
PRINTEMPS
DES
dpo
Matinale Digitale | 16 mai 2024
infoprodigital

PRINTEMPS DES dpo

Actus, Veille & Tendances

François-Xavier Cao

Co-fondateur & chief product officer

Olympe.legal

Olympe .LEGAL

AI act et RGPD

Quelques précisions récentes concernant leur articulation et leur application

Loyauté et surveillance

Être précautionneux dans la prise de précautions

Accès et réutilisation des données

Quelques précisions à connaître quand des données servent finalement à autre chose

AI act et RGPD

Un guide sur l'IA et la protection des données

Intelligence artificielle

DE DATENSCHUTZKONFERENZ • 07/05/2024

La Conférence sur la protection des données (CPD) qui réunit au niveau fédéral les autorités de protection allemandes a publié un guide d'orientation sur l'intelligence artificielle et la protection des données, à destination des entreprises et des pouvoirs publics. Le guide aborde de manière pratique les questions que les responsables de traitement doivent se poser et auxquelles ils doivent répondre lors de l'utilisation, du choix, de la mise en œuvre et de l'utilisation d'applications d'intelligence artificielle (finalité, obligation de transparence, droits des personnes concernées, exactitude des données...). En revanche, le développement des IA et l'entraînement des modèles sont hors du champs de ce guide.

Le guide examine à l'aide d'exemples les critères importants en fonction des exigences du RGPD et fournit des lignes directrices pour les décisions correspondantes.

Le rapport sur l'IA préconise d'aller vers une vision collective des données personnelles

Intelligence artificielle

Poser une question

FR GOUVERNEMENT.FR • 13/03/2024

La Commission de l'intelligence artificielle a remis au gouvernement le 13 mars 2024 [son rapport](https://www.gouvernement.fr/actualite/25-recommandations-pour-lia-en-france) contenant 25 recommandations pour faire de la France un acteur majeur de la révolution technologique de l'intelligence artificielle. Il aborde bien sûr la question de la protection des données personnelles, sous un angle assumé : réduire la protection individuelle pour augmenter l'innovation dans un bénéfice collectif. Ainsi, le rapport demande à "faciliter l'accès aux données", à "moderniser le mandat de la CNIL et de son collège", ou encore à "supprimer certaines procédures d'autorisation préalable d'accès aux données de santé". "_La notion même de donnée personnelle, qui constitue la clé d'application du RGPD, suscite des interrogations dans un contexte croissant d'utilisation de données collectives_", avancent les auteurs du rapport, qui veulent pousser vers une forme de négociation collective des droits à la protection des données, plutôt qu'une liberté individuelle. "_Que ce soit au travers d'associations, de syndicats ou de tout autre collectif organisé, des accords relatifs aux traitements des données et à l'utilisation de systèmes d'IA pourraient permettre d'accroître l'effectivité de la garantie des droits de chacun_", écrivent-ils. "_Il importe de trouver la voie d'une gouvernance collective de la donnée qui pourrait, dès aujourd'hui, utiliser les marges de manœuvre juridiques sous-exploitées du RGPD et, à terme, poser les jalons d'une évolution du cadre juridique qui prendrait mieux en considération l'évolution des modes d'utilisation des données_". De quoi faire débat. Ce ne serait pas une évolution, mais une révolution du droit de la protection des données personnelles.

La CNIL publie une fiche pratique sur la réutilisation des données pour de l'IA

Intelligence artificielle Réutilisation des données

Poser une question

FR CNIL • 08/04/2024

Dans le cadre de ses activités d'information et de sensibilisation, la CNIL publie une fiche pratique sur la manière dont les organismes peuvent s'assurer de la conformité au RGPD d'une réutilisation de données personnelles par des systèmes d'intelligence artificielle. Elle complète une information plus large sur la conception des systèmes d'IA compatibles RGPD.

