreront jamais à la convention sur la cybercriminalité car leurs intérêts sont ailleurs ; ces Etats sont aujourd'hui bien connus, ne serait-ce que par le résultat des enquêtes qui ont mis à jour de véritables filières ayant des origines territoriales communes.

Cet objectif participe entièrement de la lutte contre la criminalité organisée, dont Internet sert de plus en plus de vecteur, et revêt autant d'importance que la lutte contre les paradis fiscaux et le blanchiment de l'argent du crime mise en oeuvre par *l'Organisation de coopération et de développement économique (O.C.D.E.).* Les Etats-parties à la convention sur la cybercriminalité devraient prendre des initiatives à cet égard afin que l'ensemble de la communauté internationale se dote de normes minimales communes.

Recommandation n° 53
sur l'entraide pénale internationale

1- Limiter le recours à l'entraide pénale internationale aux données qui le méritent. Cette voie n'est ni adaptée, ni appropriée pour l'obtention des données relatives à l'identité et au trafic, qui, compte-tenu de leur nombre mais aussi de leur moindre gravité au regard des libertés individuelles, doivent pouvoir être directement obtenues des prestataires techniques qui en disposent, sur le fondement du droit national préconisé à cet effet.

2- Maintenir l'obligation, pour les prestataires techniques, de stockage des informations dont ils disposent, et étendre sur le plan international cette obligation, pour les besoins de la coopération policière comme l'entraide pénale internationale suppose de maintenir

3- Définir un dispositif *"Schengen"* de coopération simplifiée en matière de cybercriminalité, pour l'obtention des données de contenu comme pour la mise à exécution des décisions propres à mettre un terme à des activités ou contenus illégaux via Internet.

4- Conduire, au plan international, une action résolue contre les cyber-paradis, par le biais de l'adoption de normes minimales, voire d'un processus de sanction.

III.6.- de la réponse aux victimes d'infractions

Sur un plan général, la politique française d'aide aux victimes, impulsée par le ministère de la Justice, est l'une des plus avancées au plan international ; elle a d'ailleurs inspiré, pour partie, la récente *Directive 2012/29 de l'Union européenne concernant les droits, le soutien et la protection des victimes*. Ceci étant, elle n'a pas encore été adaptée aux cyber-victimes. Il est venu le temps de combler cette lacune.

Nombre de recommandations déjà formulées dans ce rapport concernent directement les victimes ; il est apparu néanmoins utile de les mettre en perspective, tout en formulant de nouvelles préconisations.

Toute politique en matière de victimes est fondée sur **une appréhension des attentes** qui, en l'état, n'est guère satisfaite [194] alors mêmes que ces dernières, s'agissant de la cybercriminalité, sont souvent spécifiques. Deux conséquences doivent en être tirées : une association plus systématique, dans les organismes institutionnels, tant du réseau INAVEM que des associations de consommateurs et des représentants des entreprises ; une mobilisation, à l'initiative notamment de la Chancellerie et de ses organismes ad hoc, des organismes de recherche, en particulier universitaires [195].

La **prévention**, générale ou ciblée, constitue, on l'a vu, un élément essentiel pour éviter des passages à l'acte qui transforment l'internaute en victime. La sensibilisation des victimes potentielles sur le type d'actions malveillantes dont elles peuvent être la cible et la façon de s'en prémunir ou d'en diminuer l'impact, constitue ainsi la seconde des priorités, au même titre que la facilitation des signalements en ligne.

Toutefois, en terme de victimes, la sensibilisation n'épuise pas les exigences de la prévention. Trop souvent, les atteintes à la vie privée sont la conséquence des données introduites sur Internet, en particulier sur les réseaux sociaux, par l'internaute lui-même, alors qu'il n'a aucunement conscience que ces données, parfois très intimes, sont condamnées à demeurer en ligne sa vie entière et même au-delà et risquent de l'exposer à une exploitation nuisible. C'est la question du **droit à l'oubli** qui se pose.

La Commission européenne a présenté sur ce point un projet très ambitieux puisque le droit à l'oubli concernait toute information contenue dans un traitement concernant une personne identifiée ou identifiable *(cf. La communication de la Commission sur la protection de la vie privée dans un monde en réseau : un cadre européen relatif à la protection des données, adapté aux défis du 21˚s.).* Eu égard au caractère général de ce projet et à la mobilisation considérable des lobbies, notamment de la part de certains prestataires techniques d'Internet, il a suscité une opposition considérable et n'a pas été adopté.

---

[194] Sauf, sans doute, en terme de cyber-harcèlement en milieu scolaire, compte-tenu des enquêtes menées par l'Education nationale.

[195] Seule, en l'état, l'université de STRASBOURG *(Groupe de recherches-actions sur la criminalité organisée - GRASCO)* paraît disposer d'un département-recherche consacré aux cyber-victimes

La préconisation du groupe interministériel sur ce point est plus modérée et sans doute plus réaliste, puisqu'elle consiste à **limiter le droit à l'oubli aux informations recelées par Internet durant la minorité d'un individu**, en reconnaissant à ce dernier ou à ses représentants légaux, durant cette même minorité ou une fois devenu majeur pendant un délai à déterminer, le droit d'obtenir du juge des enfants l'effacement des données le concernant, sans qu'il soit fait de distinction, car la preuve est impossible à rapporter, entre celles qu'il a lui-même introduites et celles générées par autrui. Une telle requête pourrait d'ailleurs être déposée, soit à titre préventif, soit en réaction à une utilisation malveillante des données en question.

