Analyse d'impact relative à la protection des données dans l'Union européenne : une protection des personnes plus solide en complétant le nouveau cadre juridique

Kloza, Dariusz; Van Dijk, Niels; Gellert, Raphaël Maurice; Borocz, Istvan Mate; Tanas, Alessia; Mantovani, Eugenio; Quinn, Paul

Published in:
d.pia.lab Policy Brief

Publication date:
2018

Document Version:
Final published version

Analyse d'impact relative à la protection des données dans l'Union européenne : une protection des personnes plus solide en complétant le nouveau cadre juridique

d.pia.lab Note de Politique N° 1/2017

Dariusz KLOZA, Niels VAN DIJK, Raphaël GELLERT, István BÖRÖCZ,
Alessia TANAS, Eugenio MANTOVANI et Paul QUINN
Laboratoire bruxellois pour l'analyse d'impact relative à la protection des données et de la vie privée (d.pia.lab)

Le présent document émet des recommandations permettant à l'Union européenne (UE) de compléter l'obligation d'effectuer une analyse d'impact relative à la protection des données (AIPD), telle que définie dans le Règlement Général sur la Protection des Données (RGPD), dans le but d'arriver à une protection plus solide des données à caractère personnel. En avril 2016, l'UE a mis la dernière main à la partie essentielle de la réforme du cadre juridique visant la protection des données personnelles. L'Union prépare actuellement les mesures de mise en œuvre et les lignes directrices donnant pleinement effet aux nouvelles dispositions juridiques avant leur mise en application à partir de mai 2018. Parmi d'autres « nouveautés », cette réforme introduit l'obligation juridique de réaliser une AIPD. Or, cette obligation comporte quelques faiblesses. La présente note cherche à y remédier en apportant des informations supplémentaires à l'actuel processus d'élaboration de politiques, notamment en proposant de « meilleures pratiques » permettant d'arriver à un type d'analyse d'impact générique, qui pourrait être préconisé pour plusieurs domaines (section II). La section III présente une première évaluation de la manière dont ces meilleurs pratiques se rapportent à l'obligation spécifique de procéder à une analyse d'impact, c'est-à-dire, l'AIPD, déterminée par le RGPD. Ces deux sections sont précédées de quelques informations générales sur les analyses d'impact en tant que telles. La section I présente en ce sens une définition et un aperçu historique, ainsi que les avantages et inconvénients des analyses d'impact en général. Enfin, la section IV fournit des recommandations en vue de compléter l'obligation de procéder à une AIPD telle que requise par le RGPD. Ces recommandations proposent notamment : (1) d'élargir la portée de l'obligation de mener une AIPD dans le cadre du RGPD ; (2) de développer des méthodes pour réaliser une telle analyse ; (3) d'établir auprès des autorités de protection des données (APD) des « centres de références » entièrement axés sur la réalisation des AIPD. La présente note de politique s'adresse surtout aux décideurs politiques actifs au niveau de l'UE et des Etats Membres, nonobstant l'intérêt potentiel qu'il pourrait soulever auprès de leurs homologues dans d'autres parties du monde.

I. INTRODUCTION

I.1. CONTEXTE

La loi européenne sur la protection des données à caractère personnel récemment réformée obligera les responsables du traitement à effectuer une analyse d'impact des opérations de traitement de données qui sont « *susceptible[s] d'engendrer un risque élevé pour les droits et libertés des personnes physiques* » chaque fois que leurs données personnelles sont traitées. Cette nouvelle obligation, dénommée « analyse d'impact relative à la protection des données » ou en abrégé « AIPD », est censée jouer un rôle essentiel dans le système de protection des droits fondamentaux mis en place au sein de l'UE. La relative nouveauté de cette obligation et la mise en vigueur imminente de la nouvelle loi ne forcent pas seulement les parties prenantes à s'adapter rapidement, mais également suscitent de vifs débats tant au sein de l'UE qu'au-delà : les décideurs politiques et les APD sont intéressées à mieux déterminer les contours exacts de la politique relative à l'AIPD, alors que les organisations privées et publiques sont plutôt concentrées sur leur mise en conformité vis-à-vis de cette nouvelle obligation.

I.2. HISTORIQUE

Une analyse d'impact est un outil utilisé pour évaluer les éventuelles conséquences d'une initiative sur une préoccupation ou des préoccupations sociétale(s) pertinente(s), si cette initiative présente un danger pour ces préoccupations, permettant de prendre une décision bien informée sur l'opportunité et les conditions de mise en œuvre de l'initiative en question ; le but

 | ISSN 2565-9936

ultime étant de protéger ces préoccupations sociales de façon adéquate.

