Sur les évaluations d'impact dans les politiques numériques

Description

Les évaluations ou analyses d'impact sont devenues des outils de politique publique présents dans de nombreux champs de l'action publique. Parfois considérées comme une caractéristique d'une « managérialisation » de la société[1], elles ont d'abord été utilisées dans le cadre de politiques environnementales avant d'être intégrées à la panoplie d'instruments utilisés dans le cadre des politiques de régulation des risques dans la société de l'information[2]. Les analyses d'impact sur la vie privée ont acquis de l'importance à partir des années 1990 en tant qu'instrument éthique permettant de vérifier l'efficacité des premières lois de protection de la vie privée et des données à caractère personnel[3]. En l'état actuel du droit de l'Union européenne, c'est l'article 35 du règlement général sur la protection des données (RGPD) qui impose aux acteurs concernés, dans certains cas, la conduite d'une étude d'impact en matière de protection des données.

> LES ANALYSES D'IMPACT SUR LA VIE PRIVÉE ONT ACQUIS DE L'IMPORTANCE À PARTIR DES ANNÉES 1990 EN TANT QU'INSTRUMENT ÉTHIQUE

Le Digital Services Act (DSA) adopté en 2022 et la proposition de règlement sur l'intelligence artificielle (IA), encore en cours de négociation, introduisent également des mécanismes qui rappellent l'évaluation d'impact. Toutefois, l'efficience de cet instrument reste questionnée. Dans quelle mesure impose-t-il à la personne qui se trouve dans l'obligation d'évaluer les impacts de son projet d'y renoncer, si les risques ne sont pas maîtrisés ? Quelle efficacité peut-on attendre d'un tel dispositif, en particulier à l'égard des systèmes d'intelligence artificielle (IA) à haut risque ?

Le présent article est une synthèse des échanges entre chercheurs de plusieurs disciplines qui ont eu lieu autour de cette question lors d'une journée d'études, organisée le 24 novembre 2022 par le Groupe de travail sur la gouvernance et la régulation d'internet du GDR Internet, IA et société du CNRS[4]. Ces échanges se sont concentrés en premier lieu sur la démarche de l'analyse d'impact définie dans le RGPD, avant d'aborder les évaluations d'impact dans le projet de règlement sur l'IA.

Dans le RGPD, des méthodes d'analyse d'impact hétérogènes aux résultats variables

Les articles 35 et 36 du RGPD exigent des responsables du traitement (RT) de données à caractère personnel la réalisation d'une analyse d'impact sur la protection des données (AIPD) de ceux de leurs projets qui

combinent des facteurs de risque.

LES AIPD ONT POUR FINALITÉ DE MINIMISER LES RISQUES POUR LES « DROITS ET LIBERTÉS »

Les AIPD ont pour finalité de minimiser les risques pour les « droits et libertés ». Bien que cette qualification fasse encore l'objet de débats doctrinaux, le consensus d'intégrer la jurisprudence de la Cour européenne des droits l'homme comme objectif cardinal semble être acquis en droit européen[5]. Toutefois, la réalité de sa mise en œuvre semble plus incertaine. L'annexe 2 des lignes directrices sur l'AIPD[6] éditées par l'article du Groupe Article 29 (devenu CEPD – Comité européen de la protection des données – ou EDPB – European Data Protection Board) illustre cette problématique. Ces dernières ont été adoptées en 2017, c'est-à-dire entre l'adoption du RGPD en 2016 et son entrée en application le 25 mai 2018. Cette temporalité significative explique, entre autres, le flou entourant cette annexe. Elle énonce, en une seule page, tous les principes à respecter pour la réalisation d'une AIPD conforme au texte européen. Succinctement, ces principes peuvent être regroupés en quatre catégories :

- le cycle de vie des données,
- les dispositions de l'article 5 du RGPD sur la conformité du traitement,
- les dispositions de l'article 32 du RGPD sur la sécurité informatique du traitement,
- l'appréciation des risques pour les « droits et libertés » et les mécanismes correctifs.

