

1. La CNIL se penche sur l'impact économique du RGPD

La Commission Nationale Informatique et Liberté française a procédé à une revue des différentes études réalisées pour essayer de dégager l'impact économique du RGPD depuis son entrée en vigueur, il y a cinq ans.

Un résumé est disponible à l'adresse suivante : <https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres>. A partir de celle-ci un lien mène vers l'article complet publié dans la Revue Européenne des Médias et du Numérique.

Il en ressort principalement que si cet impact est difficile à mesurer faute d'étude précise sur le rapport coûts/bénéfices dans la totalité des secteurs économiques concernés, les contraintes engendrées pour les entreprises, si elles peuvent paraître lourdes et coûteuses, ont également des effets positifs notamment en termes d'image et de confiance du consommateur, ce qui a nécessairement un impact économique favorable. De plus, se pose la question de la place que la société souhaite accorder aux droits et libertés fondamentaux des individus au travers de l'utilisation de leurs données personnelles dans la mesure où ces droits ne doivent pas revêtir de valeur marchande mais être considérés comme des acquis sociaux à protéger et ce, même si cela a un coût pour certains acteurs du marché.

A l'heure où la Principauté élabore un nouveau texte sur la protection des données en vue de moderniser sa législation et d'obtenir une décision européenne d'adéquation, ces éléments peuvent nourrir la réflexion quant à l'importance de la législation sur les données à caractère personnel.

2. La Cour de Justice de l'Union Européenne se prononce sur la conciliation du droit du public à l'accès aux documents officiels et la conciliation avec le droit des données personnelles

Dans un arrêt du 7 mars 2024, la Cour de Justice de l'Union européenne saisie d'une question préjudicielle par une juridiction finlandaise juge que :

« L'article 2, paragraphe 1, et l'article 4, point 2, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), doivent être interprétés en ce sens que : la communication orale d'informations relatives à d'éventuelles condamnations pénales en cours ou déjà purgées dont une personne physique a fait l'objet constitue un traitement de données à caractère personnel, au sens de l'article 4, point 2, de ce règlement, qui relève du champ d'application matériel de ce règlement dès lors que ces informations sont contenues ou appelées à figurer dans un fichier.

Les dispositions du règlement 2016/679, notamment l'article 6, paragraphe 1, sous e), et l'article 10 de celui-ci, doivent être interprétées en ce sens que :

elles s'opposent à ce que des données relatives à des condamnations pénales d'une personne physique figurant dans un fichier tenu par une juridiction puissent être communiquées oralement à toute personne aux fins de garantir un accès du public à des documents officiels, sans que la personne demandant la communication ait à justifier d'un intérêt spécifique à obtenir lesdites données, la circonstance que cette personne soit une société commerciale ou un particulier n'ayant pas d'incidence à cet égard. ».

Pour ce faire, elle a notamment énoncé, sur la première question, qu'il n'était pas contesté que les informations demandées constituaient des données personnelles et qu'elles étaient contenues dans un « *fichier de données à caractère personnel tenu par une juridiction* », peu important que ce fichier soit tenu sous forme de base de données électronique ou de fichiers ou registre physique.

Sur la deuxième question, elle a estimé que :

« Afin de déterminer si une communication au public de données à caractère personnel relatives à des condamnations pénales est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, au sens de l'article 6, paragraphe 1, sous e), du RGPD, et si la législation autorisant une telle communication prévoit des garanties appropriées pour les droits et les libertés des personnes concernées, au sens de l'article 10 de ce règlement, il y a lieu de vérifier en particulier si, eu égard à la gravité de l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel causée par ladite communication, celle-ci apparaît justifiée, et notamment proportionnée, aux fins de la réalisation des objectifs poursuivis.

Quant à la gravité de l'ingérence dans ces droits, la Cour a déjà jugé que le traitement des données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes est, en raison de la sensibilité particulière de ces données, susceptible de constituer une ingérence particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, garantis par les articles 7 et 8 de la Charte. En effet, dès lors que de telles données portent sur des comportements qui entraînent la désapprobation de la société, l'octroi d'un accès à ces mêmes données est susceptible de stigmatiser la personne concernée et de constituer ainsi une ingérence grave dans sa vie privée ou professionnelle.