Les analyses d'impact et les autres techniques d'évaluation similaires ont été développées en réponse à l'émergence de dangers nouveaux, pas encore entièrement connus à ce moment-là, mettant en péril des préoccupations tant individuelles que collectives. Elles visent donc à remédier à l'incertitude et au risque. Par exemple, les évaluations de technologie (ET), développées aux Etats-Unis dans les années 1960, étaient initialement utilisées comme un outil permettant aux scientifiques de mieux cerner les conséquences éventuellement dangereuses de leurs inventions. Ultérieurement, ces évaluations ont été institutionnalisées, d'abord comme un moyen pour assurer la sécurité générale des produits, et ensuite, progressivement, comme un outil portant sur un plus large éventail de préoccupations relatives à la société et à la technologie. De la même manière, les évaluations des incidences sur l'environnement (EIE) sont apparues comme une réponse à la dégradation graduelle de l'environnement naturel. Les expériences positives avec les ET et EIE ont contribué à leur popularité dans le monde entier et ont résulté dans une prolifération, voire institutionnalisation, d'évaluations d'impact dans les domaines les plus divers, allant des systèmes de santé à la protection des données à caractère personnel, en passant par la réglementation (gouvernance), la sécurité nationale et les pratiques de surveillance.

La prolifération des études d'impact sur la vie privée (EIVP) et des analyses d'impact relative à la protection des données (AIPD) peut être attribuée à trois facteurs principaux : (1) la place toujours plus envahissante des nouvelles technologies dans la vie individuelle des personnes et dans les relations sociales ; (2) l'importance croissante du traitement des données personnelles à des fins d'économie contemporaine, de sécurité nationale, de recherche scientifique, de développement technologique, de relations interpersonnelles, etc. ; (3) la confiance amoindrie à l'égard des nouvelles technologies et de la manière dont celles-ci sont exploitées par les organisations publiques et privées. Et pourtant, quelques 50 ans après l'apparition des premières analyses d'impact, celles-ci ne font toujours pas l'objet de pratiques clairement tranchées. Il n'y a que quelques domaines, tels que les EIE, où elles ont évolué jusqu'à acquérir une expérience considérable et une certaine maturité. Dans d'autres domaines, leur identité est toujours en phase de développement (par exemple, les analyses d'impact « sociétal » ou les AIPD) ou leur introduction est encore en phase de revendication (par exemple, les droits humains).

Les EIVP, et ultérieurement les AIPD, ont fait leur apparition dans les années 1990 et se sont institutionnalisées sous plusieurs formes et à plusieurs niveaux de contraintes, d'abord dans les juridictions de droit coutumier (anglo-saxon), telles que la Nouvelle-Zélande, l'Australie et le Canada. En Europe, le Royaume-Uni était le premier pays à développer en 2007 une politique relative à l'EIVP. A ce stade, l'UE a mis en place deux politiques d'EIVP sectorielles et facultatives : la première concerne les applications de l'identification par radio fréquence (RFID, *Radio Frequency Identification*) (2009), et la seconde les « réseaux intelligents » (*smart grids*) (2012). Dans le paquet pour améliorer la réglementation (2015), la vie privée et les données à caractère personnel forment l'un des nombreux thèmes faisant l'objet d'analyses au sein des processus législatifs et politiques de l'UE. Suite à l'approbation du RGPD et de la directive relative à la protection des données traitées dans les domaines de la police et de la justice pénale (2016), une politique imposant la réalisation d'une analyse d'impact sera introduite pour la première fois dans le domaine de la protection des données personnelles, et ce à partir de mai 2018. Ce développement n'est pas un phénomène isolé. En effet, la modernisation récemment finalisée de la « Convention 108 » du Conseil de l'Europe, et la nouvelle loi relative à la protection des données proposée en Suisse (si adoptée dans son état actuel) introduisent toutes les deux une politique similaire.

I.3. AVANTAGES

Les mérites des analyses d'impact résident principalement dans leur contribution à (1) la prise de décision informée et (2) la protection des préoccupations sociétales. La première catégorie d'avantages attire généralement les organisations publiques et privées car elle leur fait profiter des bénéfices de la réflexion anticipative, *ex ante*. Les analyses permettent à ce type d'organisations de réfléchir tant sur les conséquences de leurs initiatives projetées que sur les moyens pour minimiser, voire éviter les effets négatifs ou imprévus, avant que ceux-ci ne se produisent (à travers un « système d'alerte précoce »), ce qui leur permet non seulement de faire des économies mais aussi de gagner la confiance du public. En outre, les analyses d'impact permettent de faciliter la mise en conformité avec les exigences légales et autres exigences réglementaires telles que les normes. Etant une « obligation de meilleurs efforts », elles constituent également une évidence de diligence raisonnable, ce qui peut limiter, voire exclure, toute responsabilité juridique. Ces analyses d'impact démontrent également que ces organisations assument leur responsabilité (*accountability*) vis-à-vis des autorités réglementaires, dont le travail sera partiellement facilité. Enfin, les analyses d'impact, à condition d'être effectuées de manière transparente, permettent aux organisations d'attirer la confiance du public en montrant qu'elles prennent les préoccupations sociétales au sérieux. Ainsi, le secteur privé recourt souvent aux analyses d'impact pour prouver sa responsabilité sociale.