Une méthodologie respectant ces principes serait donc conforme aux dispositions de l'article 35 du RGPD. Le diable se cachant dans les détails, de grandes possibilités de modulation de l'étendue de l'appréciation restent ouvertes au RT de l'organisation concernée. En particulier, la rédaction de la dernière étape relative à l'analyse de risque offre au RT la latitude d'analyser les risques pour les droits et libertés ou bien de se limiter à une analyse des risques de cybersécurité et de leur impact sur les droits et libertés. La méthodologie proposée par le Groupe de travail Article 29 dans ses lignes directrices de 2017 ne fait d'ailleurs aucune référence à la recherche des risques pour les libertés qui seraient générés par un traitement de données intègres, disponibles et confidentielles (c'est-à-dire non sujettes à risque sur le terrain de la sécurité). Pourtant, l'objet d'une analyse d'impact sur les droits et libertés est conceptuellement d'évaluer les risques que génère un traitement de données pour ces droits et libertés, une fois qu'a été vérifiée la conformité de ce traitement ou de ce projet à la législation applicable, dont le RGPD et l'obligation de sécurité que ce dernier pose en son article 32. L'évaluation des seuls risques posés par un défaut de sécurité constitue un dévoiement de l'instrument qui empêche, en réalité, l'analyse d'impacts de remplir son objectif.

On observe ainsi qu'en fonction de l'orientation « politique » donnée à l'évaluation ou analyse, l'assiette de ces risques diminue radicalement selon que ceux-ci sont recherchés eu égard à tous les aspects dutraitement, ou uniquement dans le cadre d'un risque de sécurité impactant les données.

L'ÉVALUATION DES SEULS RISQUES POSÉS PAR UN DÉFAUT DE SÉCURITÉ CONSTITUE UN DÉVOIEMENT DE L'INSTRUMENT

Ceci conduit à différencier « analyse d'impact sur la vie privée » et « analyse d'impact relative à la protection des données », dont le périmètre se voit ainsi largement amputé, alors que ces deux examens, conceptuellement, devraient renvoyer à la même réalité[7].

Le choix consensuel du G29 de 2017 situe ses lignes directrices au milieu du gué – c'est-à-dire entre une réelle volonté de protection de la vie privée des personnes concernées promues par certains États membres (l'Allemagne, par exemple) sans pour autant constituer un obstacle à l'innovation promue par d'autres États membres (la France et l'Irlande). Ainsi, on constate une multitude de méthodologies appliquées à partir de ces lignes directrices. Celles-ci ont pu être proposées par des autorités de protection des données personnelles[8], par des agences nationales de cybersécurité[9], par des cabinets de conseil ou encore par divers centres de recherche européens, à l'instar de PRIAM[10]. Les besoins ou la complexité du traitement de données personnelles influent sur le recours à une méthodologie préexistante ou à une élaboration *ad hoc*. À une méthodologie succincte axée sur les risques découlant de défaillances de cybersécurité, ainsi que la propose la Cnil (Commission nationale de l'informatique et des libertés)[11], peut être opposée une méthodologie plus exhaustive, davantage orientée sur la protection de la vie privée, telles que le sont les méthodes PRIAM ou encore MANDOLA[12]. Un même traitement de données personnelles soumis à l'une ou l'autre de ces approches ne fera pas apparaître les mêmes risques, en tout cas pas en même nombre. À cette problématique s'ajoute celle de la subjectivité du RT. L'annexe 2 des lignes directrices du G29 sur l'AIPD lui laisse en effet le soin d'évaluer *« la probabilité et la gravité »* des risques, discrétionnairement et souverainement. Certes, les lignes directrices imposent une obligation d'appréciation *« du point de vue des personnes concernées »*, mais cette formule laconique ne semble pas faire échec à la possibilité, pour le RT, de conduire l'analyse dans ses intérêts propres.

UNE MINIMISATION DES RISQUES PAR LE RESPONSABLE DU TRAITEMENT DANS SON AIPD DEMEURE SOUVENT UNE RÉALITÉ

N'oublions pas que l'AIPD s'insère, par principe, dans des procédures de conformité. En d'autres termes, sa réalisation n'a qu'une finalité probatoire : il s'agit d'une formalité administrative visant à démontrer la

conformité de procédures internes à l'organisation concernée, ce qui a pour effet d'écarter l'obligation de publication des AIPD.

