Institut Mines-Télécom

CHAIRE CONNECTED CARS & CYBER SECURITY

TELECOM Paris

IP PARIS

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

Claire Levallois-Barth
Jonathan Keller

Rapport de recherche
Novembre 2021

en partenariat avec

Douzième chaire d'enseignement et de recherche de Télécom Paris, la Chaire de recherche *Connected Cars & Cyber Security* (C3S) a été fondée en collaboration avec NOKIA, RENAULT, VALÉO et WAVESTONE afin de répondre aux défis techniques, sociaux, éthiques et économiques générés par les voitures connectées et, bientôt, autonomes. La conception d'un tel objet autonome, mobile en milieu humain doit en effet prendre en compte la cybersécurité comme facteur de réussite. Pour répondre à ces interrogations, cinq grands axes ont été définis :

1. analyse de risques et sûreté de fonctionnement
2. protection des données et de leurs flux en temps réel, cryptographie et agilité
3. authentification, identité et empreinte comportementale
4. résilience « *by design* »
5. protection des données personnelles impliquées dans le véhicule connecté (aspects juridiques et sociétaux)

Recherches effectuées dans le cadre de l'axe 5 de la Chaire C3S www.telecom-paris.fr/c3s

Sous la direction de Claire Levallois-Barth (Institut Mines-Télécom / Télécom Paris) et de Monsieur Christophe Jouvray (Valéo), les partenaires de l'axe 5 de la Chaire *Connected Cars & Cyber Security* ont orienté les recherches sur l'Analyse d'impact pour la protection des données (AIPD), obligation imposée par l'article 35 du Règlement Général pour la Protection des Données (RGPD).

Cette recherche appliquée s'est concentrée sur un contexte des voitures connectées pour discuter de l'interaction entre cet outil découlant d'une obligation légale, et les besoins opérationnels du secteur automobile.

Sur ce cinquième axe, la Chaire C3S travaille de façon rapprochée avec la Chaire Valeurs et Politiques des Informations Personnelles (VP-IP) de l'Institut Mines-Télécom.
www.informations-personnelles.org

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

Claire Levallois-Barth

Jonathan Keller

Le présent rapport présente les résultats des recherches de l'Axe 5 de la Chaire *Connected Cars & Cybersecurity* portant sur la méthodologie d'Analyse d'Impact relative à la Protection des Données (AIPD), telle que prescrite par l'article 35 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD ») explicitées par les Lignes directrices du Comité européen de la protection des données (CEPD), adaptée à un contexte de véhicule connecté.

Pour répondre à cette problématique, un cas pratique reprenant différentes hypothèses de traitements de données personnelles par différents acteurs a été défini en collaboration avec les partenaires de la Chaire (Partie 1, page 9).

Ce cas pratique appelé Biomem offre la possibilité d'appliquer quatre méthodologies d'analyse d'impacts (celles développées par la Commission nationale de l'informatique et des libertés, par D. LE METAYER de l'INRIA appelée *Privacy Risk Analysis Methodology*, par le *National Institute of Standards and Technology* étasunien et par le *Bundesamt für Sicherheit in der Informationstechnik* allemand) pour en déduire leur efficacité dans un tel contexte et en tirer les mesures d'atténuation des risques adéquates (Partie 2, Chapitre 2, page 46).

Le rapport souligne la difficulté d'un choix univoque d'une méthodologie pour répondre à des besoins pratiques dans le contexte suscité (Partie 2, Chapitre 3, page 62).

En effet, aucune « méthodologie-miracle » n'est répertoriée. Chacune de ces méthodologies présente des avantages et des inconvénients rendant leur application concrète ou leur examen, par une autorité nationale de contrôle, problématique. Cette incomplétude découle des lacunes volontaires des Lignes directrices du CEPD manifestant la volonté d'une neutralité méthodologique pour l'appréciation du traitement de données personnelles vis-à-vis des droits et libertés des personnes concernées. Cette incomplétude provient de l'absence d'indicateurs quantifiant précisément l'étendue des dits risques (ces points sont étudiés en préambule de la Partie 2, Chapitre 1, page 34).

Étant un outil d'identification et d'atténuation des risques pour les droits et libertés, les AIPD se rapprochent des analyses du risque effectuées lors de la décision d'application du principe de précaution utilisé par la Cour de Justice de l'Union Européenne en droit de l'environnement « *préalablement à la commercialisation d'un produit nocif* ». Ce même principe se retrouve dans les mesures d'appréciation des atteintes des droits et libertés par la Cour Européenne des Droits de l'Homme pour juger des garanties instaurées au préalable par les États (Partie 3, Chapitre 1, page 94).

Enfin, les différentes méthodologies choisies avec les partenaires de la Chaire *Connected Cars and Cybersecurity* invitent à prendre en compte, au même titre que les droits et libertés, les dommages subis par le responsable du traitement. Les différents dommages envisagés sont alternativement réputationnels ou financiers. Leurs conséquences peuvent être sanctionnées par des décisions judiciaires. Nous étudierons ainsi les décisions déjà rendues par les juridictions anglo-saxonnes et leur éventuelle mais difficile adaptabilité en droit français (Partie 3, Chapitre 2, page 114).

Δ

Est retenue comme définition d'un « véhicule connecté » celle du Pack de conformité pour le véhicule connecté (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* ».

Sommaire

Une table des matières détaillée est disponible page 160, ainsi qu'une table des paragraphes numérotés, page 164.

Introduction

Cette partie introductive souligne la difficulté de l'appréhension des risques pour les droits et libertés mentionnés par le RGPD. Cette difficulté provient principalement de la pauvreté des sources doctrinales sur ce sujet au moment de la réalisation de cette étude. En effet, les articles de chercheurs juridiques se contentent, pour l'instant, de paraphraser les Lignes directrices du Comité européen de la protection des données sans pour autant les expliciter. De plus, les Analyses d'Impact relatives à la Protection des Données (AIPD) déjà réalisées par les organismes sont couvertes par le secret des affaires.

L'identification et l'atténuation des risques pour les droits et libertés par l'AIPD relèvent des obligations relatives au respect du Principe de protection des données dès la conception et par défaut.

1 La numérisation de certaines fonctions du véhicule automobile, voire son autonomisation, constitue une source d'espoirs mais aussi, il faut bien le reconnaître, d'inquiétudes. Parmi ces dernières, la crainte d'un panopticon numérique élaboré à l'insu des conducteurs, voire des constructeurs, via la collecte et l'utilisation des données personnelles des premiers, se dessine. La prévention d'une telle crainte est anticipée par le Règlement Général pour la Protection des Données, dont l'article 35 impose au responsable de traitement une concertation avec les parties prenantes (sous-traitants et fournisseurs de technologies) préalablement à un traitement de données personnelles menaçant les droits et libertés des personnes concernées.

Le présent rapport est donc consacré à la problématique de la détermination d'une méthodologie d'Analyse d'Impact relative à la Protection des Données dans un cadre de gestion de données personnelles impliquant plusieurs parties. L'objet de l'axe 5 de la Chaire C3S étant d'apporter des éléments de réponse à cette problématique, le présent rapport se concentrera sur le domaine du véhicule connecté.

► La CNIL entretient une confusion sémantique en recourant à la terminologie de *Privacy impact assessment*[1] (« *Évaluation d'impact relative à la vie privée* », EIVP) en lieu et place de l'utilisation du terme officiel d'**Analyse d'Impact relative à la Protection des Données** (ci-après « AIPD »). Les deux méthodologies[2] sont différentes dans leur assiette. La première méthodologie explore des impacts plus vastes de l'utilisation des données personnelles, là où l'AIPD repose exclusivement sur les questions propres aux données personnelles.

La principale difficulté méthodologique rencontrée lors de la réalisation de cette recherche est la pauvreté des sources légales et doctrinales en la matière. Pauvreté qui se reflète non par le nombre d'articles mais par le caractère peu pratique de leur contenu. Pour paraphraser les propos de M. le Professeur X. MAGNON, la doctrine juridique a connu une « *euphorie avec une logique concurrentielle extrêmement forte, qui sera ‹ le premier à organiser une journée sur (l'AIDP), qui sera le premier à écrire un guide sur (l'AIPD), qui sera le premier à commenter dans une revue lue par les avocats › afin d'obtenir peut-être le Graal, à savoir la consultation privée* »[3]. Cette effervescence doctrinale entraîne une confusion juridique quant à la définition précise des obligations imposées pour réaliser une AIPD conforme à la réglementation en vigueur[4]. En d'autres termes, la multiplication d'opinions doctrinales crée ainsi des confusions et des amalgames avec d'autres types analyses d'impact, prévues pour des matières juridiques connexes au droit des données personnelles. Les analyses d'impact relatives à l'éthique en sont une illustration[5].

Une contextualisation liminaire s'impose avant d'aller plus loin : définissons ce que signifient les risques pour les données personnelles, et la manière dont ces risques sont appréciés.

---

1 Voir par exemple https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

2 Ici, « *méthodologie* » fait référence à l'AIPD et à l'EIVP en tant que telles. Plus loin, le terme désignera, pour simplifier, 4 instances de ces méthodologies, qui sont étudiées en détail dans ce rapport.

3 X. MAGNON, « *La doctrine, la QPC et le Conseil constitutionnel : quelle distance ? Quelle expertise ?* », Colloque du 14 juin 2013 à l'Université de Toulouse 1 Capitole, https://www.dailymotion.com/video/xvfuy0.

4 Voir infra §3, page 3.

5 Voir par exemple la contribution de P. DE HERT, « *A human right perspective on privacy and DPIA* », in Privacy Impact Assessment, Springer, 2012, qui préconise l'utilisation de l'éthique.

Section 1. **La difficile appréhension du risque**

2 Influencée par les actuaires, l'appréhension du risque est généralement effectuée en termes statistiques et probabilistes. Toutefois, un apport substantiel de cette compréhension du risque provient des travaux de U. BECK[6]. Cet auteur insiste sur l'institutionnalisation du risque et l'apparition de nouveaux risques, qualifiés de « *manufacturés* », reposant sur la progression de la science et des technologies. Ces risques manufacturés sont de nature à potentiellement occasionner des dégâts allant au-delà des prévisions anticipées.

Pour tenter d'appréhender les risques afin de les anticiper pour les maîtriser, les « *évaluations d'impacts* » invitent les producteurs à apprécier préalablement ces menaces pour déterminer l'utilité industrielle génératrice d'un risque sociétal, notamment environnemental. Le scandale *Cambridge Analytica* invite ainsi à qualifier l'utilisation massive de données personnelles comme étant un risque sociétal.

3 Reprenant cette approche d'autorégulation préventive, l'article 35 du RGPD impose la réalisation, dans certaines circonstances, d'une analyse d'impact relative à la protection des données[7]. Cette obligation doit être considérée comme remplissant deux fonctions distinctes :

- Définir et évaluer les risques en matière de données personnelles traitées par le responsable de traitement préalablement au déploiement d'un traitement pour identifier et réduire les risques inhérents, et
- Disposer d'un outil de gestion d'appréciation pour la prise de risques pour prioriser les mesures adéquates à installer, déployer et paramétrer.

Ces deux fonctions doivent permettre au responsable de traitement de déterminer pleinement les risques juridiques lui incombant lors de la mise en œuvre d'un traitement de données.

La caractérisation des risques reste cependant mal aisée, le RGPD maintenant une confusion en assimilant le droit au respect des « *données personnelles* », accordé aux personnes concernées, aux « *droits et libertés des personnes physiques* ». Une telle vision introduit ainsi les prémices d'un régime de responsabilité civile de plein droit, c'est-à-dire que la faute démontrée entraîne obligatoirement la responsabilité du responsable de plein droit.

4 La réalisation d'une analyse d'impact en matière de données personnelles participe à la mise en œuvre d'un nouveau principe clé introduit par le RGPD, le « *principe de responsabilité* » (ou « *accountability* »)[8]. Selon cette nouvelle conception de la gestion des données personnelles, les responsables de traitement sont tenus de respecter les droits et obligations imposés par la législation européenne et **de fournir les preuves de ce respect**. Le principe de responsabilité se traduit concrètement par l'obligation du responsable de traitement de documenter par écrit toutes

---

6 U. BECK, « *Risk Society: Towards A New Modernity* », Sage pub., 1992, p. 260.

7 Voir infra §25, page 35.

8 Art. 5 du RGPD. Groupe de travail de l'article 29, Avis n°3/2010 sur le principe de responsabilité, WP 173, adopté le 10 juillet 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf, European Data Protection Supervisor, « *Accountability on the ground Part I : Records, registers and when to do Data protection impact Assessment* », v.1.3., Juil. 2019, https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf, voir également K. DEMETZOU, « *Data protection impact assessment, and the unclarified concept of « high risk » in the GDPR* », Computer Law & security review 35 (2019) 105342.

les mesures garantissant que les traitements des données personnelles réalisés sont conformes à la réglementation en vigueur à peine de subir des sanctions financières élevées[9].

Or l'AIPD, au même titre que les nouveaux principes de respect de la protection des données par défaut (« *Data Protection by default* ») ou dès la conception (« *Data Protection by design* »)[10], doit faire l'objet d'une documentation écrite démontrant sa réalisation. De plus, et concrètement, le respect de ces principes se cumule en fonction de leurs applications. Par exemple, outre son aspect de gestion d'acceptation des risques, l'AIPD doit également anticiper l'application du principe de *Data Protection by design* au traitement de données personnelles envisagé pour démontrer la licéité du traitement et la preuve d'une prise en compte de ce nouveau principe.

5 La principale difficulté méthodologique soulevée lors de l'élaboration d'une analyse d'impact réside dans l'absence de détermination précise du risque dans toutes ses dimensions (assiette, occurrence ou probabilité, échelle de gravité) en matière de données personnelles.

L'évaluation d'impact technologique étasunienne, comme l'évaluation d'impact environnemental européenne, visent précisément des situations « *réalistes* », c'est-à-dire se situant dans une réalité mesurable et concrète. Dès lors, si l'autorité compétente estime que les risques « *réels* » sont trop importants, le projet soumis est tout simplement interdit au nom du principe de précaution. Se situant dans un contexte purement « *immatériel* » et aux effets tout autant immatériels, l'AIPD se trouve dans l'impossibilité d'être soumise à des appréciations scientifiquement démontrées. Ceci entraîne des approximations quantitatives et qualitatives des risques.

Ces approximations sont d'autant plus importantes que le RGPD reste vague sur l'assiette du risque à prendre en compte. Or, cette assiette conditionne le choix de la méthodologie à employer pour respecter le principe de responsabilité posée par l'article 35 du RGPD. L'ignorance de l'étendue de l'assiette du risque entraîne des erreurs lors de l'appréciation des risques.

---

9 Dans ce sens, voir par exemple L. PAILLIER, « *Les outils technologiques de la compliance et le RGPD : la protection des données dès la conception* », in M.-A. FRISON-ROCHE, (dir.), « *Les outils de la Compliance* », série «Régulations & Compliance», Journal of Regulation & Compliance et Dalloz, 2021, p. 279-286, N. METALLINOS, « *Le principe d'accountability : des formalités préalables aux études d'impact sur la vie privée* », Comm. Com. Elec., 2018, dossier 11, W. MAXWELL, S. TAIEB, « *L'accountability, symbole d'une influence américaine sur le RGPD* », D. IP/IT, 2016, p.123.

10 Art. 25 du RGPD.

Section 2. La différenciation entre l'Analyse d'Impact relative à la Protection des Données (AIPD), l'Évaluation d'Impacts pour la Vie Privée (EIVP) et l'*Ethic Impact Assessment* (EIA)

6 L'infidèle traduction de « *Data Protection Impact Assessment* » (ci-après « DPIA » ou en français « AIPD ») en « *Évaluation d'Impacts pour la Vie Privée* » (ci-après « EIVP » qui est l'équivalent anglais du « *Privacy impact assessment* » ou « PIA ») par certains auteurs et autorités illustre ce risque de confusion entre ces notions.

> Précisions : L'EIVP ou PIA est une obligation étasunienne initialement posée par la Section 208 de l'*E-Government Act* adoptée en 2002 afin de s'assurer que l'utilisation des données personnelles collectées par les administrations fédérales soient respectueuses de la « *Privacy* »[11] des administrés. Il doit être noté que l'impressionnante transaction FTC c. Facebook de 2019[12] offrait les prémices d'une institutionnalisation des évaluations d'impact pour la vie privée dans les gouvernances étasuniennes[13].

7 Convergeant sur de nombreux aspects, l'AIPD imposée par le RGPD et l'EIVP étasunienne divergent quant à la finalité recherchée.

L'AIPD européenne porte strictement sur le respect du droit des données personnelles – c'est-à-dire concrètement la licéité du traitement des données personnelles (collecte), la gestion subséquente des données personnelles (traitement) et le respect de l'exercice des droits de la personne concernée –, là où l'EIVP étasunienne porte exclusivement sur les modalités du respect de la *Privacy* – c'est-à-dire la non-intrusion dans la vie informationnelle d'une personne par des tiers non autorisés[14]. Au travers de la qualification du « *risque élevé pour les droits et libertés des personnes physiques* », le paragraphe 1er de l'article 35 du RGPD renvoie incidemment au respect de la vie privée, au même titre que les autres « *droits et libertés* » visées par le considérant 75 du RGPD.

Toutefois, la convergence des méthodologies AIPD et EIVP s'effectue au niveau de l'identification de risques[15] et des mesures d'atténuations. **L'implémentation opérationnelle d'une AIPD efficace réduira donc de nombreux risques identifiés par l'EIVP.** Cette confusion sémantique s'accroît avec des amalgames sur une « *éthicisation* » de l'AIPD, entretenus par des autorités nationales de contrôle et par la Cour de Justice de l'Union européenne (CJUE). En d'autres termes, certaines méthodologies proposées proposent d'inclure des considérations éthiques dans l'analyse d'impact pour la protection des données alors même que ces considérations ne sont pas évoquées par le RGPD.

---

11 Pour une vision comparative voir R. CLARKE, « *An evaluation of PIA guidance documents* », IDPL, 2011, Vol.1, n°2, pp. 111-120.

12 Transaction conclue entre la FTC et Facebook du 24 juillet 2019 du 24 juillet 2019, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

13 Voir dans ce sens le Chapitre 7 de la décision FTC précitée.

14 Dont l'un des principaux théoriciens, Daniel SOLOVE a répertorié dans son célèbre article « *A taxonomy of privacy* » (University of Pennsylvania Law Review, Vol. 154 n°3, 2006, pp. 477-564), quatre types de dommages (la collecte d'information, le traitement d'information, la dissémination d'informations, l'invasion) sous divisés en sous-catégorie de dommages distincts.

15 Voir Tableau 1, page 6.

	AIPD	EIVP	EIA	Évaluation de Conformité
Fondement juridique	Lignes directrices AIPD du CEPD (UE)	M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (États-Unis)	SATORI (« *a common framework for ethical values, principles and approaches for ethics assessment in the European Context* ») (UE)	Proposition de règlement sur l'Intelligence Artificielle (UE)
Éléments à prendre en compte	Droits des données personnelles - Conformité - Exercice des droits - Risques pour les droits et libertés *Ex : Comment sont collectées puis traitées les données personnelles et quels risques découlent de leurs mésusages ?*	Risque d'intrusion dans la vie privée - Données personnelles - Éléments de la vie privée *Ex : Comment les données personnelles collectées peuvent-elles engendrer un désagrément pour une personne sur la base de sa vie privée ?*	Risque de discrimination ou de traitements inéquitables *Ex : Comment les traitements de données personnelles peuvent-ils engendrer des désagréments pour un groupe ?*	Risque de discrimination ou d'exclusion à certains droits fournis par des services publics ou par des entreprises privées
Étendue des sujets de droit	Personne physique concernée *ou* Groupes de personnes physiques concernées *Ex : les personnes physiques concernées*	Personnes physiques *et par incidence* des groupes « *d'intérêts* » (ethnique, politique, sexuel) *Ex : les personnes physiques*	Groupes « *d'intérêts* » (ethniques, politiques, sexuel) Société	Personnes ou groupes de personnes utilisant un objet comprenant une intelligence artificielle intégrée à un composant de sécurité
Finalité	Protéger les « *droits et libertés* » menacés par une mauvaise gestion des données en instaurant des mesures techniques ou organisationnelles adéquates	Protéger le droit au respect à la vie privée des personnes physiques en implémentant des mesures techniques ou organisationnelles adéquates	Protéger un intérêt sociétal menacé par une nouvelle technologie en s'interrogeant sur sa pertinence et sur la bonne implémentation de mesures correctives	Faciliter les obligations administratives auprès des autorités certificatrices

*Tableau 1. Récapitulatif des différences entre l'analyse d'impact relative à la protection des données (AIPD), l'évaluation d'impact sur la vie privée (EIVP), l'*ethic impact assessment *(EIA) et l'évaluation de conformité*

8 L'AIPD doit également être distinguée de l'*Ethics Impact Assessment* (ci-après « EIA »). L'EIA porte sur la pertinence, d'un point de vue éthique, à implémenter un projet[16]. Bien que relevant davantage de finalités politiques et communicationnelles, cette évaluation porte sur l'assurance que les « *algorithmes* » examinés préalablement à leur déploiement ne contiennent aucun biais entraînant des exclusions sociales ou des discriminations. **Ainsi, l'EIA porte davantage sur l'identification de risques sociétaux et de programmation que sur des risques relatifs à la gestion des données personnelles.**

> Après avoir envisagé de rendre obligatoire les EIA afin de susciter la confiance du public dans le déploiement de l'intelligence artificielle sur le territoire de l'Union européenne[17], la Commission européenne semble s'être ravisée dans la dernière version du projet de règlement sur l'intelligence artificielle d'avril 2021 pour privilégier des évaluations de conformité pour des intelligences artificielles à « *risque élevé* »[18]. Bien que posées par les articles 9 et 17 du projet de règlement, ces évaluations ne font pas l'objet d'une méthodologie explicitée. Lorsqu'elles sont applicables, les propositions du règlement seront mentionnées dans le présent rapport.

La méthodologie varie donc en fonction du droit qui doit être protégé ainsi que de son étendue.

Notre étude portant sur la transposition opérationnelle de l'article 35 du RGPD dans le véhicule connecté/autonome, nous nous concentrerons en priorité sur l'étude des AIPD et de certaines méthodologies d'EIVP présentées comme répondant aux conditions de l'article 35 du RGPD. Cet article ne traitant pas des aspects éthiques, les EIA ont été exclus de cette recherche.

9 Pour répondre à la problématique soulevée, nous avons retenu quatre méthodologies[19] :

- L'analyse d'impact relative à la protection des données personnelles de la Commission Nationale pour l'Informatique et les Libertés (**CNIL**) – AIPD
- La méthodologie Privacy Risk Analysis Methodology (**PRIAM**) de Mme Sourya Joyee De et de M. Daniel Le Metayer (Inria) – EIVP
- La méthodologie du National Institute of Standards and Technology (**NIST**) étasunien – EIVP
- La méthodologie du Bundesamt für Sicherheit in der Informationstechnik (**BSI**) allemand – AIPD

La méthodologie proposée par la CNIL, autorité nationale de contrôle compétente en matière de données personnelles, nous semble en effet incontournable compte tenu de la nationalité des partenaires de la *Chaire Connected Car and Cybersecurity*.

Les deux auteurs de la méthodologie PRIAM étant des chercheurs spécialisés en ingénierie informatique, leur approche technique nous est apparue comme complémentaire et pertinente, et ce d'autant plus que cette méthodologie très développée questionne la pertinence de la méthodologie CNIL.

Plus ancienne et se fondant sur une approche différente, la méthodologie BSI peut être définie comme une méthodologie « clefs en main » formulée par une autorité nationale de normalisation.

---

16 SATORI, « *A common framework for ethical impact assessment* », Annex 1, A reasoned proposal for a set of share ethical values, principles and approaches for ethics assessment in the European Context, Delivrable D4.1., pp. 79, spéc. p. 7, https://satoriproject.eu/media/D4.1_Annex_1_EIA_Proposal.pdf.

17 Commission européenne, « *Livre blanc Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance* », COM(2020) 65 final, 19 février 2020.

18 Commission européenne, *Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'Intelligence Artificielle*, COM (2021) 206 final, 21 avril 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=FR

19 Explicitées dans la Partie 2, page 29 du présent rapport.

Elle ne laisse aucune marge de manœuvre à l'analyste dans la réalisation de son analyse d'impact. La rigidité d'une telle méthodologie interroge sur la pertinence de son utilisation dans le cadre d'un traitement complexe de données personnelles par une pluralité d'acteurs.

Enfin, la méthodologie NIST a été publiée au cours de notre recherche. Bien que relevant d'un droit étranger au droit de l'Union européenne, son utilisation est pertinente dans une approche comparative pour déterminer si les méthodologies européennes peuvent être exportées en répondant aux besoins étasuniens et, réciproquement, si les méthodologies étasuniennes peuvent être transposées en droit européen.

Pour saisir la pertinence, les divergences et les convergences de ces quatre méthodologies, nous avons défini un cas pratique avec les partenaires de la Chaire C3S (Partie 1, page 9). Nous avons ensuite appliqué celui-ci aux différentes méthodologies présentées afin de définir leur compatibilité avec les préconisations posées par le RGPD (Partie 2, page 29). Enfin, la notion même de risque a été étudiée plus amplement pour appréhender sa signification jurisprudentielle et ainsi déterminer une grille de lecture de « risques » existant réellement sur le plan juridique (Partie 3, page 91).

L'objet du présent rapport est donc de se concentrer :

- sur les AIPD fournies par la CNIL et le BSI,
- sur les EIVP fournies par le PRIAM et le NIST.

Chacune de ces méthodologies possède des avantages et inconvénients avec une assiette de risques différents.

Le rapport a pour objet de mettre en avant ces différents points pour déterminer quelle méthodologie d'analyse d'impact relative à la protection des données serait la plus utile pour un traitement de données personnelles impliquant une pluralité de responsables de traitement dans le cas du véhicule connecté.

Partie 1

Définition du cas pratique Biomem

Cette partie décrit le traitement de données personnelles défini dans l'Axe 5 de la Chaire C3S pour servir de cas pratique.

Le traitement correspond au service Biomem, service qui a pour vocation d'identifier un passager par reconnaissance faciale pour lui offrir l'accès au service de *Video On Demand* (VOD) auquel il est abonné. Des services accessoires, comme la signalisation de points d'intérêts sur le trajet par l'utilisation de données de localisation, couplés avec des métadonnées de l'utilisateur, peuvent être proposés.

Les modalités de fourniture du service varient en fonction de l'hypothèse où ledit service est fourni par une entité autonome (**hypothèse 1, « Biomem-Indé »**), ou qu'il est fourni par le constructeur du véhicule (**hypothèse 2, « Biomem-Constructeur »**) ou alternativement fourni par le fournisseur de VOD en tant que service ancillaire (**hypothèse 3, « Biomem-VOD »**).

Le cas pratique regroupe trois traitements de données personnelles distincts pour refléter cette réalité opérationnelle. Ces différents traitements seront analysés sous l'empire du droit positif, c'est-à-dire le RGPD et la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive Vie privée et communications électroniques, ou directive ePrivacy).

La démonstration sera faite, tout d'abord, que le premier traitement correspondant à la création du profil utilisateur, « *personne concernée* » au sens du RGPD, n'est guère problématique.

Le deuxième traitement concerne la reconnaissance faciale. Ce traitement pose question aux niveaux du recueil du consentement et des garanties de sécurité informatique exigées. Toutefois démonstration sera faite que le traitement de données personnelles biométriques relève de l'exemption domestique, exonérant ainsi le responsable du traitement de nombreuses obligations.

Enfin, le troisième traitement de données correspondant aux données de localisation spécifiquement est régi par la directive ePrivacy, le RGPD étant silencieux sur ce sujet. Toutefois, la qualification de service de la société de l'information entraîne l'inapplication de cette directive pour la majorité des traitements envisagés.

10 Cette première partie présente le cas pratique Biomem utilisé pour tester les quatre méthodologies retenues. Après avoir souligné la pertinence de notre cas pratique regroupant ces différentes hypothèses de travail (Chapitre 1, page 12), les règles de droit applicables seront énoncées (Chapitre 2, page 18).

Chapitre 1 Présentation des trois hypothèses du cas pratique Biomem

Chapitre 1 Présentation des trois hypothèses du cas pratique Biomem

11 Le service Biomem, notre cas pratique, correspond à une application téléchargeable sur un dispositif d'infodivertissement installé dans un véhicule connecté. Après souscription au service Biomem[20], l'application installée dans le véhicule utilise le dispositif technique vidéo présent pour identifier par reconnaissance faciale le(s) passager(s) (adulte(s) ou mineur(s)) du véhicule pour faciliter leur accès direct au service de vidéo à la demande auquel ils sont abonnés[21]. De plus, le service Biomem propose des contenus associés à des points d'intérêts se situant sur le trajet réalisé par le véhicule connecté sous réserve d'activation de la géolocalisation par le conducteur[22]. Ces contenus sont sélectionnés par le jeu d'une mise aux enchères des données de localisation auprès d'annonceurs publicitaires.

12 Ce cas pratique considère ainsi le véhicule connecté comme un support collectant et traitant des données personnelles. À ce titre, différents types d'acteurs sont impliqués :

- les constructeurs de véhicules,
- les équipementiers,
- les fournisseurs de services tiers, par exemple les fournisseurs de vidéos à la demande.

