MINISTÈRE
DE LA JUSTICE

Liberté
Égalité
Fraternité

FRANCE22

Tableau comparatif sur l'encadrement de l'accès en données ouvertes aux décisions de justice

Synthèse des réponses

Propos liminaire :

Le 27 janvier 2022, la présidence du groupe «Justice en ligne» transmettait aux États membres un questionnaire visant à établir un comparatif de la mise à disposition des décisions de justice et des conditions d'encadrement de leur réutilisation.

La présente note a vocation à synthétiser les réponses transmises :

- 21 réponses provenant d'États membres[1] ;
- 1 réponse provenant de la Cour de justice de l'Union Européenne.

L'Office des publications a également présenté une réponse Du fait de sa position particulière, non producteur des décisions diffusées, il a été fait le choix de présenter les réponses de cette instance à part dans la présente restitution.

Dans un certain nombre de cas, le dispositif de publication des décisions est en cours de mise en place. Il a été fait le choix dans cette synthèse de prendre en compte ce qui a été annoncé comme étant la vision cible.

Focus

Dans l'ensemble, il apparait que la mise à disposition des décisions de justice est engagée pour l'ensemble des États membres. Cette mise à disposition est limitée, pour une grande majorité des États membres, à une sélection de ces décisions, sélection qui peut être effectuée dans un but de protection d'intérêts particuliers (sécurité, vie privé des personnes) ou d'identification de décisions d'intérêt particulier.

En ce qui concerne les risques liés à l'exploitation de ces décisions, le principal risque identifié est celui relatif aux données personnelles (réidentification, vie privée, droit à l'oubli, à la sécurité, etc.). Ce risque peut concerner les parties comme les personnels de justice. En conséquence, la mesure de prévention de ces risques la plus partagée est l'anonymisation ou la pseudonymisation[2] des décisions, laquelle est pratiquée par tous les répondants, que ce soit sur une partie de leurs décisions ou sur la totalité d'entre elles.

Au-delà de ces mesures de pseudonymisation, beaucoup d'États encadrent la réutilisation des décisions de justice. Beaucoup des obligations sont des obligations standards en matière de mise à disposition en open data, mais des mesures et obligations spécifiques ont été également prévues par certains États, notamment liées aux finalités de la réutilisation.

Très peu de suivi des réutilisations est effectué par les répondants ; il n'y a sauf rares exceptions ni instance de concertation ni autorité de contrôle spécifiquement dédiée.

Enfin, l'accès aux décisions intégrales (non pseudonymisées) est en général réservé aux parties et aux personnels pour les besoins de leur activité juridictionnelle, mais leurs droits d'accès peuvent être restreints.

[1] *Allemagne, Autriche, Belgique, Croatie, Espagne, Estonie, France, Grèce, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovénie, Suède, Tchéquie*

[2] *La pseudonymisation et l'anonymisation sont deux modalités de traitement de données personnelles visant à assurer la protection des données à caractère personnelles. Le Règlement général relatif à la protection des données (RGPD) définit la pseudonymisation comme «un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires». L'anonymisation, en revanche, vise à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. La différence entre anonymisation et pseudonymisation réside ainsi dans le caractère réversible ou non de la dissimulation des données à caractère personnel. Pour la suite des développements, le terme pseudonymisation sera préféré, le caractère irréversible de l'identification des personnes mentionnées dans les décisions de justice ne peut jamais être assuré de manière absolu.*

Sommaire

Mise à disposition des décisions de justice p.1

Identification des risques p.2

Mesures liées aux données p.3

Obligations imposées aux réutilisateurs p.4

Suivi des réutilisations p.5

Instance des concertation p.5

Autorité de contrôle p.6

Accès aux données intégrales p.7

ANNEXES p.9

1. Mise à disposition des décisions de justice

Tous les répondants mettent, ou prévoient de mettre, à disposition sous forme électronique et à des fins de réutilisation, une sélection ou toutes les décisions de justice rendues par les juridictions de leur ressort.

Il existe cependant des différences dans les modalités de mise à disposition.

Tout d'abord, il y a des différences concernant le périmètre de mise à disposition des décisions de justice. L'ensemble des répondants, à l'exception de la Cour de Justice de l'Union européenne, opère une sélection parmi les décisions mises à disposition.