La deuxième catégorie d'avantages concerne les gouvernements. Les analyses d'impact aident ceux-ci à remplir leur mission consistant à offrir une protection pratique et efficace des préoccupations sociétales pertinentes – telles que certains droits humains, dont la

vie privée – en faveur de l'individu en particulier et de la société en général. Pour les personnes physiques, les analyses d'impact sont des moyens qui leur permettent de faire entendre leurs préoccupations, par exemple à travers la participation publique, ce qui renforce la justice procédurale. En effet, les analyses d'impact cherchent à concilier les intérêts de diverses parties et contribuent de la sorte à dessiner une « ligne rouge ténue » entre des intérêts légitimes mais à première vue incompatibles, tels que la sécurité nationale et la protection des données à caractère personnel (comme c'est le cas des AIPD), ou des intérêts qui sont à première vue en concurrence, tels que l'économie nationale et la protection de l'environnement (comme c'est le cas des EIE). Comparées à d'autres outils de protection, les analyses d'impact fournissent une portée de protection plus étendue que les vérifications de conformité, souvent réduites à de simples exercices de « cases à cocher ».

I.4. INCONVÉNIENTS

Certains critiques avancent que les analyses d'impact constituent un fardeau inutile et une surcharge administrative, qui alourdissent une bureaucratie déjà envahissante, engendrent des dépenses superflues et génèrent des délais dans la prise de décision, voire même un ralentissement du processus de développement. Il n'est donc pas étonnant que l'un des souhaits souvent exprimés consiste à les rendre rapides, simples et bon marché. Les adversaires soulignent la complexité du processus d'analyse dans la pratique et les difficultés que celui-ci amène, tout comme le manque d'expérience pratique et les conseils et contrôles minimalistes ou non-existants. Ils s'interrogent sur leur valeur ajoutée par rapport aux autres techniques d'évaluation telles que les contrôles de conformité, et mettent en question leur efficacité, en signalant le large pouvoir d'appréciation par rapport à l'éventuelle conduite des analyses et de la méthode utilisée à cet effet.

D'autres griefs portent sur le fait que les analyses d'impact sont utilisées juste « pour la forme » afin d'être en règle avec une exigence réglementaire ; qu'elles sont uniquement effectuées avec un minimum d'efforts ; ou qu'elles servent seulement à légitimer des initiatives intrusives. En outre, les organisations ont parfois tendance à mener leurs analyses *in abstracto* au lieu de les utiliser comme un moyen permettant d'étudier les conséquences de leurs initiatives projetées. Elles confondent souvent les analyses d'impact avec les audits. Les organisations considèrent à tort que les conséquences ne concernent qu'elles-mêmes (en termes de risques financiers ou de réputation), et oublient souvent d'évaluer aussi les effets de leurs initiatives en fonction des personnes et du grand public. Une dernière critique porte sur le fait que les analyses d'impact sont souvent réalisées trop tard, c'est-à-dire, lorsque l'élaboration d'une initiative ne peut plus être influencée de manière significative. Certains opposants laissent entendre que l'étendue des analyses d'impact, lorsqu'elles sont obligatoires, est trop restreinte, laissant ainsi un trop grand nombre d'activités hors de leur portée. De plus, les analyses d'impact réalisées manquent le plus souvent de transparence, c'est-à-dire que le processus dans son ensemble est opaque, difficile à comprendre à cause de son haut niveau de complexité technique, et que les résultats finaux et les recommandations sont difficiles, voire impossible, à trouver. Souvent, elles n'incluent pas la participation publique ou ne lui donne pas assez de portée, ce qui rend la participation publique dénuée de sens.

II. MEILLEURES PRATIQUES POUR LES ANALYSES D'IMPACT

A partir d'une étude comparative des analyses d'impact telles que pratiquées à travers plusieurs domaines, les auteurs tentent d'esquisser les éléments constituant les « meilleures pratiques » pour mener une évaluation ; celles-ci servent de base à la création d'un type d'analyse d'impact générique, à préconiser pour plusieurs domaines. Cet exercice permet aux auteurs d'évaluer dans la section suivante l'obligation de mener une AIPD dans le cadre du RGPD.

1. L'analyse d'impact est un processus systématique, mené selon une méthode appropriée, et effectué en temps opportun. Elle est entamée en amont du cycle de vie d'une seule initiative ou de plusieurs initiatives similaires (telles qu'une technologie proposée ou une mesure législative), et en tout cas avant le déploiement de celle(s)-ci ; elle se poursuit tout au long du cycle de vie des initiatives et, le cas échéant, est réexaminée à mesure que la société change, les dangers évoluent et les connaissances se développent. Elle constitue donc un « instrument vivant », influençant constamment la conception de l'initiative qui fait l'objet de l'analyse d'impact.