13 Aux fins de notre étude, nous considérons trois hypothèses subséquentes au cas pratique (voir la Figure 1, page 14, où les étapes a)b)c) ci-dessous sont schématisées, hors hypothèses) :

Biomem-Indé correspond à l'hypothèse où **le service Biomem est une application développée et fournie par une partie tierce indépendante du constructeur et du fournisseur de vidéo à la demande.** L'utilisateur installe l'application sur le dispositif d'infodivertissement présent dans le véhicule et fourni par le constructeur.

a) Biomem collecte des données personnelles lors de la souscription de l'utilisateur à savoir les identifiants au service Biomem et à ceux du fournisseur de vidéos à la demande auquel l'utilisateur est abonné. Parmi ces données personnelles, des données utilisateurs sont définies par le service Biomem afin d'associer un utilisateur à un profil défini par le fournisseur de vidéos à la demande. En outre, les données financières sont hébergées par un prestataire dédié.

---

20 Voir les variantes explorées aux alinéas (a) des §13, §14 et §15.

21 Voir les variantes explorées aux alinéas (b) des §13, §14 et §15.

22 Voir les variantes explorées aux alinéas (c) des §13, §14 et §15.

b) Après installation de l'application Biomem sur le dispositif d'infodivertissement interne au véhicule connecté, ce dispositif est utilisé pour créer et stocker le gabarit biométrique[23] associé au profil utilisateur. Ce gabarit est associé au profil défini sur le fournisseur de vidéos à la demande. Lors de l'activation de Biomem par le conducteur du véhicule depuis le tableau de bord, l'application Biomem capture une image faciale de l'utilisateur (le passager) pour le comparer avec le gabarit enregistré. L'image capturée est effacée une fois la comparaison effectuée. En cas d'association positive entre ces deux données biométriques, un certificat est envoyé au fournisseur de vidéos à la demande. Celui-ci identifie le dispositif installé dans le véhicule pour le lier au compte utilisateur afin de fournir le contenu audiovisuel.

c) Le conducteur peut, à sa discrétion, enclencher la géolocalisation du véhicule pour bénéficier d'un contenu lié au trajet parcouru. Pour ce faire, les données de localisation sont agrégées en local dans le véhicule puis transmises à la société Biomem. La société Biomem les propose sous forme de métadonnées aux annonceurs pour décider de l'opportunité d'un éventuel placement publicitaire dans une vidéo disponible à la demande.

14 Biomem-Constructeur correspond à l'hypothèse où **le service Biomem est un service ancillaire fourni par le constructeur.** Le logiciel Biomem est installé par défaut dans le dispositif d'infodivertissement fourni par le constructeur et est directement accessible sans téléchargement préalable.

a) Les données personnelles sont collectées dès l'acquisition du véhicule connecté par le conducteur, par la signature de la politique de données personnelles distinctes du contrat d'achat du véhicule connecté. Ces données correspondant aux identifiants du fournisseur de vidéos à la demande tiers sont renseignées soit à même le support d'infodivertissement, soit depuis le site internet dédié à l'application. L'utilisateur de l'application Biomem définit à ce stade les profils utilisateurs utilisés par le fournisseur de vidéos à la demande.

b) L'activation manuelle de l'application Biomem pré-installée sur le dispositif d'infodivertissement est utilisé pour créer et pour stocker le gabarit associé au profil utilisateur. Ce dernier est associé au profil défini par le fournisseur de vidéos à la demande. Lors de l'activation de Biomem par le conducteur, l'application capture une image de l'utilisateur pour la comparer avec le gabarit. L'image capturée est immédiatement effacée après avoir effectué la comparaison. En cas d'association positive entre ces données biométriques, un certificat est envoyé au fournisseur de vidéos à la demande pour fournir le contenu. Celui-ci identifie le dispositif installé dans le véhicule pour le lier au compte utilisateur afin de fournir le contenu audiovisuel.

c) Le conducteur peut, à sa discrétion, enclencher la géolocalisation pour bénéficier d'un contenu adapté au trajet. Pour ce faire, les données de localisation sont agrégées en local dans le véhicule avant d'être proposées sous forme de métadonnées pseudonymisées aux annonceurs, qui décident de l'opportunité d'un éventuel placement publicitaire à insérer dans une vidéo disponible à la demande.

15 Biomem-VOD correspond à l'hypothèse où **le service Biomem est une application développée par le fournisseur de vidéos à la demande fournie dans le véhicule connecté.** L'application est installée par l'utilisateur sur le dispositif d'infodivertissement.

a) Les données personnelles de l'utilisateur à ce service et les profils utilisateurs sont renseignés lors de l'inscription initiale au service fourni par le fournisseur de vidéos à la demande.

b) Après installation de l'application sur le dispositif d'infodivertissement fourni par le constructeur pour équiper le véhicule connecté, le dispositif est utilisé par le service de vidéos à la demande

---

23 CNIL, « *Un gabarit biométrique, c'est, quoi ?* », https://www.cnil.fr/fr/cnil-direct/question/biometrie-un-gabarit-biometrique-cest-quoi, qui définit le gabarit biométrique comme désignant : « *les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques (empreinte digitale, forme de la main, iris…), biologiques (ADN, urine, sang…) ou comportementales (démarche, dynamique de tracé de signature…) de la personne concernée* ».

Figure 1. Flux de données personnelles générées dans le cas pratique Biomem
Sur cette figure, aucune hypothèse (1-3) n'est faite sur le type d'acteur proposant le service Biomem. Seules les étapes a)-b)-c) sont développées.

pour créer et pour stocker le gabarit associé au profil utilisateur. Lors de l'activation de Biomem par le conducteur, l'application capture une image de l'utilisateur pour la comparer avec le gabarit. Cette image est effacée après la comparaison effectuée. En cas d'association positive entre ces données biométriques, un certificat est envoyé au fournisseur de vidéos à la demande pour fournir le contenu. Celui-ci identifie le dispositif installé dans le véhicule pour le lier au compte utilisateur afin de fournir le contenu audiovisuel

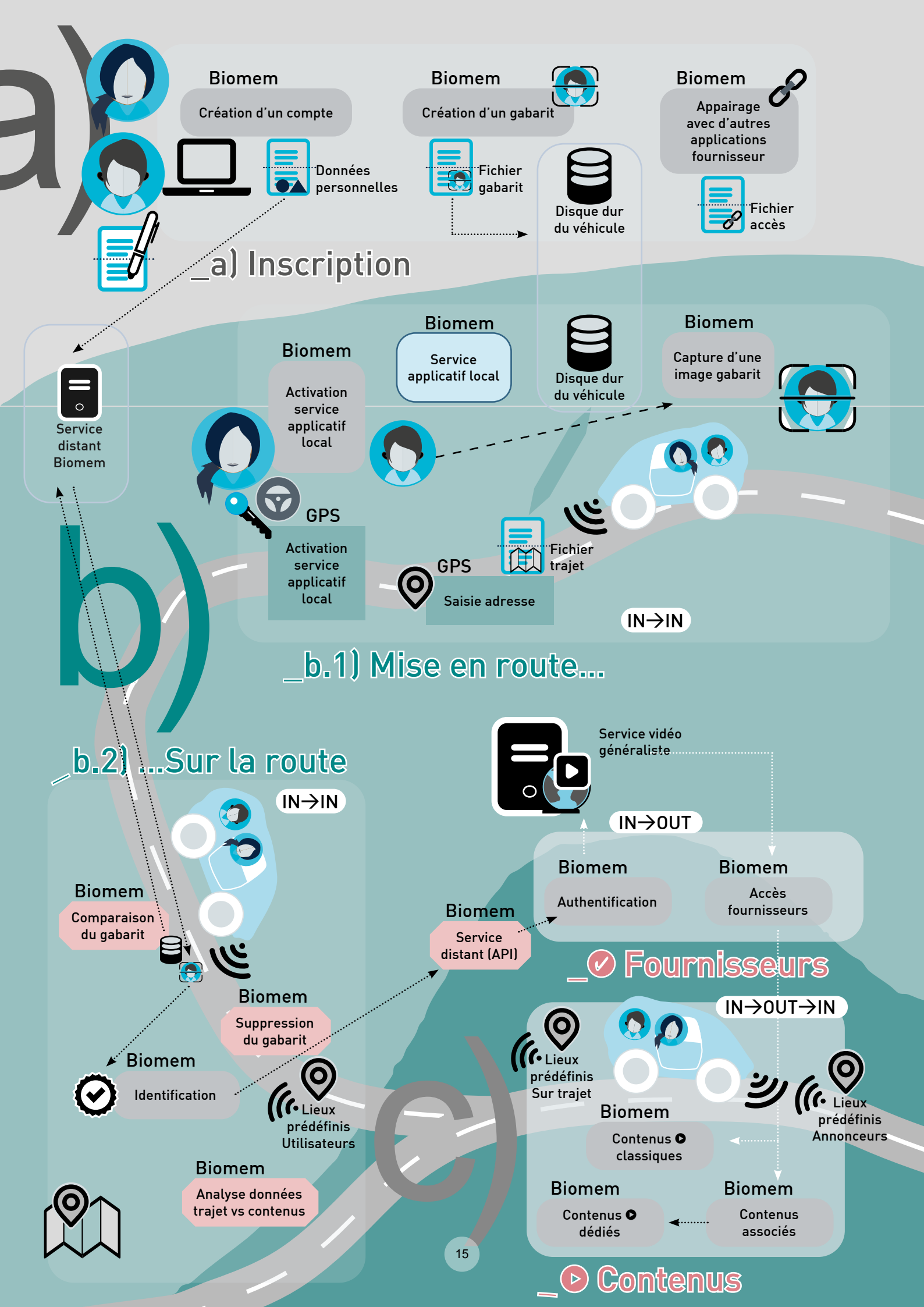
c) Le conducteur peut, à sa discrétion, enclencher la géolocalisation pour fournir un contenu lié au trajet. Le fournisseur de vidéos à la demande effectue lui-même les enchères relatives à la publicité contextuelle.

La variation des trois hypothèses du cas pratique Biomem conditionne l'éligibilité des acteurs à la qualification de « *responsable du traitement* » telle que définie par le RGPD. Selon l'article 4-7° du RGPD, le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

- Pour Biomem-Indé (hypothèse 1)
  - L'éditeur indépendant est responsable de traitement pour les données d'inscription (création du profil utilisateur Biomem) et géolocalisation (publicité ciblée)
  - La plateforme de VOD est responsable de traitement pour l'identification de l'accès aux comptes en ligne et les logs de connexion (accès au contenu utilisateur VOD)
  - Le constructeur est fournisseur de technologie (obligation de sécurité informatique)
- Pour Biomem-Constructeur (hypothèse 2)
  - Le constructeur est responsable de traitement pour les données d'inscription (création du profil utilisateur Biomem) et de géolocalisation (publicité ciblée)
  - La plateforme de VOD est responsable de traitement pour l'identification de l'accès aux comptes en ligne et les logs de connexion (accès au contenu utilisateur VOD)
- Pour Biomem-VOD (hypothèse 3)
  - Le constructeur est fournisseur de technologie (obligation de sécurité informatique)
  - La plateforme de VOD est responsable de traitement pour l'intégralité des traitements (accès au contenu utilisateur VOD et publicité ciblée

	Hypothèse 1 Biomem-Indé	Hypothèse 2 Biomem-Constructeur	Hypothèse 3 Biomem-VOD
Rôle de Biomem	Responsable de traitement pour l'identification biométrique (données biométriques) et la publicité ciblée (données de localisation)	n/a	n/a
Rôle du constructeur	Fournisseur de technologie	Responsable de traitement pour l'identification biométrique (données biométriques) et la publicité ciblée (données de localisation)	Fournisseur de technologie
Rôle de la plateforme de VOD	Responsable de traitement pour la fourniture des services VOD (données utilisateurs et logs de connexion)	Responsable de traitement pour la fourniture des services VOD (identification des comptes et logs de connexion)	Responsable de traitement pour l'ensemble des traitements

Tableau 2. Présentation résumant les trois hypothèses explorées


Biomem
Création d'un compte
Données personnelles
Biomem
Création d'un gabarit
Fichier gabarit
Biomem
Appairage avec d'autres applications fournisseur
Fichier accès
Disque dur du véhicule
_a) Inscription
Service distant Biomem
Biomem
Activation service applicatif local
Biomem
Service applicatif local
Disque dur du véhicule
Biomem
Capture d'une image gabarit
GPS
Activation service applicatif local
GPS
Saisie adresse
Fichier trajet
IN→IN
_b.1) Mise en route...
_b.2) ...Sur la route
IN→IN
Service vidéo généraliste
IN→OUT
Biomem
Comparaison du gabarit
Biomem
Service distant (API)
Biomem
Authentification
Biomem
Accès fournisseurs
_ Fournisseurs
Biomem
Suppression du gabarit
IN→OUT→IN
Biomem
Identification
Lieux prédéfinis Utilisateurs
Lieux prédéfinis Sur trajet
Biomem
Contenus classiques
Lieux prédéfinis Annonceurs
Biomem
Analyse données trajet vs contenus
Biomem
Contenus dédiés
Biomem
Contenus associés
_ Contenus

Chapitre 2 Droit applicable aux traitements effectués par Biomem

Chapitre 2

Chapitre 2 Droit applicable aux traitements effectués par Biomem

Le présent chapitre se concentrera sur le droit applicable. La directive (UE) ePrivacy s'applique à notre cas pratique du fait de l'inscription d'informations sur le terminal de l'utilisateur et des données de localisation. Bien que la majorité des services fournis par Biomem relèvent de la qualification des services de la société de l'information définie par l'article 5-3° de la directive ePrivacy, l'utilisation des données de localisation à des fins de fourniture de contenus contextuels entraîne la soumission de ce traitement au consentement explicite de la personne concernée.

Le RGPD s'applique pleinement à notre cas pratique. À titre liminaire, les différentes obligations posées par le RGPD seront rappelées.

Puis, l'analyse du droit applicable aux données d'enregistrement au service soulignera les obligations devant traditionnellement être respectées dans le cadre du RGPD.

Les traitements envisagés concernent également des données biométriques, dont le régime est encadré par l'article 9 du RGPD. Cet article dispose que ce type de données est susceptible d'engendrer des risques importants pour ces libertés et droits (données politiques, de santé, etc.). Ces risques importants qualifient ce type de données comme étant des catégories particulières de données à caractère personnel (ci-après « *données sensibles* »). Bien que non directement visées par l'article 9 du RGPD et encadrées par la directive ePrivacy, le caractère attentatoire à la vie privée des données de localisation les rend éligibles à être considérées comme des données sensibles.

Ainsi, les données biométriques sont traitées, dans le cadre de Biomem, sous le contrôle exclusif de la personne concernée. Ce contrôle entraîne l'application de l'exemption domestique cantonnant le responsable de traitement à des obligations de sécurité informatique.

Enfin, en tant que données sensibles, la finalité du traitement des données de localisation entraîne l'obligation pour le responsable du traitement de collecter le consentement de la personne concernée ou de son représentant légal.

L'étude des dispositions de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[24] (ci-après « directive ePrivacy ») doit être effectuée pour démonter qu'elle n'est que partiellement applicable à Biomem (Section 1). Puis, les règles de droit relatives au RGPD seront exposées (Section 2, page 23). Le projet de règlement sur l'Intelligence Artificielle[25] prévoit également certaines dispositions qui sont applicables à Biomem, mais étant encore en négociation, il n'est pas traité dans le présent document.

Section 1. L'application délicate de la directive ePrivacy à Biomem

La directive ePrivacy adoptée en 2002 est strictement applicable à la protection des données personnelles dans le contexte des communications électroniques. Elle constitue une disposition spéciale complétant le cadre général de la protection[26] établi par la directive 95/46/CE adoptée en 1995[27]. Cette directive a été remplacée en 2016 par le RGPD. Le RGPD prime[28] donc en cas

---

24 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE L 201 du 31.7.2002, p. 37–47, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32002L0058.

25 Commission européenne, Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'Intelligence Artificielle, COM (2021) 206 final, 21 avril 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=FR.

26 Article 1-2 de la directive ePrivacy : « *Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1* ».

27 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE L 281, 23.11.1995, p. 31–50.

28 Article 2 de la directive ePrivacy selon lequel : « *Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive «cadre»)(8) s'appliquent aux fins de la présente directive* ».

de contradiction entre les deux textes ou encore d'une lacune de la *lex speciali*[29] édictée par la directive ePrivacy. Cette *lex specialis*, délicate d'application, amène à distinguer les conditions de recueil du consentement de l'utilisateur en ce qui concerne ses données de trafic et de localisation (Sous-Section 1, page 20) et en ce qui concerne le stockage d'une information sur son terminal (Sous-Section 2, page 21).

Sous-Section 1. Les conditions de recueil du consentement de l'utilisateur en ce qui concerne les données de trafic et les données de localisation

16 La directive ePrivacy s'applique au véhicule connecté uniquement si celui-ci est qualifié d'équipement terminal. Cette qualification de véhicule connecté comme équipement terminal n'est pas évidente. Du fait du principe de neutralité technologique, ni le RGPD, ni la directive ePrivacy ne définissent précisément cette notion. Toutefois, le Groupe de travail de l'Article 29[30] a précisé dans son avis 8/2014 sur les évolutions récentes relatives à l'internet des objets que « *tous les objets qui sont utilisés pour recueillir et ensuite traiter les données de la personne dans le cadre de la prestation de services dans l'IdO sont considérés comme des moyens au sens de la directive* »[31].

Par ailleurs, dans ses Lignes directrices 1/2020 sur le véhicule connecté, le CEPD se réfère à la définition d'un équipement terminal fournie par la directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux[32]. Ainsi, selon l'article 1, point 1 de cette directive, constitue un « *équipement terminal* » :

> « *a) tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations ; dans les deux cas, direct ou indirect, la connexion peut être établie par fil, fibre optique ou voie électromagnétique ; une connexion est indirecte si un appareil est interposé entre l'équipement terminal et l'interface du réseau public;*
> *b) les équipements de stations terrestres de satellites* ».

Dès lors, le CEPD conclut que « *pour autant que les critères susmentionnés soient remplis, il convient de considérer le véhicule connecté et l'appareil qui lui est raccordé comme un « équipement terminal » (au même titre qu'un ordinateur, un téléphone intelligent ou une télévision intelligente), et les dispositions de l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques » s'appliquent le cas échéant* ».

Par ailleurs, la directive ePrivacy protège, non par la personne concernée à l'instar du RGPD, mais l'utilisateur, qu'elle définit à l'article 2, point a) comme étant « *toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service* ». Cette qualification étend le champ de la protection

---

29 Considérant 10 de la directive ePrivacy selon lequel : « *Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels* ».

30 Groupe de travail informel, aussi appelé G29, regroupant les diverses autorités nationales de contrôle créé par la directive 95/46/CE. Le RGPD a remplacé ce groupe de travail par le Comité Européen pour la Protection des données (CEPD).

31 Groupe de travail de l'article 29, Avis 8/2014 sur les développements récents sur l'internet des objets, adopté le 16 septembre 2014, pp. 24, spéc. p. 10, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

32 CEPD, Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité citant la directive 2008/63/CE du 20 juin 2008 relative à la concurrence des équipements terminaux de télécommunication, JOCE L162, 21.06.2008, p. 20–26.

de la directive ePrivacy. Ainsi, dans notre espèce, « *l'utilisateur* » vise indubitablement le spectateur identifié par le système Biomem, et non le propriétaire du véhicule.

Contrairement au RGPD[33] qui ne définit pas les données de (géo)localisation, ce type de données est explicitement défini par l'article 2-c de la Directive ePrivacy comme étant « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* »[34]. Leur régime est déterminé par l'article 9 qui distingue les données de localisation traitées à des fins de trafic et celles « *autres que des données relatives au trafic* ». Dans cette dernière hypothèse, qui vise des services à valeur ajoutée[35] comme, par exemple, des conseils sur le guidage routier ou des informations sur l'état de la circulation, les données concernant des utilisateurs ou des abonnés ne peuvent être traitées qu'après avoir été rendues anonymes ou moyennant leur consentement, dans les conditions prévues par le RGPD.

► Ainsi dans notre cas pratique, l'envoi du certificat après l'identification biométrique de la personne concernée, second traitement envisagé par le service Biomem, est nécessaire à des fins de trafic des télécommunications, c'est-à-dire « *en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ». Le consentement de l'utilisateur n'a pas à être recueilli[36].

► À l'inverse, le troisième traitement de Biomem-VOD concernant la géolocalisation du véhicule à des fins de fournitures de vidéos contextuelles comprenant des contenus publicitaires relève des « *services à valeur ajoutée* » entraînant l'obligation de recueillir le consentement.

Sous-Section 2. Les conditions de recueil du consentement de l'utilisateur lors de l'installation ou du stockage d'une information sur son terminal

17 En ce qui concerne l'installation ou le stockage d'une information sur un terminal par un fournisseur de communications électroniques, la directive ePrivacy impose de recueillir l'autorisation de l'utilisateur ou de l'abonné, à moins que ce stockage ne soit automatique, intermédiaire et transitoire et qu'il ait lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques[37].

Dans son arrêt Planet 49[38], la CJUE précise au point 68 que « la directive 2002/58 fait référence au « *stockage d'information* » et à « *l'obtention de l'accès à des informations déjà stockées », sans qualifier ni préciser que celles-ci devraient être des données à caractère personnel* ». Ainsi toute « *ingérence* » dans un terminal par un fournisseur de communications électroniques entraine l'application de la directive ePrivacy, quel que soit le type d'information installée. La mise en demeure 2020-015 du 15 juillet 2020 de CNIL précise, pour sa part, que le stockage concerne

---

33 Infra §18, page 23 et s.

34 Complétée par le considérant 14 de la même directive qui précise la définition par « *la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée* ».

35 Le service à valeur ajouté est défini par l'article 2-point g de la directive ePrivacy « *tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation* ».

36 Article 5-2 de la directive ePrivacy.

37 Considérant 25 de la directive ePrivacy.

38 CJUE, Arrêt du 1er oct. 201, C 673-17, Bundesverband c. Planet 49Gmbh.

toute « *opération (à distance) de lecture ou d'écriture sur l'ordiphone de l'utilisateur* » autre que la sécurisation effectuée par l'application[39].

► Dans le cadre de Biomem, l'enregistrement du gabarit biométrique prévu est réalisé par la personne concernée/l'utilisateur du service. De plus, le certificat identifiant la voiture connectée comme autorisée à accéder au compte de vidéo à la demande relève des données de trafic. Dans les deux cas, le consentement de la personne/l'utilisateur n'a pas à être recueilli.

Cette interprétation est confirmée par les Lignes directrices 1/2020 sur les véhicules connectés. En effet, pour toutes les applications d'infodivertissement, le Comité européen de protection des données estime que l'article 5-3° de la directive ePrivacy s'applique. L'interprétation du CEPD est réalisée en deux temps[40]. Tout d'abord, le Comité rappelle le principe du recueil du consentement éclairé de la personne concernée préalablement à tout stockage ou accès à une information sur son équipement terminal par le responsable du traitement. Dans un second temps, il se réfère aux deux exemptions alternatives qui tempèrent ce principe :

1. Lorsque le stockage ou l'accès vise exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou
2. Lorsque le stockage ou l'accès est strictement nécessaire au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. À titre d'exemple, le consentement n'est pas requis si le traitement des données est nécessaire pour fournir les services de navigation GPS demandés par la personne concernée lorsque ces services peuvent être qualifiés de services de la société de l'information.

Sous réserve de ces exemptions, les dispositions de l'article 9 relatif aux données de localisation autres que les données relatives au trafic de la directive ePrivacy entraînent néanmoins par principe le recours au consentement, comme le rappellent les Lignes directrices 4/2020 du CEPD relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de Covid 19[41].

► Dans le cadre de Biomem, et quelle que soit l'hypothèse choisie, l'installation et l'activation du service par le conducteur – abonné – doivent être interprétées comme un service explicitement requis par l'utilisateur. Ainsi, l'installation du certificat permettant l'identification du véhicule comme étant autorisé par le fournisseur de vidéo en ligne à diffuser son contenu sur le dispositif installé dans le véhicule sera considérée comme un service de la société de l'information. Dans cette hypothèse, le responsable du traitement est affranchi de l'obligation de recueillir le consentement.

► Néanmoins, la collecte de données de localisation à des fins de mise aux enchères des lieux prédéfinis par les annonceurs bien que considérée comme un service à valeur ajoutée, n'est pas un service explicitement requis par l'utilisateur : cette collecte est soumise au recueil du consentement.

---

39 Voir CNIL, délibération MED 2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé, spéc. II, 2 de la délibération.

40 CEPD, Lignes directrices 1/2020 sur les véhicules connectés, spéc. p. 5-6 §§14-18.

41 CEPD, Lignes directrices 4/2020, relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de Covid 19, adoptées le 21 avril 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf, voir spécifiquement §11.

Section 2. L'application du Règlement Général sur la Protection des Données

La présente section expose les régimes de droit applicables aux données personnelles d'inscription au service Biomem (Sous-Section 1, page 24), aux données biométriques (Sous-Section 2, page 25) et enfin aux données de localisation (Sous-Section 3, page 27).

18 Les trois différentes hypothèses de traitements de données personnelles contenues dans le cas pratique présentent peu de complexités juridiques. En effet, elles sont envisagées par le Pack de conformité, Véhicules Connectés et données personnelles de la CNIL d'octobre 2017[42] puis par le CEDP en 2021 dans ses lignes directrices sur les véhicules connectés. Toutefois, l'évolution des jurisprudences étasuniennes[43], européennes[44] et françaises[45] relatives à la protection des données personnelles questionne les modalités d'application du RGPD dans des environnements pluripartites comprenant un responsable de traitement en position dominante. À l'exception du premier traitement correspondant à l'inscription au service Biomem, les deux autres traitements portent sur des données dites sensibles telles que définies par l'**article 9 du RGPD** (données biométriques, et bien que définies par la directive ePrivacy, les données de localisation). De façon générale, quel que soit le type de traitement effectué dans le cadre de Biomem, le responsable du traitement est tenu de respecter les obligations suivantes prévues par la loi Informatique et Libertés[46] (ci-après « **LIL** ») et le RGPD :

- Le respect de la licéité du traitement (**Art. 7 de la LIL a** et **Art. 6 du RGPD**) ;
- Le respect de la transparence lors de la collecte des données personnelles **(Art. 6-1° de la LIL** et **Art. 5-1°, a du RGPD**) ;
- Le respect de la finalité du traitement (**Art. 6-2° de la LIL** et **Art. 5-1°, b du RGPD**) ;
- Le respect du principe de minimisation des données personnelles (**Art. 6-3° de la LIL** et **Art. 5-1°, c du RGPD**) ;
- La durée limitée de conservation des données (**Art. 6-5° de la LIL** et **Art. 5-1°, e du RGPD**) ;
- La sécurité des données (**Art. 34 de la LIL** et **Art. 5-1°,f du RGPD**) ;
- L'exercice des droits par les personnes concernées (**Art. 48 à 56 de la LIL** et **Art. 12 et s. du RGPD**).

---

42 CNIL, Pack de conformité, Véhicules Connectés et données personnelles, v.1., éd. Octobre 2017, https://www.cnil.fr/sites/default/files/atoms/files/pack_vehicules_connectes_web.pdf.

43 Voir dans ce sens l'accord transactionnel conclu entre la Federal Trade Commission et Facebook du 24 juillet 2020 qui impose une meilleure gestion dans le partage des données entre le réseau social et les applications reposant sur celui-ci, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

44 Voir dans ce sens par exemple les arrêts de la CJUE Wirtschaftsakademie (C 210/16 du 5 juin 2018) et FashionID (C/40/17 du 29 juil. 2019) qui redéfinissent la répartition des responsabilités lors d'un traitement effectué au travers d'un module fourni par un acteur dominant et réutilisé par un service tiers.

45 Voir dans ce sens les délibérations de la CNIL, Google (Délibération n°SAN-2019-001 du 21 janvier 2019), Stop covid (Décision n°MED-2020-015 du 15 juil. 2020) et Spartoo (Délibération n°SAN-2020-003 du 28 juillet 2020) qui questionnent chacune d'entre elles la réalité du consentement, la sécurité des données personnelles collectées et enfin le traitement de données tierces.

46 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018, texte 1.

Sous-Section 1. Les dispositions du RGPD applicables aux données d'inscription

19 L'inscription au service Biomem est le traitement de données personnelles le plus courant. Ces modalités d'inscriptions répondent au droit commun des données personnelles selon les modalités exposées ci-dessus.

	La licéité s'effectue sur le fondement de l'exécution du contrat conclu…	L'information est fournie à la personne concernée par une politique de confidentialité en ligne du service et…	La finalité recherchée est…	Les données collectées sont…	Les données sont conservées…	La sécurité est garantie par…
Biomem Indé (service indépendant)	entre Biomem et l'utilisateur	dans les CGU de Biomem-Indé	l'accès au service Biomem	- données de souscription à Biomem Indé - données d'accès aux services VOD - données du profil utilisateur	pour la durée contractuelle puis la durée légale d'archivage	des mesures de sécurité informatique et logique
Biomem-Constructeur (service ancillaire du constructeur)	entre le constructeur et l'utilisateur	dans un document distinct de l'achat du véhicule*		-données d'accès aux services VOD - données profils utilisateurs		
Biomem- VOD (service annexe du fournisseur de VOD)	entre le service de VOD et l'utilisateur	dans l'annexe au contrat de souscription au service VOD		- données comprises lors de la souscription au service VOD		

Tableau 3. Récapitulatif des obligations posées par le RGPD pour le traitement de données personnelles relatif à l'inscription au service Biomem
**« dans un document distinct de l'achat du véhicule »*[47]

47 Voir CNIL, Pack de conformité, Véhicules connectés et données personnelles, note supra, spéc. p. 13.

Sous-Section 2. **Les dispositions du RGPD applicables aux données biométriques**

20 La fonctionnalité principale fournie par le service Biomem repose sur l'identification automatique de l'utilisateur du service de vidéos à la demande par la comparaison entre la représentation photographique conservée dans le véhicule (« *Gabarit* ») avec une image capturée par le dispositif de lecture de vidéos installé dans le véhicule. Cette finalité répond donc au caractère fonctionnel de l'identification entraînant l'élection de l'image à la qualification de données biométriques. L'article 4-14° du RGPD définit ces dernières comme étant : « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ». Étant considérées comme des données sensibles, **les traitements de données personnelles biométriques** sur le terminal utilisé par la personne concernée doivent répondre tant aux exigences de la loi Informatique et Libertés que du RGPD. Les dispositions prévues par le **pack de conformité de la CNIL** doivent être en partie écartées de la présente espèce. L'hypothèse soulevée par l'autorité française porte sur un usage purement interne des données biométriques entraînant l'application de l'exemption domestique[48]. Or, le traitement Biomem de données biométriques entraîne, après une authentification de la personne concernée, l'émission du certificat du véhicule connecté vers le fournisseur de vidéos tiers, qui ne contient pas de données biométriques. Ainsi, les données biométriques restent sous le contrôle exclusif de la personne concernée puisque cette dernière est l'unique détentrice du support local sur lequel sont exclusivement conservées ses données biométriques. Seul un certificat confirmant l'authentification est émis vers le serveur distant du fournisseur de vidéos à la demande.