LA CEDH MET À LA CHARGE DES ÉTATS UNE OBLIGATION POSITIVE D'ASSURER UNE PROTECTION EFFECTIVE DES LIBERTÉS FONDAMENTALES

En conséquence, et sous réserve que ledit traitement soit scrupuleusement examiné par la Cnil, une minimisation des risques par le responsable du traitement dans son AIPD demeure souvent une réalité, d'une part, car l'obligation de conformité peut s'avérer coûteuse en termes de ressources humaines et financières, d'autre part, car elle peut être perçue comme contraire aux intérêts du RT ou de son projet. De nombreux risques sont donc écartés au bénéfice du déploiement effectif du traitement pour assurer le retour sur investissement à l'entreprise, au détriment du respect des droits et libertés.

Des exigences de « nécessité » et de « proportionnalité » conformes aux dispositions de la CEDH

Quelle que soit la méthode retenue, une AIPD devrait conceptuellement viser à appliquer les exigences de nécessité et de proportionnalité posées dans la Convention européenne de sauvegarde des droits de l'homme et libertés fondamentales (CEDH)[13]. En effet, le RGPD doit être conforme au droit primaire qui organise la protection des droits et libertés fondamentaux. *A minima*, il ne peut le contredire. Idéalement, il est supposé le transposer *in concreto* au contexte des traitements de données à caractère personnel. En effet, la CEDH – premier texte de référence en matière de protection des libertés en Europe – met à la charge des États une obligation positive d'assurer une protection effective des libertés fondamentales dans le rapport des individus entre eux. Cette obligation s'ajoute à leur obligation de s'abstenir de porter aux libertés des limitations arbitraires[14].

Les conditions de la protection des droits et libertés fondamentaux dits « conditionnels », en premier lieu de la protection de la vie privée, peuvent être résumées en ces deux exigences : celles de « nécessité » et de « proportionnalité ». Plus précisément, la vie privée *lato sensu*[15] ne peut légitimement souffrir de limitation que si cette dernière poursuit efficacement une finalité déterminée, de manière strictement minimisée, l'ensemble devant encore être entouré de garanties permettant à cette affirmation d'avoir lieu[16]. Les dispositions du RGPD sont donc supposées constituer le cadre de référence des correctifs devant être mis en œuvre afin qu'un traitement de données à caractère personnel respecte les droits et libertés fondamentaux. Une telle lecture permet notamment de comprendre des notions telles que celles de « compatibilité » et d'« intérêt légitime », qui ne visent en définitive qu'à s'assurer de la nécessité et de la proportionnalité, respectivement, d'une finalité spécifique et d'un traitement pouvant se dispenser du consentement de la personne concernée.

L'ARTICLE 35 DU RGPD EXIGE DE DILIGENTER UNE AIPD DANS LES SITUATIONS DE TRAITEMENT GÉNÉRANT DES RISQUES PARTICULIERS POUR LES LIBERTÉS

Cette lecture permet surtout d'appréhender l'objet et le contenu de l'article 35 du RGPD qui exige de diligenter une AIPD dans les situations de traitement générant des risques particuliers pour les libertés. Cet article impose de manière cohérente une nouvelle analyse de nécessité et de proportionnalité, avec pour corollaire la définition d'éventuels correctifs additionnels à déployer, dont les résultats renforceront l'adéquation au respect des dispositions du RGPD.

L'article 35 impose également une analyse de risque pour les droits et libertés, en utilisant une méthode d'analyse de risque afin de vérifier que les données traitées et les libertés pouvant être impactées par le traitement ne soient pas exposées à qui vise en réalité à vérifier plus en détail la proportionnalité du traitement, en s'assurant qu'elle n'est pas affaiblie par des risques, pour les données traitées et les libertés, qui n'auraient pas été décelés durant les analyses de conformité RGPD et de proportionnalité.