2. Les analyses d'impact étudient les éventuelles conséquences d'une initiative par rapport aux préoccupations sociétales, tant individuelles que collectives : dans le cas d'une AIPD, il s'agit de la protection de personnes chaque fois que leurs données personnelles sont traitées, alors que dans le cas d'une EIE, il s'agit de l'environnement naturel et humain. L'évaluation préliminaire (définition du périmètre, définition du contexte), la participation publique et la consultation d'experts contribuent à tenir à jour la liste des préoccupations. Au besoin, plusieurs types d'analyses d'impact sont effectuées pour une initiative donnée, lesquelles sont menées autant que possible de manière intégrée.

3. Les initiatives n'exigent pas toutes la réalisation d'une analyse d'impact. Le besoin est déterminé par des facteurs tels que la nature, la portée, le contexte et l'objectif de l'initiative faisant l'objet de l'analyse, ainsi que par le nombre et le type de personnes touchées par l'initiative, etc. Les analyses d'impact sont cependant obligatoires au moins pour toutes les initiatives susceptibles d'avoir des effets

très négatifs pour des préoccupations sociétales pertinentes.

4. Il n'existe pas de méthode « panacée » pour la réalisation d'analyses d'impact. Ce qui importe, c'est de trouver la méthode d'analyse appropriée, permettant d'arriver à une compréhension optimale et à un traitement adéquat de tous les effets potentiels de l'initiative envisagée. Ces méthodes couvrent un large éventail d'approches, allant de la gestion quantitative ou qualitative du risque jusqu'à la prospective scientifique, en passant par la planification à l'aide de scénarios. Elles peuvent également être appuyées par un vérification de conformité portant sur les obligations juridiques ou autres exigences réglementaires telles que les normes techniques.

5. Le processus de l'analyse d'impact identifie, décrit et étudie non seulement les conséquences éventuelles, tant positives que négatives, prévues ou inattendues, de l'initiative faisant l'objet de l'analyse, mais également les solutions possible (recommandations) permettant de traiter ces conséquences.

6. Les analyses d'impact constituent des « obligations de meilleurs efforts ». Comme il n'est pas possible de réduire les conséquences négatives en termes absolus – tout comme il n'est pas possible de maximiser celles qui sont positives – les organisations y répondent au meilleur de leurs possibilités, en fonction des connaissances et, dans une mesure raisonnable, de leurs ressources disponibles.

7. L'évaluateur (ou l'équipe d'évaluateurs) du processus d'analyse d'impact a les connaissances et l'expertise nécessaires afin de pouvoir le mener à bien, conformément au type d'analyse d'impact concerné.

8. Le processus d'analyse d'impact est documenté (plus précisément, par écrit) et est raisonnablement transparent. La transparence implique notamment un accès public et libre, c'est-à-dire, illimité, à toutes les informations pertinentes. Le grand public est informé du processus d'analyse et ses termes de référence, plus spécifiquement de la méthode utilisée, ainsi que de l'avancement de l'analyse. L'ébauche et la version finale du rapport de l'analyse d'impact sont facilement accessibles, sans préjudice des informations qui doivent légitimement rester secrètes.

9. Le processus d'analyse d'impact est délibératif, ce qui se manifeste essentiellement à travers la participation publique. Les parties prenantes externes, aussi représentatives que possible – qu'elles soient des personnes et/ou des organisations de la société civile concernées ou touchées par l'initiative faisant l'objet de l'analyse – sont identifiées et informées de manière significative sur le processus, et leurs opinions sont activement recherchées et dûment prises en considération à travers la consultation et la co-décision. Les informations fournies et recherchées sont solides, précises et complètes. Les particuliers et/ou leurs représentants disposent de moyens effectifs pour faire entendre leurs voix, notamment devant une juridiction ou un tribunal similaire. En parallèle, toutes les personnes actives au sein de l'organisation initiatrice de l'initiative qui fait l'objet de l'analyse, c'est-à-dire les parties prenantes internes, participent au processus d'analyse aux mêmes conditions. Toute exception à la participation publique, si elle s'avère justifiée, est interprétée de manière restrictive.

10. L'organisation soutenant l'initiative est responsable du processus de l'analyse d'impact. Les décideurs au sein de l'organisation sélectionnent, entre autres, la méthode d'analyse et les évaluateurs chargés de sa réalisation. A la fin du processus, ils approuvent le rapport final de l'analyse d'impact et supervisent ensuite la mise en œuvre des solutions proposées (recommandations). Une entité externe telle qu'une autorité réglementaire ou un organe d'audit examine minutieusement la qualité du rapport. Les critères de sélection sont transparentes. De cette manière, l'organisation est en mesure de démontrer que le processus a été mené de manière satisfaisante. Lorsque la réalisation de l'analyse d'impact est obligatoire, la non-conformité et les mauvaises pratiques sont sanctionnées de manière proportionnelle.