21 Notre hypothèse de travail se rapproche, toutefois, des faits décrits dans la **délibération n° 2016-212 du 7 juillet 2016**[49] rendue par la CNIL sous l'empire de la directive 95/46/CE[50]. L'espèce se situait alors dans une demande d'autorisation à la CNIL formulée par une société désireuse de mettre sur le marché son dispositif d'identification par empreinte digitale permettant à la personne concernée d'accéder à son compte bancaire. Techniquement, cette société prévoyait des conditions d'appairage d'un appareil mobile comprenant des données biométriques à un serveur distant et soumettait celui-ci au consentement de la personne concernée. Ces conditions font écho aux prescriptions de sécurité des données personnelles formulées par le pack de conformité de la CNIL[51] reprises dans les Lignes directrices 1/2020 du CEPD[52]. Selon ces autorités de contrôle, le gabarit correspondant à l'image de référence des données biométriques et à la suppression immédiate des empreintes réalisées à titre de comparaison doit être conservé localement. Cette obligation de conservation implique le contrôle exclusif du gabarit par la personne concernée ou son représentant légal. Dans le contexte spécifique de la voiture connectée, les autorités européennes et françaises invitent à ce que le gabarit soit conservé sous forme chiffrée sur un système d'information décorrélé de celui consacré à la conduite du véhicule. De surcroît, les deux autorités exigent du responsable du traitement qu'il fournisse des moyens d'identification alternatifs à la reconnaissance biométrique.

---

48 Voir Pack de conformité, spéc. p. 21-22.

49 Délibération de la CNIL n°2016-212 du 7 juillet 2016 autorisant l'association Natural Security Alliance à mettre en œuvre un système d'authentification biométrique basé sur la détention d'un ordiphone ou d'un support individuel contenant une application, placé sous le contrôle des personnes concernées, aux fins d'accès à des services.

50 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

51 Voir spécifiquement p. 21-22 du pack de conformité.

52 Voir spécifiquement p. 13, §§ 62-64.

	Le consentement de la collecte de données biométriques sera effectué auprès…	Outre les icônes de (dés) activation sur le tableau de bord, l'information relative à la collecte des données biométriques se manifeste par l'activation du service par la personne concernée…	La finalité recherchée est…	Les données biométriques collectées et conservées sont…	Hormis les données biométriques collectées à des fins de comparaison, qui sont effacées après la comparaison avec le gabarit, le gabarit est conservé…	La sécurité des données biométriques est garantie par leur chiffrement par défaut dans le véhicule connecté, et en particulier par…
Biomem Indé (service indépendant)	de la personne concernée par le responsable de traitement	à l'enrôlement effectué en local sur l'application Biomem	l'identification de la personne concernée par l'application Biomem pour accéder aux services VOD après l'émission d'un token en cas d'identification positive	le gabarit en basse résolution (les données biométriques sont effacées après comparaison)	jusqu'à la désinstallation du logiciel ou jusqu'à sa suppression manuelle	un chiffrement fourni par Biomem Indé des données biométriques avec des algorithmes à l'état de l'art
Biomem-Constructeur (service ancillaire du constructeur)					jusqu'à deux mois de non utilisation du logiciel ou sa suppression manuelle	les données biométriques qui sont chiffrées sur un système d'information distinct aux fonctions vitales du véhicules, et par les capteurs qui doivent être résistant aux attaques considérées comme triviales
Biomem- VOD (service annexe du fournisseur de VOD)					jusqu'à la désinstallation du logiciel ou sa suppression manuelle	un chiffrement fourni par Biomem VOD des données biométriques avec des algorithmes à l'état de l'art

Tableau 4. Récapitulatif des obligations posées par le RGPD pour le traitement de données personnelles biométriques par le service Biomem

Sous-Section 3. Les dispositions du RGPD applicables aux données de localisation

22 Le conducteur ayant installé le service Biomem peut activer le service de géolocalisation pour obtenir la fourniture de contenus vidéos contextualisés en fonction des points d'intérêts se trouvant sur le trajet du véhicule. Contrairement aux données biométriques, les données de localisation sont définies par la directive ePrivacy[53]. Toutefois, des mentions peuvent être trouvées dans le RGPD dans les définitions des données personnelles[54] et du profilage. L'article 4-4° du RGPD définit ce dernier traitement comme une méthode « *évalu(ant) certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant (…) la localisation ou les déplacements de cette personne physique* ». Ces données sont susceptibles d'être qualifiées de sensibles « *pour évaluer certains aspects personnels relatifs à une personne physique* »[55]. En outre, le CEPD estime que « *les trajets effectués sont très caractéristiques car ils permettent de déduire le lieu de travail et de résidence, ainsi que les centres d'intérêt (loisirs) du conducteur, et peuvent éventuellement révéler des informations sensibles telles que la religion à travers le lieu de culte, ou l'orientation sexuelle à travers les lieux visités* »[56]. Les **données de localisation** sont, à l'instar des données biométriques, soumises à des modalités spécifiques[57]. La personne concernée doit pouvoir contrôler l'activation de la collecte pour maintenir le contrôle sur l'utilisation de ses données personnelles sensibles. Toutefois, le RGPD délègue en partie la compétence de l'appréciation de la modalité des données sensibles aux États Membres[58]. Cette délégation emporte donc une marge de manœuvre indiquée dans les Lignes directrices 1/2020 du CEPD sur les véhicules connectés faisant écho aux prescriptions formulées par le pack de conformité de la CNIL[59].

23 Dans l'hypothèse de « *Pay as you drive insurance* » voisine à notre cas d'usage Biomem, le CEPD divise le traitement de données de localisation en deux parties. Le premier traitement porte sur la collecte de données personnelles de localisation à partir d'un service de communication publiquement disponible. Ce dernier est soumis à la directive ePrivacy, imposant donc le recueil du consentement. En revanche, pour le second traitement portant sur l'accès ou le stockage de données personnelles sur le terminal, le CEPD rappelle que la directive ePrivacy ne s'applique pas[60].

Toutefois, notre hypothèse de travail retient aussi la possibilité que ces données de localisation soient pseudonymisées en local[61] pour les agréger au profil utilisateur et en extraire des métadonnées. Ces métadonnées font l'objet d'une mise aux enchères en temps réel auprès d'annonceurs. Dans ce cas, le consentement éclairé de la personne concernée doit être collecté dans les conditions définies par le RGPD en amont de la mise aux enchères[62].

---

53 Voir supra §16, page 20 et s..

54 Article 4-1° du RGPD.

55 Article 4-4° du RGPD.

56 Voir dans ce sens les Lignes directrices 1/2020 du CEPD sur les véhicules connectés, p. 12 §60.

57 Voir dans ce sens les Lignes directrices 1/2020 du CEPD sur les véhicules connectés, p. 13, et pack de conformité de la CNIL, p. 29-30.

58 Dans ce sens, voir une lecture combinée des considérants 10 et 51 du RGPD.

59 Dont les exemples relatifs aux données de localisation traités dans le scénario 2 In->Out du pack de conformité (p. 22-31) offrent un panorama de différentes finalités.

60 Lignes directrices 1/2020, p. 22 §§ 105-106.

61 Voir dans ce sens les Lignes directrices 1/2020, p. 22 §108 et pack de conformité, p. 24 sous « *pour la finalité 1* ».

62 Décision n°2018-042 de la CNIL du 30 octobre 2018 mettant en demeure la société VECTAURY.

	Le consentement se manifestera par l'interface infodiver-tissement fournie par le constructeur et sera collecté par…	Outre les icônes de (dés) activation sur le tableau de bord, l'information relative à la collecte des données de localisation se manifeste par l'activation manuelle du service par la personne concernée…	La finalité recherchée est…	Après leur agrégation en local, et avant la mise aux enchères publicitaires, les données de localisation sont associées…	Hormis les logs de connexion conservés à des fins probatoires, les (méta) données sont…	La sécurité est garantie par des mesures de pseudo-nymisation traitées sur le support de l'utilisateur…
Biomem Indé (service indépendant)	Biomem-Indé	Information sur la page Internet dédiée de Biomem-Indé	la proposition de contenus et publicités contextuelles adaptée au trajet de la personne concernée	aux métadonnées issues du compte utilisateur	effacées lors de la désactivation du service	seules les métadonnées du trajet sont fournies au responsable de traitement
Biomem-Constructeur (service ancillaire du constructeur)	Biomem-Constructeur par l'intermédiaire de l'interface info-divertissement fourni	Information sur la page Internet dédiée de Biomem-constructeur				
Biomem- VOD (service annexe du fournisseur de VOD)	Biomem-VOD par l'interface du fournisseur de contenu	Information sur la page Internet dédiée de Biomem-VOD			effacées lors de la désactivation du service (sauf les logs de connexion archivés à titre probatoire)	les données pseudo-nymisées sont traitées de façon distincte du certificat émis à la connexion et à l'interruption du service

Tableau 5. Récapitulatif des obligations posées par le RGPD pour le traitement de données personnelles de localisation par le service Biomem

Nous pouvons remarquer que les obligations du responsable du traitement posées par le RGPD sont relativement similaires dans les trois hypothèses. En effet, le consentement semble être le fondement le plus indiqué pour encadrer les différents traitements Biomem. Les différences se situent davantage au niveau de la production de l'information préalable puisque les conditions varient en fonction du fondement du traitement. En revanche, les exigences relatives à la sécurité informatique des données personnelles varient peu puisque les données personnelles hautement sensibles sont traitées à l'intérieur du véhicule.

Mise à jour : Sous réserve des dispositions d'ordre public, l'article 5 de la proposition de règlement sur l'intelligence artificielle prévoit une interdiction des systèmes de reconnaissance par biométrie, dès lors que ces systèmes sont déployés dans un espace accessible au public. Cet espace est défini par l'article 4-39° comme étant « *tout espace physique accessible au public, indépendamment de l'existence de conditions d'accès à cet espace* ». Une telle définition exclut donc le véhicule automobile privé de son champ d'application.

Partie 2

Les méthodologies d'analyse de risque en matière de protection de données personnelles

La présente partie établit une comparaison entre les Lignes directrices concernant l'Analyse d'Impact relative à la Protection des Données (AIPD) publiées par le Comité européen de la protection des données avec les quatre méthodologies employées pour les cas pratiques susmentionnés.

Pour ce faire, le Chapitre 1, page 34, décrira lesdites Lignes directrices et la manière de déterminer si le traitement est « *susceptible d'engendrer un risque élevé* » aux fins du RGPD (Chapitre 2, page 46). Nous présenterons ensuite les méthodologies choisies pour en tirer des conclusions sur leur pertinence en matière de conformité au RGPD et de leur mise en œuvre opérationnelle (Chapitre 3, page 62).

Partie 2

Cette partie porte plus précisément sur les méthodologies d'impact.

En se focalisant dans un premier temps sur le contenu des Lignes directrices du CEPD consacrées à l'analyse d'impact relative à la protection des données, nous en tirerons les principes directeurs, c'est-à-dire les objectifs à respecter, et les acteurs à impliquer.

Ainsi les Lignes directrices se concentrent tout d'abord sur l'éligibilité d'un traitement à l'obligation de réaliser une AIPD avant de décrire succinctement le contenu de cette obligation.

Pour qu'un traitement soit soumis à cette obligation, celui-ci doit remplir a minima 2 des 9 critères d'éligibilité. Les paragraphes 4 et 6 de l'article 35 du RGPD offrent aux Autorités Nationales de Contrôle (ANC) la possibilité d'ajouter de nouveaux critères. La CNIL a ainsi inséré 4 critères d'éligibilité supplémentaires contraignant à la réalisation d'une AIPD. Parmi ceux-ci se trouvent les traitements relatifs à la géolocalisation[63].

En pratique, l'appréciation de ces critères reste à l'entière discrétion du responsable de traitement entraînant – parfois – l'écartement (in)justifié de certains d'entre eux par le responsable de traitement.

Après avoir rappelé la liberté de forme dans la méthodologie, le CEPD impose le respect de plusieurs étapes dans la réalisation de l'AIPD. Tout d'abord, (1) la première étape oblige le responsable du traitement à définir le cycle de vie des données personnelles pour identifier tous les types de vulnérabilités. (2) La seconde étape porte sur la nécessité et la proportionnalité des mesures dont le bon respect permet de préconfigurer la protection des données dès la conception ou par défaut. (3) La troisième étape porte sur l'analyse des risques en tant que tels pour décrire les différentes formes d'appréciation du risque interprétées par le CEPD. Cette analyse repose en grande partie sur une approche portant sur les impacts analysés à partir d'événements calculés en termes de vraisemblance ou de gravité. Enfin (4) la quatrième étape invite à conclure l'AIPD par une présentation des mesures d'atténuation des risques identifiés[64]. Ces mesures d'atténuation doivent répondre à « l'état des connaissances » tout en ayant un coût raisonnable. Toutefois cette dernière étape impliquant des mesures concrètes ne sera abordée qu'à titre illustratif.

Les recherches réalisées dans le cadre de l'axe 5 de la Chaire Connected Cars and Cybersecurity ont principalement porté sur la troisième étape. Ainsi, selon que l'on réalise une AIPD ou une EIVP, l'appréciation du risque est effectuée avec des menaces correspondantes différentes. Or, la classification des menaces basées sur la sécurité informatique (accès/modification/disparition), telle que prônée par la CNIL, altère l'appréciation des risques pour les données personnelles en se limitant aux seules obligations techniques. Au-delà de cette question de l'assiette du risque se pose également celle de la typologie de risque, invitant à considérer les risques, alternativement, et rarement cumulativement, comme internes à la structure (ex : salarié mécontent) ou externes à celle-ci (ex : hacker), entraînant donc un positionnement limitant l'analyse en elle-même.

Enfin, nous démontrerons que l'appréciation de la vraisemblance et de la gravité doit être abordée sous l'angle des personnes concernées et non, simplement, en fonction de l'unique point de vue du responsable de traitement.

---

63 Voir CEPD, Opinion 9/2018 on draft list of the competent supervisory authority of France regarding the processing operations subject to the requierement of a DPIA, 25/09/2018 https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_fr_sas_dpia_list_en.pdf.

64 La quatrième étape sera écartée de notre étude du fait de son caractère purement pratique.

Cette Partie se conclura par l'examen des méthodologies retenues, pour souligner leurs éléments convergents et divergents.

- La méthodologie CNIL (AIPD) répond *a minima* aux besoins des responsables de traitement de données personnelles « simples ». Cette méthodologie comporte un biais de sécurité informatique qui limite l'analyse des risques pour les « droits et libertés » des personnes concernées.

- La méthodologie PRIAM (EIVP, conçue sur le modèle d'une AIPD) semble être la plus adaptée aux traitements de données personnelles complexes et multipartites. Bien que respectant les obligations des Lignes directrices du CEPD, cette méthodologie souffre néanmoins d'une exhaustivité trop contraignante pour révéler son efficacité.

- La méthodologie BSI (AIPD) est une méthodologie clef en main offrant toutes les informations nécessaires pour réaliser une AIPD. Toutefois, cette méthodologie est obsolète car antérieure au RGPD et trop rigoureuse pour offrir aux opérationnels des adaptations factuelles nécessaires.

- Enfin, relevant du droit étasunien, la méthodologie NIST (EIVP) n'offre que trop peu d'accroches avec les Lignes directrices du CEPD pour s'avérer utile. Cette méthodologie est néanmoins utile pour apprécier les risques du point de vue de l'entreprise.

Ainsi pour 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 utile. Les risques formulés dans cette analyse sont susceptibles d'être pris en compte par la Cour de justice de l'Union européenne. Enfin, notre étude démontera que la distinction entre EIVP et AIPD s'amoindrit car on constate la convergence de l'assiette de risques considérée dans les deux cas.

Chapitre 1 La position du Comité européen de la protection des données sur les AIPD

Chapitre 1 La position du Comité européen de la protection des données sur les AIPD

Outre son exécution préalable à l'instauration du traitement de données personnelles, la réalisation d'une AIPD regroupe deux objectifs : celui d'être un outil d'évaluation des risques et de leur gestion subséquente. Ce second objectif vise à décider de l'opportunité d'identifier les risques pour les réduire en amont puis, en cas de risque résiduel, déterminer les mesures atténuations pertinentes pour en calculer les risques de réalisation, là où le premier objectif repose sur une appréciation subjective du niveau de risque encouru[65]. Les Lignes directrices AIPD du CEPD mentionnent principalement la gestion du risque, reléguant au second plan leur analyse. À cet égard, une lecture attentive de cette doctrine européenne concentre tout d'abord l'analyse des risques sur l'éligibilité des traitements envisagés à l'obligation de réalisation de l'AIPD (Section 1). Toutefois, l'approche réalisée en pratique inverse cette vision, témoignant la difficulté de la pratique à traduire opérationnellement le flou rédactionnel desdites Lignes directrices (Section 2, page 38).

Section 1. L'analyse d'impact d'un traitement de données personnelles et les acteurs impliqués

Cette section aborde tout d'abord les conditions d'éligibilité d'un traitement de données personnelles à faire l'objet d'une AIPD (§1) avant d'aborder les éléments requis pour sa réalisation (Sous-Section 2, page 37). Ces différents éléments permettront d'établir une grille de lecture utilisée pour formuler des critiques dans la section 2 du présent chapitre.

Sous-Section 1. L'absence de méthodologie et de critère uniques

24 À titre liminaire, il importe de signaler que sont explicitement exclues du présent rapport les obligations de réalisation d'évaluation d'impact sur la protection de données personnelles issues de textes normatifs autres que le RGPD[66], ne relevant pas du droit commun et donc de notre cas pratique. Les Lignes directrices concernant l'AIDP et la manière de déterminer si le traitement

65 R. GELLERT, « *Understanding the notion of risk in the general data protection regulation* », Computer Law & Security Review 34 (2018), pp. 279-288.

66 À savoir, la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (Article 27), JOUE L 119, 4.5.2016, p. 89–131, et règlement UE 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (Article 39), JOUE L 295, 21.11.2018, p. 39–98.

est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679[67] (ci-après « **Lignes directrices AIPD** ») formulées par le Groupe de Travail de l'Article 29 puis reconnues par le CEPD interprètent les dispositions prévues par l'**article 35 du RGPD** (reproduit dans le présent document en Annexe 1, page 152). Ce dernier article pose les conditions selon lesquelles une AIDP doit être réalisée. **Estimant qu'une seule méthodologie ne peut être applicable à toutes les situations**[68], les Lignes directrices invitent les responsables de traitement à analyser factuellement le traitement pour en tirer les éléments nécessaires à la « **gestion des risques** »[69]. **Cette invitation est encadrée par des prescriptions obligatoires prévues à l'Annexe 2**[70] **desdites Lignes directrices**[71]**.**

25 Par principe, l'AIPD est une obligation pour certains types de traitements de données prévus par le RGPD[72]. Le texte européen prévoit explicitement une liste de cinq critères distincts (1 à 5 ci-dessous). Dans son interprétation de l'article 35 du RGPD, le CEPD ajoute quatre nouveaux critères (6 à 9 ci-dessous) :

1. « *évaluation ou notation* »
2. « *prise de décision automatique* »
3. « *surveillance systématique* »
4. les « *traitements de données sensibles ou données à caractère hautement personnel* »
5. les « *données à grande échelle* »
6. « *le croisement ou combinaison d'ensembles de données* »
7. les « *données concernant les personnes vulnérables* »
8. l'« *utilisation innovante ou application de nouvelles solutions organisationnelles* »
9. les « *traitements empêch(a)nt les personnes concernées de bénéficier d'un service ou d'un contrat* »

---

67 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, adoptées par le Groupe de travail de l'article 29 sur la protection des données le 4 avril 2017 et mises à jour le 4 octobre 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

68 Lignes directrices AIPD, p. 20.

69 Id.

70 Voir Tableau 8, page 41 ci-dessous

71 Infra §25.

72 Ainsi l'article 35-3° prévoit une obligation pour les prises de décisions automatiques sur la base d'évaluation des personnes (a), le traitement de données personnelles sensibles (b) et une surveillance systématique à grande échelle (c).

En outre, les autorités nationales de contrôle ont la possibilité d'ajouter leurs propres critères. Ainsi la CNIL ajoute quatre critères supplémentaires pour des traitements concernant certains types de données ou certaines applications (10 à 13 ci-dessous)[73] :

10. Biométriques,
11. Génétiques,
12. De localisation,
13. À des fins de surveillance des salariés.

Pour qu'une situation soit considérée comme devant être soumise à une AIPD, le traitement doit comprendre au minimum deux « critères » des treize critères alternatifs énoncés. **Cette étape correspond à l'analyse du « seuil »**[74] où le « *traitement (…) susceptible d'engendrer un risque élevé* »[75] est constitué. Le responsable du traitement[76] est tenu donc de définir si le traitement qu'il projette d'implémenter peut-être qualifiable en tant que générateur d'un tel risque pour les « droits et libertés » des personnes concernées.

> Mise à jour proposition de règlement sur l'IA : Le texte prévoit l'obligation de réaliser une analyse d'impact pour les intelligences artificielles à « *haut risques* ». Contrairement au RGPD qui définit une liste exhaustive de traitements soumis à une AIPD, le règlement sur l'IA effectue un renvoi à son annexe III. Celle-ci est susceptible d'être actualisée par la Commission européenne. Les risques élevés identifiés relèvent alternativement de la sécurité des infrastructures essentielles, de l'exclusion de personnes à des droits ou à des services, ou d'une surveillance étatique trop importante.

26 Encore faut-il, pour déterminer une telle éligibilité à réaliser cette obligation, apprécier l'étendue du « *traitement* ». Sans remettre en cause la définition d'un traitement de données personnelles fournie par l'article 4-2° du RGPD[77], les Lignes directrices AIPD interprètent le premier paragraphe de l'article 35 du RGPD pour sous-diviser le traitement en une ou plusieurs « *opération(s)* »[78]. Cette distinction offre la possibilité de réaliser une seule AIPD lorsque différents responsables de traitement sont impliqués[79]. Cette AIPD doit mentionner le rôle précis de chacun d'entre eux et les obligations subséquentes leur incombant dans la protection des « *droits et libertés* » de la personne concernée[80]. En pratique, une interprétation alternative est retenue. Le responsable du traitement de données personnelles subdivise le traitement en plusieurs « *opérations* » distinctes lui permettant ainsi d'écarter les opérations « *triviales* » pour se concentrer sur les seules « *opérations* »

---

73 Voir l'avis 9/2018 du CEPD sur le projet de liste établi par l'autorité de contrôle compétence de la France concernant les opérations pour lesquelles une AIPD est requise (article 35-4° du RGPD) adopté le 25 septembre 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_fr_sas_dpia_list_fr.pdf.

74 Ou traduit en anglais par « *Threshold assessment* », mentionné par le Contrôleur européen de la protection des données, in « *Accountability on the ground part I: Records, registers and when to Data Protection Impact Assessment* », v.1.3, juillet 2019, https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf, p. 35, spéc. p. 11, K. DEMETZOU, « *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation* », Computer Law & Security Review 35 (2019) 105342, définit quant à elle cette étape comme l'examen de haut niveau (« *high level screening test* »).

75 CEPD, Lignes directrices, p. 9 et s..

76 Voir les développements spécifiques infra Sous-Section 2, page 37 sur cette question précise.

77 À savoir « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

78 Voir infra Chapitre 4, Section 2, page 53.

79 Lignes directrices spéc. p. 9.

80 Id.

« *susceptibles d'engendrer des risques élevés* ». Les autres opérations ne sont mentionnées qu'à titre accessoire. Cet examen de haut niveau correspond donc à la première étape de la gestion du « *risque* » pour le responsable de traitement[81] afin de déterminer l'opportunité de la réalisation d'une AIPD. Cette détermination doit être documentée en comprenant l'avis du Délégué à la Protection des Données (ou DPO pour *Data Protection Officer*).

Sous-Section 2. La participation des différentes parties prenantes directement impliquées dans le traitement

27 Les Lignes directrices AIPD du CEPD rappellent que l'article 35-2° du RGPD impose au(x) responsable(s) de traitement(s)[82] la réalisation de l'AIPD[83]. Elles mentionnent les participants chargés de la réalisation de l'AIPD, à savoir :

1. L'**équipe opérationnelle**, c'est-à-dire le « *maître d'ouvrage* »[84], est qualifiée par le CEPD comme étant le responsable de traitement. Ce département dans l'organisation juridique du « responsable de traitement » définit en effet les modalités et moyens du traitement. En d'autres termes, il détermine concrètement la raison du traitement, les modalités de la collecte des données personnelles, leur traitement ainsi que leur conservation[85]. Cette équipe opérationnelle est chargée de l'appréciation de la proportionnalité de la finalité du traitement des données personnelles[86], ainsi que de la définition de leur cycle de vie.
2. Le **Délégué à la Protection des Données** (DPO) est consulté dans le cadre de la réalisation de cette AIPD[87]. Toutefois, les Lignes directrices AIPD du CEPD cantonnent ce dernier à un seul rôle de conseil et de prescriptions dans l'accompagnement de la réalisation de l'AIPD.
3. Le **responsable de la sécurité des systèmes d'information** (RSSI) est invité au même titre que le DPO à apporter son expertise sur les systèmes d'informations utilisés pour définir les « *besoins en matière de sécurité ou de besoins opérationnels* »[88]. Ces besoins sont précisément exprimés lors du stade de la description technique et juridique du traitement et de la prise en compte des aspects cybersécurité des risques pour la protection des données[89].
4. Les éventuels **sous-traitants** doivent également participer à la réalisation de l'AIPD.
5. Dans le cadre d'un système pluripartite, les « **parties prenantes** », c'est-à-dire tant les équipes opérationnelles de chacun des responsables de traitement, que les DPO et les RSSI sont tenus de participer à l'élaboration de l'AIPD. Il importe de souligner que les parties prenantes ne prennent pas en compte les personnes concernées, utilisateurs finaux, relevant de la catégorie de « *personnes impliquées* ».

28 Le CEDP souligne que « *le responsable du traitement reste responsable en dernier ressort* » de la validation de l'AIPD, permettant ainsi une délégation partielle de l'obligation d'effectuer une AIPD à travers une prestation de service accordée à un tiers[90]. **Partielle, car le représentant légal du responsable de traitement doit, au nom du principe de responsabilité, rester décisionnaire de l'opportunité de mise en œuvre du traitement.** Ce caractère décisionnaire, étape relevant

---

81 Voir infra Partie 3 sur cette question.

82 Voir supra §24, page 34.

83 Lignes directrices AIPD, p. 17.

84 Pour reprendre la terminologie informatique.

85 Article 35-7, a du RGPD.

86 Article 35-7, b du RGPD.

87 Article 35-2 du RGPD.

88 Lignes directrices AIPD, p. 18.

89 Voir infra respectivement 1. et 4 du §29, page 38.

90 Les aspects de responsabilités contractuelles sur l'obligation de conseil d'un prestataire seront explorés en Partie 3.

de la « *gestion des risques* », engendre pour conséquence **l'entière discrétion du responsable de traitement dans l'appréciation des risques identifiés par le prestataire de service dans le cadre du traitement prévu**.

Les Lignes directrices AIPD ne se concentrent que peu ou pas sur la méthodologie à employer[91]. Elles définissent, en effet, des critères à prendre en compte dans la réalisation de l'analyse d'impact, tout en laissant le choix de la forme aux responsables de traitements[92]. Cette solution introduit certes une souplesse, mais aussi des incertitudes lors de la réalisation opérationnelle de l'AIPD.

Section 2. Les retours pratiques sur les quatre étapes de l'AIPD

29 La réalisation d'une AIPD pour un nouveau traitement de données personnelles *ab initio* invite à une lecture croisée des documents rédigés par le CEPD, à savoir, en 2017, les Lignes directrices AIPD et en 2019, les Lignes directrices relatives à la protection des données personnelles dès la conception et par défaut (ci-après « **Lignes directrices DPbDD** »)[93]. En tant qu'outil d'identification et de gestion du risque, **l'AIPD peut constituer une aide à la conformité à l'article 25 du RGPD dans l'accompagnement du déploiement d'un traitement de données personnelles**. En effet, de nombreuses terminologies utilisées par les Lignes directrices AIPD ont été affinées par les Lignes directrices DPbDD, chronologiquement ultérieures. De surcroît, elles invitent à réaliser une AIPD afin de respecter une partie des critères de la protection par défaut[94].