La protection particulière que requiert un mineur et sur laquelle tout le monde s'accorde, comme les drames générés par certaines atteintes, notamment du droit à l'image, devrait favoriser un consensus sur ce point.

Une fois l'infraction commise, c'est **l'information** qui s'impose, sur la façon d'y répondre et les différentes solutions ou démarches qui s'offrent à la victime, en terme de prise de contact avec des structures associatives ou professionnelles susceptibles de lui venir en aide, de consultation d'un avocat en particulier pour certaines atteintes à la vie privée, d'action au civil ou de dépôt de plainte.

A cet effet, **un guide des droits des victimes de la cybercriminalité** devrait être préparé par la Chancellerie, en liaison avec les autres départements ministériels, les associations des victimes et les entreprises. Il devra prendre en compte les principales infractions intéressant les victimes ainsi que les différents types de victimes, dans la mesure où ceux-ci appelleraient des informations particulières. Une telle action d'information doit, au surplus, être relayée par les structures d'accès au droit, car c'est bien d'un droit nouveau qu'il s'agit en réalité.

L'une des premières démarches qui s'offre à la victime, notamment en cas d'injure ou de diffamation, consiste, à défaut de connaissance de l'auteur ou de l'éditeur, **à dénoncer l'infraction à l'hébergeur, voire au fournisseur d'accès**, pour qu'il la retire si elle s'avère manifestement illicite.

Force est de constater que l'appréciation faite d'un tel caractère est, le plus souvent, restrictive, ne serait-ce que pour des raisons de responsabilité, ce qui oblige la victime à saisir le juge civil, voire à déposer plainte, pour faire reconnaître son droit.

Sur ce point, les préconisations du groupe interministériel sont de deux sortes: l'une consiste à faire obligation au prestataire concerné, outre de faciliter la transmission en ligne de telles demandes, de répondre de manière succinctement motivée à l'intéressé en cas de rejet ; l'autre, plus ambitieuse, consiste à créer **une autorité de médiation**, s'inscrivant dans la délégation interministérielle qu'il est projeté de créer ; cette autorité pourrait être saisie en ligne du rejet, examiner le caractère manifestement illicite et ordonner au prestataire les mesures propres à faire cesser le dommage ou rejeter, une nouvelle fois, la demande [196].

[196] A noter que dès 1996 *la Commission nationale consultative des droits de l'homme* proposait la création d'un observatoire avec, notamment, un rôle de médiation entre les professionnels d'Internet et les utilisateurs

L'action de cette autorité viendrait compléter les mécanismes déjà mis en oeuvre dans le cadre du droit de la consommation pour le commerce en ligne ou par certaines autorités administratives indépendantes *(cf. le rôle assigné au Défenseur des droits en matière de discriminations)*. Il est, en effet, de l'intérêt de chacun d'instituer un tel mode alternatif de règlement des litiges, simple et gratuit, en amont de l'intervention judiciaire, afin de rendre plus effectifs les droits des personnes lésées, étant entendu que les dispositions de l'art. 6-I.2 et 3 de la loi du 21.06.2004 ne font pas actuellement l'objet d'un contrôle, sauf l'hypothèse - relativement rare - d'une action civile fondée sur les dispositions de l'art. 6-I.8 de la même loi, et d'éviter, dans le même temps, la surcharge des juridictions civiles.

Vient ensuite souvent le temps de **la plainte**.

On l'a vu aussi, certaines infractions liées aux technologies numériques induisent un nombre de victimes très important envers lesquelles le traitement pénal classique n'est pas adapté : le processus de dépôt de plainte est perçu, à la fois par les victimes et les services chargés de les accueillir, particulièrement lourd pour un résultat peu tangible du point de vue de chaque cas individuel.

La 1ère réponse consiste ainsi à favoriser **le dépôt de plainte en ligne** ; déjà préconisée pour les cyber-escroqueries, **la plainte en ligne mériterait d'être élargie à l'ensemble des infractions réalisées via Internet**.

Certes, il existe déjà la possibilité d'effectuer une pré-plainte en ligne, mais elle n'est guère aujourd'hui utilisée, sans doute car elle n'entraîne pas les effets juridiques d'une plainte en bonne et due forme et ne fait pas l'économie d'une convocation et donc d'un déplacement devant le service de police ou l'unité de gendarmerie compétent.

Rapide et simple, susceptible d'être réalisée dès après la constatation de l'infraction, économique pour les services d'investigation voire pour les parquets, la plainte en ligne présente aussi l'avantage d'être orientée, selon les nécessités, soit vers une plate-forme centralisée de traitement *(cf. les escroqueries)*, soit vers le service ou l'unité compétentes.

Son efficacité, déjà testée *par la Commission nationale de l'informatique et des libertés* pour ses besoins propres, dépend toutefois de son exhaustivité - d'où le recours à des modèles d'imprimés CERFA selon la nature de la plainte-, ainsi que d'une organisation stricte des services, en terme d'enregistrement comme de traitement.

Si elle doit être encouragée et, dans toute la mesure possible, systématisée pour les atteintes aux biens, la plainte en ligne n'est toutefois pas adaptée aux atteintes aux personnes ou aux infractions qui, de par le préjudice subi, demandent une réaction immédiate; au surplus, il faut aussi tenir compte des victimes qui, pour des raisons culturelles, linguistiques ou tout simplement en raison d'un manque de familiarité avec Internet, ne pourront pas ou ne souhaiteront pas y avoir recours.