11. L'indépendance de l'évaluateur – qu'il soit externe ou interne – est garantie : il n'accepte, ni ne sollicite des instructions de quiconque, et dispose de suffisamment de ressources, que ce soit en termes de temps, argent, effectifs, connaissance et expertise, locaux et infrastructure.

12. Le processus de l'analyse d'impact est suffisamment simple, c'est-à-dire pas indûment compliqué. La méthode est un instrument au service de ceux qui l'utilisent. Pour cette raison, elle est structurée, cohérente et facile à comprendre ; et elle évite d'être trop prescriptive et compliquée, et de faire un usage abusif de ressources. Il y a un compromis inhérent entre la simplicité d'utilisation, la technicité et la précision de l'analyse.

13. Le processus de l'analyse d'impact s'adapte aux caractéristiques de l'initiative faisant l'objet de l'évaluation et aux particularités de l'organisation initiatrice. En effet, il n'existe pas de méthode passe-partout, et celle-ci est fonction du type et de la complexité de l'analyse (développement technique, recherche scientifique, projets de loi), ou du type et du nombre de personnes concernées ou touchées (la sécurité nucléaire est tout autre chose que la protection des données personnelles). Si possible, l'analyse est associée à des analyses d'impact portant sur d'autres domaines. L'analyse s'adapte également à des différences géographiques et culturelles.

14. Le processus de l'analyse d'impact est inclusif. Ce critère garantit que le plus grand nombre de parties prenantes, de préoccupations sociétales pertinentes et de phases de développement (tant au niveau de l'initiative qu'au niveau du processus) soient intégrés au processus d'analyse, et ce en fonction des préoccupations sociétales et le type d'évaluation. L'analyse est basée sur les connaissances de spécialistes et non-spécialistes (à travers la participation publique).

15. Le processus de l'analyse d'impact est réceptif. La méthode et le processus évoluent en tirant des leçons d'expériences antérieures acquises dans d'autres techniques d'évaluation (telles que les ET, les EIE, la gestion des risques, etc.), et en tenant compte de connaissances issues de disciplines associées (telle que la loi) et des changements de la société.

16. Pour porter leurs fruits, les analyses d'impact nécessitent un environnement favorable. Elles ont besoin d'un soutien de haut niveau de la part des responsables politiques et des décideurs, et d'un esprit de coopération entre les parties prenantes externes et internes. Les régulateurs fournissent une orientation et de l'assistance pratique au cours du processus d'analyse sous la forme de formations adéquates, de lignes directrices, d'explications et de conseils.

LES DISPOSITIONS RGPD PERTINENTES

- « Lorsqu'un type de traitement ... est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue … une analyse de l'impact ... » (Art 35.1)
- « L'autorité de contrôle établit ... une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise » (Art 35.4)
- « L'analyse contient au moins ... les mesures envisagées pour faire face aux risques ... compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées » (Art 35.7.d)
- « Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu ... » (Art 35.9)
- « Les violations … font l'objet d'amendes administratives pouvant s'élever jusqu'à 10.000.000 EUR ... » (Art 83.4)

III. EVALUATION DE L'OBLIGATION D'UNE AIPD DANS LE CADRE DU RGPD

Les auteurs examineront à présent le type d'analyse d'impact prévu par l'Art. 35 du RGPD, dénommé AIPD, à la lumière des meilleures pratiques d'un type d'analyse d'impact générique, tel que décrit dans la section précédente. Un accent particulier sera mis sur quelques-unes des spécificités de la nouvelle loi relative à la protection des données qui sera d'application au sein de l'UE ; il s'agit notamment du principe de la responsabilité (*accountability*); de l'« ancrage légal » de l'AIPD ; et de l'approche fondée sur le risque.

1. Le RGPD, dans son champ d'application, oblige les responsables du traitement, assistés au besoin par les sous-traitants, d'effectuer une AIPD pour certaines opérations de traitement « *susceptible[s] d'engendrer un risque élevé pour les droits et libertés des personnes physiques* ». Le non-respect de cette obligation est lourdement sanctionné. Ainsi, le RGPD déplace l'attention des mesures réactives aux mesures anticipatives.

2. En obligeant les responsables du traitement à effectuer une AIPD « *avant le traitement* » et à revoir leurs analyses dans les cas où les risques et/ou les opérations de traitement auraient changé, le RGPD implique que l'AIPD est un processus systématique et un « instrument vivant ».

3. La portée de l'obligation de mener une AIPD suit celle du RGPD : celui-ci protège le droit fondamental à la protection des données personnelles tout comme les autres droits et libertés fondamentaux concernés par le traitement des données personnelles. Le RGPD portant uniquement sur le traitement des données à caractère personnel, il ne contient pas d'éléments permettant de sauvegarder d'autres préoccupations sociétales pertinentes, découlant, par exemple, du traitement de données anonymes. De cette manière, la portée de la protection est incomplète.