Sans rentrer dans le détail des critères à respecter, l'Annexe 2 des Lignes directrices AIPD établit une liste d'informations à renseigner dans une méthodologie utilisée pour réaliser une AIPD. Une classification en quatre étapes est possible :

1. La description exhaustive des modalités techniques et juridiques du traitement (flux de données, détermination du traitement, supports)[95] ;
2. L'appréciation de la nécessité du traitement envisagé et de la proportionnalité des mesures du respect des droits et libertés des personnes concernées ;
3. L'analyse du risque *per se*[96];
4. Une appréciation critique de l'évaluation d'impact par le DPO et les « *parties intéressées* ».

---

91 Le CEDP effectue un renvoi (in Lignes directrices, p. 18-20, spéc. p.20) à l'annexe 2 pour le contenu réel attendu de l'AIPD.

92 Voir dans ce sens Section 2, page 38 du présent chapitre.

93 CEPD, « *Guidelines 4/2019 on article 25, Data protection by design and by default* », 13 nov. 2019, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en, ci-après « Lignes directrices DPbDD » (*Data Protection by Design and by Default*).

94 Id. spéc. p.9, §§.28-31.

95 Nous renvoyons le lecteur à l'Annexe 2, page 154 du présent rapport, reproduisant l'Annexe 2 des Lignes directrices.

96 Voir infra Chapitre 2.

Étape	Acteurs	Caractère obligatoire
Description du traitement voir plus bas §30	Maître d'ouvrage	Oui
	RSSI	Oui
Description de la nécessité du traitement et de la proportionnalité des mesures voir §31	Maître d'ouvrage	Si existant
	RSSI	Oui
	DPO	Si existant
Appréciation des risques pour les droits et libertés voir §§32, page 42	Maître d'ouvrage	Oui
	RSSI	Oui
	DPO	Si existant
Implémentation des mesures, et garanties supplémentaires voir §35, page 43	DPO	Oui
	« Parties intéressées »	Encouragé

Tableau 6. Répartition des participants en fonction des quatre étapes définies par le CEPD

Sous-Section 1. La description du traitement

30 Pour définir précisément les tenants et aboutissants de la conformité du projet, la première étape est réalisée par le maître d'ouvrage pour justifier de la finalité du traitement ainsi que de sa mise en œuvre des points de vue opérationnels, techniques et juridiques en « *détermin(ant) les finalités et les moyens du traitement* » de données personnelles prévu. **En d'autres termes, l'équipe opérationnelle justifie le pourquoi du traitement devant être effectué** (afin de répondre aux besoins opérationnels exprimés). Cette première étape entend contraindre le responsable de traitement à s'interroger sur l'opportunité et la pertinence du traitement projeté.

Sous-Section 2. La nécessité et la proportionnalité des mesures présentes

31 La seconde étape renvoie aux mesures implémentées pour être conforme aux dispositions du RGPD. Le CEPD prévoit aussi deux phases distinctes pour déterminer les modalités :

- portant strictement sur la nécessité et la proportionnalité du traitement (1°) et renvoyant explicitement aux principes :
  - De finalité des données (Article 5-1-b du RGPD) ;
  - De minimisation des données (Article 6 du RGPD) ;
  - D'exactitude/de qualité des données (Article 5-1-c du RGPD) ;
  - De limitation de la conservation des données (Article 5-1-e du RGPD).
- contribuant au respect du droit des personnes concernées posées par le chapitre III du RGPD (Articles 12 à 23 du RGPD) ainsi que les articles 28 et 34 du RGPD et, le chapitre V relatif à l'exportation des données en dehors de l'Union européenne (2°).

1°) Ces principes énoncés du RGPD trouvent échos dans les Lignes directrices DPbDD qui, après les avoir présentés[97], précisent plus clairement leurs caractères[98].

97 Lignes directrices DPbDD, p. 11-13.

98 Lignes directrices DPbDD. Pour la finalité des données voir p. 18, le principe de minimisation voir p. 19, l'exactitude des données, voir p. 21, la limitation de la conservation, voir p. 22-23.

Principe	Article du RGPD	Critères posés par les Lignes directrices DPbDD
Finalité du traitement de données personnelles	5-1-b	Prédétermination des données personnelles Spécificité du traitement Orientation de la finalité Nécessité du traitement Compatibilité de la nouvelle finalité avec celle déclarée à la personne concernée Limitation de réutilisation des données personnelles Vérification régulière de l'adéquation avec le traitement par le responsable de traitement Limitation technique de réutilisation
Minimisation des données	6	Pertinence des données personnelles par rapport à la finalité Nécessité du traitement Limitation des données personnelles Agrégation des données personnelles Pseudonymisation des données personnelles Anonymisation des données personnelles Effacement du traitement
Exactitude des données	5-1-c	Fiabilité de la source de données personnelles Degré d'exactitude des données personnelles Mesurabilité de l'exactitude Vérification régulière de l'adéquation entre les données personnelles et le traitement par le responsable de traitement Rectification des données personnelles erronées Limitation des erreurs accumulés Accès aux données personnelles par la personne concernée Mise à jour des données personnelles
Limitation de la conservation des données	5-1-e	Suppression (automatique) des données Définition des modalités du stockage Politiques de rétentions de données précises Efficacité de l'anonymisation/suppression Justification de la durée de conservation des données personnelles Redondance et logs

Tableau 7. Correspondance entre les principes énoncés pour la conformité du traitement et les critères énoncés dans les Lignes directrices DPbDD

2°) Les modalités du respect des droits des personnes varient en fonction du fondement de licéité du traitement déterminé par le responsable de traitement. Dans le cas pratique Biomem-Indé (§13, page 12), portant sur des traitements reposant alternativement sur l'exécution contractuelle (**Article 6-b du RGPD**) ou sur le consentement (**Article 6-a du RGPD**), la personne concernée est en droit d'invoquer le respect du droit au principe de transparence et du principe de loyauté. Ces deux principes sont explicités dans les Lignes directrices DPbDD du CEPD. Toutefois, l'exercice du droit à la portabilité des données personnelles[99] est susceptible de poser un problème dans les hypothèses de Biomem-Indé et Biomem-Constructeur[100].

Principe	Article du RGPD	Critères posés par les Lignes directrices DPbDD
Principe de transparence **(« vis-à-vis des informations fournies à la personne concernée »)**	Lecture conjointe des articles 12, 13, 14 et 34 du RGPD	Clarté pour la personne concernée Sémantique adaptée pour le public visé Accessibilité des informations Contextualisation des informations en fonction de la forme et du moment de la collecte des données personnelles Design universel Multicanal (papier, site internet, courriel)
Principe de loyauté	5-1-a	Pertinence du fondement du traitement Différentiation entre les licéités des traitements Finalité spécifique du traitement Nécessité du traitement Respect de l'autonomie de la personne concernée Possibilité pour la personne concernée de retirer son consentement Balance des intérêts du responsable de traitement et de la personne concernée Prédétermination de la finalité avant l'exécution du traitement Cessation du traitement Ajustement des données personnelles Configuration par défaut Allocation précise des obligations incombant à chaque responsable de traitement impliqué

Tableau 8. Correspondance entre les principes énoncés pour le respect du droit des personnes concernées et les critères énoncés dans les Lignes directrices DPbDD

99 Prévu par l'article 20 du RGPD.

100 Ces deux hypothèses correspondent aux situations où le responsable du traitement est soit l'éditeur d'un logiciel hébergé dans le véhicule, soit le constructeur du véhicule connecté. Dans ces deux cas, les données biométriques et de localisation ne peuvent pas être *de facto* extraites du véhicule. En plus de leur chiffrement, notre cas pratique prévoit une absence d'interopérabilité des données biométriques avec des systèmes d'informations tiers. Les données de localisation sont quant à elles effacées à la fin du trajet.

Sous-Section 3. **L'analyse des risques en tant que tels**

32 La troisième étape formulée par le CEPD correspond à l'obligation définie par l'**article 35-7°,c du RGPD**[101] d'identifier les risques dans l'AIDP. Un renvoi au paragraphe premier de ce même article est effectué pour définir les circonstances requérant la réalisation d'une AIPD[102]. En d'autres termes, le paragraphe premier ne mentionne les risques que de façon incidente. Il convient alors de se reporter aux **considérants 84 et 90** du RGPD qui précisent les modalités de l'appréciation du risque et qui rappellent le caractère probatoire de l'AIPD[103]. Ainsi, ces deux considérants imposent l'évaluation d'un risque à partir de son « *origine, (…) nature, (…) particularité* ». Mais ces considérants suggèrent une appréciation alternative de chacun des risques (accès illégitime aux données, modification non désirées des données et disparition des données) du point de vue de la personne concernée et non du responsable de traitement. Cette étape permet d'envisager les « *mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre* »[104] comme moyen d'atténuation des risques. Le considérant 90 prévoit que ces mesures – proportionnelles à la probabilité et la gravité du risque – soient mentionnées dans l'analyse.

33 Après avoir défini, « *l'origine, la nature, la particularité et la gravité des risques* » puis les « *sources de risques* », les **impacts** sur les « *droits et libertés* » des personnes concernées doivent être analysés en cas d'**événements** « *tels qu'un accès illégitime aux données, une modification non désirée de celles-ci ou leur disparition* ». Bien que traitant spécifiquement de l'analyse des risques comme étape préalable à l'implémentation des mesures pour la protection des données dès la conception / par défaut, le CEPD apparente ces événements/risques, dans son annexe 2 des Lignes directrices AIPD, aux dispositions relatives à la sécurité informatique prévues par l'article 32-1°,b du RGPD[105]. À la suite de cette identification, les menaces conduisant à un accès illégitime, à une modification non désirée de ces données ou à leur disparition doivent être prises en compte pour calculer leur **vraisemblance** et leur **gravité** permettant ainsi l'étude des **mesures d'atténuation du risque**.

Δ Il est intéressant de noter que la version française du RGPD utilise la notion de « gravité » pour traduire à la fois « *severity* » (Art. 35 du RGPD) et « *gravity* » (Art. 83 du RGPD). La *gravité-severity* renvoie à la « gravité » telle qu'étudiée, c'est-à-dire le risque à prévoir et à atténuer. À l'inverse, la *gravité-gravity* renvoie à la gravité du risque réalisé. Sous réserve de précision contraire, la « gravité » mentionnée renvoie à la *gravité-severity*.

34 Comme précisé, les mesures doivent être proportionnelles aux risques identifiés. Le **considérant 84** relativise cette obligation en rappelant que celles-ci doivent répondre à l'état des connaissances et à un coût (raisonnable) de mise en œuvre. Les Lignes directrices DPbDD définissent, pour leur part, l'**état des connaissances** comme étant « *une obligation continue de veille technologique à*

---

101 Article 35-7,c du RGPD qui dispose « *une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1* ».

102 Selon l'article 35-1 du RGPD, « *Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »

103 Selon le considérant 84 du RGPD, « *Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement.* » ; et selon le considérant 90 du RGPD *in fine* « *Cette analyse d'impact devrait (…) démontrer le respect du présent règlement* ».

104 Les « *mesures appropriées* », « *l'état des connaissances* » et les « *coûts liés à leur mise en œuvre* » sont des notions développées par les Lignes directrices DPbDD, voir infra §33 et suivants.

105 Lignes directrices DPbDD, p. 9, §28.

la charge des responsables de traitement sur les plans organisationnels et techniques pour faciliter la mise à jour de ces mesures ». Le **coût** est défini quant à lui par un rappel de l'obligation du responsable de traitement d'investir dans des mesures garantissant le respect des droits et libertés des personnes concernées.

Sous-Section 4. L'appréciation critique de l'analyse d'impact

35 En l'absence de respect des obligations décrites, le RGPD prévoit « *une amende administrative pouvant s'élever jusqu'à 10 000 000 euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé* » étant retenu en cas de non-réalisation d'une AIPD[106] ou d'une analyse incorrecte[107]. Toutefois, les fondements justifiant cette sanction doivent être relativisés. À notre sens, les analyses doctrinales de Mme DEMETZOU[108] sont erronées. La chercheuse estime que le respect du formalisme énoncé par le RGPD, tel qu'interprété par le CEPD, suffit à se voir reprocher la réalisation d'une AIPD « *incorrecte* ». À notre sens, les aspects formels des AIPD ne peuvent fonder un grief à l'encontre du responsable de traitement souhaitant s'affranchir des listes prévues par le CEPD. Comme le démontrera la section suivante, les grandes lignes méthodologiques sont respectées par les praticiens. Des libertés pratiques sont néanmoins prises sur les points flous de la doctrine officielle.

106 Article 35, §§ 1, 3 et 4.

107 Article 35, §§ 2 et 7 à 9, Voir spécifiquement infra Partie 3.

108 K. DEMETZOU, « *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation* », Computer Law & Security Review 35 (2019), 105342.

Chapitre 2 Les retours des expériences sur les modalités de réalisation de l'AIPD

Chapitre 2

Chapitre 2 Les retours des expériences sur les modalités de réalisation de l'AIPD

36 Notre analyse critique sur les retours d'expérience repose sur :

- les entretiens réalisés entre décembre 2019 et juin 2020 auprès de 6 professionnels (Consultants, chercheurs, et DPO d'entreprises spécialisés en objets connectés ou/et informatiques, de ministères) sur la base du questionnaire reproduit en Annexe 3, page 156 ;
- le rapport en date du 6 juillet 2020 réalisé par le Contrôleur européen à la protection des données sur l'implémentation des AIPD par les autorités européennes[109] ;
- les AIPD réalisées par le ministère de la Justice néerlandais et par l'équivalent irlandais de la Haute Autorité de Santé (« *Health Service Executive* » ou « HSE ») qui emploient tous les deux une méthodologie respectueuse des Lignes directrices AIPD du CEPD mais qui différent dans leur rédaction,
- la doctrine juridique[110] et les arrêts rendus[111] par les différentes juridictions compétentes sur la question des AIPD ;
- l'illustration de ces critiques au travers du cas pratique Biomem (cf. page 12).

37 Hormis les travaux doctrinaux français au lendemain de l'entrée en vigueur du RGPD[112] et quelques articles doctrinaux étrangers concomitants à celle-ci, les questions des modalités de réalisation d'une AIPD n'ont pas été abordées au niveau des juridictions locales[113], et n'ont fait l'objet de publications par les institutions publiques[114], que depuis peu (septembre 2020). Seule la recherche

---

109 Contrôleur européen de la protection des données, *Survey on Data Protection Impact Assessments under Article 39 of the Regulation*, 6 juillet 2020, https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en.

110 Voir les travaux de K. DEMETZO et R. GELLERT cités antérieurement, ainsi que les travaux du DPIA LAB dirigé par ce dernier, http://www.dpialab.org/.

111 CJUE, 8 avril 2014, C-293/12 et C-594/12, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a..

112 Voir la citation de X. MAGNON supra §1, page 2.

113 Voir dans ce sens Décision de la CNIL n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des Solidarités et de la Santé, et Cour d'appel administrative d'Écosse du Sud, R (Bridges) v. CC South Wales, 11 août 2020, [2020] EWCA Civ 1058, https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/.

114 Voir dans ce sens ministère de la Justice néerlandais, DPIA Office 365 for the Web and mobile Office apps, 20 juin 2020, https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps, Health Service Executive (ci-après « DPIA HSE »), DPIA Covid Tracker App, 26 juin 2020, https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20.

académique informatique[115] semble s'intéresser à cette question en France[116]. Si l'apport de la norme ISO 29134 « *Information technology — Security techniques — Guidelines for privacy impact assessment* » a constitué un outil significativement éclairant des modalités de la réalisation de cette pratique, son emploi reste toutefois limité[117], du moins pour l'instant. Dans un premier temps, les Lignes directrices AIPD prévues par le Comité européen de la protection des données seront explicitées (Section 1) pour ensuite les confronter aux retours de praticiens (Section 2, page 53).

Section 1. L'interprétation pratique des obligations de conformité relatives à l'AIPD

38 Cette section reprend les retours pratiques pour analyser les différentes étapes mentionnées dans le chapitre précédent. Ainsi les quatre étapes précisées distingueront les prescriptions théoriques de la réalité du terrain. Malgré l'existence de méthodologies institutionnelles[118], les retours pratiques démontrent une divergence tant dans le choix[119] que dans l'utilisation *per se*[120] des méthodologies disponibles. Cette divergence s'explique par une méconnaissance de l'outil et par la liberté méthodologique permise par le CEPD entraînant une variation importante dans l'examen effectif de l'analyse de risques[121] et une hétérogénéité des méthodologies AIPD utilisées[122]. Ces disparités

Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf, «*EDPS, survey on DPIA under article 39 of the Regulation* », 6 juillet 2020.

115 Voir les travaux de Daniel LE METAYER (infra Chapitre 2) dont C. Castelluccia, D. Le Métayer. « *Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode.* » [Rapport de recherche] Inria Grenoble Rhône-Alpes. 2019, https://hal.inria.fr/hal-02373093/document.

116 Voir en Belgique la Chaire DPIA LAB au sein de l'université libre de Bruxelles dont les travaux seront mentionnés par la suite.

117 Les praticiens interviewés ont précisé connaître l'existence de cette norme mais ne pas l'avoir achetée. Les autorités ne mentionnent aucunement son existence. Cette question n'est abordée que de façon incidente par l'expression d'un besoin de standardisation dans le rapport du Contrôleur européen des données personnelles.

118 Voir infra Chapitre 3, page 62 du rapport.

119 Ainsi un cabinet d'avocat français nous a expliqué préférer la méthodologie de l'*Information Commissioner's Office* (ICO) pour des raisons d'expériences professionnelles.

120 Lors d'un entretien, un consultant nous a expliqué utiliser les étapes posées par la méthodologie AIPD de la CNIL pour ne pas « *heurter* » les agents de la CNIL.

121 *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. p. 6 « *There is a remarkable spread regarding the length of the DPIAs provided, which ranges from five to 55 pages.* »

122 La majorité des praticiens consultés utilisent la méthodologie CNIL (3) qui peut être amendée en fonction des besoins, l'un des praticiens consultés utilise sa propre méthodologie, un DPO sous-traitant à une société de conseil ignore la

illustrent au mieux une liberté dans l'interprétation des Lignes directrices du CEPD, ou *a minima*, le respect minimaliste de l'obligation de réaliser à une AIPD[123].

Sous-Section 1. La définition du seuil déclenchant l'obligation de la réalisation d'une AIPD

39 Les retours des praticiens interrogés sur l'appréciation du seuil imposant la réalisation d'une AIPD[124] trouvent écho dans le rapport du Contrôleur européen à la protection des données[125] qui souligne lui aussi le caractère discrétionnaire de l'appréciation du seuil[126]. Cette situation conduit parfois au fractionnement d'un traitement, quand il inclue deux critères d'éligibilité à cette obligation, pour rester artificiellement sous le seuil[127]. A contrario, l'AIPD du HSE[128] mentionne implicitement ces seuils[129], là où celle réalisée par le ministère de la Justice des Pays-Bas se concentre uniquement sur les « *risques élevés* » identifiés comme fondement de l'AIPD[130]. Le rapport du Contrôleur européen révèle, quant à lui, deux tendances.

1. La première tendance est une utilisation de l'AIDP pour des solutions d'informatique en nuage, c'est-à-dire le recours à des solutions logicielles hébergées sur des serveurs appartenant soit aux donneurs de licences, soit à ses sous-traitants. Cette hypothèse a justifié la réalisation d'une AIPD par le ministère de la Justice des Pays-Bas pour l'implémentation de la solution Microsoft dans ses services. Cette tendance démontre aussi des questionnements sur la protection des données personnelles dans des circonstances de dématérialisation totale de l'outil de travail, et des possibilités de constituer une intrusion importante dans la vie privée des salariés par le recoupement de données personnelles.
   Une telle vision est également présente dans la décision de la CNIL relative à l'application mobile Stop Covid[131]. En effet, l'autorité française reproche au ministère de la Santé français de ne pas avoir pris en compte le système d'identification reCaptcha installé dans la première version de l'application. Cette fonctionnalité, un service proposé par Google, ouvre en effet la possibilité d'interconnexion de jeux de données permettant l'identification des utilisateurs de cette application et constitue dès lors un risque important d'atteinte aux données personnelles de santé.
   Enfin, la dématérialisation de ces services numériques entraîne la possibilité de transférer des données personnelles en dehors du territoire européen. Ainsi, dans sa Foire Aux Questions interprétative de l'arrêt C-311/18[132], le CEPD rappelle l'interdiction du transfert des données personnelles vers les États-Unis. Cette interdiction ne doit donc pas pourtant être interprétée comme un nouveau critère de l'AIPD justifiant une obligation de réalisation[133]. L'exportation de

méthodologie utilisée dès lors qu'elle répond aux obligations légales et le dernier la méthodologie de l'*Information commissioner's office* (ICO), le DPIA réalisé par le ministère de la Justice néerlandais a été fait à partir de la méthodologie de l'ICO (voir dernière note, page 46), le DPIA du HSE ne mentionne aucune méthodologie précise.

123 Voir infra §45, page 53 et s. sur la question de la détermination du risque.

124 Voir supra Chapitre 3, Section 1, page 34.

125 Voir dans ce sens *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. pp. 8-10.

126 Voir dans ce sens Center for Information Policy Leadership (ci-après « CIPL »), « *Risk, high risk, risk assessment and DPIA under the GDPR* », 21 oct. 2016, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf, spéc. p. 7, qui déclarait alors : « *the actual process or methodology of risk assessment, i.e. how the various risky activities or threats and harms should be assessed, weighed and evaluated, should largely be left to individual organisations* ».

127 Voir infra §40, page 49.

128 « Health Service Executive».

129 Voir Health Service Executive (ci-après « DPIA HSE »), DPIA Covid Tracker App, p. 3.

130 Voir ministère de la Justice néerlandais, « *DPIA Office 365 for the Web and mobile Office apps* », p. 7.

131 Voir CNIL, Délibérations MED 2020-15 du 15 juillet 2020 et MEDP-2020-003 du 16 juillet 2020 résumées sur https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles.

132 Arrêt CJUE, 16 juillet 2020, C-311/18, Data Protection Commissioner c.Maximillian Schrems et Facebook Ireland.

133 Cette question est indirectement adressée à la fin de la section 2 du chapitre 3 de cette partie.

données personnelle est soumise à des dispositions spécifiques prévues par les articles 44 à 50 du RGPD.

2. La seconde tendance identifiée par le Contrôleur européen concerne la thématique des critères élisant un traitement à l'obligation légale de réaliser une AIPD. L'appréciation discrétionnaire des critères par les responsables de traitement entraîne la minimisation ou l'écartement d'un des critères afin de rester sous le seuil sans justifier réellement ce choix[134]. Ce caractère discrétionnaire traduisant un respect minimaliste des dispositions de l'article 39 du RGPD démontre une volonté réelle de certaines agences européennes de ne pas se soumettre aux AIPD. Les entretiens avec des responsables juridiques de collectivités territoriales justifient leur volonté d'écarter leurs traitements des AIPD par l'impossibilité technique et organisationnelle d'implémenter toutes les mesures adéquates. Au cours d'un de ces entretiens, un responsable expliqua ainsi que seuls les fonctionnaires titulaires étaient formés aux dispositions du RGPD, tandis que les vacataires en contrat à durée déterminée ne reçoivent aucune formation spécifique pour le traitement des données personnelles et ne sont tenus que par le renvoi à de vagues dispositions contractuelles de confidentialité.
Enfin, l'arrêt de la Cour d'Appel d'Écosse fonde l'obligation de réaliser une AIPD sur le droit national[135] dont les dispositions ne mentionnent guère de seuil autre que les « *risques élevés* »[136]. Cette imprécision démontre la difficulté d'appréciation de ces risques élevés qui peut parfois tenir de l'arbitraire, les tribunaux contrôlant seulement le formalisme du respect des obligations légales comme par exemple la fourniture d'une information claire aux personnes concernées.

40 Les praticiens de l'AIPD soulignent aussi la difficulté de l'appréciation du seuil antérieurement à la réalisation du schéma représentant le flux des données personnelles. En effet, le schéma des flux de données personnelles permet de visualiser l'intégralité de leur cycle de vie, révélant ainsi – en partie – certains « *risques élevés* ». Or, effectuer l'analyse du seuil préalablement à la réalisation du flux de données n'offre pas cette révélation[137].

> Retours Pratiques : Un entretien a révélé que l'AIPD était réalisée uniquement lorsque le traitement prévu s'avérerait être pertinent, c'est-à-dire au moment de son industrialisation. Bien que traitant des données personnelles, les phases d'expérimentation réalisées sur le terrain ne faisaient l'objet, d'après ce DPO, d'aucun encadrement juridique. Un autre entretien réalisé auprès d'un consultant a souligné la possibilité de subdiviser le traitement global, sujet à l'obligation d'une AIPD, en plusieurs traitements distincts. Cette division présentationnelle permet ainsi d'introduire des traitements autonomes qui répondent au mieux à un seul critère, dérogeant ainsi à l'obligation de réaliser une AIPD tout en étant, de prime abord, conforme au RGPD.
>
> Biomem comprend trois opérations distinctes (l'inscription, la reconnaissance faciale et la géolocalisation) pour une finalité première (la recommandation publicitaire contextuelle à une géolocalisation fournie par un service de VOD à un passage identifié par un système de reconnaissance faciale).

---

134 Voir *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. p. 9.

135 Cour d'appel administrative d'Écosse du Sud, R (Bridges) v. CC South Wales, 11 août 2020, [2020] EWCA Civ 1058, §29 où le juge administratif rappelle que le fondement de cette obligation légale est l'article 64 du *Data Protection Act* de 2018, là où la CNIL dans sa décision du 15 juillet 2020 se fonde sur l'article 35-7°,a du RGPD.

136 Article 64 du Data protection Act « *Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.* »

137 Voir dans ce sens les travaux du DPIA Lab de l'ULB qui invitent à commencer par la réalisation des flux de données, « *Data protection impact assessment in the European Union: developing a template for a report from the assessment process* », 2020, disponible en téléchargement à https://dpialab.wordpress.com/publications/, pp. 29, spéc. p. 5.

Deux possibilités s'offrent à nous :

- ces trois opérations distinctes pourraient devenir des traitements autonomes susceptibles d'être considérés comme n'entraînant pas de « *risque élevé* » écartant ainsi l'obligation d'une AIPD.
- dans l'hypothèse Biomem VOD, où l'application est exclusivement fournie par le service de vidéos à la demande, le constructeur ne serait considéré que comme un « *fournisseur de technologie* » tenu de s'assurer seulement des risques élevés relatif à « *la sécurité des données* », telle que définie à l'article 20 du RGPD.

Sous-Section 2. Les relations entre les acteurs participants à l'AIPD

41 À l'instar des Lignes directrices AIPD, le rapport du Contrôleur européen souligne le caractère pluripartite de la réalisation de l'AIPD[138]. La composition des participants d'une AIPD varie en fonction de la taille de l'entreprise. Un représentant de la DSI doit systématiquement être impliqué. La présence du DPO varie en fonction de son existence dans l'entreprise du responsable du traitement[139], de son éventuelle disponibilité ou de sa sollicitation par le consultant[140]. Les retours des DPO consultés reflètent l'impression que cet acteur n'est cantonné qu'au seul rôle de validation. Le rapport du Contrôleur européen souligne ce constat au sein des institutions européennes[141]. Les DPO n'ayant pas recours à des consultants estiment, quant à eux, avoir exclusivement la charge de la réalisation des AIPD. Cette position leur permet de profiter des relations interpersonnelles dans leur entreprise pour obtenir les informations nécessaires à la réalisation de l'AIPD. En effet, la transmission de l'information pertinente est caractérisée comme étant l'un des principaux obstacles rencontrés par les consultants, entraînant parfois de longs retards dans la fourniture de l'AIPD. Ce sentiment de « *team building* »[142] dans la définition des pires scénarios relatifs au traitement est également ressenti par les clients de ces consultants interrogés. En effet, ces clients interrogés estiment que l'expertise de ces consultants est parfois floue, mal expliquée et ne répond qu'aux besoins de conformité court-termistes du département finançant la seule consultation. Le suivi et la mise à jour de l'AIPD sont généralement considérés comme relevant exclusivement des obligations du responsable de traitement ou d'une prestation supplémentaire. Enfin, les différents entretiens relativisent l'implication des sous-traitants dans la fourniture d'informations pertinentes à la réalisation de l'AIPD, leur préférant, à titre subsidiaire, les documentations techniques afférentes.

Sous-Section 3. L'appréciation de la licéité

42 La seconde étape de l'AIPD est en pratique assez classique en droit des données personnelles puisqu'elle reprend les obligations traditionnelles posées par le chapitre II du RGPD. Cette étape ayant été traitée au Chapitre 2, page 18, les présents développements se concentreront sur les points pratiques soulevés par les documentations mentionnées précédemment au §36, page 46. Ainsi, il est nécessaire de rappeler que le choix du fondement de licéité est purement contextuel et qu'il relève presque du choix discrétionnaire du responsable de traitement.

---

138 Rapport du Contrôleur européen, p. 14-17.

139 L'un des consultants propose comme service supplémentaire de sensibiliser le DSI aux problématiques des données personnelles.

140 Ainsi lors d'un de nos entretiens, un DPO a souligné n'avoir été consulté qu'au début du contrat de prestation par le consultant et à la fin de la prestation pour livrer ses observations.

141 Voir *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. pp. 13-14 où sur les 25 AIPD réalisées par les autorités européennes, seules « *18 are consulted (…);11 are involved in drafting; 7 are or were involved in the provision and the design of the respective template; five review the finalized product (…) and three mention their involvement in drafting the records and keeping the register* ».