C'est là qu'une 2ème réponse en terme de **sensibilisation spécifique des agents préposés au recueil des plaintes** revêt toute son importance, tant pour s'assurer du caractère exhaustif des éléments recueillis - car il manque souvent des précisions essentielles aux plaintes actuelles - que pour améliorer l'accueil des plaignants en cas de violation grave de la vie privée, de harcèlement, ou tout simplement pour les aider à surmonter le sentiment de culpabilité que peut engendrer une trop grande crédulité.

Encore faut-il pouvoir déposer plainte au regard de **la trop courte prescription de la loi sur la presse** qui ne prend pas encore suffisamment en compte le fait que, trop souvent, la victime ne prend connaissance des infractions commises sur Internet qu'une fois passé le délai fatidique des trois mois.

Pour **les entreprises**, qui sont souvent l'objet d'atteintes graves et aux enjeux importants, la possibilité de déposer plainte ne suffit pas ; il faut encore savoir auprès de qui et sous quelles formes, tout en étant assuré d'une certaine confidentialité, car c'est souvent la crainte de voir l'affaire évoquée dans la presse dès le lendemain de ce dépôt qui justifie les fortes réticences d'une partie des chefs d'entreprise.

Or, police et justice sont souvent perçues comme connaissant mal le monde de l'entreprise, mais l'inverse est aussi vrai. A cet égard, il est préconisé de créer, sur l'ensemble du territoire, un réseau de référents pour les entreprises, grandes ou petites, victimes de cybercriminalité, pris parmi les policiers ou gendarmes spécialisés de niveau 3 ; cette démarche mériterait d'être coordonnée avec *la Direction centrale du renseignement intérieur* et la création préconisée d'un CERT dans la mesure où les attentes des entreprises concernent aussi le volet technique de l'atteinte.

Une telle liste de référents pourrait être utilement diffusée avec le concours des chambres de commerce et des organisations patronales, en lien avec les pôles de compétitivité qui procèdent déjà à de l'information sur la protection de l'intelligence économique.

Reste une attente commune à l'ensemble des catégories de victimes, mais qui n'est pas spécifique à la cybercriminalité : **leur information sur les suites données à leur plainte**, y compris les plaintes en ligne préconisées, doit être améliorée.

Si cette information peut être de deux types - globale sur l'action des services et les réponses judiciaires apportées à la cybercriminalité, et individuelle par rapport à chaque victime -, c'est cette dernière qui est la plus attendue. Le groupe interministériel est conscient des obstacles tenant à la masse des infractions dont sont saisis les services répressifs ainsi que de la durée des enquêtes et des procédures pénales : la réponse ne relève pas de la norme.

Si la possibilité de se constituer partie civile en cas d'ouverture d'information, si l'avis à victime systématiquement décerné en cas de poursuites répondent à une telle exigence, c'est l'absence de toute information pendant l'enquête ou en cas de dessaisissement d'un parquet ou encore le caractère stéréotypé des avis de classement qui posent problème.

Deux solutions sont préconisées à cet égard : s'agissant des plaintes émanant du monde de l'entreprise, confier au référent policier ou gendarme, avec l'aval du ministère public, de tenir informé le plaignant ; en ce qui concerne les victimes individuelles, il revient aux associations d'aide aux victimes habilitées par la Justice de jouer ce rôle d'information, notamment dans le cadre des bureaux d'aide aux victimes.

Il sera toutefois nécessaire, dans l'avenir, mais l'observation vaut pour l'ensemble des victimes, d'être plus ambitieux et de doter les parquets de ressources humaines de greffe leur permettant de constituer de véritables services de traitement des requêtes, ou, encore mieux, de permettre à chaque victime et, au-delà, aux justiciables civils de **pouvoir consulter directement en ligne l'état d'avancement de leurs affaires**.

De manière générale, les plaignants individuels doivent être accompagnés par **les associations d'aide aux victimes** précitées lorsqu'elles en font la demande dès après l'information qui leur est obligatoirement dispensée lors de leur dépôt de plainte - et il faudra prévoir un mécanisme comparable pour les plaintes en ligne inséré dans l'avis de réception automatisé -.

Un tel dispositif s'avère toutefois insuffisant lorsqu'il s'agit d'une victime gravement traumatisée soit en raison de la nature de la cyber-infraction *(atteintes au respect de la vie privée, atteintes visant des mineurs, préjudice grave...)*, soit eu égard à la vulnérabilité même de la personne : en pareille hypothèse, et à l'exemple des politiques mises en oeuvre dans certains ressorts, le groupe interministériel préconise que, avec le soutien de l'INAVEM, le parquet, sous la forme d'instructions générales ou sur mandat individuel dans le cadre du traitement en temps réel, oriente ce type de victimes vers les associations en question, afin qu'elles leur apportent l'aide et l'assistance, voire le soutien psychologique nécessaires.

Le renforcement de l'effectivité de la Justice, tant pénale que civile, grâce à l'accroissement, déjà évoqué, des moyens d'investigation, répond aussi à l'attente des victimes.

Toutefois, ce qui importe pour les victimes, tout particulièrement en cas de blocage de leur ordinateur ou d'atteintes à la vie privée, c'est **la cessation de l'infraction** dans les meilleurs délais, c'est-à-dire sans attendre le terme d'une enquête ou d'une procédure.