4. Le RGPD exige la réalisation d'une AIPD en cas de « *risque élevé* ». Cette obligation limite la portée d'une AIPD à quelques types d'opérations de traitement de données. Les APD peuvent étendre ce répertoire, mais elles peuvent aussi le limiter. Mais le RGPD permettant un niveau de protection supérieur aux données sensibles et aux données relatives aux condamnations pénales et aux infractions ; cet élément est repris dans la portée de l'obligation de mener une AIPD.

5. Le RGPD réunit les concepts de « risque » et de « droit », lesquels appartiennent traditionnellement à des domaines de connaissance et d'organisation sociétale très différents. Les droits sont définis et spécifiés par les tribunaux à travers de concepts juridiques, souvent de manière rétroactive après des violations alléguées de la loi. Le concept de risque appartient à la gestion des risques telle qu'appliquée au sein d'organisations. Il est souvent défini à travers des concepts scientifiques de probabilité dans une tentative de traiter de manière prospective les éventuelles conséquences futures. Le rapprochement de ces deux concepts crée un nouvel objet d'analyse pour lequel il n'existe pas encore une méthode approuvée.

6. Le RGPD a introduit dans la terminologie de la protection de données celle issue de la gestion du risque en utilisant des termes tels que « risque élevé », « vraisemblance », « impact » ou « sévérité ». Or, la signification de ces termes reste très vague dans le contexte de la protection des données personnelles, ou

– dans un sens plus large – des « *droits et libertés de personnes physiques* ». Certains de ces termes pourraient être dénués de relevance ou seraient difficiles à concilier avec la loi sur la protection des données et pourraient créer des complications artificielles pour le processus d'analyse. Par conséquent, il faudra leur donner une nouvelle signification autonome.

7. Le RGPD associe les AIPD à la consultation préalable lorsque les processus d'analyse indiquent des risques résiduels présentant un niveau de risque élevé. Il confère de vastes pouvoirs aux APD, lesquelles peuvent fournir des avis écrits et même interdire les opérations de traitement envisagées si des mesures supplémentaires s'avèrent nécessaires.

8. Le RGPD fournit des critères lorsque la réalisation d'une AIPD est nécessaire. Il offre cependant très peu d'indications sur le processus même et reste largement muet sur les aspects méthodologiques. Cette approche minimaliste était supposée constituer un « ancrage légal » qui devait être complétée par des méthodes spécifiques propres à la réalisation des AIPD. Or, certains éléments-clés ne sont pas encore tranchés.

9. Le RGPD exige qu'un responsable du traitement consulte, au cours du processus d'AIPD, les personnes concernées ou leurs représentants tout en respectant les éléments qui doivent légitimement rester secrets. Or, cette obligation est comparativement faible étant donné que celle-ci s'applique uniquement « *le cas échéant* » et par rapport aux seules « *personnes concernées* » (et donc pas au grand public) ; en plus, le RGPD ne dit pas quand une telle situation se produit. Le RGPD présente encore d'autres lacunes. Ainsi, il omet de spécifier quelles sont exactement les personnes qui devraient être consultées et comment on pourrait les identifier. Il ne donne aucune indication sur les conditions dans lesquelles les personnes concernées peuvent faire appel à des représentants, ni sur ce qui peut être considérée comme représentativité légitimée, ni sur les moyens de contestation à leur disposition.

10. Le RGPD ne dit rien sur la transparence du processus d'AIPD. Plus spécifiquement, il n'y aucune obligation de rendre publics l'ébauche, la version finale du rapport, ou un résumé de ceux-ci.

11. Le RGPD contient une vague exigence obligeant le Comité Européen de la Protection des Données (CEPD) à publier des lignes directrices afin de « *contribuer à l'application cohérente du […] règlement* » ; dans ce sens, l'exigence de publier et de tenir à jour les méthodes de réalisation des AIPD pourrait relever du champ d'application de cette obligation. Ces méthodes ne pourraient être évaluées qu'au moment de leur publication.

12. Le RGPD laisse aux responsables du traitement un certaine liberté d'appréciation quant à la réalisation d'une AIPD, notamment par rapport à deux aspects. Ainsi, ils peuvent déterminer eux-mêmes si les opérations de traitement envisagées correspondent bien aux critères de risque élève prédéfinis ; et si les risques résiduels présentent un niveau de risque assez élevé pour motiver la consultation préalable. Du fait de la nature même du processus de gestion de risque, les responsables du traitement sélectionnent aussi, entre autres, la méthode d'analyse et les mesures d'atténuation des risques. Il est également aux responsables du traitement de désigner les évaluateurs ayant les compétences nécessaires pour effectuer l'évaluation, et de garantir leur indépendance. A part cela, ils doivent assurer la solidité du processus intégral et documenter celui-ci de manière appropriée. Les responsables du traitement assument l'entière responsabilité de ces choix méthodologiques.