142 Pour reprendre les termes du Contrôleur européen, voir *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. p. 9.

► Précision juridique : Un tempérament doit être apporté dans le cas d'un traitement réalisé sur le fondement d'une obligation légale[143]. Cette dernière étant l'expression de la souveraineté nationale, l'analyse d'impact subséquente porte non pas sur la finalité du traitement en fonction des « *risques élevés aux droits et libertés* » mais sur les modalités concrètes d'implémentation de ce traitement. En d'autres termes, seules sont examinées les questions de sécurité informatique et de mesures organisationnelles à implémenter au sein de la structure juridique du responsable de traitement.

Les consultants et DPO spécialisés en objets connectés précisent le recours quasi-systématique aux fondements de l'intérêt légitime et du consentement pour fonder la licéité du traitement de données personnelles.

Purpose	*Legal ground*	*Government organisations as data controllers*	*Joint controllers*	*Microsoft as data controller*
Type of data processing		*Contents and cloud logs Office for the Web, logs Connected Cloud Services, Processor Connected Exp, logs Azure AD*	*Telemetry Office for the Web, Telemetry mobile Office apps, traffic to 3d parties & Controller Connected Exp.*	*Same types of processing as joint controllers*
Providing the service, incl. troubleshooting and bug fixing	*Consent*	✗	✗	✗
	Contract	✓	✗	✗
	Legitimate & Public interest	✓	✗	✗
Providing updates	*Consent*	✗	✗	✗
	Contract	✓	✗	✗
	Legitimate & Public interest	✓	✗	✗
Security	*Consent*	✗	✗	✗
	Contract	✓	✗	✗
	Legitimate & Public interest	✓	✗	✗
17 different purposes mobile Office apps and the Controller Connected Exp., including transfer of personal data to third parties	*Consent*	✗	✗	✗
	Contract	✗	✗	✗
	Legitimate & Public interest	✗	✗	✗

Figure 2. *Tableau explicatif des fondements de licéité dans l'AIPD réalisée par le ministère de la Justice néerlandais*
(extrait de ministère de la Justice néerlandais, DPIA Office 365 for the Web and mobile Office apps, p. 103)

143 Article 6-e du RGPD.

Sous-Section 4. Les problématiques remontées pour un traitement pluripartite

L'analyse du schéma de flux de données offre la possibilité d'identifier toutes les parties prenantes, définissant ainsi la répartition de leurs obligations[144]. Ainsi dans l'hypothèse où l'un des acteurs collecte et traite des données personnelles au lieu de n'être tenu qu'aux seules opérations de maintenance et de sécurité, il se voit requalifié comme responsable de traitement, et doit dès lors figurer, en tant que tel, dans l'AIPD[145]. Rien ne précise l'obligation d'annexer à l'AIPD le contrat[146] fixant les responsabilités entre les différents responsables conjoints[147]. Cette annexe peut rendre les éléments contractuels dans sa forme exhaustive ou sous une forme agrégée.

43 Dans un contexte de responsabilité conjointe, la question de l'information de la personne concernée incombe généralement au responsable de traitement de premier niveau[148]. La jurisprudence de la CNIL a permis d'affiner des directives précises quant à la fourniture de cette information préalable[149]. L'exécution de l'obligation d'informations préalables à la personne concernée est obligatoire pour éviter le risque élevé d'asymétrie d'informations[150], c'est-à-dire conformément aux préconisations prévues par les principes de transparence et de loyauté[151].

Dans les Lignes directrices 1/2020 sur la voiture connectée, le CEPD préconise le recours à des icônes sur le tableau de bord. L'objection de la disponibilité de cette information au seul conducteur et au passager se situant à l'avant du véhicule peut être faite. D'autre part, par sa forme, cette information est limitée, ce qui peut faire l'objet d'un grief dans un contentieux futur quant à la conformité de l'information.

44 Cette obligation de coopération s'étend également aux sous-traitants[152]. Toutefois, les praticiens privés et publics montrent une difficulté à mobiliser les éventuels sous-traitants dans la réalisation de l'AIPD[153]. Ces derniers se contenteraient seulement de fournir une documentation technique avec des spécificités relatives aux données personnelles. Les résultats du présent rapport identifient deux obstacles. Le premier, méthodologique, concerne les modalités de coopération à l'AIPD par les acteurs, et les marges de manœuvre disponibles pour éviter que l'implémentation de mesures adéquates ne devienne un poste de coût trop important pour les parties. Le second est l'implication des gestionnaires de « *plateformes importantes* », disponibles uniquement dans l'hypothèse de marchés importants. Toutefois, le rapport du Contrôleur européen propose comme innovation juridique de conditionner le contrat de prestation informatique, objet de la sous-traitance, à l'assistance à la réalisation de l'AIDP et au respect des mesures adéquates définies, contraignant ainsi le sous-traitant à une obligation de coopération.

---

144 Voir infra §49, page 56.

145 Voir dans ce sens CNIL, Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des Solidarités et de la Santé.

146 Comme mentionné dans le « *data sharing code of practice* » de l'ICO anglaise dont la première version date du 15 juillet 2019, https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf.

147 Définie à l'article 26 du RGPD.

148 Voir supra §14, page 13 (et suivants), sur la seconde hypothèse du cas pratique Biomem.

149 Voir dans ce sens CNIL, Décision n° MED 2018-042 du 30 octobre 2018 mettant en demeure la société VECTAURY, Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC et enfin Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des Solidarités et de la Santé.

150 Voir dans ce sens CEPD, Lignes directrices 1/2020 relative au véhicule connecté, spéc. p.10 §§44 et s.

151 Voir supra Tableau 8, page 41.

152 Article 35-8 du RGPD.

153 Voir dans ce sens *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. pp. 16-17.

Section 2. **L'appréciation de l'analyse des risques** *per se*

45 Lors des entretiens, beaucoup d'avis divergents ont été formulés au sujet de l'AIPD. Toutefois, une constante semble faire consensus : le flou définitionnel des « *risques élevés* » au sens de l'article 35 du RGPD et de son interprétation par le CEPD. Ainsi, hormis les autorités de contrôle, tant les autorités institutionnelles[154], que les chercheurs[155], sans oublier les groupes de réflexions de praticiens[156], reprochent cette absence définitionnelle suscitant des interprétations diverses. Ces divergences s'en ressentent dans l'assiette du risque à prendre en compte, dans sa qualification en tant que « *risque élevé* » et par conséquent dans le calcul et dans l'appréciation de la vraisemblance et de la gravité de la réalisation de ce risque. Cette dispersion entraîne donc une cacophonie méthodologique permettant l'inscription de certains « *risques élevés* » en lieu et place d'autres risques. La confusion est alimentée par le texte même du RGPD. Les considérants 65, 83, 85[157] de ce texte font état de « *dommages* » correspondant aux « *risques élevés* » mentionnés par l'article 35.

46 Le CEPD, influencé par la CNIL, accepte l'héritage de la méthodologie d'analyse des risques de sécurité informatique prescrite à l'article 32 du RGPD pour définir les objectifs contenus dans l'analyse de protection des données personnelles[158]. Ce positionnement entraîne l'utilisation terminologique propre à l'analyse de risque en cybersécurité (« *événement* », « *menace* », « *source de risque* »)[159]. Toutefois, dans l'analyse préconisée par le CEPD dans ses Lignes directrices AIPD, l'institution européenne part de « *l'impact* » sur les « *droits et libertés* » pour en tirer des « *événements* » à partir desquels les « *menaces* » doivent être identifiées. La logique juridique se base traditionnellement sur un déroulement naturel reposant sur un postulat de départ avec un fait générateur (menace) suscitant (événement) un dommage (impact)[160]. Or, le CEPD fait le choix d'une inversion totale de la chaîne de causalité. Ce choix est cependant compréhensible dans le cadre d'une politique d'approche par les risques[161] dans lequel l'AIPD est le symbole d'une réflexion aboutie, car pluripartite, du responsable de traitement. Il semble d'autant plus justifié dans une vision anticipatrice du risque. Ainsi, le présent rapport se focalise sur la question de l'identification des risques et des menaces (Sous-Section 1, page 54) avant de s'intéresser à leur appréciation (Sous-Section 2, page 56).

---

154 Voir *EDPS, Survey on DPIA under Article 39 of the Regulation*.

155 Dans ce sens D. LE METAYER et S. JOYEE DE, « *Priam: a privacy risk methodology* », 14 avril 2016, https://hal.inria.fr/hal-01302541/document, pp. 51, spéc. p. 39 qui justifient leur démarche en comparant leur démarche avec les travaux antérieurs, DPIA LAB, « *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* », https://cris.vub.be/files/37820556/dpialab_pb2017_1_final_FR.pdf, p. 9 spéc. p. 8 §5.c. où les auteurs invitent à « *clarifier la terminologie utilisée* ».

156 Dans ce sens, CIPL, « *Risk, high risk, risk assessment and DPIA under the GDPR* », p. 6 qui en appelait déjà en 2016 à une définition collective du risque.

157 Ainsi que les considérants 75, 83 et 85 du RGPD.

158 Voir supra §32, page 42.

159 Dans ce sens D. LE METAYER et S. JOYEE DE, « *Priam: a privacy risk methodology* », spéc. p. 39 qui formule ce reproche à l'égard de la méthodologie CNIL.

160 Voir infra Partie 3, Chapitre 2, page 114.

161 Dans ce sens R. 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* », 2016, Eur. Data Prot. L. Rev. 481.

Sous-Section 1. La problématique de l'identification des risques

47 Ayant toujours été qualifiées comme problématiques[162], les analyses de risques pour la protection des données entraînent une assiette de risques importante difficilement déterminable. Ainsi, de nombreuses analyses d'impact pour la protection des données prennent en compte des risques relevant davantage de l'évaluation d'impact pour la vie privée[163] ou d'éléments connexes mais se trouvant hors du champ traditionnel de la protection des données personnelles[164]. Ces éléments connexes, tels que l'adoption technologique d'un outil par les utilisateurs[165], impactent indirectement les personnes concernées. Bien qu'entrant incidemment dans le cadre de l'AIPD, cette extension aux risques indirects illustre la volonté implicite exprimée par le RGPD de contraindre le responsable du traitement à vérifier la pertinence du traitement et sa licéité par son changement d'échelle. Cette vision étendue à plusieurs niveaux de sources de risques reste exceptionnelle. Le retour d'expérience des praticiens illustre une analyse des risques plus restreinte en se reposant, parfois, sur la trilogie « *accès-modification-disparition* » propre à la sécurité informatique. Certains d'entre eux contestent cette typologie de menace, l'estimant problématique par rapport au droit des données personnelles. La problématique de la « *réutilisation illicite des données* » notamment comprend à la fois l'accès et la modification des données. De surcroît, aucune référence explicite n'est faite à la trilogie « *accès-modification-disparition* »[166] dans les cinq types de risques explicitement identifiés par les Lignes directrices relatives au véhicule connecté du CEPD[167].

48 Les sources de risques prises en compte comprennent rarement l'appréciation des risques cumulant à la fois des vulnérabilités provenant des aspects organisationnels et des aspects technologiques et une analyse portant à la fois sur les risques internes à la structure réalisant le traitement et les risques externe à ladite structure. La variation des sources de risques est contextuelle, et seules les AIPD faisant l'objet d'une vérification obligatoire auprès de la CNIL prennent en compte toutes les sources de risques, les autres analyses ne portant que sur les sources de risques les plus évidentes et immédiates.

Se pose toutefois la question du moment de l'appréciation des sources de risques relatifs au respect des droits de la personne concernée. Certains praticiens professent son examen au seul moment de la conformité, là où d'autres définissent la prise en compte de l'exercice effective de ces droits comme une source de risques autonomes.

► La vision pragmatique, préconisée par les partenaires de la Chaire C3S, est d'implémenter l'exercice de ces droits de la personne concernée au niveau de la conformité pour, soit écarter ce risque, soit le mentionner de manière à en réduire la gravité au moment de l'analyse de risque.

---

162 Voir supra §46, page 53.

163 Voir par exemple DPIALAB, « *Data protection impact assessment in the European Union: developing a template for a report from the assessment process* », version 5.2., 30 juin 2020, https://owncloud.vub.ac.be/index.php/s/nKSbYOV5lHrKKnV, p. 29 spéc. p. 10 où les auteurs incluent les risques mentionnés au considérant 4 du RGPD (liberté d'opinion, d'expression, de la vie privée…), voir également D. LE METAYER, S. DE JOYEE, PRIAM.

164 DPIALAB. p. 11 où sont pris en compte l'évaluation environnementale du projet de traitement, l'évaluation éthique, etc. Voir DPIA HSE, qui prévoit comme risque le dysfonctionnement de la technologie Bluetooth et sa consommation énergétique, p. 37.

165 Id., qui identifie comme risque l'absence d'utilisation de l'application de *contact tracing*, p. 34, ou l'absence de pertinence de celui-ci dans un contexte de pandémie, p. 36.

166 La seule mention qui en est faite est lors de la présentation des catégories de données, et plus spécifiquement des données révélant les infractions, pour souligner le besoin d'implémenter des mesures adéquates afin d'assurer l'inaccessibilité de ces données, p.13, §65.

167 CEPD, Lignes directrices 1/2020 relatives au véhicule connecté, spéc. p. 10-12 §§44-57.

	Source de risque organisationnel	Source de risque technologique	Source de risque interne	Source de risque externe	Respect des droits des personnes concernées
Fichiers administratifs publics	Maximal	Moyen	Moyen	Minimal	Moyen
IoT	Minimal	Moyen	Moyen	Important	Minimal
IoT de santé	Maximal	Maximal	Maximal	Maximal	Maximal
Logiciels	Minimal	Minimal	Minimal	Moyen	Moyen
Base de données	Moyen	Minimal	Moyen	Important	Minimal
Biomem-indé	Maximal (de nombreuses parties prenantes)	Moyen (le logiciel et le dispositif sont fournis par des tiers)	Minimal (mesures organisationnelles)	Important (mesures technologiques)	Important (information qui doit être disponible en permanence)
Biomem-constructeur	Moyen (sécurité)	Important (technologie propriétaire)	Moyen (mesures organisationnelles et technologiques)		Moyen (renvoi à l'annexe du contrat à l'achat du véhicule et aux *privacy policies*)
Biomem-VOD	Minimal (un seul acteur)		Minimal (mesures organisationnelles)		Minimal (renvoi au contrat initial conclu en ligne)

Tableau 9. Retour d'expériences sur l'identification des sources de risques et comparaison avec le cas pratique Biomem

Un enseignement peut être tiré des AIPD mises à disposition par les institutions publiques : l'identification de nombreuses sources de risques entraîne un calcul du risque moins poussé[168] (et donc des mesures « *adéquates* » plus génériques) qu'une identification de peu de risques, qui elle entraîne une réelle analyse avec des mesures adéquates plus adaptées aux risques[169]. La seconde option est indubitablement optimale et devra faire l'objet d'une introduction par le responsable du traitement réalisant l'AIPD dans laquelle la démarche d'exclusions de certains risques sera expliquée, à l'instar de l'analyse d'impact réalisée par le ministère de la Justice néerlandais relative aux services Microsoft.

168 Dans ce sens, HSE, p. 33-50, annexes E et F, qui listent les sources de risques et les mesures adéquates proportionnelles.

169 Dans ce sens, ministère de la Justice, DPIA, pp. 114-128 où l'AIPD analyse chacun des risques avant d'établir une correspondance spécifique avec des mesures adéquates organisationnelles et techniques.

Sous-Section 2. **L'appréciation des risques**

49 L'obligation d'analyse des risques « *du point de vue des personnes concernées* » est un concept difficile à appréhender. Comme le souligne le Contrôleur européen à la protection des données, « *the risks towards the 'rights and freedoms' of the data subjects is a concept difficult to be grasped, as there is no immediate connection between the processing of personal data and how adversely that could affect rights and freedoms. Data processing is seen as something ethereal that has no direct impact on the lives of the data subjects, and if so happens, it is only limited cases under exceptional circumstances* »[170].

En pratique, l'analyse des risques implique d'utiliser certaines méthodologies qui présentent l'inconvénient majeur de se limiter aux seuls points de vue juridiques ou réputationnels. Ces méthodologies sont ainsi utilisées comme aides à l'analyse des risques liés au traitement de données personnelles, puis à la gestion de ces risques[171]. Cependant, l'absence de définition des sources de risques, à la fois dans le RGPD et dans les Lignes Directrices sur les AIPD, entraîne une réelle difficulté à identifier et à calculer ces risques. Il n'est donc pas surprenant que les méthodologies étudiées présentent de réelles divergences d'interprétation à ce propos[172].

L'examen des AIPD réalisées par les institutions démontre une divergence dans les méthodes de calcul basées sur la vraisemblance[173] et la gravité[174]. Ainsi, l'AIPD effectuée par le ministère de la Justice néerlandais définit *in concreto* la gravité[175], en qualifiant le risque par rapport à l'atteinte aux droits de la personne concernée par un traitement illicite, avant de se concentrer sur la vraisemblance de la réalisation d'un tel risque. Le caractère quasi-systématique de la vraisemblance est présent dans cette analyse d'impact. Cependant, le ministère de la Justice n'offre pas une vision précise des critères permettant l'appréciation de la vraisemblance[176]. À l'inverse, le Health Service Executive irlandais effectue son calcul de risque sous la forme d'un tableau listant risque, vraisemblance et impact, dans trois colonnes respectives, suivies d'une note attribuée à la seconde et à la troisième colonne. Ces deux notes sont ensuite multipliées pour obtenir un score, déterminant ainsi le niveau de criticité du traitement[177].

---

170 Voir *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. p. 7.

171 Sur cette thématique Partie 3, page 91.

172 *EDPS, Survey on DPIA under Article 39 of the Regulation*, spéc. p. 23 : « *The tool concerning calculation of risk could be more detailed* ».

173 Voir dans ce sens K. DEMETZOU, p. 9 qui rappelle que la vraisemblance était judiciairement caractérisée par une « *simple possibilité* ». L'auteure relativise ses propos en déclarant que cette vision était antérieure au RGPD. Toutefois, l'arrêt Schrems du 16 juillet 2020 tendrait à lui donner tort par son analyse superficielle de la condition de vraisemblance.

174 Voir infra Chapitre 3 où nous reviendrons sur l'exclusion de la gravité par la méthodologie PRIAM. Toutefois, K. DEMETZOU (id.) rappelle que la seule analyse d'un risque à la lueur de la gravité doit être requalifiée d'« *inférence* ».

175 Deux mentions sont notables. La première est à la reprise de la définition posée par l'ICO (p. 117). Le ministère analyse ensuite les risques en fonction du type de traitement de données et de la vraisemblance avant de mentionner de nouveau la gravité à titre conclusif (p.127).

176 Ainsi dans le risque du refus au droit d'accès à la personne concernée (p. 121-122), l'analyste déclare : « *The impossibility for data subjects to exercise their fundamental privacy rights per definition leads to a high risk. In addition, the processing of personal data about the use of some mobile Office apps for marketing purposes can lead to major risks and impact for the data subjects, through unlawful further processing of personal data of employees, but also through the re-identification of pseudonymised data by linking unique identifiers from multiple sources. The probability that these risks occur is 100%, now that Microsoft has refused to grant the requested access* ».

177 Cette méthode de calcul se retrouve également dans la méthodologie NIST (infra Chapitre 3) et dans la méthodologie développée par le DPIALAB, p. 21,1.1.5.-b avec pour méthode de calcul « (R = L[P] * S) ».

Likelihood	Score
Highly Unlikely	1
Unlikely	2
Possible	3
Likely	4
Highly Likely	5

Impact	Score
Negligible	1
Minor	2
Moderate	3
Major	4
Critical	5

Overall	Score
Low	1-7
Medium	8-14
High	15-25

Figure 3. *Méthode de notation par le Health Service Executive*
Voir note[178]

Comme nous le verrons, ce type de calcul se retrouve également dans les méthodologies de la CNIL ou du NIST. Le résultat permet de prioriser les traitements susceptibles d'engendrer des risques importants afin de déterminer les risques résiduels. Toutefois, les extraits de l'AIPD réalisées par le HSE (Figure 4 et Figure 5) illustrent la réalité des praticiens. En effet, la notation reste discrétionnaire, soumise à l'appréciation de l'analyste, sujet à une validation par le représentant légal de la structure.

50 La notation issue du calcul de risque questionne donc la sincérité de la correspondance de la notation aux dommages anticipés de la personne concernée par le responsable de traitement. Ce dernier, rédacteur ou validateur de l'AIPD, peut relativiser l'étendue du dommage anticipé. En effet, si le **considérant 84** du RGPD dispose que : « *Certains types de traitements et l'ampleur et la fréquence des traitements sont susceptibles d'engendrer un tel risque élevé et peuvent également causer un dommage ou porter atteinte aux droits et libertés d'une personne physique* », ce même considérant limite l'assiette de cette atteinte à la seule question du « *traitement des données personnelles* ». Le lien effectué entre « *l'ampleur et la fréquence des traitements* » et le dommage ou les risques d'atteinte aux droits et libertés de la personne concernée tels que décrit par le **considérant 75** du RGPD[179], définit, lui, les types de dommages opposables au responsable de traitement.

178 Id., p. 22. Tableau repris de https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf.

179 « *Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées* ».

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
1.	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the HSE's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes	If the app is successful there is a high risk that other uses will be seen as attractive to introduce. Also, uses may include informal use in the private sector for purposes the app is not intended for	Any increase in app purposes has the potential to impact all users of the app, and to potentially undermine public confidence in the app	4	5	20
2.						

Figure 4. Notation du risque par le HSE avant l'application d'une mesure adéquate

No.	Risk	Measures to Mitigate Risk	Likelihood with measures in place	Impact with measures in place	Residual Risk	Measures approved	Remaining risk to data subjects
1.	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the HSE's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes, or for other purposes not in line with the original purpose	- Implement clear and transparent communication including DPIA and source code publication - Terms of reference of the App Advisory Committee to include the purposes and to charge the Committee with ensuring data is processed in line with those purposes and any changes are carefully assessed, are lawful, are lawfully introduced, and reflected in the DPIA - Ongoing assessment of the app, the data it processes and in particular an ongoing assessment for changes from an ethical, data and privacy perspective - Ensure app is entirely voluntary to use - Monitor continuously for misuse that violates the app's voluntary nature with a view to legislating if required to protect this design principle - Charge Governance Committee with wind down once the COVID-19 crisis is over	2	1	2	Yes	Little risk remaining to data subjects if all measures are implemented as all changes require to respect legislation, and informal (outside of public bodies) use will be protected if misuse is detected
2.							

Figure 5. Notation du risque par le HSE après l'application d'une mesure adéquate

> Plusieurs praticiens ont déclaré opter pour des systèmes de notations paires, évitant ainsi les notes « *neutres* » et contraignant le représentant légal du responsable de traitement à se positionner dans l'analyse des risques.

51 C'est à ce niveau d'appréciation que l'utilisation de la notion de « *droits et libertés* » devrait être exclue pour se concentrer uniquement sur le droit à la protection des données personnelles, comme l'indique le considérant 84 du RGPD. En effet, une analyse des risques concentrée sur un autre sujet que la protection des données, c'est-à-dire l'utilisation des données pour une finalité recherchée, relève davantage de l'EIVP ou de l'EIA. Mais le considérant 146 du RGPD prévoit que le juge de l'Union européenne dispose de la compétence d'interpréter les « *dommages* » comme une notion autonome entrouvrant la possibilité d'une requalification dans ce sens.

Néanmoins, nous ne pouvons que préconiser l'emploi de méthodologies d'analyses de menaces de la vie privée rigoureuses. On peut ici se référer à la méthodologie dite LINDDUN – préconisée par la méthodologie NIST – pour déterminer les seuls risques touchant au respect de la vie privée[180]. Il est également possible de se rapporter à l'analyse des sources de risques établie indirectement par le groupe de travail de l'article 29 dans son avis 05/2014 sur les techniques d'anonymisation[181]. Dans cet avis, le groupe de travail de l'Article 29 développe trois critères pour apprécier l'efficacité d'une anonymisation des données personnelles : l'individualisation[182], la corrélation[183] et l'inférence[184]. Antérieur au RGPD, cet avis ne fait l'objet d'aucune reconnaissance par le CEPD interrogeant sa validité normative.

52 Enfin, afin de prendre en compte le « *risque social important* » mentionné au **considérant 85** du RGPD, d'aucuns proposent de définir ce nouveau risque pour mieux le prévenir[185]. Cette démarche est à l'heure actuelle difficile à implémenter, car aucune méthodologie n'offre de modalités pour l'appréciation d'un risque encouru par une communauté ou ayant un impact national.

---

180 Voir dans ce sens la méthodologie NIST qui y fait référence ou la méthodologie PRIAM qui s'en inspire ouvertement.

181 Groupe de Travail de l'article 29 sur la protection des données, Avis 05/2014 sur les techniques d'anonymisation, adoptée le 10 avril 2014, https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr.pdf.

182 L'avis 05/2014 (p.13) définit l'individualisation comme « *la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données* ».

183 L'avis 05/2014 (p.13) définit la corrélation comme « *la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée, ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes)* ».

184 L'avis 05/2014 (p.13) définit l'inférence comme « *la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs* ».

185 Voir le *Centre for Information Policy Leadership*, références supra. spéc. p. 27-28 §5.3-c, EDPS, « *Accountability on the grounds* », spéc. p. 30 qui effectue un lien entre les nouvelles technologies et leurs conséquences sociétales non anticipées. Dans le même sens DPIALAB, « *AIPD dans l'UE : une protection plus solide pour les personnes : une protection juridique des personnes plus solides en complétant le nouveau cadre juridique* », p. 3.

Chapitre 3 L'analyse des quatre méthodologies retenues sous le prisme des Lignes directrices AIPD du Comité européen de la protection des données

Chapitre 3 L'analyse des quatre méthodologies retenues sous le prisme des Lignes directrices AIPD du Comité européen de la protection des données

La présentation de chacune des quatre méthodologies explorées (CNIL, PRIAM, BSI, NIST) sera d'abord réalisée (Section 1) pour en tirer leurs caractéristiques propres permettant leur croisement et leur comparaison (Section 2, page 83).

Section 1. Présentation et critiques des méthodologies utilisées

Pour répondre à notre problématique de recherche d'un traitement de données personnelles impliquant plusieurs parties dans un contexte de véhicule connecté, nous avons retenu quatre méthodologies distinctes :

- L'analyse d'impact pour la protection des données personnelles de la Commission Nationale pour l'Informatique et les Libertés française (**CNIL**) (Sous-Section 1, page 63) ;
- La méthodologie *Privacy Risk Analysis Methodology* (**PRIAM**) de Sourya Joyee De et de Daniel Le Metayer (Sous-Section 2, page 68) ;
- La méthodologie du *Bundesamt für Sicherheit in der Informationstechnik* allemand (**BSI**) (Sous-Section 3, page 73) ;
- La méthodologie du *National Institute of Standards and Technology* étasunien (**NIST**) (Sous-Section 4, page 75).

Outre l'application de ces méthodologies au cas pratique Biomem, nous avons choisi de retenir les cinq risques tels que définis par le CEPD dans ses Lignes directrices 1/2020 sur le véhicule connecté[186]. Ces cinq risques sont :

1. Le manque de contrôle et l'asymétrie de l'information ;
2. La qualité du consentement de l'utilisateur ;
3. La réutilisation illicite des données personnelles ;
4. La collecte excessive des données ;
5. La sécurité des données personnelles.

Démonstration sera faite que certaines méthodologies sont incomplètes quant à l'identification des risques pour la protection des données. Ainsi, la méthodologie NIST invite, par exemple, à se reporter à la méthodologie de modélisation des menaces pour la vie privée proposée dans le cadre d'une collaboration entre les groupes de recherche DistriNet et COSIC de l'université de KU

186 Lignes directrices 1/2020, p.10-12 §§42-57.

Leuven belge[187]. À l'inverse, les concepteurs de la méthodologie PRIAM estiment leur méthodologie autosuffisante[188].

Sous-Section 1. La méthodologie de la CNIL

53 Mise à jour d'une méthodologie antérieure au RGPD[189] adoptée en 2012 par la CNIL, la méthodologie AIPD « *Privacy Impact Assessment* » est accessible sur le site internet de la Commission[190]. Elle se compose de quatre documents distincts[191] et d'une version logicielle régulièrement mise à jour permettant de réaliser l'analyse conformément au formalisme fortement recommandé par la CNIL[192]. Méthodologie courte (13 pages), il faut atteindre la sixième page pour que la méthodologie soit abordée par une vue d'ensemble des flux de données (*data flow*) avant d'étudier les principes fondamentaux[193]. L'étude des risques est, comme l'illustrent le titre de la page 8 et le renvoi explicite à l'article 32 du RGPD, consacrée aux « *risques liés à la sécurité des données* ». Cette approche correspond à **la première étape** posée par le CEPD (« *Description exhaustive des modalités techniques et juridiques du traitement* »).

La seconde étape posée par le CEPD, l'appréciation de la nécessité du traitement envisagé et de la proportionnalité des mesures du respect des droits et libertés, est subdivisée en deux parties :

- dans un premier temps, la nécessité et la proportionnalité sont succinctement examinées à travers le renseignement brut des informations relatives à la finalité, aux fondements, à l'adéquation, à la mise à jour et à la durée de conservation des données personnelles ;

187 Pour *Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance*, https://www.linddun.org/.

188 Voir dans ce sens PRIAM, pp. 39-40, https://hal.inria.fr/hal-01302541/document.

189 https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf.

190 https://www.cnil.fr/en/privacy-impact-assessment-pia.

191 La méthodologie en tant que telle, les connaissances de base, le modèle du PIA, et un cas pratique illustratif « Captoo » et l'application aux objets connectés. Ces différents documents sont disponibles au lien suivant : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd.

192 La première version a été mis à jour le 24 juin 2020.

193 C'est-à-dire « *l'évaluation des mesures garantissant la proportionnalité et la nécessité des mesures* » et « *l'évaluation des mesures protectrices des droits de la personne concernée* ».