Le projet de règlement sur l'IA : des évaluations d'impact à la gestion de risque

Les différentes approches évoquées plus haut, incluant les standards internationaux en matière de gestion de risque, comme les normes ISO 27001, 27005 et 31000, auxquelles se conforment, par exemple, la méthode de gestion des risques de l'ENISA (European Network and Information Security Agency – Agende de l'Union européenne chargée de la sécurité des réseaux et de l'information) et la méthode EBIOS publiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), ont pour points communs trois éléments de contenu :

- l'identification et l'évaluation des risques associés à un projet,
- la détermination des mesures permettant de les réduire,
- la mesure du degré d'acceptabilité de ces risques, lequel peut conduire à la décision d'abandon du projet du fait de risques résiduels trop élevés.

Ces mêmes éléments sont repris dans les textes européens récemment adoptés ou proposés pour régir les technologies et services numériques. Ainsi, les articles 34 et 35 du règlement sur les services numériques obligent désormais les très grandes plateformes et les très grands moteurs de recherche en ligne à conduire des évaluations de risque et à proposer de manière correspondante des mesures d'atténuation de ceux-ci.

L'UTILISATEUR EST DÉFINI COMME LA PERSONNE QUI DÉPLOIE UN SYSTÈME

D'IA, ET NON COMME LA PERSONNE QUI EST CONCERNÉE PAR CE DÉPLOIEMENT

Dans la proposition de règlement sur l'IA de la Commission européenne, plusieurs dispositions dessinent un schéma au moins pour partie similaire. En effet, lorsqu'un système d'IA est identifié comme étant « à haut risque » à la lumière des définitions contenues dans le texte, l'article 17 de la proposition de règlement impose au fournisseur du système d'IA de maintenir une documentation portant entre autres sur les procédures de test et d'évaluation de ce système ainsi que sur les systèmes de gestion des risques prévus à l'article 9 de la proposition. Ce dernier prévoit notamment *« l'identification et l'analyse des risques connus et prévisibles associés à chaque système d'IA à haut risque »* et *« l'adoption de mesures appropriées de gestion des risques »*. En cas de risques résiduels, une information du seul utilisateur du système d'IA est prévue, et non de l'ensemble des personnes potentiellement concernées, lesquelles peuvent être des tiers à la relation entre le fournisseur et son utilisateur. En effet, l'utilisateur est défini par ce texte comme la personne qui déploie un système d'IA, et non comme la personne qui est concernée par ce déploiement.

L'article 15(1) de cette proposition prévoit également que *« la conception et le développement des systèmes d'IA à haut risque sont tels qu'ils leur permettent, compte tenu de leur destination, d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de manière cohérente à cet égard tout au long de leur cycle de vie »*.

Là encore, l'expression « niveau approprié » emprunte la sémantique de la gestion de risque. Sans autre précision, ceci peut être perçu comme poursuivant une logique différente de celle proposée dans le RGPD, lequel insère l'examen des risques au cœur d'une vérification plus globale de la nécessité et de la proportionnalité d'une action potentiellement limitative de droits et de libertés (en l'occurrence, un traitement de données à caractère personnel).

À travers ce choix, la Commission européenne semble vouloir contourner l'exigence de respect absolu des libertés – peut-être par crainte de l'entrave qu'elle pourrait constituer pour les développements technologiques – en pariant sur la quête d'une robustesse dont la démonstration apporterait un gage scientifique de fiabilité.

À TRAVERS CE CHOIX, LA COMMISSION EUROPÉENNE SEMBLE VOULOIR CONTOURNER L'EXIGENCE DE RESPECT ABSOLU DES LIBERTÉS

Ceci, en niant largement, au passage, les conclusions de l'étude d'impact qui accompagne le texte de la proposition (même si cette étude reste partielle), de même que les conclusions du Comité (EDPB) et du contrôleur (European Data Protection Supervisor – EDPS) européens à la protection des données[17].