Telle est la raison pour laquelle le groupe interministériel propose, outre les attributions conférées au médiateur, d'accroître les pouvoirs du juge des référés ainsi que du juge d'instruction ou du juge des libertés et de la détention en cours d'enquête, à l'égard des prestataires techniques d'Internet.

***L'effet miroir* d'Internet**, résultant de la reprise massive en ligne et en temps quasi réel d'une atteinte à la vie privée, à la réputation ou au droit à l'image, pose toutefois un problème particulier puisque, par exemple, le déférencement ordonné au gestionnaire d'un moteur de recherche ne saurait concerner qu'un site précis et non un propos tenu sur un blog, sauf à pouvoir bloquer les interrogations faites à partir d'une identité particulière, si tel est le cas *(cf. les précédents s'agissant des contrefaçons ou des jeux illicites).*

Telle est la raison pour laquelle il est préconisé, d'accompagner l'injonction de retrait, de déférencement ou de blocage d'une obligation, à mettre en oeuvre par le prestataire sous le contrôle de l'agence de régulation déjà citée, une surveillance spécifique pendant une certaine durée.

La **réparation du préjudice subi par la victime** constitue un autre enjeu. En effet, les victimes de la cybercriminalité sont très souvent démunies : pertes financières directes liées à certaines escroqueries en ligne et non garanties par une assurance ou l'obligation de remboursement des intermédiaires de paiement (en cas de mandat-cash par exemple), dommages causés à leur système informatique *(qu'il s'agisse d'un ordinateur personnel ou d'outils de travail)*, impact psychologique ou sur l'image de la personne...

Or, faute d'identification ou d'appréhension du délinquant, plus que toute autre catégorie de victimes, elles ne peuvent obtenir, le plus souvent, des dommages et intérêts.

En premier lieu, qu'il s'agisse d'un particulier ou d'une entreprise ou toute autre organisation, il est important, pour la prise en compte à sa juste mesure de l'importance de chaque cas individuel, que les victimes soient en mesure d'évaluer et de justifier correctement leur préjudice. Cela relève des mesures de prévention et d'information du public comme de la formation et de l'accompagnement des personnes chargées de prendre ou de traiter les plaintes, ou d'aider les victimes.

En second lieu, s'il importe de vérifier la réalité de la couverture du dommage au titre des assurances, l'indemnisation de solidarité doit pouvoir prendre le relais lorsque, comme c'est le cas en matière de cybercriminalité, l'action de l'Etat dans son rôle répressif ne s'avère pas suffisamment effectif : si les fraudes à la carte bancaire bénéficient d'un dispositif spécifique, les escroqueries sont aussi indemnisables sous certaines conditions, il est vrai restrictives.

Toutefois, le groupe de travail a estimé qu'une éventuelle modification des dispositions de l'art. 706-14 du C.P.P. ne pouvait être examinée sous le seul angle des cyber-infractions, même si une évolution de la jurisprudence quant à l'appréciation de la faute de la victime lui semble opportune. Reste la question d'une possible indemnisation par le commerce en ligne, lorsque son imprudence est à l'origine du dommage, qui mérite d'être attentivement examinée.

En dernier lieu, **la pénologie** pourrait être utilement adaptée afin de mieux prendre en compte les attentes des victimes. A ce titre, plusieurs préconisations peuvent être faites :

- la faculté d'ordonner la diffusion de la condamnation ou d'extraits sur Internet n'est, en l'état, ni juridiquement possible dans toutes les affaires relevant de la cybercriminalité, ni, en pratique, souvent mise en oeuvre.
  A l'instar du droit du travail, qui privilégie la publicité et l'affichage, la diffusion des condamnations sur Internet, notamment en ce qui concerne les infractions à la liberté de la presse mais aussi les autres atteintes à la personne et les escroqueries, devrait être, tout à la fois, facilitée et rendu plus systématique.

- par-delà, il est proposé la création d'une nouvelle peine complémentaire consistant en la réparation des dommages spécifiques causés à la victime, sous la forme, par exemple, tant de la réparation du système informatique endommagé par un prestataire habilité que du *"nettoyage du net"* s'agissant des atteintes à la réputation ou à l'image d'une personne dont la mise en oeuvre pourrait être confiée à l'autorité de médiation déjà citée, et cela aux frais du condamné ou, à défaut, du Fonds de garantie des victimes d'infractions, qui dispose d'une action récursoire.

- enfin, au titre de la prévention de la réitération et hors le champ de la délinquance organisée, il est recommandé de recourir soit à un stage d'éducation civique adapté à cette problématique, soit au module de sensibilisation précitée, soit à des travaux d'intérêt général spécifiques au sein de structures adaptées, voire de pouvoir soumettre les personnes condamnées à des restrictions temporaires de l'accès ou de l'usage d'Internet *(sur le modèle des chèques de banque pour les infractions relevant du droit des moyens de paiement)*, accompagnées d'un dispositif de contrôle logiciel, voire d'un contrôle sur place par des professionnels. Et cela sans préjudice de la peine complémentaire d'interdiction d'un tel accès pendant une certaine durée dont la création est proposée pour les atteintes aux mineurs.