- dans un second temps, l'exercice du droit des personnes est traité de la même manière, c'est-à-dire par l'indication de la méthode d'information préalable, la méthode de recueil du consentement, l'exercice des droits d'accès et de portabilité, les modalités d'exercice des droits, la définition des précises des obligations du sous-traitements et l'indication sur d'éventuels transferts des données personnelles.

Pour la troisième étape (« *Appréciation des risques pour les droits et libertés* »), la CNIL choisit l'analyse prônée par l'interprétation du considérant 90 du RGPD par le CEPD pour définir le « *risque* », c'est-à-dire proche de l'analyse de sécurité informatique des données personnelles. Ainsi après avoir invité l'analyste à mentionner les mesures existantes pour prévenir les risques, la CNIL définit ceux-ci en se référant à ses modalités de réalisation :

« (1) comment **des sources de risques** (ex. : un salarié soudoyé par un concurrent)

(2) pourraient exploiter les **vulnérabilités des supports de données** (ex. : le système de gestion des fichiers, qui permet de manipuler les données)

(3) dans le cadre de **menaces** (ex. : détournement par envoi de courriers électroniques)[194] et (4) permettre à des **événements redoutés** de survenir (ex. : accès illégitime à des données)

(5) **sur les données à caractère personnel** (ex. : fichier des clients) et

(6) ainsi provoquer des **impacts sur la vie privée des personnes concernées** (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels)[195]. »

Cherchant certes à qualifier certaines notions (« *risques* », « *vulnérabilités* », « *événements redoutés* »), cette définition, qui a le mérite d'être proposée, est néanmoins critiquable sur plusieurs points.

Le point le plus évident est que les quatre premières conditions relèvent de la sécurité informatique, reléguant au second rang les risques relatifs aux données personnelles. Le vocabulaire est similaire à celui employé dans les méthodologies d'analyse du risque en cybersécurité d'EBIOS[196]. Si cet examen est optimal dans l'hypothèse d'un fournisseur de technologie répondant parfaitement à la crainte exprimée par le CEPD quant à la sécurité des données personnelles collectées dans le véhicule connecté, il reste moins adapté à un traitement plus large.

Les deux derniers éléments générateurs (vulnérabilités et menaces) peuvent être substitués par n'importe quels autres types de faits générateurs des dommages. Ce choix assumé par la CNIL, entraîne un examen *a minima* des traitements de données personnelles en se focalisant uniquement sur la conformité informatique et organisationnelle. Le risque devient un terme « *tautologique* » englobant tout aléa, autre que les obligations de conformité, se trouvant dans le périmètre d'intervention du responsable de traitement. Bien que la CNIL décrète une causalité entre ces différents critères, le lien ainsi établi est discutable.

Outre cette définition du risque comprenant six éléments générateurs, la CNIL apprécie le niveau du risque au travers de la vraisemblance des menaces et de la gravité des impacts sur la vie

194 Notre ajout.

195 Notre ajout.

196 Voir dans ce sens ANSSI, *EBIOS Risk Manager*, 2019, p. 96, https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf, p. 93, spéc. pp. 82-91, où le risque est défini comme la « *possibilité qu'un événement redouté survienne et que ses effets impactent les missions de l'objet de l'étude* ». Les termes utilisés par la CNIL trouvent leur inspiration dans les méthodologies d'analyse du risque en cybersécurité d'EBIOS.

privée. Le critère de vraisemblance doit être apprécié sous le prisme des « menaces » regroupant les « *sources de risques* » engendrant les « *supports des données* », là où le critère de gravité regroupe les « *événements redoutés* » subdivisés par « *données personnelles* » engendrant « *des impacts potentiels* »[197].

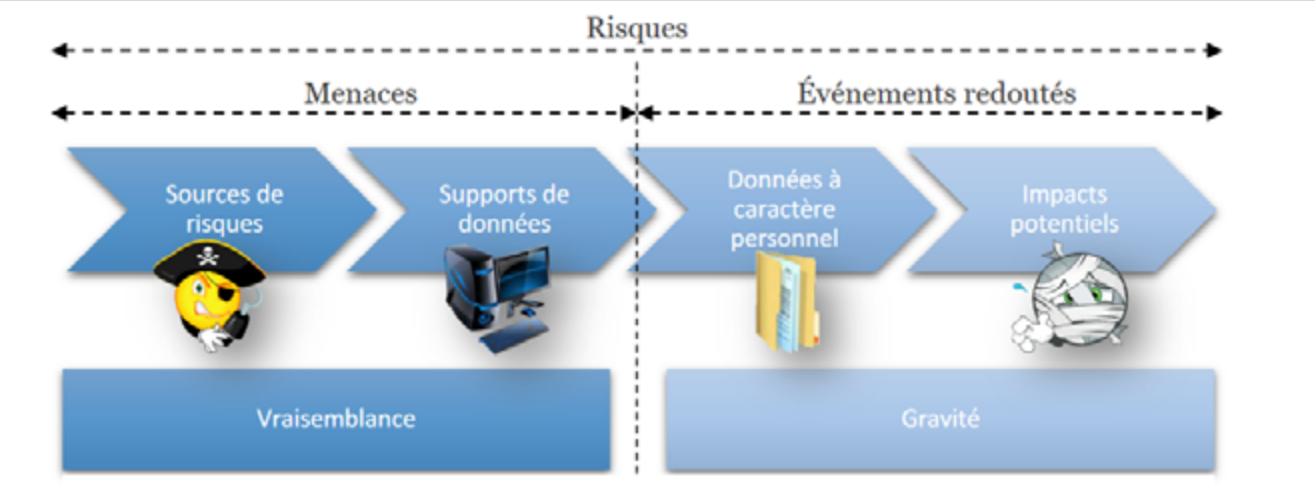


Figure 6. Résumé de l'appréciation par la CNIL dans sa méthodologie AIPD[198]

54 La lecture du document portant sur les « *bases de la connaissance* »[199] illustre cette problématique en définissant la vraisemblance[200] et la gravité en fonction des circonstances au travers de, respectivement, la facilité d'accès aux données[201] et l'impact potentiel subi par les personnes concernées[202]. Cette appréciation doit être faite par la prise « *en compte du risque du point de vue de la personne concernée* ». Toutefois, bien qu'éclairant sur la probabilité des faits générateurs à prendre en compte (*vraisemblance*) et sur l'importance des impacts des personnes concernées (*gravité*), l'analyse reste soumise à l'appréciation des analystes dans les limites énoncées aux chapitres précédents. Cette appréciation est d'autant plus subjective que les impacts consistent à « interpréter » les désagréments subis par les personnes concernées et leur facilité à surmonter les difficultés pour revenir à une situation antérieure.

La « [prise] *en compte du risque du point de vue de la personne concernée* » est donc faussée au travers d'un standard de référence biaisé avec des dommages éloignés de la gestion des données personnelles[203] mais se rapprochant davantage d'une évaluation d'impact sur la vie privée. En effet, les dommages potentiels pris en compte pour apprécier la gravité sont, pour la plupart, non directement liés à la gestion des données *per se*, ouvrant ainsi indéfiniment le champ d'examen des risques à prendre en compte par le responsable de traitement. Ils présupposent une action positive du responsable de traitement ou d'un tiers[204].

---

197 Voir CNIL, la méthode, spéc. p. 9, Définitions, sous Gravité : « *Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées* ».

198 Id. p. 8.

199 CNIL, Bases de la connaissance : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf.

200 CNIL, Bases de la connaissance, p. 5.

201 En prenant en compte les motivations de l'attaquant à l'instar de ce qui est fait en sécurité informatique.

202 Id. p. 3-5

203 Voir dans ce sens Partie 3.

204 Infra Partie 3.

Enfin, l'analyse des risques pour la protection des données personnelles par le biais des risques à la sécurité informatique dénature la première catégorie d'analyse. Formulée d'une autre façon, la méthodologie NIST[205] prévoit le recours à la méthodologie LINDDUN pour déterminer les risques pour la vie privée. En revanche, la méthodologie CNIL, théoriquement autosuffisante, englobe des éléments de la méthodologie EBIOS, dénaturant ainsi l'identification des risques aux « *droits et libertés* ». L'exemple de la fuite de données personnelles interroge la catégorie de risque pertinente pour l'analyser. La fuite de données personnelles ne correspond pas directement à :

- Un risque d'accès aux données personnelles puisque les données sont déjà diffusées et accessibles aux tiers ;
- Un risque de modification des données personnelles par des personnes non autorisées même si ces données pourront par la suite être modifiées par des tiers du fait de leur accessibilité
- Un risque d'effacement des données personnelles puisque rien n'indique que la fuite desdites données personnelles ait engendré l'effacement des données stockées par le responsable de traitement.

Ainsi de prime abord, l'analyse des risques proposée par la méthodologie CNIL semble être limitée à une utilisation purement interne et quasi-exclusive aux traitements des données personnelles.

> La méthodologie CNIL peut être illustrée par l'application de notre cas pratique. Ainsi, les données des utilisateurs relatives aux préférences audiovisuelles peuvent révéler, par exemple, des intérêts politiques/sexuels/ethniques estimés triviaux. Un salarié de Biomem (**source de risque-1**) accédant au système de gestion de données (**vulnérabilité des supports de données-2**) décide de transmettre ces préférences personnelles à une société de courtage publicitaire (**menace-3**). La **vraisemblance du risque** est constituée au niveau **important**[206]. Ces données personnelles (**données personnelles-5**) sont ensuite traitées par la société de courtage (**événement redouté-4**) pour des courriels personnalisés (**impact sur la vie privée des personnes concernées-6**). Dans de telles conditions, la **gravité** estimée varierait entre **négligeable** (les personnes concernées ne connaissent que quelques désagréments très facilement surmontables[207]), et **limitée** (la personne concernée ne subit que des désagréments significatifs facilement surmontables).

L'emploi de la méthodologie CNIL est facilité par la mise à disposition d'un logiciel spécifique PIA[208]. La méthodologie est indubitablement conforme aux prescriptions du CEPD, puisque la CNIL a contribué à son élaboration.

Figure 7. Catégorisation des dommages (extrait des bases de connaissance de la CNIL, p. 3-4)

55 Outre les défauts cités ci-dessus, plusieurs entretiens réalisés avec des praticiens ont souligné la difficulté technique d'utiliser cette méthodologie pour un traitement de données personnelles comprenant plusieurs acteurs (co-responsables de traitement ou plusieurs sous-traitants). En effet, le niveau de granularité d'informations à fournir entraîne soit l'impossibilité d'utiliser le logiciel PIA, soit une analyse *a minima* offrant pour unique avantage de se conformer au formalisme imposé par la CNIL. Certains praticiens ont néanmoins précisé que la méthodologie CNIL s'avère optimale pour des traitements « *simples* » : elle permet de respecter les dispositions de l'article 35 du RGPD tout en encourant un risque juridique minimum[209]. Ces professionnels considèrent l'AIDP, pour

205 Infra Sous-Section 4, page 75.

206 Pour reprendre la gradation définie par les Bases de connaissance, p. 5, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf.

207 Pour reprendre la gradation définie par les Bases de connaissance, p. 3-5.

208 Disponible https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

209 Voir supra §35, page 43.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) - Maux de tête passagers	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : spams) - Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) - Publicité ciblée pour des produits de consommation courants	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données - Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) - Perte de temps pour paramétrer ses données - Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non respect de contre- indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (*whistleblowing*, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	- Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre- indications) - Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	- Détournements d'argent non indemnisé - Difficultés financières non temporaires (ex. : obligation de contracter un prêt) - Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) - Interdiction bancaire - Dégradation de biens - Perte de logement - Perte d'emploi - Séparation ou divorce - Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - *phishing*) - Bloqué à l'étranger	- Affection psychologique grave (ex. : dépression, développement d'une phobie) - Sentiment d'atteinte à la vie privée et de préjudice irrémédiable - Sentiment de vulnérabilité à la suite d'une assignation en justice - Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) - Victime de chantage - *Cyberbullying* et harcèlement moral

reprendre les propos du Contrôleur européen à la protection des données, comme une obligation de « *box ticking* » (« *liste à cocher* »).

Toutefois, le DPO d'une société d'objets connectés estime que la méthodologie de la CNIL est parfaitement adaptée pour les fournisseurs de technologies. En effet, ces derniers étant soumis aux dispositions de l'article 32 du RGPD et à une évaluation des risques à des fins d'émulation d'applications fournies par des tiers, l'analyse d'impact axée sur les aspects de sécurité informatique répond à ces besoins de sécurité informatique sous l'unique réserve que le fournisseur de technologie ne soit pas également responsable de traitement.

56 La notation de la gravité et de la menace offre donc à l'analyste une hiérarchie entre les risques détectés afin de déterminer les mesures d'atténuation adéquates applicables (« *étape 4 : appréciation critique de l'AIPD* »). À l'instar de la méthodologie BSI, le document de la CNIL intitulé « *les bases de connaissances* » offre un panorama de mesures applicables au traitement afin d'atténuer les risques.

De manière générale, soulignons que le formalisme imposé par la méthodologie CNIL est difficilement applicable pour un traitement complexe comprenant plusieurs opérations comme dans le cas de Biomem. En effet, dans le cadre de notre étude, nous avons dû ajouter plusieurs onglets au document Excel[210] afin de réaliser une analyse détaillée des différentes opérations. À partir des trois hypothèses Biomem[211], il est possible de déterminer les éléments réunis dans le Tableau 10 ci-contre.

Le correctif principal à apporter à la méthodologie CNIL consiste à conserver la partie analyse du risque selon la trilogie de menaces « *Accès illicite, Modification, Disparition des données personnelles* » assurant ainsi les aspects cybersécurité, tout en ajoutant de nouveaux onglets pour incorporer les analyses de risques propres à la protection des données personnelles de type LINDDUN[212].

Tableau 10. Résumé de l'application du cas pratique Biomem dans la méthodologie AIPD de la CNIL

Sous-Section 2. La méthodologie PRIAM de S. JOYEE DE et de D. LE METAYER

57 La méthodologie française « *Privacy Risk Analysis Methodology* » développée en 2016 par S. JOYEE DE et D. LE METAYER relève davantage, malgré sa dénomination, de l'analyse d'impact pour la protection des données que de l'évaluation d'impact sur la vie privée[213]. En effet, bien que reposant sur les prescriptions du CEPD, cette méthodologie se distingue des autres par un haut degré de granularité des informations requises pour sa réalisation. Cette granularité permet d'identifier des risques directs pour la protection des données et l'identification de risques indirects pour la protection de la vie privée. Ce niveau de détails offre une meilleure vision du cycle de vie des données personnelles et le risque d'utilisation secondaire. Les rédacteurs étant chercheurs en sécurité informatique, nous notons toutefois un biais cognitif entraînant dans certaines parties une augmentation des descriptions des informations techniques. Ainsi, **pour la première étape posée par le CEDP**, là où la méthodologie CNIL n'impose qu'une description superficielle, l'analyse PRIAM impose une description fouillée de l'intégralité des procédures[214] et du matériel[215] utilisés lors du

210 Après avoir utilisé le logiciel PIA fourni par la CNIL, nous avons exporté toutes les questions et demandes d'informations à renseigner sur un document de type tableur.

211 Supra §14, page 13.

212 Voir supra §52, page 59 in fine.

213 Voir infra §58, page 70.

214 C'est-à-dire quelle donnée est collectée par quel traitement.

215 Ainsi par exemple doivent être mentionnés le matériel *per se*, les logiciels et les serveurs hébergeant les données personnelles.

	Responsable de traitement	Parties prenantes	Obligation de conformité (Obligations d'informations et exercice des droits)	Étude du respect des obligations de sécurité	Pertinence de la définition des risques
Biomem-Indé	**Biomem**	**Constructeur** Fournisseur de technologie *et* **Fournisseur de VOD** Sous-traitant	**Non**, Biomem n'est qu'un intermédiaire fournissant une brique technique embarquée entre la voiture connectée et la plateforme de VOD. La question de l'exercice des droits implique la participation des autres acteurs.	**Moyen** Seule la sécurité de l'application est évaluée. Un chiffrement supplémentaire peut être rajouté pour assurer la sécurité du gabarit conservé dans le terminal de la voiture connectée.	**Peu adaptée** Cadre pluripartite entraînant potentiellement des problèmes de communications entre le fournisseur de technologie et le fournisseur de VOD (responsable de traitement).
Biomem-Constructeur	**Constructeur**	**Fournisseur de VOD** Sous-traitant	**Oui**, en adéquation avec les prérequis posés par les Lignes directrices AIPD.	**Maximal** Le support et le traitement sont évalués dans leur ensemble.	**Adaptée** en ce qui concerne le fournisseur de technologie. Les obligations de responsable de traitement sont traitées de façon secondaire.
Biomem-VOD	**Fournisseur de vidéo à la demande**	**Constructeur** Fournisseur de technologie		**Minimum** Les solutions relatives à la sécurité se réalisent au niveau du véhicule, l'application n'intégrant que des fonctionnalités limitées de la plateforme.	**Peu adaptée** Les risques de sécurité informatiques sont existants mais secondaires. Ceux-ci sont principalement gérés par le constructeur.

traitement des données personnelles. Ce niveau de détail a l'avantage de fournir un flux de données précis. L'analyse PRIAM invite ensuite à effectuer l'inventaire de chacune des parties prenantes et la répartition de leurs rôles respectifs[216] pour définir les relations entre celles-ci. L'exercice de la conformité du traitement des données est effectué dans l'étape suivante. Bien qu'antérieure aux Lignes directrices *Privacy by Design* adoptées par le CEPD en 2019, cet exercice anticipe en grande partie certaines de ses prescriptions. **La seconde étape correspondant à la justification de la nécessité et de la proportionnalité** se traduit par la description pour chaque type de données personnelles, de son caractère sensible, sa précision, son volume, la forme de la collecte, son origine, sa finalité, sa durée de conservation, sa visibilité pour la personne concernée et les moyens mis à la disposition de la personne concernée pour intervenir sur la gestion de ses données.

58 **La troisième étape, l'analyse des risques,** est sous-divisée en plusieurs onglets. Ainsi, les sources de risques sont réparties en fonction des parties prenantes définies précédemment. Leur description prend en compte les personnes impliquées, personnes physiques ou morales, leur positionnement dans le traitement de données personnelles[217], la valeur de l'exploitation des données personnelles, la motivation à obtenir celles-ci et les moyens présumés à disposition pour l'obtention de ces informations. Une telle analyse met en valeur les sources de risques **(1)** qui devront être prises en compte dans l'analyse de risque *per se*. Les faiblesses **(2)**, principalement techniques, sont ensuite examinées selon une liste de critères qui est appliquée successivement aux traitements, aux matériels puis aux logiciels. Certaines faiblesses peuvent ainsi être écartées pour ne retenir que celles menaçant l'intégrité du système d'informations traitant les données personnelles. Suite à la qualification des faiblesses, huit hypothèses[218] d'événements redoutés **(3)** sont analysées à partir de quatre descriptions[219].

59 Une fois ces différents critères quantifiés, la méthodologie PRIAM invite à apprécier le risque. D'une part, la vraisemblance est appréciée en associant un événement redouté **(3)** à une faiblesse **(2)**, elle-même analysée par une source de risque **(1)** pour qualifier la catégorie de risque sous-divisée elle-même en plusieurs sous-catégories de type de dommages[220]. D'autre part, la « *gravité* » est appréciée en définissant la victime du dommage[221], et selon l'intensité de l'impact engendré par ledit dommage. Cette méthode dite de l'arbre à dommage (*harm tree*) découle d'une transposition aux données personnelles et de la protection du respect au droit à la vie privée d'une approche propre à la sécurité informatique comme l'attestent les différentes étapes d'appréciation des événements redoutés et des faiblesses. Elle se concrétise aussi par un calcul de probabilité reproduit ci-après (Figure 8) dont le résultat est associé à une valeur de réalisation (Figure 9). Toutefois, les auteurs de cette méthodologie n'indiquent pas le sort des éventuels risques résiduels déterminés lors de la quatrième étape posée par le CEPD. Au contraire, leur démarche semble être axée sur le recommencement de l'EIVP jusqu'à la disparition complète du risque. Cette méthodologie invite ainsi implicitement le responsable de traitement à trouver une mesure adéquate afin d'éviter de consulter l'autorité nationale de contrôle dans les conditions prévues par l'article 36 du RGPD.

---

216 Comprenant la personne concernée, le responsable de traitement, le sous-traitant, les tiers.

217 Dans l'entité du responsable de traitement / sous-traitant, tiers, proche de la personne concernée.

218 Ces huit hypothèses d'événements redoutés correspondent à une collecte trop importante de données personnelles, l'accès non autorisé aux données, la modification non autorisée de données, la réutilisation illicite des données personnelles, l'inférence des données personnelles, le stockage de données personnelles, la divulgation de données personnelles, la rétention de données personnelles.

219 L'échelle, l'irréversibilité, l'étendue de l'exposition suite à la réalisation de l'événement redouté et enfin la difficulté technique de réparer le dommage.

220 Dommages physique, économique, psychologique, réputationnel ou sociétal.

221 Si le dommage concerne un individu, un groupe ou la société dans son ensemble.

1. Find the value of *exploitability* for each leaf node in the harm tree.
2. For each exploitation, choose the values of the relevant attributes of the risk source most likely to exploit the privacy weakness leading to the harm.
3. Find out the likelihood of each of these exploitations from the above *exploitability* value and values of the relevant risk source attributes.
4. Compute the likelihood of each feared event and harm according to the following rules, where P_i is the likelihood of ith child node:

   R1. AND node with independent child nodes: $\prod_i P_i$.
   R2. AND node with dependent child nodes: $Min_i(P_i)$, i.e., minimum of the likelihoods of the child nodes.
   R3. OR node with independent child nodes: $1 - \prod_i(1 - P_i)$.
   R4. OR node with dependent child nodes: $\sum_i P_i$.

Figure 8. Méthode de calcul de probabilité des risques pour la méthodologie PRIAM

1. *Negligible (N)* for $p < 0.01\%$;
2. *Limited (L)* for $0.01\% \leq p < 0.1\%$;
3. *Intermediate (I)* for $0.1\% \leq p < 1\%$;
4. *Significant (S)* for $1\% \leq p < 10\%$;
5. *Maximum (M)* for $p \geq 10\%$.

Figure 9. Valeur de probabilité de réalisation d'un risque pour la méthodologie PRIAM

60 L'analyse des risques proposée par la méthodologie PRIAM se distingue des Lignes directrices AIPD du CEPD en partant du postulat que l'importance accordée à la gravité doit être minimisée. Le postulat repose sur l'idée que le calcul de la gravité du risque constitue une opération inutile et que l'étude des modalités d'atténuation de la vraisemblance du risque et des méthodes d'atténuation du dommage en cas de réalisation prévaut[222]. Contrairement à la conception adoptée par la CNIL dans sa définition du dommage[223], ces auteurs estiment que la réversibilité du dommage doit être priorisée dans le cadre d'un traitement de données mais qu'il est au nécessaire de minimiser sa réalisation. Néanmoins, leur définition du dommage subi par la personne concernée, la « *privacy harm* », converge vers la définition des dommages posés par la CNIL. En effet, le dommage est défini comme étant : « *The negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events* »[224]. Un tel positionnement se rapproche effectivement plus de la vision de l'EIVP que de l'AIPD où la seule intrusion dans la vie privée de la personne physique entraîne la constitution de l'atteinte à ce droit. Pour justifier cette approche, la méthodologie PRIAM repose sur les risques de la vie privée telle que définis par l'auteur étasunien D. SOLOVE[225]. Cette approche étasunienne est plus protectrice et plus large que l'approche promue par le RGPD relative à la protection des droits et libertés pour la personne concernée. Les auteurs de la méthodologie PRIAM ont cependant pris en compte les prérequis de la conformité définis par le texte européen.

61 Revers de la médaille de l'exhaustivité des informations relatives au traitement de données personnelles, la granularité et la précision entraînent une description technique longue à constituer dans le cadre d'une prestation de service de consultants. **La méthodologie ne diffère peu ou pas en fonction du cas pratique. En effet, le flux de données et les prérequis de sécurité**

222 Méthodologie PRIAM, spéc. p. 36, « *Since severity is an inherent measure of the damage caused by a harm, it cannot be reduced. The only factor that is in our control is the likelihood of harms which in turn depends on the likelihood of feared events and those of privacy weaknesses. A counter-measure can reduce the likelihood of one or more privacy weaknesses and thus reduces the likelihood of the harm that these privacy weaknesses lead to* ».

223 Voir supra §54, page 65.

224 Méthodologie PRIAM, p. 28.

225 Daniel J Solove. « *A taxonomy of privacy* », University of Pennsylvania law review, 2006, pp. 477-564.

changent peu, seuls les risques vis-à-vis de la conformité subissent une réelle variation car tous les cas de figure sont explorés. Néanmoins, du retour même de D. LE METAYER, rencontré lors des entretiens, sa méthodologie est utilisée dans le cadre d'un traitement de données personnelles en cours de constitution ; elle est difficilement transposable dans le cadre d'une AIPD effectuée à des fins de régularisation d'un traitement pour lequel une AIPD n'aurait pas été réalisée. Ainsi, à la différence des autres méthodologies, cette méthodologie est adaptée pour une conformité effectuée en une seule fois, et non par exécutions successives. En d'autres termes, là où la méthodologie CNIL, par exemple, met en exergue les opérations critiques pour implémenter des mesures adéquates en priorité laissant à l'écart les opérations moins critiques avant le déploiement, la méthodologie PRIAM repose sur une itération des opérations de prévention d'apparition du risque. Ceci explique donc pourquoi l'analyse ne priorise pas les risques identifiés par un système de notation mais par l'utilisation de statistiques de réalisation.

	Responsable de traitement	Autres parties prenantes	Obligation de conformité	Obligation de sécurité	Pertinence de définition des risques
Biomem-Indé	**Biomem** Le fournisseur d'application	**Les parties prenantes et les sources de risques**	**Oui**, parfaitement en adéquation avec les Lignes directrices AIPD du CEPD.	**Élevé** puisque tous les cas de figure sont explorés.	**Très adaptée** à un traitement en cours d'élaboration pluripartite **Moins adaptée** pour un traitement de données personnelles simple Certains risques sont difficilement appréciables d'une façon objective, comme les risques sociétaux.
Biomem-Constructeur	**Constructeur**				
Biomem-VOD	**Fournisseur de vidéos à la demande**				

Tableau 11. Résumé de l'application du cas pratique Biomem avec la méthodologie PRIAM

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name		Description of privacy target
P1	Safeguard of quality of personal data	P1.1	Ensuring fair and lawful processing through transparency	E.g. providing a description of the data processing activities required for product and service delivery, ensuring internal and external transparency. See Directive 95/46/EC, Section I, Article 6 (a).
		P1.2	Providing purpose specification and limitation	See Directive 95/46/EC, Section I, Article 6 (b).

Figure 10. Définition d'une « Privacy target » par la méthodologie BSI

Sous-Section 3. La méthodologie du *Bundesamt für Sicherheit in der Informationstechnik*

62 La méthodologie du BSI est utilisée lors de l'application de la technologie RFID (*Radio Frequency identification*) dans des applications, entre autres, de transport. Sa description nécessite 280 pages, dont une majorité dédiée aux applications de transport et aux traitements automatiques de certaines applications dans le secteur automobile. Bien que datant de 2011, cette méthodologie n'est pas pour autant désuète ou totalement contraire aux Lignes directrices AIPD. Elle commence par l'étude d'un flux de données définissant les parties prenantes et permettant ainsi de déterminer les « *Privacy targets* » (« *cibles pour la vie privée* ») applicables. Ces cibles généralistes se voient attribuer un code (P.1). Un sous-code correspondant à un sous-risque plus raffiné est défini (P.1.1.). Ce sous-risque correspond à une mesure préconisée par la directive 95/46/CE relative à la protection des données. Parmi ces différentes « *cibles pour la vie privée* », les risques liés à la conformité à la législation des données, répondent ainsi à la condition posée pour la seconde étape des lignes directrices AIPD du CEPD. Contrairement à leur dénomination, ces « *cibles pour la vie privée* » portent uniquement sur la protection des données personnelles et non pas sur le respect de la vie privée.

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
T1	Lack of transparency – Missing or insufficient service information	T1.1	Incomplete or insufficient information describing the service. The operation details (data flows, data locations, ways of transmission, etc.) and the impacts of the RFID application are not sufficiently explained to the data subject. An RFID emblem is not displayed on the website of the RFID operator.	P1.1
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable	P1.1
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	P1.1 P1.2
		T1.4	Existing information describing the service is not easily understandable and / or special knowledge is needed to understand it, e.g. jurisdictional terminology, company-internal abbreviations, a distinct language, etc	P1.1
		T1.5	Existing information describing the service is not kept up-to-date.	P1.1
		T1.6	Information provided in conjunction with an RFID emblem does not cover all areas and purposes for which RFID is used in a facility.	P1.1 P1.2
	…of transpare…	T1.7	No privacy statement is available.	P1.1
		T1.8	Existing…	

Figure 11. Définition d'une menace par la méthodologie BSI
Une menace est associée à une « Privacy Threat » (T1.), sous-divisée ensuite en une sous-menace plus fine (T1.1.). Chaque sous-menace est associée à une ou plusieurs « cibles pour la vie privée ».Voir note [226]

226 BSI, *Privacy Impact Assessment Guideline*, p. 24, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf.

La prédéfinition et l'association des « *Privacy targets* » à des menaces facilitent le travail de l'analyste dans la réalisation de la troisième étape. Il s'agit donc d'associer les menaces crédibles aux types de données concernées aux « *Privacy targets* » pour apprécier les différents types de dommages tant du point de vue de la personne concernée que de l'opérateur. Cette appréciation entraîne une notation entre 1 et 3 et correspond à un dommage dont le niveau est reproduit ci-dessous.