La fiche rappelle dans un premier temps que le responsable de traitement a le droit de réutiliser des données pour une finalité non prévue initialement si la nouvelle finalité est compatible avec celle de la collecte initiale (ce qui est présumé pour les fins statistiques et de recherche scientifique), ce qui demande de réaliser un "**test de compatibilité**" qui doit notamment prendre en compte :

- l'existence d'un lien entre la finalité initiale et la finalité du traitement ultérieur envisagé ;
- le contexte dans lequel les données personnelles ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de la relation entre les personnes concernées et le responsable du traitement ;
- le type et la nature des données, en particulier en fonction de leur sensibilité (données biométriques, de géolocalisation, concernant des mineurs, etc.) ;
- les éventuelles conséquences du traitement ultérieur envisagé pour les personnes concernées ;
- l'existence de garanties appropriées (telles que le chiffrement ou la pseudonymisation).

La fiche aborde également les cas de réutilisation des données lorsqu'elles proviennent de bases de données accessibles publiquement, ou de bases de données acquises auprès d'un tiers.

Un bac à sac réglementaire pour l'IA au Danemark

Intelligence artificielle

Poser une question

DK DATATILSYNET • 07/03/2024

A l'instar des bacs à sable déjà lancés par la CNIL depuis plusieurs années, son homologue danoise a annoncé cette semaine l'ouverture d'un bac à sable réglementaire pour l'IA, "*où les entreprises et les autorités peuvent accéder gratuitement à une expertise et à des conseils pertinents sur le cadre juridique actuel, en se concentrant dans un premier temps sur le RGPD*". Des programmes seront lancés d'une durée de 3 à 6 mois. Pour information, l'AI Act rend obligatoire la création de tels bacs à sable réglementaires dans tous les états membres de l'Union européenne, afin de faire en sorte que la réglementation ne soit pas vécue comme un frein à l'innovation.

AI Act : le Garante veut être désigné autorité compétente

Intelligence artificielle

Poser une question

IT GPDP • 25/03/2024

Le président du Garante per la protezione dei dati personali (GPDP), Pasquale Stanzione, a écrit à la cheffe du gouvernement italien Giorgia Meloni et aux présidents des deux chambres parlementaires pour demander que le Garante soit nommé autorité de référence pour l'application de l'AI Act, approuvé par le Parlement européen le 13 mars dernier. En effet, le règlement sur l'intelligence artificielle demande aux états membres de désigner une autorité nationale en charge de la régulation de l'IA, mais laisse chacun libre de son choix. Or si celui de l'autorité chargée de la protection des données personnelles est le plus probable, il ne s'impose pas nécessairement.

Pour M. Stanzione, "*compte tenu de l'étroite interrelation entre l'IA et la protection des données, de l'expertise déjà acquise sur le terrain par les DPA en matière de prise de décision automatisée (article 22 du règlement UE 2016/679) et des éléments d'indépendance qui caractérisent leur statut*", la désignation du Garante s'impose pour réguler l'intelligence artificielle en Italie. Il rappelle que le règlement

Loyauté et surveillance

Un enquêteur privé ne peut pas traiter secrètement des données librement accessibles sur Internet

Loyauté du traitement

Poser une question

FR COUR DE CASSATION • 07/05/2024

Dans un arrêt du 30 avril 2024, la chambre criminelle de la Cour de cassation indique que "*le fait que les données à caractère personnel collectées par [un enquêteur privé] aient été pour partie en accès libre sur internet ne retire rien au caractère déloyal de cette collecte, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées*".

Le prévenu avait été condamné par la cour d'appel de Versailles à deux ans de prison avec sursis et 20 000 euros d'amende pour avoir, entre 2009 et 2012, **sur le fondement de l'article 226-18 du code pénal** qui punit "*le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite*". L'enquêteur privé condamné avait répondu aux demandes du directeur de la sécurité de la société commanditaire pour effectuer des recherches sur des salariés, candidats à l'embauche, clients ou prestataires, portant notamment sur des antécédents judiciaires, renseignements bancaires et téléphoniques, véhicules, propriétés, qualité de locataire ou de propriétaire, situation matrimoniale, santé, et déplacements à l'étranger. Dans ce cadre, il effectuait des recherches sur Internet, notamment sur les réseaux sociaux.