Recommandation n° 54
relative aux réponses aux victimes d'infractions

Une politique d'aide aux cyber-victimes volontariste et adaptée suppose de

1- mieux appréhender les attentes des victimes

2- créer un guide des droits des victimes de la cybercriminalité

3- instituer, sous l'égide du juge des enfants, un droit à l'oubli s'agissant des données relatives aux mineurs

4- faciliter les demandes de retrait adressées par les victimes aux prestataires techniques d'Internet en instituant, au sein de la future délégation interministérielle, une autorité de médiation

5- généraliser la possibilité de déposer plainte en ligne ; améliorer concomitamment le recueil des plaintes par les policiers et les gendarmes

6- diffuser aux entreprises une liste d'enquêteurs-référents

7- mieux informer les victimes des suites données à leurs plaintes, par un dispositif sécurisé accessible en ligne

8- mobiliser les associations d'aide aux victimes et les associations de consommateurs

9- accroître les pouvoirs du juge des référés pour faire cesser l'infraction ; confier des pouvoirs similaires au juge des libertés et de la détention

10- confier au juge civil comme pénal la possibilité d'associer à l'injonction de retrait, de défèrencement ou de blocage, d'une obligation de surveillance spécifique limitée dans le temps pour limiter *l'effet-miroir*

11- adapter la pénologie en prenant mieux en considération les besoins des victimes

12- améliorer la réparation du préjudice, y compris en mobilisant les professionnels.

III.7.- de la politique pénale

Il revient au Garde des Sceaux, ministre de la Justice, de conduire la politique pénale déterminée par le Gouvernement.

Cette politique pénale, qui donne de l'intelligence à l'action de la police judiciaire et du ministère public, est un élément central de la stratégie préconisée pour lutter contre la cybercriminalité.

Elle doit, tout à la fois, définir les priorités, préciser les schémas de compétence, adapter les modes de traitement à la spécificité des différents contentieux, mobiliser les moyens procéduraux les plus pertinents, mettre en exergue les réponses pénales les plus appropriées, définir les conditions d'une meilleure effectivité des décisions, traiter de la coopération pénale internationale, spécifier la politique d'aide aux victimes sans négliger les questions propres aux entreprises, mobiliser les partenaires indispensables, et évaluer les résultats.

Elle repose nécessairement sur une bonne connaissance des attentes comme des forces et faiblesses de l'existant ; elle suppose aussi, par nature, une large concertation, non seulement avec le ministère de l'Intérieur, mais avec nombre d'autres acteurs, publics comme privés ; elle requiert encore de prendre en compte des autres types de règlement des conflits, qu'ils relèvent des alternatives, des réponses administratives, des procédures civiles sur la protection de la vie privée, ne serait-ce que pour définir la juste place du pénal ; elle doit nécessairement enfin tenir compte des capacités des services de police judiciaire comme des parquets, du siège comme du greffe, ainsi que des pouvoirs propres des procureurs de la République et du rôle d'impulsion et de coordination imparti aux procureurs généraux.

Les développements précédents permettent de faire l'économie d'entrer plus avant dans le détail.

Certains points méritent toutefois d'être mis en exergue car ils n'ont pas été abordés jusqu'ici.

1.- **le constat de l'existant**

Il mérite d'être dressé, non pas tant en ce qui concerne les difficultés rencontrées car le groupe interministériel s'est employé à les cerner, mais s'agissant de la réalité de la délinquance appréhendée par chaque parquet, des réponses qui y sont apportées, des initiatives locales prises.

La diffusion du présent rapport en pourrait être l'occasion, à charge, pour les parquets d'y associer aussi les services de police judiciaire qui oeuvrent sous leur direction ainsi que les magistrats instructeurs. Il serait aussi opportun, à cette occasion, de dresser un bilan de la coopération pénale se rapportant à la lutte contre la cybercriminalité mise en oeuvre directement par ces magistrats avec leurs homologues étrangers.

Le futur rapport de politique pénale rendant compte de l'activité 2014 devra aussi permettre d'affiner le constat et de rendre compte des premières évolutions.

2.- **les critères de compétence territoriale**

Certaines des recommandations précédentes concernent déjà cette question, qu'il s'agisse de la reconnaissance d'une compétence concurrente à la juridiction parisienne ou aux juridictions inter-régionales spécialisées (J.I.R.S.), ou du nouveau critère de compétence territoriale tenant au domicile de la victime ou au siège social de l'entreprise. D'autres préconisent une centralisation des plaintes afin de favoriser les recoupements indispensables à une meilleure orientation et à un traitement plus efficace de certains contentieux, essentiellement les escroqueries et les fraudes aux cartes bancaires.

Toutes nécessitent que soient préalablement fixés, au titre de la politique pénale, des critères prioritaires d'attribution sans lesquels l'objectif d'effectivité recherché ne sera pas atteint.

S'agissant des atteintes aux systèmes automatisés de traitement de données, la mise en oeuvre de la compétence parisienne ne devrait pas soulever de difficultés particulières, puisqu'elle repose sur la nature des cibles *(les administrations de l'Etat, les opérateurs d'importance vitale),* le principe de la compétence concurrente n'étant là que pour permettre le maintien d'un traitement strictement local par le parquet concerné lorsque l'atteinte ne revêt aucun caractère de gravité. Il en est d'ailleurs de même pour le cyber-terrorisme.