Protection demand	Criteria for the assessment of protection demand					
	General description	Operator perspective		Data subject perspective		
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well- being	Personal freedom
Low - 1	**The impact of any loss or damage is limited and calculable.**	Only **minimal** impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.	The financial loss is **acceptable** to the organisation.	The processing of personal data could **adversely** affect the social standing of the data subject. The data subject's reputation is threatened for a **short period** of time.	The processing of personal data could **adversely** affect the financial well-being of the data subject.	The processing of personal data **does not endanger the personal freedom** of those concerned.
Medium - 2	**The impact of any loss or damage is considerable.**	**Considerable** impairment of the reputation / trustworthiness of the organisation can be expected.	The financial loss is **considerable**, but does not threaten the existence of the organisation.	The processing of personal data could have a **seriously adverse** effect on the social standing of the data subject. The data subject's reputation is threatened for a **longer period** of time.	The processing of personal data could have a **seriously adverse** effect on the financial well-being of the data subject.	The processing of personal data **could endanger the personal freedom** of those concerned.
High - 3	**The impact of any loss or damage is devastating.**	An **international or nation-wide** loss of reputation / trustworthiness is conceivable, possibly even endangering the existence of the organisation.	The financial loss **threatens the existence** of the organisation.	The processing of personal data could have a **devastating** effect on the social standing of the data subject. The data subject confronts a **lasting** loss of reputation.	The processing of personal data could have a **devastating** effect on the financial well-being of the data subject.	The processing of personal data **could seriously endanger the personal freedom** or result in the injury or death of the data subject.

Figure 12. Définition des dommages par la méthodologie BSI
Voir note[227]

227 *Privacy Impact Assessment Guideline*, p. 21.

Cette notation permet de déterminer le type de « *controls* » applicables à chaque situation, apportant ainsi les garanties adéquates en termes de protection des droits et libertés des personnes concernées.

63 Cette méthodologie est intéressante à deux égards. Elle permet de prendre en compte des risques encourus par l'opérateur au même titre que les dommages affectant la personne concernée. Cette vision est plus opérationnelle que la version idéaliste fournie par le RGPD. Une telle vision contraint le représentant légal à une compréhension des risques juridiques et réputationnels correspondant à l'importance du risque lié au traitement des données personnelles de la personne concernée. Par ailleurs, son application est *prima facie* simple.

64 Cependant, son caractère « *clefs en main* », propre au « *PIA-Cadre* », limite la personnalisation par le responsable de traitement. L'insertion de nouvelles « *cibles pour la vie privée* » s'avère ainsi difficile, empêchant toute évolution ultérieure. La méthodologie ne semble pas être adaptée à un système pluripartite du fait de sa rigidité structurelle. Son ancienneté ne la rend pas pour autant totalement obsolète. En effet, de nombreuses obligations de conformité préexistaient dans la directive 95/46/CE, même si les droits des personnes concernées ont été renforcés par le RGPD. Ceux-ci peuvent aisément être inclus dans la méthodologie.

Sous-Section 4. La méthodologie du *National Institute of Standards and Technology* (États-Unis)

65 Dernière méthodologie institutionnelle d'analyse d'impact en date de janvier 2020, la méthodologie NIST s'insère dans la définition d'un système de traitement global. En d'autres termes, la réalisation de cette évaluation d'impact pour la vie privée (EIVP)[228] n'est qu'une étape parmi d'autres dans le processus de conformité concernant le traitement des données personnelles entrepris. Les travaux du NIST entendent sensibiliser les sociétés étasuniennes à la problématique des données personnelles. En effet, bien que le droit fédéral étasunien des données personnelles soit spécifique à certains secteurs et n'ait pas une portée générale, le besoin d'une loi omnibus – c'est-à-dire une loi protectrice des données personnelles applicables à tous les secteurs – se fait sentir de plus en plus fréquemment depuis la décision C-362/14 Maximillian Schrems[229] rendue par la Cour de Justice de l'Union Européenne (CJUE), et surtout depuis la transaction conclue en 2019 entre la *Federal Trade Commission* (FTC) et Facebook. Dans cette transaction, l'autorité de protection des consommateurs a imposé à Facebook la réalisation d'une EIVP[230] périodique. La méthodologie préconisée par le NIST n'est pas conforme aux prescriptions des Lignes directrices AIDP éditées par le CEPD. Mais cette absence de conformité est d'autant plus intéressante à étudier pour déterminer les interactions entre le droit européen de protection des données et le proto-droit étasunien.

66 L'EIVP proposée par le NIST se décompose en trois documents distincts :

1. Un document texte comprenant un questionnaire en deux parties qui correspond à l**a première étape posée par le CEPD**. La première porte sur le traitement de données en lui-même en requérant du responsable de traitement la description de celui-ci, ses besoins techniques et les mesures de « *privacy* » déjà adoptées. La seconde partie du questionnaire porte sur le cadre de la gouvernance déjà mis en place quant aux règles de « *privacy* ». Ainsi l'analyste doit indiquer les lois applicables, les normes techniques et politiques[231] auxquelles le responsable du traitement se soumet ou adhère, les objectifs explicites ou implicites relatifs au respect du droit à la vie

228 Voir pour la distinction supra §7, page 5.

229 Arrêt CJUE, 16 juillet 2020, C-311/18, Data Protection Commissioner c.Maximillian Schrems et Facebook.

230 Voir infra Section 2, page 83.

231 À savoir les « *Fair Information Practice Principles, Privacy by Design principles, ethics principles* ».

privée. Le document se conclut par la détermination de « *la tolérance du risque admissible par l'organisation dans sa gestion des données personnelles* »[232].

2. Un document, tableur, portant sur l'évaluation du « *design* » du système. Son objectif est de déterminer les risques pour la « *privacy* » dans le cas de systèmes, produits ou services, pour déterminer les conditions de la vraisemblance d'une action au travers d'une identification et d'un catalogage des risques. Ce document comprend quatre onglets :

   a Le premier, qui reprend les informations renseignées dans la première partie du document visé au 1°), a pour objectif de déterminer la capacité du respect de la « *privacy* » par le système d'information. Cette capacité est analysée à partir des six critères suivants[233] :
      - *Predictability (enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system),*
      - *Manageability (providing the capability for granular administration of PII including alteration, deletion, and selective disclosure),*
      - *Dissociability (enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system),*
      - *Confidentiality (preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information),*
      - *Integrity (guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity),*
      - *Availability (ensuring timely and reliable access to and use of information or an information system)*

   b L'onglet suivant reprend les facteurs contextuels entourant le traitement. Cette analyse entraîne une description de l'organisation, du support sur lequel est effectué le traitement de données et enfin du point de vue de la personne concernée. Ce dernier point est intéressant puisque doivent être documentés les intérêts de la personne concernée sur sa « *privacy* », sa compréhension technologique et enfin « *any demographic factors that would influence the understanding or behavior of individuals with respect to the data actions being taken by the system(s)* ».

   c Le dernier onglet porte sur une description écrite du flux de données avec les actions correspondantes.

3. Le troisième document, tableur, porte sur l'analyse de la gravité et l'appréciation du risque. Ce document doit être lu sous le prisme du très court « *Catalog of Problematic Data Actions and Problems* »[234] listant les actions, c'est-à-dire les traitements au sens du RGPD, à appliquer aux données[235] et les problèmes subséquents[236]. Ainsi, à partir des actions décrites dans le dernier onglet du second document, des événements redoutés sont analysés selon les actions problématiques sur les données sous-divisés en problème subséquents. La vraisemblance de ces derniers est calculée sur une note comprise entre 1 et 10.

   a Les premières colonnes correspondantes aux actions des données, sous-divisées en événements redoutés eux-mêmes associés aux potentielles actions problématiques, sont analysées en fonction de l'impact des risques du point de vue de l'entreprise. Ce point de vue prend en compte le coût de la non-conformité, le coût direct pour le « *business* », le coût réputationnel et le coût d'implémentation d'une culture « *privacy* » dans l'entreprise pour s'assurer

---

232 NIST, PIA, Worksheet 1, p. 4 : « *Document your organization's risk tolerance with respect to privacy from your organization's enterprise risk management strategy* », https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md.

233 Qui seront repris dans le Tableau 12, page 81.

234 Voir supra note « NIST, PIA, Worksheet 1, p. 4 »

235 Les « *risques* », dans la formulation CNIL.

236 Les « *dommages* », dans la formulation CNIL.

d'une conformité organisationnelle. Chacun de ces coûts se voit attribuer une note entre 1 et 10. Toutes les notes attribuées à un coût sont ensuite additionnées. (Figure 13)

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Enregistrement au service Biomem	Fuite de données	Induced disclosure, insecurity, unanticipated revelation	dignity loss	3
			economic loss	4
			loss of self determination	6
			loss of trust	8
	Asymétrie de l'information	Appropriation	loss of trust	2
	Accès non autorisé	Distortion, appropriation, re-identification, stigmatization, surveillance	dignity loss	4
			economic loss	4
			loss of self determination	4
			loss of trust	4

Figure 13. Extrait de l'application de la méthodologie NIST au cas Biomem pour le calcul de la vraisemblance
Voir note[237]

b Les actions de données, c'est-à-dire les traitements au sens du RGPD, sont ensuite associées à tous les potentiels impacts pour l'entreprise. Les notes discrétionnairement attribuées par le responsable de traitement à la vraisemblance et à l'impact, lors des premières étapes, sont utilisées pour calculer le risque par problème potentiel. Une note globale est attribuée par la multiplication de toutes les notes des potentiels impacts. (Figure 14)

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Organizational Impact Factors					Total Business Impact (per Potential Problem)
				Non compliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Enregistrement au service Biomem	Fuite de données	Induced disclosure, insecurity, unanticipated revelation	dignity loss	2	4	3	4		13
			economic loss	2	3	3	4		12
			loss of self determination	3	6	3	4		16
			loss of trust	2	3	3	4		12
	Asymétrie de l'information	Appropriation	loss of trust	3	4	3	4		14
	Accès non autorisé	Distortion, appropriation, re-identification, stigmatization, surveillance	dignity loss	3	4	3	4		14
			economic loss	2	4	3	4		13
			loss of self determination	2	4	3	4		13
			loss of trust	2	3	3	4		12

Figure 14. Extrait de l'application de la méthodologie NIST au cas Biomem pour l'appréciation de la gravité
Voir note[238]

c Enfin le dernier onglet comprend une classification des différents risques associés à leurs notes pour apprécier la priorité des risques et y appliquer les mesures correspondantes. (Figure 15)

237 Worksheet 2, Onglet « *Data action analysis* ».

238 Worksheet 3, Onglet « *Risk* ».

Data Actions & Summary Issues	Potential Problems for Individuals	Likelihood	Impact	Risk per Potential Problem	Risk per Data Action
Enregistrement au service Biomem					515
Fuite de données	dignity loss	3	13	39	279
	economic loss	4	12	48	
	loss of self determination	6	16	96	
	loss of trust	8	12	96	
Asymétrie de l'information	loss of trust	2	14	28	28
Accès non autorisé	dignity loss	4	14	56	208
	economic loss	4	13	52	
	loss of self determination	4	13	52	
	loss of trust	4	12	48	

Figure 15. Extrait de l'application de la méthodologie NIST au cas Biomem pour le calcul des risques
Voir note[239]

Data Actions & Summary Issues	Potential Problems for Individuals	Point Label	Likelihood	Impact
Enregistrement au service Biomem				
Fuite de données	dignity loss	A	3	13
	economic loss	B	4	12
	loss of self determination	C	6	16
	loss of trust	D	8	12
Asymétrie de l'information	loss of trust	E	2	14
Accès non autorisé	dignity loss	F	4	14
	economic loss	G	4	13
	loss of self determination	H	4	13
	loss of trust	I	4	12
Création d'un compte biométrique				
Risque de discrimination sur profilage ethnique	dignity loss	K	3	35
	economic loss	L	3	34
	loss of self determination	M	3	33
	loss of trust	N	9	36
Sécurité des données	dignity loss	P	9	28
	economic loss	Q	3	37
	loss of self determination	R	3	30
	loss of trust	S	3	30
Risque de non exercice des droits	economic loss	T	9	32
	loss of self determination	U	3	32
	loss of trust	V	9	34
	dignity loss	W	8	32
Création d'un profil utilisateur sur la base de la géolocalisation				

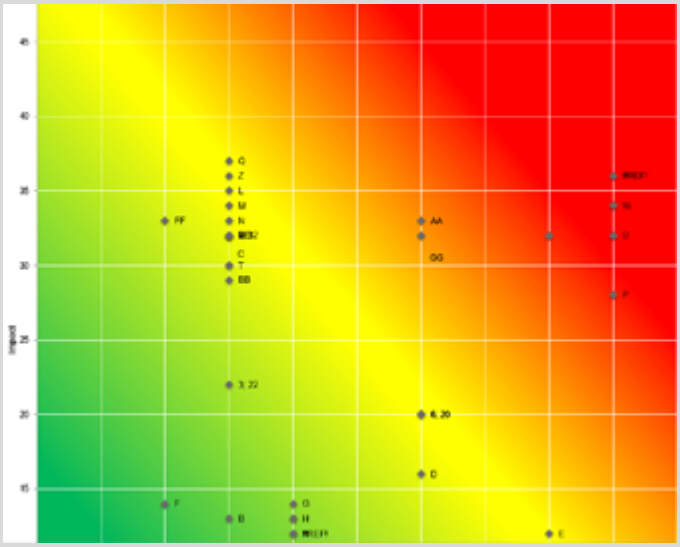


Figure 16. Extrait de l'application de la méthodologie NIST au cas Biomem pour la priorisation des risques
Les «point labels» sont positionnés dans le schéma à droite.
Voir note [240]

239 Worksheet 3, Onglet « *Risk* ».

240 Worksheet 3, Onglet « *Risk Prioritization* »

67 Par l'approche innovante de son interface, la méthodologie NIST est la plus aisée à utiliser. S'inspirant ouvertement de l'analyse de menaces LINDDUN[241], elle en reprend certains risques[242]. Les dommages correspondent à ceux posés par le CEPD[243]. Toutefois, l'inconvénient de cette méthodologie repose sur l'absence de conformité par rapport aux droits de la personne concernée définis par le RGPD. En effet, comme l'illustre le second onglet du second document, l'information apportée à la personne concernée peut être « sommaire » et dépendre de sa compréhension. Plus important dans notre domaine, la méthodologie étasunienne ne semble pas prendre en compte les lois étatiques[244] ou les lois sectorielles[245] relatives aux données personnelles. Ainsi toute donnée personnelle est traitée, indépendamment de sa valeur normative (donnée sensible par exemple), et uniquement au travers du calcul du risque et de la vraisemblance. Cette solution nuit à l'appréciation du risque en ne permettant pas d'apprécier réellement les risques importants. Ceux-ci sont uniquement étudiés au seul prisme de l'impact économique subi par l'entreprise responsable de traitement, ignorant ainsi l'importance de cette donnée pour la personne concernée. Ce défaut peut être concrètement résolu en accordant une importance moindre aux des données personnelles estimées comme « *triviales* ». Enfin, étant principalement une réponse pratique à une problématique juridictionnelle, cette méthodologie ne semble pas encore suffisamment aboutie, ni adaptable à une situation pluripartite.

Sous-Section 5. Les enseignements apportés par les quatre méthodologies

68 L'application des quatre méthodologies aux hypothèses alternatives de notre cas pratique Biomem démontre une difficulté d'application de certaines d'entre elles à des traitements complexes pluripartites. La comparaison des résultats obtenus dans les quatre cas indique une prédominance de l'analyse de la vulnérabilité sur celle de la gravité.

Les trois menaces définies par les Lignes directrices relatives au véhicule connecté du CEPD – l'asymétrie de l'information, la qualité du consentement de l'utilisateur et la sécurité des données – sont traitées succinctement par les différentes méthodologies utilisées quel que soit le cas pratique dans lequel on se situe : Biomem Indé, Biomem-Constructeur et Biomem-VOD. Ce défaut s'explique par le fait que deux de ces deux menaces (l'asymétrie de l'information et la qualité du consentement) sont difficilement quantifiables. Elles sont énoncées lors de l'analyse de la conformité qui conduit non pas à une prise en compte et donc une quantification du risque, mais à une réponse binaire (oui/non). Les éléments de la conformité doivent être simplement listés. Pourtant, dans les hypothèses de Biomem-Indé et Biomem-VOD, le constructeur est considéré comme fournisseur de technologie. Seule l'hypothèse 2, où le service Biomem Constructeur est un service ancillaire, conduit à qualifier ce dernier de responsable de traitement. Les Lignes directrices relatives au véhicule connecté du CEPD désignent ledit véhicule comme point de contact optimal pour la collecte du consentement par un enclenchement manuel. Cet élément varie peu ou pas, que l'on se situe dans Biomem-Indé, Biomem-Constructeur ou Biomem-VOD.

---

241 Lors de la conférence *Computer, Privacy and Data Protection* du 22 janvier 2020 à Bruxelles, Belgique, Naomi Lefkovitz, une des rédactrices de la méthodologie NIST, a expliqué s' être inspirée directement de l'analyse LINDDUN.

242 Voir infra Section 2, page 83.

243 Ainsi l'on retrouve la perte de dignité, les risques de discrimination, la perte économique, la perte d'autonomie, de liberté et le dommage physique.

244 Voir par exemple la Section 503.001.du *Business and Commerce Code* du Texas spécifiquement dédiée à la donnée biométrique.

245 Comme l'HIPAA, Health Insurance Portability and Accountability Act of 1996.

suite page 82

	CNIL (AIPD)	PRIAM (EIVP)	BSI (AIPD)	NIST (EIVP)
Adéquation avec les Lignes directrices AIPD	Parfaite	Parfaite	Obsolète	Inadapté
Adéquation avec les Lignes directrices DPbDD	Oui	Oui	Presque	Non
Exhaustivité	Non (adaptable)	Oui	Oui	Non
Faisabilité	Aisée	Compliquée	Longue	Agréable
Conformité à l'exercice des droits des personnes concernées	Limpide	Traité sous l'angle du risque	Prévue	Non prévue
Types de dommages	Matériel, immatériel, direct et indirect	Matériel, immatériel, direct et indirect Individuel, collectif et sociétal	Du point de vue de l'entreprise : dommage réputationnel et financier Du point de vue de la personne concernée : atteinte réputationnelle, aux libertés individuelles et au bien-être financier	Atteinte à la vie privée
Adaptation à un environnement multipartite	Adaptable	Adaptée	Peu adaptée	Peu adaptée
Itérativité (possible conformité sur plusieurs périodes temporelles)	Oui par la définition des mesures prioritaires	Non	Non	Oui par la définition des mesures prioritaires
Appréciation du risque au regard des droits et libertés des personnes	CIA : Confidentialité, Intégrité, Accessibilité (cybersécurité)	*Harm Tree* et inspiration de la méthodologie LINDDUN	Défini par la méthodologie	Inspiration de LINDDUN mais sans prendre en compte la spécificité des données
Appréciation du risque pour le responsable du traitement	Non	Non	Oui (réputationnel et financier)	Oui principalement, en prenant en compte le coût financier découlant de l'absence de conformité, de la perte d'affaires, de la perte réputationnelle, et des mises à jour des procédures internes relatives au traitement des données personnelles
	CNIL (AIPD)	PRIAM (EIVP)	BSI (AIPD)	NIST (EIVP)

	CNIL (AIPD)	PRIAM (EIVP)	BSI (AIPD)	NIST (EIVP)
Méthode d'appréciation des risques (vraisemblance)	Source de risque exploitant une vulnérabilité du support dans le cadre de menace (§55, page 66)	Événement redouté associé à une faiblesse analysée en source de risque (§59, page 70)	*Privacy target* appréciée à partir d'une *threat* pour se voir apposer des *controls* correspondants (§62, page 73)	*Data action* associée à une problématique sur les *data actions* ayant des impacts potentiels pour les individus (§66-3§a, page 76)
Méthode d'appréciation des risques (gravité)	Événement redouté sur les données personnelles provoquant des impacts sur la vie privée (§55, page 66)	La gravité est appréciée en fonction du type de dommage et de son étendue (§59, page 70)	Une *privacy target* est appréciée à partir d'une *threat* pour se voir apposer des *controls* correspondants (§62, page 73)	La gravité est appréciée en fonction des impacts financiers pour l'organisation (responsable de traitement) en fonction des *data actions* et des problématiques subséquentes (§66-3§b, page 77)
Notation des risques pour la gravité	Sur 4 niveaux (négligeable, limitée, importante, maximale)	Non applicable	Sur 3 niveaux (faible, important, haut)	1 à 10 pour déterminer la gravité et la vraisemblance puis multiplication des deux notes qui prioritérisent les mesures à instaurer (§66, page 75, *in fine*)
Type d'impacts pour la personne concernée	Impact corporel, matériel, moral	Dommage physique, économique, mental, réputationnel, sociétal Au niveau individuel, d'un groupe spécifique et de la société dans son ensemble	Impact réputationnel, sur le bien être financier du responsable de traitement, les libertés individuelles de la personne concernée	Perte de dignité, discrimination, perte économique, perte d'autodétermination (autonomie, liberté, dommage physique)
	CNIL (AIPD)	PRIAM (EIVP)	BSI (AIPD)	NIST (EIVP)

Tableau 12. Bilan des différentes méthodologies

L'utilisation de la méthodologie la plus adaptée à ce type de traitement complexe reste la **méthodologie PRIAM**. Cette dernière se révèle en revanche difficile à réaliser du fait du niveau de granularité de l'information exigée. Cette méthodologie ne prend pas en compte, malheureusement, l'intégralité des processus réalisés par les fournisseurs de technologies, c'est-à-dire les supports technologiques du traitement. Dans de telles circonstances, ces acteurs sont qualifiés de sous-traitant, ou ne voient leur support technologique être examiné qu'à partir de la documentation technique fournie. Ainsi, les sources de risques sont seulement examinées à travers le prisme des vulnérabilités informatiques et processuelles.

Les résultats obtenus par l'utilisation de la **méthodologie BSI** entraînent une homogénéité des sous-menaces aux impacts. Les notations sont quasiment inexistantes. De plus l'application des mesures empêche le responsable du traitement d'appliquer des initiatives non prévues par cette méthodologie.

Les résultats révélés par la **méthodologie NIST** sont, du fait de sa spécificité étasunienne, assez homogènes. Cette homogénéité se concentre à l'instar des autres méthodologies sur les analyses des vulnérabilités.

69 Le biais de sécurité informatique préféré dans l'approche quantitative du risque posé par le considérant 90 du RGPD tel qu'interprété par les Lignes directrices AIPD du CEPD entraîne un système de notation arbitraire dans presque toutes les méthodologies. Cette approche rejoint en partie celle de la méthodologie de calcul de risque par la **méthodologie CNIL**. La lecture de la jurisprudence des délibérations de la CNIL et de certains arrêts de la CJUE invite le lecteur à y percevoir des soupçons de la théorie de l'équivalence des conditions[246]. Cette dernière inscrit l'intégralité des faits ayants directement ou indirectement concouru à un dommage potentiel dans la notion de risque. À l'inverse, la théorie de la causalité adéquate se concentre sur les faits ayant directement concouru au dommage réellement réalisé[247]. Dans une telle configuration, le non-respect du RGPD correspond au fait générateur, le risque pour les droits et libertés tel que décrit par la suite correspond au lien de causalité et le dommage, potentiel, est apprécié en fonction de la « gravité » définie par le considérant 87 du RGPD (« *gravity* »). La lecture des délibérations de la CNIL fait apparaître que la gravité (« *severity* ») est écartée au profit de la seule étude de la vraisemblance[248]. La *gravité-gravity* semble être la seule à être prise en compte dans l'appréciation de l'intégralité des mesures techniques d'atténuation du risque. Cette approche souligne l'importance accordée à la sécurité informatique par l'examen de la vraisemblance sous le seul prisme de la *gravité-gravity*. Seule la **méthodologie PRIAM** semble échapper à ce biais par le recours des *harms trees* en assumant une approche principalement centrée sur la vraisemblance plutôt que sur la *gravité-severity*. Cette dernière est, rappelons-le, relayée au second plan en estimant que ce dernier indicateur ne peut pas être réduit une fois le dommage réalisé[249]. Ce choix d'évaluation conduit à une analyse de sécurité informatique allégée, orientée vers une requalification des données personnelles en informations critiques[250]. Cette criticité se ressent lors de l'examen de la *gravité-severity* où seules, sous réserve des limites énoncées ci-dessus, les méthodologies CNIL et PRIAM la définissent exclusivement au travers le prisme des droits et libertés. Proposés de manière surabondante, et bien que logiques par certains aspects[251], les dommages collectifs et sociétaux entrent dans les critiques émis par doctrine publiciste au travers de son imprécision.

---

246 Voir infra Partie 3, Chapitre 7, section 1, Sous-Section 2, page 128.

247 Voir infra Partie 3, Chapitre 6, section 2, Sous-Section 2, page 108.

248 Pour les considérations *gravité-gravity* et *gravité-severity*, voir supra encart **Δ dans le texte**, page 42.

249 PRIAM, p. 36 : « *Since severity is an inherent measure of the damage caused by a harm, it cannotbe reduced. The only factor that is in our control is the likelihood of harms which inturn depends on the likelihood of feared events and those of privacy weaknesses* ».

250 Dans ce sens, D. LANDOLL, « *The security risk Assessment handbook* », CRCP PRess, 2011, §28.

251 Nous pensons évidemment aux questions de l'évolutivité des traitements de données personnelles.

Sans la mentionner explicitement, la **méthodologie BSI** étudie la gravité par la prise en compte des risques tant au niveau de l'opérateur que de celui de la personne concernée[252]. Cette dernière approche se retrouve dans la **méthodologie NIST**. Celle-ci se concentre davantage sur les aspects opérationnels et financiers de l'entité responsable de traitement, excluant les dommages subis par la personne concernée de son étude. Ainsi les différentes conceptions posées par les méthodologies sur la gravité du dommage indiquent que cette condition est considérée comme subsidiaire, entraînant donc une appréciation relevant de l'arbitraire de l'évaluateur.

70 Hormis **la méthodologie BSI** qui laisse peu de marge de manœuvre à l'évaluateur, les **trois autres méthodologies étudiées** reposent, conformément au **considérant 90 du RGPD**, sur une appréciation à la fois **quantitative** et **qualitative** des risques. Cette confusion des genres entraîne selon nous un enchevêtrement d'estimation objective et subjective. L'estimation objective mise en avant par l'analyse quantitative repose sur des calculs complexes à partir de valeurs précises. Or l'origine de ces valeurs, encore en cours d'élaboration technique, laisse l'évaluateur seul souverain de son estimation. À l'inverse, l'analyse qualitative, certes plus adaptée à un traitement spécifique, souffre d'une appréciation totalement arbitraire. Ce caractère arbitraire convertit l'AIDP en seule preuve de la conformité, limitant ainsi les efforts de l'évaluateur.

Dans une telle perspective, **une approche complète telle que celle poursuivie par la méthodologie PRIAM nous semble être la vision optimale**. En effet, une présentation exhaustive des vulnérabilités et des menaces démontrerait, à l'autorité nationale de contrôle, une réelle volonté de l'évaluateur à identifier puis atténuer les risques.

Section 2. Caractéristiques des quatre méthodologies et conformité aux Lignes directrices AIPD du Comité européen de la protection des données

71 Cette recherche a pour but de déterminer quelle méthodologie examinée serait optimale pour la réalisation d'une analyse d'impact relative aux données personnelles d'un traitement comprenant plusieurs opérations distinctes, comprenant des données sensibles et impliquant plusieurs acteurs, dans un contexte de mobilité automobile. Comme il pouvait être prévisible, chaque méthodologie présente des avantages et des inconvénients. La description effectuée dans la partie précédente démontre l'intersection des méthodologies examinées, permettant d'apprécier les qualités de certaines d'entre elles. Aussi, nous nous concentrerons dans un premier temps sur le cœur de la problématique, c'est-à-dire l'analyse des risques en elle-même (§1). Dans un second temps, après avoir rappelé les convergences relatives à la conformité et l'exercice des droits, des pistes de convergences des méthodologies seront explorées pour tenter de définir une AIPD plus opérationnelle (Sous-Section 2, page 88).

Sous-Section 1. Les convergences et divergences des quatre méthodologies dans l'identification des risques et des menaces

A. Classifications critiques et correspondances des risques

72 De prime abord, l'utilisation de l'analyse des menaces LINDDUN est intégrée à cette section. Cette méthodologie définit un champ sémantique spécifique à l'identification des menaces relatives à la protection de la vie privée. Sa pertinence de l'analyse des menaces est d'ailleurs reconnue explicitement par son inclusion dans la méthodologie NIST. De l'aveu de ses rédacteurs, la méthodologie PRIAM s'en inspire directement. Comme il sera démontré, les terminologies posées la méthodologie LINDDUN sont suffisamment larges pour correspondre à une ou plusieurs menaces/risques définies par d'autres méthodologies.

252 Voir supra §62, page 73 et §63, page 75..

L'analyse des événements redoutés pris en compte dans la détermination des risques telle que développée par la **CNIL** découle d'un biais en sécurité informatique provenant des rédacteurs de cette méthodologie. Ainsi, sans se reposer intégralement sur la méthodologie de détection des menaces et d'événements redoutés LINDDUN, il est possible de voir **des correspondances entre les différentes méthodologies**[253] trouvant un écho dans **les Lignes directrices DPbDD** du CEPD et complétant ainsi la conformité. La comparaison entre les différentes sources d'événements redoutés démontre l'inclusion de certains risques dans certaines méthodologies, et l'exclusion d'autres risques. **Or une augmentation des hypothèses d'événements redoutés, orientées principalement sur les risques de la vie privée, renforcerait indéniablement les modalités d'analyse** tout en restant dans le cadre flou des Lignes directrices AIPD du CEPD.