13. Le RGPD est censé tenir compte des différences géographiques et culturelles relatives à la protection des données à caractère personnel. Plus particulièrement, les dérogations nationales se rapportant, par exemple à la liberté d'expression, doivent être prises en considération lors du processus d'évaluation.

14. Le RGPD reste largement muet sur les rôles et responsabilités qui doivent être assumés au cours de la réalisation d'une AIPD. Surtout le rôle du délégué à la protection des données (DPD) n'est pas très clair. Le RGPD lui demande d'assister l'évaluateur dans sa tâche en lui donnant des conseils par rapport au processus d'analyse, mais sans fournir davantage de précisions à ce sujet.

IV. RECOMMANDATIONS

De tout ce qui précède, il ressort que l'obligation de mener une AIPD dans le cadre du RGPD répond déjà à un certain nombre de critères de meilleures pratiques généralement appliquées en matière d'analyses d'impact, mais qu'elle présente aussi des lacunes par rapport à un certain nombre d'autres aspects. Pour cette raison, les auteurs formuleront dans ce qui suit des recommandations destinées spécifiquement aux décideurs politiques européens afin de leur permettre de « combler le vide ». Ces recommandations sont au nombre de trois : les auteurs proposent d'abord d'élargir la portée de l'obligation à mener une AIPD. Ensuite, ils recommandent de développer plusieurs méthodes pour conduire une AIPD, ce qui permettra de remédier à certaines omissions et lacunes de l'Art. 35 du RGPD. Enfin, les auteurs proposent que le CEPD et les APD nationales prennent le rôle principal et deviennent les « centres de référence » en matière d'AIPD. Les auteurs sont également réalistes par rapport à la probabilité que leurs recommandations soient effectivement mises en œuvre. En effet, ces recommandations reposent sur des pouvoirs de réglementation et de consultation délégués que le RGPD confie tant au CEPD qu'aux APD nationales et régionales.

A. Portée

1. La liste des opérations de traitement de données relevant de l'obligation AIPD devrait être étendue afin d'éviter que les opérations intrusives

n'échappent à un examen rigoureux. Cette liste devrait être tenue à jour.

2. Pour des initiatives intrusives qui sont hors de la portée de l'obligation de mener une AIPD dans le cadre du RGPD, mais qui relèvent d'un autre type d'évaluation, tel que l'EIVP, la solution recommandée consisterait à effectuer l'autre type d'analyse.

B. Méthodes

3. Le CEPD est le mieux placé pour publier et tenir à jour les méthodes à suivre pour mener une AIPD qui seront communes à l'ensemble de l'UE, alors que les APD nationales et régionales sont le mieux placées pour adapter celles-ci au contexte local, tout en respectant les objectifs d'harmonisation du RGPD. Etant donné la relative nouveauté de l'obligation de mener une AIPD, ces méthodes devraient être élaborées soigneusement.

4. Elles devront être adaptatives :

a. Il devrait y avoir plusieurs méthodes pour mener une AIPD. Elles devraient être adaptées de manière à refléter la diversité des secteurs industriels et gouvernementaux, et donc aussi des risques spécifiques inhérents à ceux-ci. Ces méthodes doivent respecter les différences juridiques, culturelles, sociales et éthiques présentes au sein des différents territoires.
b. Elles doivent également être revues périodiquement à la lumière des expériences acquises en matière des AIPD et des changements du contexte social.

5. Ces méthodes devraient notamment porter sur :

a. les conditions relatives à la participation publique : ceci implique l'identification de toutes les parties prenantes, y compris les personnes concernées ; la fourniture des informations ; les moyens pour écouter et prendre en considération leurs opinions ; les moyens de contestation à leur disposition.
b. les conditions relatives à la documentation et la transparence : ceci comprend la documentation écrite ; l'accès aux informations relatives à l'AIPD ; les registres publics des AIPD effectuées ; les informations qui doivent légitimement rester secrètes ; etc.
c. la clarification de la terminologie utilisée, plus particulièrement par rapport aux termes vagues exprimant la quantité (par exemple, « à grande échelle ») et le risque (par exemple, « risque pour un droit », « risque élevé » et « vraisemblance ») ;
d. des précisions sur les compétences et l'indépendance de l'évaluateur ;
e. des précisions sur les rôles et responsabilités des parties prenantes impliquées dans le processus de l'AIPD, plus particulièrement les rôles et responsabilités des responsables du traitement, des sous-traitants et des DPD.

6. Les méthodes devraient être réceptives et capables d'évoluer en tirant des leçons d'expériences de tentatives d'analyse d'impact antérieures. Plus particulièrement, il faudrait prendre en compte des leçons *juridiques* par rapport au fond (la substance) et la forme (la procédure) afin de faire de l'AIPD un outil d'évaluation à part entière. Les leçons portant sur la procédure concernent l'accès public aux informations pertinentes, la consultation publique et les moyens de contestation. Les leçons relatives à la substance concernent les critères d'identification de risque (par exemple, à partir du droit de la protection de données), les différents types de risques (droit de l'environnement), les nouveaux types de préjudices ou d'impact (droit de la responsabilité délictuelle) ou les degrés de probabilité (droit de la preuve).