Si l'accès du public aux documents officiels, auquel se réfère la juridiction de renvoi, constitue, ainsi qu'il découle du considérant 154 du RGPD, un intérêt public susceptible de légitimer la communication de données à caractère personnel figurant dans de tels documents, cet accès doit néanmoins être concilié avec les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, comme l'exige d'ailleurs expressément l'article 86 du RGPD. Or, eu égard notamment à la sensibilité des données relatives aux condamnations pénales et à la gravité de l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes concernées, que la

divulgarion de ces données provoque, il doit être considéré que ces droits prévalent sur l'intérêt du public à avoir accès aux documents officiels.

Pour cette même raison, le droit à la liberté d'information visé à l'article 85 du RGPD ne saurait être interprété en ce sens qu'il justifie la communication à toute personne qui en fait la demande de données à caractère personnel relatives à des condamnations pénales. ».

Bien que rendu au regard du RGPD, cette décision amène à s'interroger sur qu'il en serait en droit monégasque dans le cas d'une personne ou société sollicitant oralement ou par écrit des informations sur des antécédents judiciaires d'une personne, d'autant que sont engagées des réflexions en Principauté sur une plus large publication des décisions de justice.

(CJUE 7 mars 2024 – Affaire C-740/22, Endemol Shine Finland). Pour plus d'informations :

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=283530&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=3180634>

3. La Cour Européenne de Justice octroie la qualité de données personnelles à une combinaison de lettres et de caractères contenant les préférences d'un utilisateur d'Internet ou d'une application relatives au consentement de cet utilisateur au traitement des données à caractère personnel le concernant par des fournisseurs de sites Internet ou d'applications ainsi que par des courtiers de telles données et par des plateformes publicitaires et estime qu'une organisation sectorielle peut être responsable conjoint de traitement.

Par un arrêt du 7 mars 2024, la CJUE a été saisie d'une question préjudicielle posée par la Cour d'appel de Bruxelles (Belgique) à la suite d'une sanction infligée par l'Autorité de protection des données belge à l'Association IAB EUROPE. Cette association à but non lucratif représente les entreprises du secteur de l'industrie de la publicité et du marketing numériques au niveau européen. IAB Europe a élaboré une solution qu'elle présente comme étant susceptible de rendre conforme au RGPD ce système de vente aux enchères. Les préférences des utilisateurs sont codées et stockées dans une chaîne composée d'une combinaison de lettres et de caractères sous le nom de Transparency and Consent String (TC String), qui est partagée avec des courtiers en données à caractère personnel et des plates-formes publicitaires, afin que ceux-ci sachent ce à quoi l'utilisateur a consenti ou s'est opposé. Un cookie est également placé sur l'appareil de l'utilisateur. Lorsqu'ils sont combinés, la TC String et le cookie peuvent être liés à l'adresse IP de cet utilisateur. Lesdites enchères ont lieu en temps réel lorsqu'un utilisateur se rend sur un site ou une application et sont destinées à permettre au publicitaire de lui proposer des publicités ciblées. Quand les informations contenues dans une TC String sont associées à un identifiant, tel que, notamment, l'adresse IP de l'appareil de l'utilisateur, elles peuvent permettre de créer un profil de cet utilisateur et de l'identifier. La Cour a également estimé, sous réserve de vérification par la juridiction saisie, que cette association avait la qualité de

responsable conjoint du traitement dans la mesure où elle détermine, conjointement avec ses membres, les finalités et moyens du traitement.

La Cour a ainsi jugé que :

« 1) *L'article 4, point 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données),*

doit être interprété en ce sens que :

une chaîne composée d'une combinaison de lettres et de caractères, telle que la TC String (Transparency and Consent String), contenant les préférences d'un utilisateur d'Internet ou d'une application relatives au consentement de cet utilisateur au traitement des données à caractère personnel le concernant par des fournisseurs de sites Internet ou d'applications ainsi que par des courtiers de telles données et par des plateformes publicitaires, constitue une donnée à caractère personnel au sens de cette disposition dans la mesure où, lorsque celle-ci peut, par des moyens raisonnables, être associée à un identifiant, tels que notamment l'adresse IP de l'appareil dudit utilisateur, elle permet d'identifier la personne concernée. Dans de telles conditions, la circonstance que, sans une contribution extérieure, une organisation sectorielle détenant cette chaîne ne peut ni accéder aux données qui sont traitées par ses membres dans le cadre des règles qu'elle a établies ni combiner ladite chaîne avec d'autres éléments ne fait pas obstacle à ce que la même chaîne constitue une donnée à caractère personnel au sens de ladite disposition.