En ce qui concerne la compétence des J.I.R.S. pour les autres atteintes aux systèmes automatisés de traitement des données ou pour l'ensemble des cyber-crimes ou délits commis en bande organisée, il importe de définir des lignes directrices de saisine, comme pour tous les autres contentieux dont elles ont à connaître. Une telle définition apparaît d'autant plus importante qu'à l'exception des escroqueries organisées commises par faux ordres de virement, les J.I.R.S. ne paraissent guère saisies des autres cyber-infractions qui, pourtant, le mériteraient. Or la complexité, la gravité comme le caractère transfrontalier de certains dossiers commandent une telle saisine.

Une difficulté particulière, qui n'est d'ailleurs pas propre à la cybercriminalité, a trait à la répartition des affaires entre J.I.R.S. ; elle est, en particulier, illustrée par les escroqueries précitées pour lesquelles on constate un éparpillement des saisines entre de nombreuses J.I.R.S., sans que l'on soit, pour autant, assuré qu'il se fonde sur des bandes organisées différentes et donc sur des cibles spécifiques. La diffusion et le partage d'informations revêt ici une importance toute particulière.

Le traitement centralisé des infractions, qu'il soit induit par les signalements que reçoit PHAROS ou, demain, par la centralisation des plaintes relatives aux escroqueries et des dénonciations requises des organismes bancaires, requiert aussi une adaptation de la politique pénale en terme d'orientation et donc de choix des parquets susceptibles d'être saisis.

En effet, il revient aux organismes centraux de police judiciaire compétents d'effectuer les recoupements nécessaires pour faciliter les orientations pertinentes ; il ne leur revient pas d'en décider. Le parquet territorialement compétent en fonction du siège de ces organismes ne saurait, non plus, avoir, à lui seul, vocation à décider de la répartition des affaires concernées sur l'ensemble du territoire national. La détermination de critères de répartition par la Chancellerie, qui devra aussi, par l'intermédiaire de la future Mission Justice, établir des liens privilégiés et constants avec ces organismes, répond ainsi à une nécessité.

Un constat identique s'impose pour les juridictions de droit commun, qui ont à connaître du reste du contentieux.

En réalité et comme cela a déjà été souligné, la question ne se pose pas lorsque la cyber-infraction s'inscrit dans des relations inter-personnelles *(la majeure partie des infractions dites de presse comme des atteintes à la vie privée)*, lorsqu'elle est constatée en flagrance *(par ex., en cas de détention d'images pédopornographiques),* ou lorsque le parquet est saisi après identification de l'auteur et de son domicile *(par ex., toujours en matière de pédo-pornographie, sur dénonciation d'Interpol ou des services centraux français, ou, s'agissant des signalements de la base PHAROS, sur dénonciation de l'O.C.L.C.T.IC après exploitation).* Il en sera de même demain, si les recommandations sont suivies, s'agissant des contentieux de masse déjà cités, ceux-là même qui posaient le plus de difficultés aux services d'enquête et aux parquets.

Il reste toutefois des hypothèses dans lesquelles les services locaux continueront à être saisis sur plainte de faits commis par un auteur encore inconnu, alors même qu'ils ignorent si d'autres victimes sont aussi concernées par des faits similaires et imputables au même délinquant. La future application T.A.J. devrait, peu à peu, pallier l'impossibilité de tels recoupements.

Encore, la question du critère de compétence peut être assez aisément résolue dans l'hypothèse de l'identification d'un auteur domicilié en France, puisque cette dernière entraînera, naturellement, la saisine du parquet correspondant à ce domicile, si l'état d'avancement de l'enquête initiale ne fait pas préférer le maintien de la compétence première sur la base du futur critère lié à la victime.

C'est, en définitive, dans l'hypothèse, soit d'un auteur ou d'un site identifié mais domicilié à l'étranger, soit d'un auteur non identifié avec une pluralité de victimes, que des priorités devront être déterminées dans le cadre de la politique pénale, étant souligné que de telles procédures sont actuellement mal traitées et que les parquets sont d'autant plus réticents à accepter de regrouper des procédures multiples qu'ils ont peu de chance de les mener à bien, sauf dans le strict cadre de l'Union européenne.

Compte-tenu du constat précédent, il convient, de manière générale, d'ordonner les différents critères qui sont ou seront en concours, afin d'atteindre une effectivité maximale et économiser les forces des services d'investigation comme des parquets ; les propositions sont les suivantes [197] :

- en premier lieu, le domicile ou la résidence de l'auteur, s'il est identifié

- en second lieu, la domiciliation ou la résidence du responsable du site litigieux s'il est en France, indépendamment de la localisation du ou des serveurs nécessaires à son fonctionnement
  ou
- la localisation physique du serveur hébergeant le site litigieux, lorsqu'il se situe sur le territoire national

à défaut de tels critères,
- la domiciliation, la résidence ou le siège social de la victime *(critère à créer)*
- le lieu de commission *(disparition de fichier, remise d'argent...)*, qui peut s'assimiler aussi au lieu dans lequel le dommage a été subi *(par ex., en matière de contrefaçon)*

[197] À cet effet, les critères des parquets de CRETEIL et de PARISont été examinés

⌙ et, en cas de pluralité de parquets potentiellement compétents,

-celui qui cumule le maximum de critères de compétence ou (et) qui se caractérise par l'ampleur du préjudice causé ou le plus grand nombre de victimes domiciliées dans son ressort
-celui dans le ressort duquel est situé le service enquêteur à l'initiative de l'enquête suite à la plainte de la victime, si le dessaisissement envisagé n'est pas de nature à apporter une plus-value
-tout en tenant compte de la capacité du parquet à traiter ce genre d'enquête.