Les articles 19 et 43 instaurent bien une procédure d'évaluation de la conformité, laquelle renvoie vers une

annexe VI, qui, elle-même, renvoie vers l'article 17 et à l'ensemble des exigences énoncées au titre III, chapitre 2, mais les circonvolutions rédactionnelles adoptées par les auteurs de la proposition ne prévoient pas clairement la troisième étape de l'évaluation d'impact, qui peut conduire à une décision d'abandon. L'espoir en la capacité de démontrer la robustesse, entre autres caractéristiques techniques, des algorithmes d'IA, semble avoir remplacé cette étape.

Ceci nous paraît particulièrement regrettable, d'autant que la recherche en informatique démontre l'illusion de ce solutionnisme, particulièrement en matière de systèmes d'apprentissage automatique.

L'impossible robustesse en matière d'IA

Un axe de recherche important en informatique consiste à étudier les algorithmes résultant de l'apprentissage automatique (supervisé, non supervisé ou par renforcement). C'est en effet l'algorithme appris qui est déployé par l'utilisateur d'un système d'IA. Or, il existe l'espoir d'une solution technique à la question de la robustesse des algorithmes appris, qu'il s'agisse d'une solution permettant de garantir des niveaux de performances ou de mesurer ce qui constituerait un score de robustesse intelligible. Ce score, couplé à un seuil, permettrait alors au régulateur de définir des cas d'emplois et des niveaux de sûreté associés adéquats. Cela se pratique pour l'aéronautique, où l'on peut définir et évaluer une probabilité de panne, que l'on se charge de minimiser jusqu'à atteindre un seuil jugé acceptable. C'est de cet espoir que proviennent les prérequis inaccessibles demandés par les actuelles tentatives de régulation de l'IA.

LES ADVERSARIAL ATTACKS SONT LA MANIFESTATION DU MANQUE DE ROBUSTESSE INTRINSÈQUE DES ALGORITHMES APPRIS

Pourtant, la robustesse des algorithmes appris, c'est-à-dire la propension de ces algorithmes à maintenir leurs performances dans un monde réel incertain, est intrinsèquement impossible à garantir. D'abord, parce que dans ses formulations les plus simples, garantir la robustesse est un problème aussi difficile à résoudre que le problème initial pour lequel, faute d'une meilleure solution, on a recours à l'apprentissage automatique. Mais aussi parce que les modèles d'apprentissage employés conduisent nécessairement à la création de biais involontaires – ou fausses corrélations – dont l'activation provoquera inévitablement des erreurs de jugement[18].

Les *adversarial attacks* sont la manifestation la plus poignante du manque de robustesse intrinsèque des algorithmes appris. Elles consistent à altérer de façon subtile et intelligente l'entrée que l'on donne à l'algorithme appris pour le conduire à commettre une erreur ; une erreur au sens où un humain qui se verrait présenter l'entrée altérée (généralement une image) ne percevrait aucune différence avec l'originale et proposerait une réponse correcte. Ces attaques malicieuses tirent parti des pentes importantes (ou gradients importants) dans la fonction de décision induite par l'algorithme[19]. Si les *adversarial attacks* exploitent ces

caractéristiques pour induire des erreurs de façon contrôlées, on peut aussi tomber dans ces situations de façon aléatoire ; par exemple à cause d'une perturbation comme un reflet inhabituel sur une photo qui conduit alors à une erreur. Ainsi, une petite altération bien choisie peut exploiter ces caractéristiques et conduire à une très forte variation dans la décision. L'existence de ces attaques prouve que de telles pentes existent et qu'elles sont utilisables expérimentalement. Si elles sont présentées sous la forme d'attaques délibérées et malicieuses, il n'en demeure pas moins qu'une altération involontaire peut aussi conduire à dévaler l'une de ces pentes produites par l'apprentissage pour produire une erreur. De récents travaux ont notamment montré que les reflets sur des photos prises à travers une vitre ou encore le bruit issu d'une compression d'image peuvent régulièrement provoquer des erreurs sans pour autant changer la nature de l'entrée pour un œil humain[20].