Focus

Sélection des décisions publiées

S'agissant du mode de sélection des décisions publiées, 2 États prévoient une sélection en fonction de l'intérêt pour le public (Belgique, Suède) et 6 États indiquent que les décisions publiées sont majoritairement celles des plus hautes juridictions (Allemagne, Autriche, Croatie, Espagne, Irlande, Luxembourg).

En outre, la plupart des États prévoient une sélection liée à la nature des décisions. Ainsi, 11 répondants (Allemagne, France, Grèce, Irlande, Lettonie, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovénie) excluent certaines décisions en raison de leur caractère sensible (affaires criminelles, familiales ou impliquant des mineurs, affaires militaires ou relatives au secret défense).

3 États indiquent ne mettre à disposition que les décisions rendues publiquement (France, Grèce, Lettonie), 2 États indiquent ne mettre à disposition que les décisions non confidentielles (Portugal, Roumanie) et 4 répondants indiquent ne mettre à disposition que les décisions définitives (Cour de Justice de l'Union Européenne, Croatie, Lettonie, Portugal).

Un État prévoit un échéancier progressif de mise à disposition des décisions, par niveau d'instance et type de contentieux, à échéance 2025 (France).

Enfin, 2 États (Estonie, Malte) prévoient un principe de mise à disposition de toutes les décisions, et une exception à la discrétion de la juridiction en cas de risque d'atteinte à la vie privée des personnes.

En second lieu, c'est au niveau de la gratuité ou non des mises à disposition que les réponses divergent. 18 répondants indiquent avoir opté pour une gratuité totale et 4 pour une gratuité partielle, des frais pouvant être demandés dans certains cas.

Focus

Hypothèses dans lesquelles des frais sont demandés

Un État prévoit l'absence de gratuité si la réutilisation est destinée à des fins commerciales. Un tarif sera fixé, correspondant aux coûts du traitement du jugement concerné et de la pseudonymisation des données à caractère personnel (Espagne).

Un deuxième État permet, si la décision ne fait pas partie des décisions mises à disposition par l'État, d'en demander la mise à disposition, moyennant le paiement d'un tarif forfaitaire par page de la décision (Lettonie).

Pour un troisième État, si le demandeur ne souhaite pas passer par l'internet, il peut faire une demande de recherche de jurisprudence, qui sera payante suivant un tarif forfaitaire pour chaque recherche (Luxembourg).

Enfin, pour un quatrième État, si la demande implique des coûts additionnels ou revêt un caractère inhabituel, un tarif peut être demandé (Pologne).

2. Identification des risques

A la question : « Des risques liés à la réutilisation des décisions de justice ont-ils été identifiés ? », 9 répondants indiquent n'avoir identifié aucun risque particulier (Belgique, Croatie, Grèce, Italie, Lettonie, Luxembourg, Pologne, Slovénie, Suède)[3].

Focus

Les bénéfices de la mise à disposition des décisions de justice

Un État indique qu'aucun risque n'a été identifié, mais précise à l'inverse que la mise à disposition et l'accessibilité des décisions de justice permettent de réduire le recours à des procédures judiciaires inutiles, en offrant la possibilité de mieux connaître la jurisprudence sur un sujet donné. De même, cela permet aux parties de mieux argumenter leur demande de recours face à une décision de première instance (Lettonie).

15 répondants (Allemagne, Autriche, Cour de Justice de l'Union Européenne, Espagne, Estonie, France, Irlande, Lettonie, Lituanie, Malte, Office des publications, Pays-Bas, Portugal, Roumanie, Tchéquie) ont mentionné la ré-identification comme l'un des risques liés à la mise à disposition des décisions de justice. Ce risque de ré-identification regroupe plusieurs risques sous-jacents : sécurité des personnes ou des magistrats, vie privée des personnes, droit à l'oubli.

4 répondants mentionnent les risques liés directement au caractère officiel des données, et à l'exigence de conformité, sécurité, accès, conservation, mise à jour de ces données (Cour de Justice de l'Union Européenne, France, Lituanie, Office des publications). Un État cite le risque d'erreur dans les décisions diffusées (Irlande) et un État cite le risque de création de bases de données non-officielles suite aux publications massives (Estonie).