3.- **les critères de saisine des différents services d'enquête**

Aux critères tenant à la compétence judiciaire, doivent s'ajouter des critères plus précis s'agissant de la saisine respective des différents services centraux et territoriaux, même si la circulaire de la Direction générale de la Gendarmerie nationale énonce déjà des priorités à cet égard [198],si l'O.C.L.C.T.I.C. a une compétence exclusive pour les affaires à fort contenu international, et si les Douanes ne paraissent pas être confrontées à cette question eu égard au quasi-monopole reconnu à Cyberdouane en terme d'interface avec les opérateurs et les entreprises du commerce sur Internet.

C'est, naturellement, en fonction des compétences spécifiques de chacun de ces services, et sur la base des échanges que devra avoir à cet effet la Chancellerie avec le ministère de l'Intérieur, que devront être suggérées des lignes de conduite.

On constate, en effet, qu'en matière de cybercriminalité, les saisines de certains services centraux sont rares ou ne paraissent guère répondre à une logique cohérente, sauf de la part des parquets qui les côtoient habituellement ; d'autres juridictions saisissent des agences qui n'ont pas de compétence opérationnelle *(par ex., l'ANSSI).* Quant aux critères de répartition de compétence entre les S.R.P.J. et les directions départementales de sécurité urbaine, ils relèvent du protocole de 2007, qui nécessite une mise à jour.

Enfin, mais là encore la question ne concerne pas la seule cybercriminalité, les parquets doivent veiller à regrouper les saisines concernant les cyber-infractions les plus graves ou les plus topiques, afin d'éviter un éparpillement néfaste à l'action judiciaire. Il revient aux procureurs généraux de demander aux S.R.P.J. de tenir un état de ces infractions et d'en assurer la diffusion auprès des parquets de leur ressort.

[198] Elle pourrait utilement être mise à jour

Recommandation n° 55
relative à la politique pénale en matière de cybercriminalité

1- Dresser un constat de l'existant auprès des parquets et des services de police judiciaire.

2- Arrêter, pour la cybercriminalité, les orientations de politique pénale afin de définir les priorités, préciser les schémas de compétence, adapter les modes de traitement à la spécificité des différents contentieux, mobiliser les moyens procéduraux les plus pertinents, mettre en exergue les réponses pénales les plus appropriées, définir les conditions d'une meilleure effectivité des décisions, traiter de la coopération pénale internationale, spécifier la politique d'aide aux victimes sans négliger les questions propres aux entreprises, mobiliser les partenaires indispensables, et évaluer les résultats.

3- Préciser notamment les critères prioritaires de compétence territoriale des parquets et de saisine des services d'enquête.

Conclusion : un rapport d'étape pour une stratégie globale

Pour être récente, la cybercriminalité, cette délinquance à distance, s'avère en pleine expansion.

Certaines de ses manifestations relèvent de la délinquance organisée, menacent le monde économique, voire la souveraineté nationale ; d'autres sont le fait de simples individualités qui profitent de l'aubaine pour déverser leur haine de l'autre ou assouvir leurs penchants pervers ; le plus grand nombre cherche, comme toujours, un moyen facile de gagner de l'argent en contournant les lois et les interdits.

Toutes constituent des défis pour une société qui peine à maîtriser l'extraordinaire évolution technologique qui leur sert de support, à défendre des données personnelles mises à mal par une mémoire qui n'oublie jamais, à adapter ses réponses à un phénomène qui n'a pas de frontières, à surmonter un anonymat quasiment garanti. Mais sans doute l'invention de l'imprimerie ou du téléphone a-t-elle généré des défis du même ordre.

...Une société qui doit pleinement prendre conscience de cette face noire de l'Internet, plus discrète sans doute que le vol à main armée ou que l'attentat terroriste, mais qui recèle des menaces graves, génère des préjudices importants, trouble la vie personnelle et cause parfois la mort.

Cette face noire, même si elle est le fait d'une petite minorité, tout internaute peut en être victime, nombreux sont d'ailleurs qui l'ont déjà été, nul ne peut être assuré qu'il ne le sera pas demain.

...Prise de conscience du risque et du chemin à parcourir pour le contrer, mais sans oublier, dans le même temps, que ce système d'information et de communication relève désormais de notre quotidien, qu'il constitue une avancée considérable dont peuvent témoigner ceux qui ne sont pas nés à l'ère d'Intranet et que nul demain ne pourrait s'en passer.

Cette prise de conscience collective, l'Etat doit s'y atteler avec la même vigueur que celle qu'ill consacre à la lutte contre la fracture numérique ou au développement d'une activité riche en emplois futurs, car tous ces objectifs sont liés.

Il doit pour cela arrêter une véritable stratégie, à court et moyen terme, qui aurait vocation à s'inscrire dans une loi de programmation et qui devra être accompagnée des moyens nécessaires.

Cette stratégie, elle appelle d'abord une organisation. La délégation interministérielle à la lutte contre la cybercriminalité, placée directement sous l'autorité du Premier Ministre, permettra de donner cette impulsion, cette visibilité et cette cohérence qui manquent aujourd'hui, en coopération avec tous les acteurs publics et privés concernés, tout en renforçant les liens avec les deux autres pôles que constituent la sécurité des systèmes d'information et la cyber-défense.

Elle devra toutefois s'appuyer sur une Mission Justice spécifique, afin que la Chancellerie joue pleinement son rôle de ministère de la loi et détermine la politique pénale applicable.