73 Pour reprendre la première ligne du Tableau 13, la menace de « **linkability** » (**1-A**), définie par la méthodologie LINDDUN correspond à la capacité d'un adversaire à « *lier deux objets d'intérêt sans connaître l'identité de la personne concernée impliquée* »[254]. Cette menace est à notre sens la plus pertinente dans le contexte du véhicule connecté/autonome puisqu'elle permettrait de relier le service Biomem à un véhicule connecté à une personne concernée – que celle-ci soit propriétaire ou juste utilisatrice occasionnelle[255]. La déduction entre ces objets d'intérêt et une personne concernée est l'une des problématiques actuelles de ce secteur. Ainsi les auteurs de la méthodologie LINDDUN font découler de cette catégorie les menaces d'**identification** (1°) et d'**inférence des données personnelles** (2°) réalisées au détriment de la personne concernée.

1°) La question de l'identification des personnes concernées renvoie indubitablement aux problématiques traditionnelles rencontrées dans les modalités de la collecte de données personnelles. Les Lignes directrices DPbDD proposent des pistes pour résoudre celles-ci. Dans sa section « *minimisation de la donnée* » (**1-E**), le CEPD invite certes à recourir aux mesures « *traditionnelles* » en droit des données personnelles (*l'agrégation, la pseudonymisation ou l'anonymisation des données personnelles*) comme contre-mesures à ces risques. Mais l'autorité européenne invite surtout à recourir à la technique dite de « *data avoidance* »[256] par l'implémentation de techniques relevant de « *l'état des connaissances* »[257] pour limiter ladite collecte lorsque cela est possible.

2°) La problématique de l'inférence des données personnelles est toutefois plus pertinente dans le présent développement. À notre sens, la menace d'inférence, manifestation de la « *linkability* », relève difficilement des trois types de menace établies par la CNIL (**1-B**). La ré-identification par déduction de données implique, dans la logique sécurité informatique de la CNIL, l'accès illicite aux données. Cette dernière menace est généralement interprétée littéralement, entraînant sa constitution par une **simple consultation de la donnée personnelle**[258] **sans autorisation du responsable de traitement et/ou de la personne concernée**[259]. Cette consultation est une action indépendante à un croisement avec un autre jeu de données, action nécessaire pour permettre la ré-identification.

---

253 Voir Tableau 13.

254 K. WUYTS & W. JOOSER, « *LINDDUN a privacy threat modelling: a tutorial* », 2015, pp. 38, spéc. p. 13.

255 Voir dans ce sens, CEPD, Lignes directrices 1/2020 relatives aux véhicules connectés, p. 3, §3.

256 CEPD, Lignes directrices n°4/2019 relatives à l'article 25 « *Protection des données dès la conception et protection des données par défaut* », Version 2.0, adoptées le 20 octobre 2020, p. 19, §76 : « *Éviter tout traitement de données à caractère personnel si la finalité en question le permet* ».

257 Sur cette question, voir Partie 3, Chapitre 1, Section 2.

258 Sur cette question, voir Partie 3, Chapitre 2, Section 1 §1.

259 Voir dans ce sens CNIL, « *Les Bases de la Connaissance* », qui démontre tout le long de cette documentation que l'accès ne peut être interprété que de façon restrictive.

suite page 86

LINDDUN définit comme exemple de menace à la vie privée, la…	Qui peut être reliée aux menaces définies par la méthodologie CNIL	Ou qui peut être reliée aux menaces définies par la méthodologie NIST	Ou qui peut être reliée aux événements redoutés définies par la méthodologie PRIAM	Ou qui peuvent être liée aux menaces identifiées par les Lignes directrices Véhicule connecté	Qui peuvent être réduit par les mesures proposées par les Lignes directrices DPbDD
Linkability Un adversaire est capable de lier deux objets d'intérêt sans connaître l'identité de la personne concernée. (1-A)	Accès à la donnée pour lier la personne concernée à une information Modification de la donnée personnelle permettant la liaison entre l'information et une personne concernée (1-B)	*Appropriation* (appropriation) la donnée est utilisée d'une façon qui dépasse l'attente de la personne concernée ou son autorisation *Insecurity* (insécurité) faille de sécurité *Induced disclosure* (divulgation provoquée) Peut se réaliser quand la personne concernée se sent contrainte de fournir des informations disproportionnées à la finalité ou qui constituent la contrepartie de la transaction *Stigmatization* (stigmatisation) La donnée est liée à une identité réelle de telle façon à stigmatiser la personne concernée, causant une perte de dignité ou une discrimination. (1-C)	*Fear Event.2.* accès non autorisée aux données *Fear Event.3.* modification non autorisée aux données *Fear Event.4.* utilisation des données pour des finalités non autorisées *Fear Event.5.* inférence des données permettant une re-identification (1-D)	La réutilisation des données permet d'identifierla personne concernée grâce à un objet (1-E)	Miniminisation de données : - collecte limitée - pertinence - agrégration - suppression des données La minimisation des données offre la possibilité de se prémunir d'une menace de *linkability* (1-F)

Tableau 13. Comparaison entre les événements redoutés définis par LINDDUN et leurs correspondances avec les risques définis par les méthodologies CNIL, NIST, PRIAM, les menaces identifiées par les Lignes directrices Véhicule connecté et les prescriptions prévues par les Lignes directrices Protection des données dès la conception et par défaut
Notre notation : «1-A…1-F»[260]

260 Cette numérotation est utilisée §73, page 84 et §74, page 86.

En d'autres termes, seul l'accès à la donnée personnelle constituerait une menace, l'utilisation secondaire de la donnée étant exclue. Cette interprétation invite à examiner la seconde menace officielle, la « *modification* », dont la terminologie trompeuse tenterait d'inclure l'utilisation secondaire de la donnée. La doctrine officielle de la CNIL estime que l**a modification des données personnelles n'est qu'une modification de la valeur ou de l'information conservée par le responsable de traitement**. Cette modification entraînerait une nuisance pour la personne concernée, comme l'inaccessibilité à un service. Ainsi, un croisement de jeux de données ne constituerait pas une modification de la donnée personnelle, mais la création d'une nouvelle base de données.

Commentaires : Comme précisé, du fait de leur interprétation littérale, les menaces définies par la CNIL sont des « *menaces primaires* », c'est-à-dire portant davantage sur le fait générateur du dommage (accès/modification/effacement) que sur le contexte engendrant le dommage pour la personne concernée. Ces menaces « *primaires* » devraient être davantage qualifiées de « *vulnérabilités* » et être utilisées comme méthodes d'analyse. Mais, opérationnellement, l'analyse de menaces-vulnérabilités répond aux prescriptions de la première interprétation faite des Lignes directrices AIPD du CEPD. Bien que validant sa conformité quant à la forme à employer, cette vision questionne l'approche par les risques au travers d'une analyse purement superficielle des « *droits et libertés* » pour favoriser les seules prescriptions de sécurité informatique.

B. L'autonomisation de la notion de dommage : les incertitudes sur les futures interprétations de l'assiette

74 À l'inverse, les méthodologies plus proches d'une évaluation d'impact sur la vie privée prennent en compte des risques plus larges que ceux envisagés dans une AIPD. Ainsi, les méthodologies NIST (**I-C**) et PRIAM (**I-D**) se concentrent davantage sur les « **menaces globales** », c'est-à-dire sur l'intégralité du contexte entraînant le dommage subi par la personne concernée en prenant en compte tant le fait générateur que les utilisations secondaires. En fonction de la méthodologie, les menaces primaires sont incluses ou exclues. Ces deux méthodologies reprennent, soulignons-le, la taxonomie sur la « *Privacy* » réalisée par D. SOLOVE pour apprécier plus largement le spectre des impacts du traitement de données personnelles sur le respect de la vie privée des personnes.

La notion de « *linkability* », posée par la méthodologie LINDDUN, se retrouve dans plusieurs des notions utilisées dans les méthodologies PRIAM et NIST. Ainsi dans la méthodologie NIST, des échos de la « *linkability* » se retrouvent dans de nombreuses menaces relevant alternativement des catégories définies par E. SOLOVE de « *information processing* »[261], d'« *information dissemination* »[262] et d'« *invasion* »[263]. Bien que reconnaissant cette inspiration dans la définition des menaces[264] et des « *privacy harms* », la méthodologie PRIAM entend respecter les conditions de conformité posées par le RGPD.

Les trois menaces définies par le CEPD, c'est-à-dire l'asymétrie de l'information, la qualité du consentement de l'utilisateur et la sécurité des données, sont donc conservées dans la méthodologie PRIAM, assurant ainsi la pertinence des menaces propres au droit des données personnelles mais aussi à celles attentatoires aux « *droits et libertés* ». Les menaces étant définies largement[265], ce caractère attentatoire est analysé principalement en fonction des dommages anticipés. Or comme la troisième partie de ce rapport le démontrera, **les dommages anticipés ont de grandes chances d'être interprétés largement par la Cour de justice de l'Union européenne**. Cette

261 Correspondant dans la case I-C aux menaces « *insecurity* », « *re-identification* ».

262 Correspondant dans la case I-C aux menaces « *appropriation* »,« *induced disclosure* », « *stigmatization* ».

263 Correspondant dans la case I-C à la menace « *surveillance* ».

264 Voir dans ce sens, PRIAM, p. 47.

265 Supra «Introduction».

tendance entraînera alternativement une exigence accrue de la CNIL dans l'interprétation large des menaces, suscitant encore plus de confusion dans sa méthodologie ou suggérant une improbable incorporation de « *menaces globales* » dans sa méthodologie. Dans une telle hypothèse, l'obligation de mise à jour des AIPD contraindra à recommencer cette analyse en prenant en compte cette évolution. Par conséquent, il serait plus opportun d'utiliser une AIPD, proche d'une EIVP, prenant en compte les lacunes de la méthodologie de la CNIL.

C. La convergence sur les dommages définis par les quatre méthodologies

75 La définition des dommages subis par une personne concernée par un traitement des données personnelles varie peu en fonction des méthodologies[266]. En effet, les méthodologies CNIL et PRIAM s'appuient sur les différents types de dommages mentionnés par le considérant 75 du RGPD. Comme l'abordera la troisième partie du présent rapport, ce considérant interprète largement la notion de « *risques pour les droits et libertés* » en incluant le maximum de dommages directs ou indirects. Cette approche est logique, puisque le responsable de traitement est tenu à une anticipation large des « *risques* ». Cette liaison entre « *risques* », « *dommages* » et « *préjudice* »[267] distordant les liens de causalité élargit l'assiette des risques.

76 L'étendue d'un risque de **dommage collectif, voire sociétal, n'est abordée que par la méthodologie PRIAM, et encore de manière indirecte**. Ainsi, au stade de l'analyse des risques, cette méthodologie traite ce danger de deux manières. Tout d'abord, le risque « sociétal ou architectural » est considéré à la suite des « *dommages traditionnels* » pour l'appréciation de la vraisemblance. Il est ensuite plus précisément examiné lors de la détermination de la gravité de l'impact subi par la victime. Ainsi, cette méthodologie invite l'analyste à apprécier le risque d'un point de vue « *individuel* », en considérant un « *groupe spécifique* » et enfin au niveau de la « *société* ».

Lors d'un entretien réalisé avec l'un des concepteurs de cette méthodologie, celui-ci a illustré ce dernier type de dommage par l'exemple du scandale *Cambridge Analytica*. Bien que pertinente, cette proposition nous semble complexe à mettre en œuvre pour trois raisons.

1. Du seul point de vue de l'AIPD, une telle approche supposerait de réaliser une autre AIPD prenant en compte des vulnérabilités et des événements redoutés spécifiques[268] à des dommages immatériels collectifs. Or, même si cette éventualité est prévue au considérant 75 du RGPD, les métriques offrant une telle appréciation restent à définir.
2. Contrairement à la culture étasunienne promouvant implicitement un solutionnisme technologique, la culture européenne est idéologiquement neutre. Le déploiement d'une technologie en Europe n'a pas pour objectif de répondre à un besoin sociétal, mais à un besoin industriel ou commercial. Les politiques de confidentialité peuvent être modifiées unilatéralement des fins politiques, devenant une source de risques pour les responsables de traitement et donc par ricochet pour les personnes concernées.
3. L'impact des technologies de l'information et de la communication sur des groupes spécifiques et/ou la société dans son ensemble relève, à notre sens, davantage de l'*Ethic Impact Assessment* que de l'AIPD. Toutefois, cette classification n'est pas exclusive puisque les deux méthodologies peuvent être combinées. Dans le cadre d'une AIPD, l'analyse portera davantage sur la question de la conformité du traitement à la législation relative aux données personnelles, là où l'EIA se concentrera davantage sur les objectifs recherchés et les effets secondaires de l'implémentation de la technologie.

---

266 Voir supra Tableau 13, page 85.

267 Voir dans ce sens le considérant 75 du RGPD : « *tout autre dommage économique ou social important* ».

268 Voir Partie 3 sur les risques juridiques.

Comme précisé, la méthodologie PRIAM est la seule méthodologie à traiter directement la question du dommage collectif. Toutefois, les praticiens rencontrés lors des entretiens soulignent que celui-ci est pris en compte indirectement à des fins assurantielles. En effet, les dispositions extraterritoriales du *Sarbanes Oxley Act* étasunien[269], prévoyant la responsabilité pénale des dirigeants d'une société en cas de mauvaise gestion, imposent de provisionner le montant des sanctions juridictionnelles ou des dommages et intérêts relatifs à tout dommage susceptible d'être provoqué par la société. Dans notre matière, les dommages susceptibles d'être provoqués par la société peuvent être analysés comme la sanction pécuniaire infligée en cas de non-respect du RGPD par la société. Antérieurement au RGPD, les praticiens estimaient les sanctions rendues par les Autorités Nationales de Contrôle et/ou les dommages et intérêts accordés par les tribunaux civils lors de contentieux étasuniens afin de négocier les primes d'assurances correspondantes.

Sous-Section 2. L'adaptation des quatre méthodologies étudiées pour parvenir à une méthodologie optimale

77 Le présent paragraphe porte sur l'interprétation des différentes étapes par les quatre méthodologies étudiées. Ainsi, le Tableau 13, page 85, dresse les grandes lignes des convergences des méthodologies employées dans le cadre du cas pratique Biomem.

Comme précisé[270], la réalisation du flux de données[271] s'inspirera de la méthodologie PRIAM. Il ne fait aucun doute que toutes les méthodologies respectent **l'étape de la description du traitement** en commençant par **un flux de données** appréciant les différentes vulnérabilités des supports mais aussi des processus organisationnels dans l'organisation du responsable de traitement. Il ne fait aucun doute, non plus, que le niveau de granularité des informations requis dans la **méthodologie PRIAM** est plus important que dans les autres méthodologies. Ce **haut niveau d'information** permet ainsi une optimisation dans l'**identification des vulnérabilités techniques et organisationnelles**.

78 Les modalités du respect des droits par les personnes concernées sont toutefois sous-évaluées dans la méthodologie PRIAM et dépendent de l'analyste. Dans l'onglet appelé **« Description de la nécessité du traitement et de la proportionnalité des mesures », la méthodologie CNIL** offre une meilleure garantie du respect **des droits** au travers de son formalisme plus compréhensible pour le responsable de traitement.

Néanmoins, pour respecter parfaitement la jurisprudence de la CNIL[272], le respect du droit des personnes devrait être affiné pour chaque traitement correspondant à un responsable de traitement dédié. Comme précisé dans la présentation des **Lignes directrices 1/2020 relatives au véhicule connecté du CEPD, la demande d'exercice des droits doit pouvoir être formulée par une personne concernée vers n'importe lequel des responsables de traitements communiquant avec l'ensemble des autres responsables conjoints**. Par conséquent, la description de la nécessité du traitement, c'est-à-dire l'étape de conformité, doit renseigner les modalités exactes de l'exercice des droits[273]. Une telle obligation contraint à l'exhaustivité dans cette étape afin de parvenir à une répartition efficace des obligations entre les différents responsables de traitement impliqués.

---

269 Dont le nom officiel est : *An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes*. Pub. L. 107-204.

270 Supra §69, page 82.

271 Onglets 1.1. et 1.2.

272 Pour rappel des jurisprudences pertinentes mentionnées à la note de bas de page 26, les délibérations de la CNIL, Google (Délibération n°SAN-2019-001 du 21 janvier 2019), Stop covid (Décision n°MED-2020-015 du 15 juil. 2020) et Spartoo (Délibération n°SAN-2020-003 du 28 juillet 2020) qui questionnent chacune d'entre elles la collecte de la réalité du consentement, la sécurité des données personnelles collectées et enfin le traitement de données tierces.

273 Voir dans ce sens la condition de « *allocation of responsibility* » posée par les Lignes directrices DPbDD du CEPD.

Cette contrainte obligerait donc à compléter l'onglet II.2. « Proportionnalité et nécessité » de la méthodologie CNIL pour inclure une pluralité de responsables de traitement. De plus, cet ajout renforcerait les conditions d'interactions et d'autonomie portant respectivement pour la personne concernée sur la possibilité de communiquer et d'exercer ses droits auprès du responsable de traitement et la possibilité de jouir du plus haut degré d'autonomie possible sur ces données personnelles[274]. Ces mesures seraient respectueuses de l'interprétation de l'obligation de « *Loyauté* »[275] dans le cadre de la protection des données personnelles dès la conception par le CEPD.

79 Il est nécessaire d'aborder la question des sources de risques, principalement portant sur la question des sous-traitants et des responsables conjoints, par une digression **au sujet de la sécurité juridique des modalités de délivrance des informations relatives aux données personnelles vis-à-vis des dispositions contractuelles**. En effet, la CNIL comme le CEPD soulignent la distinction entre ces deux engagements[276], souvent unilatéraux. Les *privacy policies* se doivent d'être autonomes par rapport aux stipulations contractuelles portant sur le service impliquant le traitement de données[277].

La question de la valeur juridique des politiques de données personnelles, et de leur caractère contractuel, est omniprésente dans l'AIPD réalisée par le ministère de la Justice Néerlandaise. En effet, bien que relevant d'une obligation d'information d'origine légale imposée par le RGPD, les *privacy policies* se sont vu reconnaître un caractère contractuel incident[278] par la voie des juges judiciaires. Par conséquent, leur caractère immuable reste discutable. Ainsi, sauf dispositions contractuelles organisées dans le cadre d'un accord de consortium d'échanges de données personnelles, les responsables de traitement peuvent rester discrétionnaires de l'utilisation des données personnelles qui est faite. Cette absence d'immuabilité contractuelle dans la détermination de l'utilisation des données personnelles ouvre la possibilité pour l'un des responsables de traitement de modifier substantiellement sa gestion des données personnelles au détriment de l'accord de consortium, générant ainsi un risque pour ses partenaires.

Ainsi, pour reprendre les hypothèses de Biomem-Indé et de Biomem-VOD[279], le constructeur automobile est assimilé à un fournisseur de technologie, tiers au traitement des données personnelles. Pour autant si la question de la conformité des traitements de données personnelles n'est pour l'instant qu'incidente, puisque ses obligations découlant du droit des données personnelles sont limitées aux seuls aspects de la sécurité informatique et des modalités d'implémentation de la protection des données par défaut/dès la conception, des sous-hypothèses peuvent questionner l'étendue de ses obligations en fonction de l'identité du développeur du système d'exploitation d'infodivertissement intégré dans le véhicule connecté.

Dans l'hypothèse où le constructeur automobile est le développeur du système d'exploitation, les dispositions de la directive ePrivacy sont susceptibles de s'appliquer. L'exception à l'application de ce texte concerne un traitement des données issu de l'équipement terminal avec pour seule finalité d'assurer la sécurité des données[280].

---

274 Toutes deux visées au §65 des Lignes directrices DPbDD du CEPD.

275 CEPD, Lignes directrices DPbDD, p. 16-17, §§64-65, spéc. p. 65.

276 CNIL, Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC.

277 C'est-à-dire les conditions générales d'utilisation dans le cadre d'un service, les conditions de vente pour un produit.

278 Voir dans ce sens les jugements du TGI de Paris du 12 février 2019 (UFC-Que choisir Google) et du 9 avril 2019, UFC-Que Choisir / Facebook Inc.

279 Supra §14, page 13.

280 Voir supra Partie 1, Chapitre 2, Section 1, Sous-Section 1, page 20.

Mais dans l'hypothèse où le système d'exploitation est fourni par un tiers, les jurisprudences CJUE Wirtschaftsakademie et FashionID[281] seraient susceptibles de s'appliquer au constructeur, même si ce dernier est éligible à la qualification de fournisseur de technologie. En effet, dans cette hypothèse, les traitements de données problématiques effectués par le développeur-tiers seront susceptibles d'engager la responsabilité du fournisseur de technologie du fait du choix technique qui a été fait par ce fournisseur. En d'autres termes, les dispositions des Lignes directrices DPbDD, qui s'appliquent au fournisseur de technologie, intègrent également les choix technologiques fait par ce dernier. Choix technologiques qui doivent respecter les droits des données personnelles.

80 Dans ces conditions, rejoignant la deuxième hypothèse du cas pratique Biomem où le constructeur est responsable de traitement conjointement avec le fournisseur de vidéos à la demande, le constructeur pourra, très probablement[282] voir sa responsabilité engagée pour des traitements illicites liés à ce choix technologique. De plus, comme le souligne l'un des praticiens rencontrés, l'aspect purement théorique de l'outil contractuel est à considérer. En effet, bien que correspondant à la loi des parties, l'efficacité d'un contrat doit être relativisée sans mesure exécutoire fondée sur une décision judiciaire ou face à une société en liquidation.

> Piste de recherche : L'analyse des sources de risques intégrant la question des parties prenantes doit atteindre un degré de granularité suffisamment avancé pour refléter les obligations contractuelles souscrites par les parties concernées. Elle doit comprendre les clauses d'audit, la possibilité de suspendre contractuellement en cas de faute, avec la possibilité de substituer le sous-traitant par un autre pour la continuité du service ou à défaut la fourniture d'une brique technologique sous une licence ouverte permettant la continuité du service en faveur de la partie non fautive en attendant la régularisation par la partie fautive. Ainsi la matière contractuelle propre au droit de l'informatique doit incorporer davantage d'éléments relevant du droit des données personnelles.

81 Comme mentionné dans la section précédente, l'étude des vulnérabilités devrait prendre en compte une vulnérabilité principale, définie par une méthodologie d'analyse des données personnelles comme LINDDUN, se décomposant en sous-vulnérabilités reprenant les vulnérabilités définies par la méthodologie PRIAM[283]. Dans ces conditions, une étude sur les vulnérabilités techniques centrées sur les données personnelles (« **primaires** ») et les traitements subséquents (« **globaux** ») augmenterait le niveau de granularité de l'analyse tout en permettant d'anticiper les évolutions futures de la jurisprudence de la Cour de Justice de l'Union européenne.

> **Recommandation :** Cette granularité dans la vulnérabilité sera reprise dans le cadre du calcul du risque. Dans ces conditions, **la méthodologie PRIAM servira toujours de modèle**. Toutefois, nous écarterons pour les raisons mentionnées en (§75) les risques pour les « groupes spécifiques » et les « *risques sociétaux* » pour introduire **un système de notation « pair »[284] de l'appréciation de la « gravité », comme utilisé dans la méthodologie CNIL**. Cette solution permettra de **prioriser l'implémentation des mesures adéquates aux risques détectés** et de déterminer ainsi leur efficacité afin d'**apprécier les risques résiduels**. Toutefois, outre l'appréciation des « dommages classiques »[285], **une estimation des risques « réputationnels » et « financiers »**, telle que prévue par **les méthodologies NIST et BSI**, concrétiseraient une estimation de l'intégralité des risques encourus par la structure responsable de traitement.

---

281 Voir supra, note de bas de page en page 23.

282 Voir Partie 3.

283 Qui elle-même comprend les menaces définies par la CNIL.

284 Voir supra §50, page 57.

285 Voir Partie 3 sur la discussion de ce concept.

Partie 3

La judiciarisation des risques liés aux traitements de données personnelles

Partie 3

82 Des incertitudes, désignées sous la terminologie de « *risques* », sont principalement appréciées au niveau européen par les deux systèmes juridiques européens, celui du Conseil de l'Europe et celui de l'Union européenne. Cette appréciation est en pratique effectuée par deux cours mises en place par ces systèmes, respectivement la Cour européenne des droits de l'homme (ci-après « CEDH ») et la Cour de Justice de l'Union européenne (ci-après « CJUE »). Leur examen se base sur une interprétation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après « Convention ESDH »), lequel dispose : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* », ainsi que sur l'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après « CDFUE »), qui présente une rédaction quasi similaire[286]. Lors de son adoption en 1950, la Convention européenne de sauvegarde des droits de l'Homme ne reconnaissait pas expressément le droit à la protection des données personnelles. À l'inverse, la Charte des droits fondamentaux de l'Union européenne, adoptée en 2000, a pris acte de l'évolution de nos sociétés contemporaines en intégrant un tel droit. Ainsi, son article 8 dispose que «*Toute personne a droit à la protection des données à caractère personnel la concernant* ».

L'article 52-3° de la Charte des droits fondamentaux de l'Union européenne prévoit une application uniforme du droit de la CEDH dans l'Union européenne. Dans ce contexte, les décisions du juge des droits de l'homme ont une application, *a priori*, directe en droit de l'Union européenne.

L'interprétation large du droit au respect de la vie privée par la CEDH[287] s'étend au droit au respect des données personnelles, et par incidence à celui de vivre dans un environnement sain. La finalité poursuivie est l'anticipation de l'impact du déploiement d'innovations susceptibles de générer des dommages pour l'environnement et les consommateurs. La jurisprudence qui en découle constitue une source précieuse dans la compréhension de l'application et la portée du principe de précaution.

En effet, la CJUE a développé ces trente dernières années un corpus jurisprudentiel autour du principe de précaution offrant ainsi un cadre juridique en matière de risques sanitaires et environnementaux. Certains éléments de ce corpus ont été repris dans sa jurisprudence relative au respect de la vie privée. Concomitamment, la CEDH a apprécié les mesures mises en œuvre par les États pour prévenir d'éventuelles violations de la Convention ESDH dans l'appréciation de situations suscitant des incertitudes factuelles (Chapitre 1, page 94).

83 Nous étudierons ensuite la question de la sanction du non-respect des obligations posées par le Règlement Général pour la Protection des Données personnelles (ci-après « RGPD »). Le droit civil français ainsi que les droits étasunien et anglais nous conduiront à examiner la notion de dommage. Cette notion nous permettra d'étudier les conditions de réparation à la fois sous l'angle des amendes administratives à l'encontre du responsable du traitement et des dommages et intérêts alloués à la personne concernée (Chapitre 2, page 114).

---

286 En effet, selon l'article 7 de la Charte des droits fondamentaux de l'Union européenne, « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ».

287 La notion de « *vie privée* » est en effet une notion fonctionnelle variant en fonction des besoins de la Cour européenne des droits de l'homme.

Chapitre 1 L'appréciation des risques par la Cour européenne des droits de l'Homme et par la Cour de justice de l'Union européenne

Chapitre 1 L'appréciation des risques par la Cour européenne des droits de l'Homme et par la Cour de justice de l'Union européenne

L'AIDP correspond à l'obligation pour le responsable du traitement de s'interroger en amont du traitement de données personnelles sur le respect des « *droits et libertés* » de la personne concernée. Les modalités d'application de ces droits découlent de la jurisprudence de la CEDH. Par ailleurs, les arrêts de la CJUE relatifs au principe de précaution fournissent des enseignements utiles pour apprécier les modalités de réalisation d'une AIPD.

Nous nous concentrerons tout d'abord sur la définition du principe de précaution. Cette étape préalable à la distribution de certains produits sur le marché commun emporte l'examen d'un risque de nocivité de ceux-ci, apprécié en fonction de sa gravité et de sa vraisemblance. Toutefois à la différence de l'AIPD, cette analyse est réalisée de façon contradictoire entre une autorité nationale et/ou européenne sur la base de l'état des connaissances.

Cette dernière notion, reprise dans le RGPD, correspond à l'ensemble des connaissances disponibles au moment de l'examen de la dangerosité du produit. Elle permet ainsi d'assouplir la production de preuves scientifiques, facilitant la démonstration de l'absence de perniciosité ou la preuve de l'innocuité d'un produit. Cependant, l'état des connaissances peut être remis en cause par une preuve scientifique contradictoire de valeur identique démontrant l'absence de risque.

À l'inverse, l'analyse des risques effectuée par la CEDH est plus souple. En effet, pour examiner l'existence d'un risque en matière de droits de l'homme, cette juridiction se concentre sur les critères de gravité, de probabilité et d'acceptabilité pour déterminer si l'État membre aurait pu prendre les mesures préventives nécessaires à la réalisation du préjudice. Bien que la probabilité d'une telle atteinte soit couramment admise par la Cour, le « *seuil de gravité* » constitue l'essentiel de l'examen à partir de preuves produites par les parties et de rapports objectifs fournis par des tiers aux procès (ONG). Le critère d'acceptabilité du risque correspond à une réserve permettant aux États membres de dégager leur responsabilité face à l'imprévisibilité du comportement humain.

Or, la méthode d'appréciation des AIPD en vue de prévenir des dommages aux « *droits et libertés* » des personnes concernées invite à prendre en compte ces deux focales d'examens. Ainsi, le risque en droit des données personnelles est judiciairement apprécié de façon abstraite en se concentrant sur des manquements objectifs. La charge de la preuve de la conformité repose ici exclusivement sur le responsable du traitement. