Executive Summary n° 2

Analyse d'Impact relative à la Protection des Données : le cas des voitures connectées[1]

Janvier 2022

Claire LEVALLOIS-BARTH
Coordinatrice de la Chaire VP-IP, Enseignante-chercheuse en droit, IMT/Télécom Paris

Jonathan KELLER
Ingénieur de recherches en droit, IMT/Télécom Paris

L'Analyse d'Impact relative à la Protection des Données (AIPD), telle qu'imposée dans certaines circonstances par l'article 35 du RGPD[2], est une opération complexe qui vise à identifier, puis à atténuer les risques éventuels liés au traitement de données personnelles vis-à-vis des droits et libertés des personnes concernées.

Dans certains contextes, comme celui des véhicules connectés, des problématiques supplémentaires interviennent, notamment lorsque plusieurs responsables de traitements sont impliqués.

1 Résumé du rapport de recherche « Analyse d'Impact relative à la Protection des Données : le cas des voitures connectées », Claire LEVALLOIS-BARTH et Jonathan KELLER, novembre 2021, 192 pages.
[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JOUE L 119, 4 mai 2016, pp. 1–88.

Claire *LEVALLOIS-BARTH* et Jonathan *KELLER* ont, au sein de la Chaire *Connected Cars & Cybersecurity* (C3S) de Télécom Paris et en partenariat avec la Chaire Valeurs et Politiques des Informations Personnelles (VP-IP) de l'IMT, mené des recherches pour identifier la ou les méthodologies les plus adaptées. Ils ont étudié leur articulation et leur adaptation afin de parvenir à une méthodologie optimale.

Pour répondre concrètement à cette problématique, un cas pratique comprenant trois hypothèses de traitements de données personnelles effectués par différents acteurs a été défini. Ce cas pratique appelé **Biomem** a permis de tester les **quatre méthodologies d'analyse d'impacts** qui nous ont semblées les plus pertinentes, à savoir les méthodologies :

- **CNIL** établie par la Commission Nationale Informatique et Libertés,
- **PRIAM** (*Privacy Risk Analysis Methodology)* proposée par les chercheurs français D. JOYEE DE et D. LE METAYER de l'INRIA,
- **BSI** du *Bundesamt für Sicherheit in der Informationstechnik* allemand,
- **NIST** du *National Institute of Standards and Technology* étasunien.

L'efficacité de ces méthodologies, notamment en ce qui concerne les mesures d'atténuation des risques, a ainsi été évaluée. La recherche démontre qu'il n'existe pas de « méthodologie-miracle ». Chaque méthodologie présente des avantages et des inconvénients, ce qui rend son application concrète, ou son examen par une autorité de contrôle nationale, problématique. Cette situation s'explique notamment par le fait que les Lignes directrices concernant l'analyse d'impact relative à la protection des données publiées par le Comité Européen de Protection des Données (CEPD), qui regroupe les autorités de protection des données et notamment la CNIL, se veulent méthodologiquement neutre pour apprécier les risques éventuels liés au traitement de données personnelles. Elle provient également de l'absence d'indicateurs permettant de déterminer et de quantifier précisément l'étendue des risques (assiette du risque, probabilité et gravité).

Cas pratique Biomem, dispositif d'infodivertissement dans un véhicule connecté

Le service Biomem correspond à une application téléchargeable sur un dispositif d'infodivertissement installé dans un véhicule connecté.

Est retenue comme définition d'un « véhicule connecté » celle proposée par le Pack de conformité pour le véhicule connecté de la CNIL, à savoir : « *Véhicules qui communiquent avec l'extérieur (applications mobiles, autres véhicules, infrastructure, etc.) traitant des données personnelles collectées via les capteurs des véhicules, les boîtiers télématiques ou les applications mobiles, que les données soient traitées à bord des véhicules ou exportées vers un serveur centralisé* ».

Après souscription au service Biomem, l'application utilise le dispositif technique vidéo présent dans le véhicule pour identifier par reconnaissance faciale les passagers adultes ou mineurs afin de faciliter leur accès au service de vidéo à la demande (VOD) auquel ils sont abonnés.

De plus, le service Biomem propose des contenus associés à des points d'intérêts se situant sur le trajet réalisé par le véhicule lorsque la localisation est activée par le conducteur. Ces contenus sont sélectionnés via une mise aux enchères des données de localisation auprès d'annonceurs publicitaires.

Ce cas pratique comprend trois traitements de données personnelles qui sont analysés sous l'empire du RGPD et de la directive (UE) « Vie privée et communications électroniques », dite directive *ePrivacy*. Différents types d'acteurs sont impliqués : les constructeurs de véhicules, les équipementiers, et les fournisseurs de services tiers, par exemple les fournisseurs de VOD.

Trois hypothèses sont alors déclinées dans lesquelles le service Biomen est :

- Une application développée et fournie par une partie tierce indépendante du constructeur et du fournisseur de VOD. L'utilisateur installe l'application sur le dispositif d'infodivertissement présent dans le véhicule et fourni par le constructeur (**Biomem-Indé**) ;
- Un service ancillaire fourni par le constructeur, ce dernier installant par défaut le logiciel Biomem dans le dispositif d'infodivertissement directement accessible sans téléchargement préalable (**Biomem-Constructeur**) ;
- Une application développée et fournie par le fournisseur de VOD, cette application étant installée par l'utilisateur sur le dispositif d'infodivertissement (**Biomem-VOD).**

Traitements de données personnelles dans le cas pratique Biomem

Le cas pratique Biomen comprends trois traitements de données personnelles.

Le premier traitemen, qui correspond à la création du profil utilisateur, « personne concernée » au sens du RGPD, n'est guère problématique.

Le deuxième traitement concerne la reconnaissance faciale. Il interroge sur les niveaux du recueil du consentement et des garanties de sécurité informatique exigées. Toutefois le traitement de données biométriques restant sous le contrôle exclusif de la personne concernée, ce traitement relève de l'exemption domestique, exonérant ainsi le responsable du traitement de nombreuses obligations.

Enfin, le troisième traitement porte sur les données de localisation. Il est spécifiquement régi par la directive *ePrivacy*. Toutefois, la qualification de « service de la société de l'information » exclue l'application de cette directive pour la majorité des traitements envisagés.

Les quatre étapes d'une Analyse d'Impact relative à la Protection des Données

La réalisation d'une AIPD nécessite de se référer à deux Lignes directrices du CEPD, celles relatives aux AIPD et celles relatives à la protection des données personnelles dès la conception et par défaut (ci-après « Lignes directrices DPbDD »). En effet, les Lignes directrices DPbDD adoptées en 2019 affinent de nombreuses terminologies utilisées par les Lignes directrices AIPD de 2017. De surcroît, elles invitent à réaliser une analyse d'impact afin de respecter le principe de protection des données par défaut.

Les Lignes directrices AIPD établissent une liste d'informations que le responsable de traitement, responsable *en dernier ressort* même s'il fait appel au délégué à la protection des données (DPO), au directeur de la sécurité des systèmes d'informations (DSI) ou à d'éventuels sous-traitants, doit renseigner. Une classification en quatre étapes est possible, à savoir :

1. La description exhaustive des modalités techniques et juridiques du traitement (flux de données, détermination du traitement, supports) pour identifier les vulnérabilités ; lors de cette étape, le responsable de traitement détermine à partir d'une liste de critères fixés notamment par les Lignes directrices AIPD si le traitement est « susceptible d'engendrer un risque élevé » et donc si le traitement doit faire l'objet d'un AIPD. En pratique, cette appréciation reste à sa discrétion.
2. L'appréciation de la nécessité du traitement de données et de la proportionnalité des mesures pour assurer le respect des droits et libertés des personnes concernées ;
3. L'analyse du risque en tant que telle, cette étape reposant en grande partie sur une approche portant sur les impacts analysés à partir d'évènements calculés en termes de vraisemblance ou de gravité.
4. Une présentation des mesures d'atténuation des risques, lesquelles doivent répondre à l'« état des connaissance » tout en ayant un coût raisonnable, par le DPO et les autres « parties intéressées » comme le DSI.

Cependant, bien que manifestation du principe clé de responsabilité (ou *accountability* en anglais), la réalisation d'une AIPD rencontre de nombreux obstacles. Le responsable de traitement se voit imposer une obligation de moyen renforcée en ce qui concerne sa réalisation et une obligation de résultat pour ce qui est de la démonstration de la documentation écrite de toutes les mesures garantissant que les traitements de données personnelles effectués sont conformes à la réglementation.

Les lignes directrices AIPD sont loin de répondre à toutes les questions opérationnelles, en particulier en ce qui concerne l'appréciation des risques.

L’appréciation des risques

La principale difficulté réside dans l’absence de détermination précise du risque dans toutes ses dimensions : assiette, occurrence ou probabilité, échelle de gravité. Ainsi, selon que l’on réalise une Analyse d’Impact relatives à la Protection des Données (AIPD) à l’aide des méthodologies CNIL et BSI ou une Évaluation d’Impact sur la Vie Privée (EIVP) en recourant aux méthodologies PRIAM et NIST, l’appréciation du risque est effectuée avec des menaces correspondantes différentes même si l’on constate au final que l’assiette de risques converge.

La classification des menaces basées sur la sécurité informatique (accès /modification/disparition), telle que prônée par la CNIL, altère l’appréciation en se limitant aux seules obligations techniques. Au-delà de cette question de l’assiette du risque, celle de la typologie de risque limite également l’analyse, les risques étant considéré alternativement, et rarement cumulativement, comme internes à la structure (ex : salarié mécontent) ou externes à celle-ci (ex : hacker). Enfin, nous démontrerons que l’appréciation de la vraisemblance et de la gravité du risque doit être abordée sous l’angle des personnes concernées et non, simplement, en fonction de l’unique point de vue du responsable de traitement.

Avantages et inconvénients des méthodologies retenues, et agencement optimal

Concrètement, il n’existe pas de méthodologie unique pour réaliser une AIPD. Le responsable de traitement reste libre de procéder comme il l’entend, en choisissant l’AIPD qui lui semble la plus adaptée. Cette latitude peut être perçue, selon le contexte et le type de traitement de données personnelles, comme une opportunité ou une incertitude quant à la conformité du traitement. L’étude des quatre méthodologies retenues, puis appliquées à notre cas pratique Biomen, démontre que chaque outil présente des avantages et des inconvénients.

Notamment, les méthodologies CNIL et PRIAM offrent un niveau de granularité reflétant parfaitement le cycle de vie des données; elles permettent de s’assurer du respect du principe de la protection des données personnelles dès la conception et par défaut, sans limiter l’analyse aux aspects de sécurité informatique. Les méthodologies BSI et NIST présentent l’avantage de sortir du seul prisme du respect des droits et libertés de la personne concernée pour analyser les risques financier et réputationnel encourus par le responsable du traitement. Ces deux méthodologies doivent néanmoins être utilisées avec prudence : la méthodologie BSI est obsolète car antérieure au RGPD et la méthodologie NIST relève du droit étasunien.

Selon nous, l’analyse d’impact relative à la protection des données optimale devrait s’inspirer de ces différentes méthodologies. **Les première et troisième étapes**, correspondant à la description des flux de données personnelles et à l’appréciation des risques, peuvent s’inspirer de la méthodologie CNIL pour les traitements de données « simples » et, pour les traitements « complexes » et multiparties de la méthodologie PRIAM qui permet de détailler finement le cycle de vie des données. Cette méthodologie souffre néanmoins d’une exhaustivité très contraignante. La troisième étape peut également intégrer l’étude des « nouveaux » risques proposés par les méthodologies BSI et NIST pour intégrer les risques financiers et réputations encourus par le responsable du traitement.

Pour la deuxième étape, portant sur l'appréciation de la nécessité et de la proportionnalité du traitement, et la quatrième étape, relative aux mesures d'atténuation des risques, la méthodologie CNIL demeure le meilleur outil. Elle permet de s'assurer à la fois de la conformité du traitement de données analysé au regard des exigences posées par l'autorité nationale de contrôle et de choisir les garanties organisationnelles et techniques adéquates.

Afin de combler les lacunes méthodologiques relatives à l'appréciation du risque, le recours à méthodologie d'analyse des menaces pour la vie privée de type LINDDUN (pour « *Linkability,Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance* ») s'avère très utile. Les risques formulés dans cette analyse sont susceptibles d'être pris en compte par la Cour de justice de l'Union européenne.

La judiciarisation des risques liés aux traitements de données personnelles

L'étude dans une AIPD des risques encourus et des modalités de leur atténuation implique également de cerner la notion de risque.

À cet égard, les analyses effectuées par les Cours et tribunaux, en particulier la jurisprudence développée par la Cour européenne des droits de l'homme (CEDH) du Conseil de l'Europe et la Cour de justice de l'Union européenne (CJUE) s'avèrent riches d'enseignement. Ainsi, la CJUE recourt au principe de précaution en droit de l'environnement préalablement à la commercialisation d'un produit nocif. La notion d'« état des connaissances » exclut la responsabilité de l'analyste en cas de non prise en compte de risques futurs ou de risques qui ne seraient pas facilement détectables. Dans cette optique, l'AIPD doit se concentrer sur les risques immédiats, écartant ainsi l'étude des risques prospectifs et secondaires. La CEDH se réfère, elle aussi, au principe de précaution pour apprécier les atteintes aux droits et libertés, en particulier l'atteinte au respect de la vie privée, et juger si les garanties instaurées au préalable par les États sont suffisantes.

Par ailleurs, les conséquences des dommages réputationnels ou financiers, analysés par les quatre méthodologies étudiées, peuvent être sanctionnées par le juge judiciaire. Nous étudions donc les décisions rendues par les juridictions anglo-saxonnes en la matière et leur éventuelle mais difficile adaptabilité en droit français. Notamment, l'analyse des risques financiers découlant d'une éventuelle sanction prononcée par une autorité de contrôle nationale ou une juridiction civile peut s'avérer pertinente.

L'analyse du contentieux relatif au droit des données personnelles permet, pour sa part, de dresser le panorama des risques à considérer lors de la réalisation d'une AIPD.

Nous constatons que les politiques d'informations relatives à la collecte et à l'utilisation des données personnelles (« *privacy policies* ») revêtent une valeur purement formelle en droit français, anglais et étasunien. Cette obligation légale se présente comme une simple formalité à respecter. Une AIPD n'a donc pas à prendre en compte le droit des contrats, et donc la responsabilité contractuelle du responsable du traitement.

Du point de vue de la responsabilité extracontractuelle, l'étude démontre que la personne concernée ne peut pas invoquer tous les types de dommages. Seul le dommage moral, par exemple une atteinte à la réputation d'une personne liée à la violation de ses données personnelles, est retenu par le juge français, britannique et étasunien. Les dommages matériels, comme l'atteinte à l'intégrité physique de la personne concernée suite à la violation

de ses données, sont par principe exclus. De plus, la réparation d'un dommage moral se limite principalement au dommage moral immédiat, la victime devant démontrer l'existence d'un lien direct entre le préjudice subi et le fait générateur. Les dommages futurs sont donc *a priori* exclus, *a priori* » car la prise en compte du dommage moral basé sur le préjudice d'anxiété semble se dessiner à la fois dans les prétoires étasuniens et dans les projets de révision du RGPD.

En droit européen, la conjugaison du RGPD et d'autres types de droits nationaux, notamment le droit du travail ou de la responsabilité civile, peut faciliter le transfert de la responsabilité juridique du responsable du traitement vers le sous-traitant ou vers un salarié mal intentionné. Ainsi, sous réserve des précisions apportées, les risques organisationnels analysés lors de l'AIPD peuvent être significativement réduits via des dispositions insérées dans des chartes informatiques ou des contrats de sous-traitance.

Enfin, les critères permettant la réparation d'un préjudice subi par la personne concernée fixés par le RGPD conduisent en pratique à limiter la réparation accordée aux victimes par les juridictions civiles françaises. Il en va de même des actions de groupes inspirées des droits étasunien et britannique. Ces dernières se heurtent à l'imprécision des règles procédurales. Notamment, l'intérêt à agir du groupe reste conditionné par la démonstration d'un préjudice identique allégué par chaque demandeur. Le risque à prendre en compte lors d'une AIPD s'en trouve pour l'instant réduit.

***

Au vu de toutes ces difficultés, beaucoup de travail reste encore à accomplir pour disposer d'AIPD efficientes, et au-delà d'outils permettant de prendre en compte à la fois les risques pour les droits et libertés des personnes, les risques de non-conformité pour les entreprises, les règles éthiques notamment en matière d'intelligence artificielle et, plus généralement, les risques sociétaux dans notre société numérique désormais omniprésente.

C'est également le RGPD, texte complexe s'il en est, qu'il convient de parachever. Le règlement, adopté en 2016, s'appuie sur un nouveau paradigme, l'approche par les risques assortie d'un contrôle a posteriori. Cette approche a remplacé une protection basée principalement sur le contrôle a priori effectué par les autorités nationales en charge de la protection des données. Il serait donc pertinent de s'interroger sur les points à améliorer et de corriger, en s'appuyant sur les retours d'expérience des praticiens (délégués à la protection des données, consultants en particulier), les éléments qui auraient échappé à la vigilance du législateur. Loin d'être figées, les modalités de protection des valeurs européennes portées par le RGPD ne peuvent, pour être effectives, que se construire dans le temps.