En appel, la cour de Versailles avait estimé que le moyen de collecte de ces données est considéré comme déloyal dans les rapports employeur/employé dès lors que, issues de la capture et du recoupement d'informations diffusées sur des sites publics tels que sites web, annuaires, forums de discussion, réseaux sociaux, sites de presse régionale, comme le prévenu l'a lui-même exposé lors de ses interrogatoires, **de telles données ont fait l'objet d'une utilisation sans rapport avec l'objet de leur mise en ligne** et ont été recueillies à l'insu des personnes concernées, ainsi **privées du droit d'opposition** institué par la loi informatique et libertés.

La cour de cassation casse toutefois l'arrêt de la cour d'appel pour un motif de détermination de la prescription des faits.

La CJUE valide le traitement des adresses IP à des fins de lutte contre le piratage

Minimisation des données | Proportionnalité

Poser une question

EU CJUE • 30/04/2024

La Cour de justice de l'Union européenne (CJUE) a rendu son arrêt C-470/21 par lequel elle valide le mécanisme dit de "réponse graduée" mis en place pour lutter contre le partage illicite d'œuvres protégées par le droit d'auteur sur les réseaux pair à pair (P2P). Ce mécanisme donne à une autorité administrative (aujourd'hui l'Arcom, anciennement la Hadopi) la possibilité de rapprocher des adresses IP collectées sur les réseaux P2P par des ayants droits avec les éléments d'identification des abonnés à Internet titulaires de ces adresses IP, conservés par les fournisseurs d'accès.

La CJUE avait été saisie dans le cadre d'une procédure initiée par l'association La Quadrature du Net qui demandait à la cour de tirer les conséquences de sa jurisprudence du 6 octobre 2020, par laquelle elle avait jugé que la directive 2002/58 s'opposait à ce qu'une conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion soit effectuée pour des objectifs autres que la lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique ou la sauvegarde de la sécurité nationale.

Dans son arrêt C-470/21, la CJUE vient nuancer cette jurisprudence en insistant sur le caractère "grave" de l'ingérence, et ce qui permet de déterminant que l'ingérence est grave. En particulier, doit être considérée comme grave une ingérence qui permet de tirer des conclusions précises sur la vie privée des personnes, ce qui n'est pas le cas ou très à la marge pour des téléchargements et mises à disposition de fichiers piratés sur les réseaux P2P. Or, écrit la cour, "*la conservation généralisée et indifférenciée des adresses IP peut, le cas échéant, être justifiée par l'objectif de la lutte contre les infractions pénales en général lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs*".

La Cour cadre toutefois un tel traitement et impose des mesures techniques et organisationnelles de protection des données personnelles pour pouvoir considérer que l'ingérence n'est pas "grave" :

- assurer que chaque catégorie de données, y compris les données relatives à l'identité civile et les adresses IP, est conservée de manière pleinement séparée des autres catégories de données conservées ;
- garantir que, sur un plan technique, la séparation des différentes catégories de données conservées, notamment les données relatives à l'identité civile, les adresses IP, les différentes données relatives au trafic autres que les adresses IP et les différentes données de localisation, est effectivement étanche, moyennant un dispositif informatique sécurisé et fiable ;

Mise à jour des lignes directrices sur la vidéosurveillance

Vidéosurveillance

Poser une question

LU CNPD • 17/04/2024

La Commission nationale pour la protection des données (CNPD) informe qu'elle a mis à jour ses lignes directrices de 2018 sur la vidéosurveillance, pour tenir compte de sa jurisprudence et des lignes directrices du Comité européen de la protection des données (CEPD).

La CNPD a notamment apporté des précisions quant aux finalités qui pourraient motiver l'installation d'une vidéosurveillance, quant à la forme et le contenu de l'information à fournir aux personnes visées par la vidéosurveillance. Elle publie également des informations spécifiques pour la vidéosurveillance dans les copropriétés et pour le recours à des caméras factices. Dans ce dernier cas, la Commission recommande de ne pas en installer, principalement pour éviter des demandes d'exercices de droits ou des plaintes pour défaut d'information qui ne pourraient aboutir.

Les lignes directrices sur la vidéosurveillance rappellent en particulier que **toute personne susceptible d'entrer dans le champ de vision des caméras de vidéosurveillance doit être informée de la présence de celles-ci** avec :

1. un premier niveau de communication des informations les plus importantes via un panneau d'affichage bien visible ;
2. un deuxième niveau (par exemple un site internet vers lequel renvoie la panneau précité) qui fournit l'ensemble des informations obligatoires.