2) *L'article 4, point 7, et l'article 26, paragraphe 1, du règlement 2016/679*

doivent être interprétés en ce sens que :

– *d'une part, une organisation sectorielle, dans la mesure où elle propose à ses membres un cadre de règles qu'elle a établi relatif au consentement en matière de traitement de données à caractère personnel, qui contient non seulement des règles techniques contraignantes mais également des règles précisant de façon détaillée les modalités de stockage et de diffusion des données à caractère personnel relatives à ce consentement, doit être qualifiée de « responsable conjoint du traitement », au sens de ces dispositions, si, compte tenu des circonstances particulières du cas d'espèce, elle influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel concerné et détermine, de ce fait, conjointement avec ses membres, les finalités et les moyens d'un tel traitement. La circonstance qu'une telle organisation sectorielle n'a pas elle-même directement accès aux données à caractère personnel traitées par ses membres dans le cadre desdites règles ne fait pas obstacle à ce qu'elle puisse présenter la qualité de responsable conjoint du traitement, au sens desdites dispositions ;*

– *d'autre part, la responsabilité conjointe de ladite organisation sectorielle ne s'étend pas automatiquement aux traitements ultérieurs de données à caractère personnel effectués par des tiers, tels que les fournisseurs de sites Internet ou d'applications, pour ce qui concerne les préférences des utilisateurs aux fins de la publicité ciblée en ligne. ».*

Au vu du projet de texte en préparation sur les données à caractère personnel dont les principes sont équivalents à l'esprit et à la lettre du RGPD notamment en ce qui concerne la volonté de protection du consommateur, la Principauté pourrait être amenée à se prononcer sur ces points ou des problématiques équivalentes.

(Cour Européenne de Justice 7 mars 2024 – Dans l'affaire C-604/22, IAB Europe contre Gegevensbeschermingsautoriteit. Pour plus d'informations : <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240044fr.pdf>)

4. Un rapport sur l'Intelligence Artificielle en France

Un rapport a été remis à la présidence de la République française le 13 mars 2024 par la Commission sur l'Intelligence Artificielle contenant 25 recommandations parmi lesquelles dans le domaine des données personnelles :

- *Faciliter la circulation des données et le partage de pratiques pour tirer les bénéfices de l'IA dans les soins, améliorer l'offre et le quotidien des soignants* (recommandation 10).
- *Transformer notre approche (française) de la donnée personnelle pour mieux innover* (recommandation 15) afin d'améliorer la conciliation entre innovation et droits des personnes.
- *Mettre en place une infrastructure technique favorisant la mise en relation entre les développeurs d'IA et les détenteurs de données culturelles patrimoniales* (recommandation 16) afin de favoriser le partage de la culture tout en préservant les droits de propriété intellectuelle.

Il est également proposé que la CNIL qui s'est déjà dotée d'un service consacré à l'Intelligence Artificielle voit sa mission étendue à l'innovation et sa composition modifiée afin de mieux appréhender les nouveaux enjeux.

Au moment où Monaco souhaite développer sa volonté devenir une Principauté numérique et où une nouvelle Autorité administrative indépendante devrait remplacer la CCIN avec le vote prochain d'une nouvelle loi sur les données personnelles, se posera la question du périmètre de cette entité notamment au regard de l'IA qui est intimement liée à la problématique de la collecte et l'utilisation des données personnelles notamment eu égard au mode d'apprentissage des IA génératives.

Pour plus d'information ([Comité de l'IA générative, Recommandations pour l'IA en France](#))

*Commission de Contrôle des Informations Nominatives
Ce document est à vocation purement informative et ne peut être considéré comme reflétant une position officielle de la CCIN*