Certains États mentionnent le risque de divulgation d'informations sensibles liées au secret défense, secret d'État, secret militaire, secret des affaires (Allemagne, Tchéquie). D'autres États mentionnent le risque de divulgation de décisions confidentielles (Portugal, Roumanie).

Des répondants citent les risques liés à l'effet des analyses de masse : risque de profilage, d'atteinte à l'indépendance des juges ou encore d'atteinte à la force exécutoire des décisions de justice (Autriche, Cour de Justice de l'Union Européenne, France, Luxembourg, Pays-Bas). Certains États mentionnent également le risque d'atteinte à la notion de jurisprudence ou de précédent (France, Lituanie) et le risque de difficulté à effectuer des recherches pertinentes dans une trop grande masse de documents (Portugal).

Enfin, un répondant mentionne le risque d'incohérence du choix éditorial des éditeurs privés avec la politique de publication des juridictions (Cour de Justice de l'Union Européenne), un État mentionne le risque d'atteinte à la lisibilité de la décision (Portugal) et un autre le risque de responsabilité de l'État si les informations ne sont pas correctement anonymisées (Irlande).

Focus

Tenue d'un registre des risques

La Cour de Justice de l'Union Européenne procède à un recensement et une mise à jour annuelle de son registre des risques et les services qui la composent gèrent et mitigent leurs propres risques, y compris les risques liés à la nature des informations (juridictionnelles, administratives et publiques).

[3] *Certains de ces États ayant néanmoins évoqué des risques dans leurs réponses aux autres questions, ils peuvent être mentionnés dans la présente section.*

3. Mesures liées aux données

Le questionnaire interrogeait ensuite sur les mesures prises au moment de la mise à disposition des données afin de prévenir ces risques identifiés liés à la réutilisation des données.

Afin de prévenir le risque de réidentification et d'atteinte à la vie privée, l'ensemble des États et répondants ont mis en place une pseudonymisation des décisions mises à disposition. Un État indique que la décision est d'abord mise à disposition non pseudonymisée, et que la pseudonymisation n'est effectuée qu'après un certain délai défini pour permettre le droit à l'oubli (Estonie).

Le type de pseudonymisation pratiqué diffère selon les réponses :

- 5 utilisent l'intelligence artificielle (Autriche, France, Espagne, Roumanie, Tchéquie),
- 2 font de la pseudonymisation automatique mais sans intelligence artificielle (Lettonie, Suède),
- 6 réalisent la pseudonymisation manuellement, par le personnel de la juridiction (Allemagne, Belgique, Croatie, Grèce, Luxembourg, Pays-Bas),
- 9 n'ont pas précisé le type de pseudonymisation effectuée (Cour de Justice de l'Union Européenne, Estonie, Italie, Irlande, Lituanie, Malte, Pologne, Portugal, Slovénie).

Cette pseudonymisation est effectuée, selon les cas, selon l'appréciation de la juridiction ou en fonction des contentieux.

Un État (Croatie) indique pseudonymiser toutes les décisions à destination du public mais seulement certaines catégories de décisions à destination des juges et membres des Cours (les décisions concernant les affaires familiales, les mineurs…)

9 répondants (Allemagne, Autriche, Belgique, Estonie, Irlande, Office des publications, Pologne, Roumanie, Slovénie) mentionnent des mesures de cybersécurité (HTTPS, captcha, mesures antiscraping) et un État demande aux réutilisateurs de ne pas sur-utiliser le service (Pays-Bas).

Un État étudie l'idée d'un cachet électronique pour garantir l'authenticité des décisions publiées et la fiabilité de leurs informations (France).

Focus

Restrictions d'accès

Des restrictions d'accès sont parfois prévues.

Un État (Estonie) a prévu plusieurs mesures de cybersécurité. Tout d'abord, un renforcement du captcha est présent, pour empêcher l'accès de logiciels aux informations mises à disposition. Ensuite, il est impossible d'accéder aux décisions depuis un moteur de recherche comme Google. Il faut utiliser le moteur de recherche dédié et l'accès à cette interface se fait par API , après avoir signé une charte.