Un modèle de panneau (.pdf) est proposé par la CNPD.

Accès et Réutilisation des données

Le Garante Privacy sanctionne l'irrespect d'un droit d'accès du salarié aux documents qui le concernent

Droit d'accès

Poser une question

IT GPDP • 03/05/2024

Le *Garante Privacy* publie une décision en date du 7 mars 2024, par laquelle elle sanctionne la *Banca di Credito Cooperativa di Spinazzola* d'une amende de 20 000 euros pour n'avoir pas correctement respecté la demande d'exercice de droit d'accès à ses données formulée par un ancien employée.

La plaignante avait demandé à obtenir "*l'accès aux données personnelles contenues dans son dossier personnel, une copie de celui-ci et, en particulier, aux données contenues dans le dossier de la procédure disciplinaire (...) afin de connaître, de manière précise et ponctuelle, toutes les informations la concernant (données évaluatives et non évaluatives) concernant les faits et comportements (...) repris dans la sanction disciplinaire imposée par la Banque*". Or la banque avait gardé confidentiel le contenu d'une correspondance échangée entre elle et un tiers, qui était déterminant dans la décision de sanctionner le salarié, puisqu'elle l'accusait d'une violation du secret professionnel.

L'établissement **n'avait pas justifié son choix de ne pas transmettre cette correspondance** à son ancien employé. Interrogée par le *Garante*, la banque avait finalement expliqué qu'elle n'avait pas fourni cette documentation à l'ancien employé afin de protéger ses droits de la défense et la confidentialité des tiers concernés, ainsi que parce que le plaignant n'avait aucun intérêt à y avoir accès.

Or, le Garante rappelle que les lignes directrices du CEPD sur le droit d'accès et la jurisprudence de la CJUE indiquent que "*le responsable du traitement ne doit pas refuser l'accès au motif ou en soupçonnant que les données demandées pourraient être utilisées par la personne concernée pour se défendre en justice*", et que le demandeur n'a pas à justifier de son intérêt à accéder à des données qui le concernent.

L'AP met en garde contre les pratiques de scraping contraires au RGPD

Réutilisation des données

Poser une question

NL AUTORITEITPERSOONSGEGEVENS.NL • 02/05/2024

L'*Autoriteit Persoonsgegevens* (AP) publie un manuel sur le scraping par les particuliers et les organisations privées, qui s'intéresse à la conformité au RGPD de ces activités consistant à collecter des données accessibles publiquement sur Internet pour les réunir dans une base de données. Pour l'autorité néerlandaise, "*le scraping constitue presque toujours une violation du règlement général sur la protection des données*".

L'AP précise qu'il est toujours interdit de réaliser du scraping pour :

- créer des profils d'internautes afin de les revendre ;
- récupérer des informations sur les comptes de médias sociaux protégés ou des forums privés ;
- récupérer des données à partir de profils de médias sociaux publics, dans le but de déterminer si ces personnes bénéficient ou non d'une certaine police d'assurance.

"*Un malentendu très répandu veut que le scrapping soit autorisé parce que tout ce qui se trouve sur l'internet est de toute façon accessible à tout le monde. Mais le fait que des informations vous concernant soient publiques ne signifie pas automatiquement que vous autorisez le scraping*", explique Aleid Wolfsen, président de l'AP. Le consentement préalable reste la règle à suivre par principe, sauf à être capable de justifier par exemple d'un intérêt légitime, qui ne peut jamais être le fait de développer le chiffre d'affaires de l'entreprise.

L'AP précise que le scraping à "usage domestique" est possible (puisque hors du cadre du RGPD), ou lorsque par exemple une organisation scrappe uniquement les messages qui la concerne pour réaliser une veille d'informations.

Merci à nos partenaires

DASTRA

la gazette des communes • des départements • des régions

isep
École d'ingénieurs du numérique

COMMERCE & CONSOMMATION LSA

L'USINEDIGITALE

L'USINENOUVELLE

WITIK

L'ARGUS de l'assurance

haas AVOCATS

PRINTEMPS DES dpo

PRINTEMPS DES dpo

Le 18 JUIN 2024 au Parc des Princes

https://www.printemps-des-dpo.com/