Connaître mieux la cybercriminalité, l'appréhender quantitativement, évaluer le préjudice qu'elle représente, la mieux saisir grâce à la recherche, autant d'objectifs qui constituent la deuxième priorité.

Prévenir est le troisième mot d'ordre de la stratégie proposée ; il s'impose d'autant plus que cette délinquance, plus que toute autre, joue de nos imprudences, celles des individus comme celle des entreprises. L'internaute doit être le premier acteur de sa sécurité, mais aussi de cette lutte contre des propos insoutenables, des images scandaleuses ou des activités condamnables. Le partenariat y a aussi toute sa place, il la prend déjà. Mais il revient à l'Etat de donner l'élan, de conduire cette action sur le long terme, de structurer les pôles de compétence spécifique en fonction des besoins, des catégories, des risques, de mobiliser enfin l'industrie, la recherche, l'université.

Former, c'est la quatrième priorité, car la mobilisation attendue ne peut être le fait que des seuls initiés : former les acteurs, au premier rang desquels les agents d'investigation et les magistrats, mais, par-delà, tous ceux dont la mission est d'éduquer, d'animer, de faciliter l'accès à Internet, car on ne peut prévenir et lutter efficacement contre la cybercriminalité si on ne la connaît pas, si on ne la comprend pas.

Mobiliser aussi les professionnels et, au premier rang d'entre eux, ceux de l'Internet, dans le cadre d'une norme rajeunie définissant précisément leurs obligations ; d'une norme à vocation universelle qui doit concerner aussi bien les prestataires étrangers que français, les fournisseurs de moteur de recherche comme les hébergeurs et fournisseurs d'accès ; d'une norme propre à faciliter l'identification des cyber-délinquants, la réunion des éléments de preuve nécessaires à l'action judiciaire, les légitimes exigences d'efficacité de l'administration comme de la justice grâce à un dispositif de notification/action rénové et enrichi.

Adapter encore les modes de réponse à cette délinquance, car les schémas traditionnels sont impuissants, sans pour autant créer un droit d'exception insupportable au regard des libertés fondamentales. Cette adaptation, elle passe, là encore, par des réformes organisationnelles, avec la centralisation du traitement des contentieux de masse que constituent les escroqueries et les fraudes par cartes bancaires et avec la spécialisation du tribunal de Paris comme des juridictions inter-régionales spécialisées pour les atteintes les plus graves ; mais aussi par des pouvoirs d'investigation précisés et ajustés à la recherche d'une nouvelle effectivité ; par une meilleur contrôle des noms de domaine ; enfin par une meilleure lisibilité et une plus grande cohérence de la norme et la création d'outils d'aide à l'analyse et à la décision.

Répondre aux cyber-victimes est la septième priorité ; elle passe, entre autres, par la création d'une mission de médiation entre les internautes et les prestataires d'Internet, la reconnaissance du droit à l'oubli pour les mineurs, des processus destinés à assurer l'effectivité de l'exécution des décisions, y compris contre l'effet miroir, sans oublier les attentes particulières des entreprises.

Développer enfin les moyens d'action internationaux, telle est la dernière exigence. La réponse à une délinquance sans frontière dépend, on le sait, d'abord et avant tout, de la capacité de l'Europe à présenter un front uni et à entraîner le reste du monde, y compris dans la lutte contre les cyber-paradis. La stratégie proposée pour la France prend d'ailleurs racine dans la stratégie Européenne et s'inspire largement des réflexions menées au sein du Conseil de l'Europe comme de l'Union européenne. Rien d'utile ne se fera isolément, rien ne

se fera non plus sans la mobilisation et le volontarisme des Etats Nations, ainsi que l'illustre la coopération pénale internationale. Cette dernière doit être recentrée sur les objectifs les plus importants, mais aussi rendue plus effective en créant, dans l'espace européen, un *Schengen du numérique.*

Protéger les internautes, l'objectif est ambitieux mais réalisable.

Pour autant, le présent rapport n'a pas l'ambition de l'exhaustivité.

Compte-tenu, tout à la fois, du temps dévolu, qui n'a pas permis d'entendre l'ensemble des acteurs concernés, du prisme juridique privilégié eu égard à la composition du groupe de travail, mais aussi de la complexité du sujet, de la forte emprise internationale et enfin du caractère essentiellement évolutif de la cybercriminalité, qui nécessitera des ajustements continus, l'approche se veut forcément modeste.

Telle est d'ailleurs l'une des raisons pour laquelle des outils organisationnels sont proposés pour l'avenir.

Marc ROBERT

Le 16 février 2014

Récapitulatif des Recommandations

Annexes au rapport

Compte-tenu de leur caractère volumineux,
elles sont rassemblées dans un tome distinct.

❶ - le mandat du groupe de travail interministériel

❷ - la composition du groupe de travail

❸ - la liste des personnes entendues, des visites effectuées et des contributions reçues

❹ - le questionnaire adressé aux prestataires techniques

❺ - la carte de l'implantation des cyber-enquêteurs spécialisés en regard du siège des juridictions interrégionales spécialisées

❻ - l'étude de droit comparé

❼ - les outils pédagogiques : la liste des infractions relevant de la cybercriminalité

❽ - les outils pédagogiques : l'ébauche d'une nomenclature des cyber-infractions spécifiques

❾ - les statistiques judiciaires

❿ - les outils pédagogiques : le glossaire