Au-delà de l'absence de mise à disposition de certaines décisions, un État prévoit la possibilité de restreindre les droits d'accès à certaines décisions publiées, ou à certains utilisateurs en particulier (Autriche). Un État se réserve le droit de bloquer l'accès d'un réutilisateur s'il fait un mauvais usage ou un usage illégal des décisions publiées (Irlande).

Un État a rendu impossible le téléchargement du document mis à disposition, afin de rendre difficile le transfert vers d'autres bases de données (Roumanie). Un autre État (Belgique) empêche le scraping (technique d'extraction du contenu de site web dans le but de transformer et réutiliser la donnée).

Enfin, un répondant (Cour de Justice de l'Union Européenne) prévoit l'affichage d'un message qui rappelle aux réutilisateurs les conditions qu'ils doivent respecter.

4. Obligations imposées aux réutilisateurs

À la question : « Des obligations ou des interdictions sont-elles imposées aux réutilisateurs des données? », 7 États indiquent n'imposer aucune obligation spécifique (Croatie, Grèce, Lettonie, Malte, Pays-Bas, Suède, Tchéquie).

Focus

Encadrement juridique des réutilisations

20 répondants (seuls les Pays-Bas et la Slovénie n'en font pas mention) mentionnent des dispositifs juridiques pour encadrer la réutilisation des décisions de justice.

13 États (Autriche, Croatie, Espagne, France, Grèce, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pologne, Suède, Tchéquie) évoquent l'application de lois ou réglementations encadrant la réutilisation des décisions de justice.

9 répondants (Allemagne, Belgique, Estonie, France, Irlande, Lituanie, Office des publications, Portugal, Roumanie) prévoient des conditions générales d'utilisation ou des licences.

Un État (Estonie) impose la signature d'une convention entre les services producteurs de la donnée et les réutilisateurs.

Par ailleurs, certains répondants précisent le contenu de ces obligations : obligation de mentionner la source du document publié, de mettre à jour le document publié chaque fois que nécessaire, interdiction de modifier le document. 2 États précisent dans certains cas les règles de citation des décisions (Allemagne, Pologne).

Focus

Interdiction de certaines finalités de réutilisation

2 États (Irlande, Portugal) ont explicitement interdit certaines finalités pour les réutilisations des décisions de justice mises à disposition : commerciales ou publicitaires, illégales/frauduleuses, malhonnêtes/trompeuses/fallacieuses, offensantes, immorales.

D'autres obligations sont prévues de manière moins répandue :

- Un État (Espagne) interdit les droits exclusifs (propriété intellectuelle) sur le contenu des documents mis à disposition, et un autre État (Portugal) impose de respecter les éventuels droits intellectuels, à savoir notamment le droit d'auteur.
- Un État interdit pénalement le profilage des magistrats et personnels de greffe (France).

5. Suivi des réutilisations

9 répondants (Allemagne, Autriche, Espagne, France, Irlande, Lettonie, Office des publications, Pays-Bas) disposent de statistiques, mais uniquement sur l'accès aux documents et non sur les réutilisations.

6. Instances de concertation

Le panorama relatif à l'existence d'instances de concertation est varié. 7 répondants n'en disposent d'aucune et les 15 autres citent des structures de natures assez différentes :

- **Allemagne :** représentants de la Cour et des autorités compétentes ;
- **Autriche :** groupe de travail créé par le ministère de la Justice ;
- **Belgique :** groupe « Excellence des données » ;
- **Cour de Justice de l'Union européenne :** comité interinstitutionnel de la maintenance des données ; comité « protection des données » ; instances de gouvernance de l'institution ;
- **Croatie :** 4 centres régionaux ;
- **Espagne :** administration publique ; équipes d'analystes ; office espagnol des brevets et des marques ; projet « Easy reading » ; Bulletin officiel ; académie royale d'Espagne ;
- **Estonie :** ministère de la Justice, centre des registres et des systèmes d'information ; inspection de la protection des données ;
- **France :** groupe de travail « Réutilisation des données issues des décisions de justice » ;
- **Irlande :** ministère de la Justice ;
- **Lettonie :** ministère de la Justice et entités impliquées (Cour, professionnels, institutions…) ;
- **Luxembourg :** service de documentation ; délégué à la protection des données du parquet général ; autorité judiciaire chargée du contrôle des opérations ;
- **Malte :** stratégie maltaise pour la justice numérique ;
- **Office des publications :** groupe d'information du secteur public ; DG Connect (UE) ; groupe inter-institutionnel Lex ;
- **Roumanie :** conseil national de la magistrature ;
- **Suède :** agence suédoise pour le gouvernement numérique.