En ce qui concerne les algorithmes d'apprentissage, il s'agit de découvreurs automatiques de corrélations. Le processus d'optimisation conduisant à la formation d'un algorithme appris utilisable n'est qu'une méthode pour extraire et consigner des règles de décisions fondées sur les corrélations découvertes dans une fonction apprise. C'est en réalité un cas de métaprogrammation. Le problème est que dès qu'une quantité importante de données est disponible, il existe nécessairement des (fausses) corrélations aléatoires parmi celles-ci, qui peuvent être capturées par l'apprentissage. Cela conduit à l'existence de règles absurdes dans la fonction de décision inférée à l'issue du processus d'apprentissage[21].

Puisqu'il est impossible de certifier la robustesse des algorithmes appris par des moyens techniques, il s'agit de circonvenir les risques en construisant un cadre d'emploi minimisant ces risques. En pratique, si les études d'impacts ne garantissent pas la robustesse des algorithmes d'apprentissage, elles contournent le problème en vérifiant *a priori* la portée et la gravité potentielles des dysfonctionnements de ces algorithmes, et leur caractère « nécessaire et proportionné », « dans une société démocratique. » Mais la proposition de règlement sur l'IA de la Commission ne semble pas aller au bout de la nature juridique et politique de cette logique des évaluations d'impacts. Elle maintient au contraire l'illusion d'un « technosolutionnisme » pourtant voué à l'échec, au détriment de la protection des libertés fondamentales et de l'enjeu démocratique qu'elle véhicule.

Les critiques formulées à l'égard des études d'impact environnementales n'ont guère été retenues avant leur transposition dans les politiques publiques liées au numérique. Inversement, le caractère éprouvé de l'évaluation de nécessité et de proportionnalité telle que pratiquée par la CEDH est souvent nié ou affaibli, au profit de méthodes qui s'avèrent dès lors plus partielles ou qui font reposer la confiance sur un solutionnisme technologique auquel les recherches en informatique invitent à renoncer.

L'ABSENCE D'OBLIGATION DE PUBLICATION DES RÉSULTATS D'ÉVALUATION PRÉVIENT TOUTE POSSIBILITÉ DE CONTRÔLE DÉMOCRATIQUE

En conséquence, des méthodes hétérogènes d'évaluation d'impacts permettent d'offrir un certain blanc-seing à l'usage de technologies, alors même qu'elles sont contestables, tant dans leurs composantes qu'eu égard à la subjectivité d'analyse permise par leur laconisme ou leur opacité. Par ailleurs, l'absence d'obligation de publication des résultats d'évaluation et de leur revue régulière prévient toute possibilité de contrôle démocratique. Il n'est pourtant pas rare que ces méthodes soient préconisées par des instruments juridiques qui pourtant, dans le même temps, réaffirment la nécessité de protéger les droits et libertés fondamentaux.

A contrario de cette forme d'instrumentalisation que nous pouvons observer, une véritable protection des droits et libertés fondamentaux, dans le cadre du développement de technologies qui sont souvent de plus en plus intrusives, nous paraît appeler un renouveau de la prise de conscience de l'intérêt et de l'efficacité des exigences de nécessité et de proportionnalité, dont l'analyse est idéalement complétée par une analyse de risque pour les droits et libertés, ainsi que le préconisaient déjà, dans les années 1990, les premières méthodes de PIA.

DES EFFORTS DE VULGARISATION DES NOTIONS DE NÉCESSITÉ ET DE PROPORTIONNALITÉ SERAIENT BIENVENUS, POUR DÉMONTRER LEUR FLEXIBILITÉ ET LEUR CAPACITÉ À ACCOMPAGNER L'INNOVATION

L'article 35 du RGPD est en particulier compatible avec une telle prise de conscience, même si ses termes ne vont pas au-delà des étapes élémentaires et communes aux méthodes d'analyse d'impact sur la vie privée. En complément, des efforts de vulgarisation des notions de nécessité et de proportionnalité seraient bienvenus, tant pour expliciter le contenu de ces notions que pour démontrer leur flexibilité et leur capacité à accompagner l'innovation. Cette prise de conscience éviterait d'avoir à mettre en question régulièrement la *« maturité démocratique »*[22] de nos sociétés et l'aptitude de certains instruments juridiques à *« saper, voire* […] *détruire, la démocratie au motif de la défendre »*[23], la proposition de règlement sur l'IA en étant l'un des emblèmes.