7. Il faudrait définir les conditions de surveillance (audit) du processus d'AIPD à mettre en place par les APD (et/ou d'autres parties prenantes) ; celles-ci concernent tant les aspects relatifs au processus (tels que la qualité de l'AIPD) que ceux relatifs aux acteurs (tels que le pouvoir d'appréciation assigné aux responsables du traitement).

C. Connaissance et expertise

8. Tant le CEPD que les APD nationales et régionales devraient créer et gérer des « centres de référence » ayant la connaissance et l'expertise nécessaires en matière de l'AIPD. Ces centres devraient coopérer et s'intégrer dans une communauté plus large axée sur l'analyse d'impact, notamment en s'alignant sur des associations et/ou conférences actives dans ce domaine.

Tout compte fait, les AIPD sont de simples outils d'aide à la prise de décision. Ces analyses d'impact ne sont pas de solutions « panacées ». La qualité de protection qu'elles peuvent fournir dépend de plusieurs facteurs : de la manière dont elles sont utilisées par les responsables du traitement et les sous-traitants ; du soutien qu'elles reçoivent de la part des décideurs politiques ; et enfin, de la surveillance mise en place par les APD et les tribunaux. Certes, ces analyses d'impact présentent des difficultés. Mais si elles sont exécutées de manière honnête et si les décideurs politiques disposent de méthodes appropriées, bénéficiant d'assistance, de conseils et de surveillance, les analyses d'impact contribueront à mettre en place une protection plus solide des données à caractère personnel.

SELECTION DE SOURCES PERTINENTES

Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review* 25, no. 2 (2009): 123–135, doi:10.1016/j.clsr.2009.02.002.

David Wright and Paul De Hert (eds.), *Privacy Impact Assessment* (Dordrecht: Springer, 2012), doi: 10.1007/978-94-007-2543-0.

Dariusz Kloza, Niels van Dijk, and Paul De Hert, "Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies," in *Smart Grid Security*, ed. Florian Skopik and Paul Smith (Waltham, MA: Elsevier, 2015), 11–47, doi:10,1016/B978-0-12-802122-4,00002-X.

Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, "A Risk to a Right? Beyond Data Protection Risk Assessments," *Computer Law & Security Review* 32, no. 2 (2016): 286–306, doi:10.1016/j.clsr.2015.12.017.

Raphaël Gellert, "We have always managed risks in data protection law: understanding the similarities and differences between the rights-based and the risk-based approaches to data protection," *European Data Protection Law Review* 2, no. 4 (2016): 481–492, doi:10.21552/EDPL/2016/4/7.

István Böröcz, "Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras," *European Data Protection Law Review* 2, no. 4 (2016): 467–480, doi:10.21552/EDPL/2016/4/6.

A PROPOS DE D.PIA.LAB

Le **Laboratoire bruxellois pour l'analyse d'impact relative à la protection des données et de la vie privée**, ou **d.pia.lab**, relie la recherche fondamentale, méthodologique et appliquée, donne des formations et prodigue des conseils stratégiques et politiques sur les analyses d'impact relevant des domaines de l'innovation et du développement technologique. Quoique les aspects juridiques de la protection des données personnelles et de la vie privée constituent les axes prioritaires de nos activités, celles-ci englobent également d'autres disciplines telles que l'éthique et la philosophie ainsi que les études de surveillance et les études des sciences, des technologies et de la société (STS). Créé en novembre 2015, le Laboratoire fait partie intégrante de et s'appuie sur l'expérience du Research Group on Law, Science, Technology & Society (LSTS) établi au sein de la Vrije Universiteit Brussel (VUB), Belgique.

La base de connaissance que le Laboratoire a acquise en matière d'analyses d'impact est fondée sur plusieurs projets de recherche déjà finalisés ou en cours de réalisation tels que PIAF, ADVISE, EPINET, MATHISIS, FORENSOR, CANDID (cofinancés par l'UE), PARENT (cofinancé par l'UE et Innoviris) y compris « A Risk to A Right? Exploring a new notion in data protection law » et « Rights in Design. The Technological Reconstitution of Privacy and Data Protection » (financé par le Fonds Wetenschappelijk Onderzoek – Vlaanderen). Les opinions exprimées dans la présente note ne reflètent pas nécessairement celles des bailleurs de fonds.

Nous tenons à remercier les membres suivants du d.pia.lab Network pour leurs précieux commentaires sur une version antérieure de la présente note : Brendan van Alsenoy, Roger Clarke, Kjetil Rommetveit et Claudia Quelle. Merci également à Pradeepan Sarma pour avoir révisé la version anglaise du texte. Traduction en français par Sleutelwoord | Mot-clé bvba (mai 2018).

dpialab.org | dpialab@vub.ac.be