7. Autorité de contrôle

La répartition est sensiblement la même s'agissant des autorités de contrôle. 9 répondants n'en disposent d'aucune et 13 répondants font état d'une autorité de contrôle :

- **Allemagne :** ministère de la Justice fédéral ; office fédéral de la justice ; autorités judiciaires ;
- **Autriche :** ministère de la Justice ;
- **Belgique :** gestionnaire ;
- **Estonie :** ministère de la Justice ; inspecteur de la protection des données ;
- **Grèce :** autorité nationale de la transparence ;
- **Irlande :** autorité judiciaire ; service des tribunaux ;
- **Italie :** contrôleur de la protection des données ;
- **Luxembourg :** juridictions compétentes ; commission nationale pour la protection des données (CNPD) ;
- **Office des publications :** DG Connect (UE) ;
- **Pays-Bas :** centre de service national pour la magistrature ;
- **Pologne :** ministère de la Justice ; président de l'office de protection des données personnelles ;
- **Slovénie :** Cour suprême ;
- **Suède :** autorité suédoise pour la protection de la vie privée.

2 États étudient la possibilité de créer une autorité de contrôle dédiée (Espagne, France).

8. Accès aux données intégrales

Toutes les répondants (22) indiquent permettre l'accès aux données intégrales aux personnels des juridictions (magistrats, greffe, etc.), notamment lorsqu'ils sont en charge du dossier.

Focus

Accès des personnels des juridictions aux décisions intégrales

L'accès des magistrats et personnels des juridictions aux décisions intégrales est prévu différemment selon les États. Il peut s'agir seulement des décisions de la juridiction où ils exercent leurs fonctions (Allemagne, Autriche, Lettonie) ou seulement des décisions relatives à leur champ de compétence (Allemagne, Portugal, Roumanie).

L'accès peut s'étendre à toutes les décisions sauf affaires sensibles : affaires familiales, affaires impliquant des mineurs, affaires où le magistrat est impliqué ou excusé (Croatie, Portugal).

Cela peut être seulement pour les décisions dont ces personnels ont la charge (Espagne, Lettonie, Lituanie, Tchéquie) ou encore seulement pour les besoins de leur activité professionnelle (France, Grèce, Luxembourg, Malte, Slovénie).

Un État membre prévoit l'affichage d'un message rappelant l'interdiction de publication de ces décisions (Malte).

5 réponses n'ont pas précisé la nature de l'accès donné aux personnels des juridictions.

Les autres personnels qui ont accès aux données intégrales sont les parties et leurs avocats (Belgique, Estonie, Lituanie, Pologne, Portugal, Suède), les opérateurs de pseudonymisation ou fournisseurs de services (Irlande, Lituanie, Pays-Bas, Pologne, Slovénie), les personnels de l'inspection (Estonie, Portugal), les membres d'autorités étatiques (Estonie, Lituanie).

Focus

Accès d'un tiers aux données intégrales des décisions de justice

Un État membre permet l'accès aux décisions non pseudonymisées aux personnes démontrant d'un intérêt légitime. En matière pénale, cet accès n'est admissible que lorsque le secret judiciaire n'est plus applicable et exclut certains crimes, comme le trafic d'organes et d'êtres humains, les atteintes à la liberté sexuelle et l'autodétermination, ainsi que les procédures pénales où le droit à la vie privée est en jeu. Dans le cas des procédures civiles, l'accès peut être refusé, par exemple, lorsque des mineurs sont impliqués, ainsi que dans les cas de recherche de maternité et de paternité (Portugal).

Un État membre prévoit l'accès, rare, aux journalistes (Estonie).

© ministère de la Justice/SG/DICOM/Impression CIN 2022