Maxime Darrin est doctorant a? ILLS (International Laboratory on Learning Systems, Montre?al) et a? Universite? Paris-Saclay.

Estelle De Marco est docteure en droit prive? et sciences criminelles, consultante chez Inthemis (cabinet spe?cialise? en conformite? juridique et e?thique).

Jonathan Keller est docteur en droit public, inge?nieur de recherches, Institut Polytechnique de Paris, Institut Mines Te?le?com, Telecom Paris, de?partement des sciences e?conomiques et sociales.

Julien Rossi est mai?tre de confe?rences a? l'Universite? Paris 8, chercheur au CE?MTI (Centre d'e?tudes

sur les me?dias, les technologies et l'internationalisation.

Sources :

1. Jean-Robert Alcaras, Christèle Marchand, Guillaume Marrel, Magali Nonjon, « La "performance sociale" comme horizon ? Les directeurs départementaux de l'aide et de l'action sociales et leurs perceptions de la managérialisation », *Revue française d'administration publique* (RFAP), 2011/4, p. 757 et s.
2. Les origines environnementales de l'analyse d'impact vie privée ont été relatées entre autres par Roger Clarke, « Privacy Impact Assessment : Its Origins and Development », *Computer Law & Security Review* 25, 2, avril 2009, p. 123-135.
3. David Wright et Paul De Hert, « Privacy Impact Assessment », *Law, Governance and Technology Series 6*, Springer, 2012, p. 117 et s.
4. « Les évaluations d'impact comme instrument de politiques publiques » (https://netgouv.hypotheses.org/215).
5. Étienne Picard, « "Les droits et libertés" : un couple paradoxal », *in Mélanges en l'honneur de Frédéric Sudre, Les droits de l'homme à la croisée des droits,* LexisNexis, juin 2018, 860 p.
6. Groupe de travail de l'article 29, lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, WP 248 rév. 01, 4 avril 2017.
7. Estelle De Marco, *Comparative study between directive 95/46/EC & the GDPR including their relations to fundamental rights (Étude comparée de la directive 95/46/CE et du RGPD incluant leurs liens avec les droits fondamentaux),* mars 2018, livrable D2.10, projet UE INFORM (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, (https://www.inthemis.fr/ressources/INFORM_D2.10_Comparative_analysis_GDPR_Dir9546EC.pdf), section 2 p. 15 et s. ; Estelle De Marco, *A DPIA is a PIA : consequences in terms of implementation and scope (Une EIDP est une EIVP : conséquences en termes de mise en œuvre et de périmètre),* mars 2019, publication rédigée dans le cadre du projet INFORM (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866Publi DPIA, (https://www.inthemis.fr/ressources/A-DPIA-is-a-PIA.html).
8. À notre connaissance, seules la Cnil française et l'ICO (Information Commissioner's Office) du Royaume Uni pré-Brexit en avaient édité. Concernant les lignes directrices françaises, voir Claire Levallois-Barth, Jonathan Keller, « Analyse d'impact relative à la protection des données : le cas des voitures connectées », rapport de recherche, Institut Mines-Télécom, Télécom ParisTech, CNRS LTCI, 2021 (hal-03456922).
9. *Bundesamt für Sicherheit in der Informationstechnik,* abrévié BSI ; voir Claire Levallois-Barth, Jonathan Keller, op. cit.
10. Voir par exemple la méthodologie « Privacy Risk Analysis » (PRIAM) de Sourya Joyee De et de Daniel Le Métayer. PRIAM : [Research Report] RR-8876, Inria – Research Centre Grenoble – Rhône-Alpes, 2016 (hal-01302541) analysée dans le rapport sus-cité.

11. Avec la méthodologie « PIA » et le logiciel open source associé (https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd).
12. Voir respectivement la méthodologie « PIA » et le logiciel open source associé (https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd) ; Université de Bruxelles, Laboratory for Data Protection & Privacy Impact Assessments (https://dpialab.wordpress.com) ; Estelle De Marco, *Privact Impact Assessment of the MANDOLA outcomes* (Analyse d'impact sur la vie privée des résultats du projet MANDOLA), juillet 2017, livrable D2.4a, projet UE MANDOLA, GA n° JUST/2014/RRAC/AG/HATE/6652 (https://mandola-project.eu/publications), section 3.1.
13. Voir Estelle De Marco, *Comparative study between directive 95/46/EC & the GDPR including their relations to fundamental rights, op. cit.,* section 2.4.2.2, en particulier p. 83.
14. Voir, par exemple, Cour EDH, X. et Y c. Pays-Bas, 26 mars 1985, req ; n° 8978/80, § 23 (https://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-62162) ; Antoinette Rouvroy, « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », in Studies in Ethics, Law and Technology, volume 2, issue 1, 2008 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984), article 3, p. 9.
15. Estelle De Marco, *Comparative study between directive 95/46/EC & the GDPR including their relations to fundamental rights, op. cit.,* section 2.2.1.1 p. 18 ; Estelle De Marco, *The definition of private life (La définition de la vie privée),* mars 2019, publication rédigée dans le cadre du projet UE INFORM précité (https://www.inthemis.fr/ressources/definition-of-private-life.html).
16. Sur les notions d'efficacité, de finalité, de minimisation et de garanties, voir, par exemple, respectivement Groupe de travail de l'article 29, avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, WP 211, 27 février 2014, n° 3.19 et 3.26 (l'efficacité du traitement de données pour atteindre sa finalité doit en particulier être supérieur ou égal à l'impact sur la vie privée et les libertés) ; *Ibid*., n° 3.13 ; Jeremy McBride, « Proportionality and the European Convention on Human Rights », *in* Evelyn Ellis (ed.), *The principle of Proportionality in the Laws of Europe* (*Le principe de proportionnalité dans les lois d'Europe*), Hart Publishing, 1999, p. 23 et s. ; Cour EDH, plén., Marckx c. Belgique, 13 juin 1979, req. n° 6833/74, §31 (la Cour évoque des garanties « rendant possible » l'exercice de la vie privée. Ces garanties doivent en particulier être « adéquates et suffisantes » : voir, par exemple, Cour EDH plén., 6 septembre 1978, req. no 5029/71, Klass et autres c. Allemagne, § 50). Sur l'ensemble de ces aspects, voir Estelle De Marco et Aeris, « Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law (Impacts de l'usage des technologies biométriques et comportementales de surveillance de masse sur les droits humains et l'Etat de droit) », rapport pour le groupe des Verts/ALE auprès du Parlement européen, février 2022, https://extranet.greens-efa-service.eu/public/media/file/1/7487, section 4.1.3 p. 64.

17. Voir Estelle De Marco et Aeris, *Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law, op. cit.,* respectivement section 5.2.4, 2 (« Reversal of ECHR and EUCFR values », p. 99), sections 5.2.1, 2 et 5.2.2, et sections 5.2.3 et 5.2.4, 2.
18. Concernant les biais et erreurs générés par les systèmes de reconnaissance biométrique, voir Estelle De Marco et Aeris, « Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law », op. cit., section 5.3.4.
19. Kevin Scaman, Aladin Virmaux, « Lipschitz regularity of deep neural networks : analysis and efficient estimation », 32nd Conference on Neural Information Processing Systems (NeurIPS 2018), Montréal, Canada.
20. Dan Hendrycks, Thomas Dietterich, « Benchmarking Neural Network Robustness to Common Corruptions and Perturbations », International Conference on Learning Representations (ICLR), 2019.
21. Cristian Calude, Giuseppe Longo, « The Deluge of Spurious Correlations in Big Data », in Giuseppe Longo (dir.), *Lois des dieux, des hommes et de la nature,* Nantes, Spartacus-IDH, 2015.
22. Michel Bénichou, « Le résistible déclin du secret », *La Prévoyance des avocat*s (LPA), 20 juin 2001, no 122, p. 3 s.
23. CEDH, plén., 6 septembre 1978, req. n° 5029/71, Klass et autres c/ Allemagne, § 49.

Categorie

1. Articles & chroniques

date créée
6 juin 2023
Auteur
maximedarrin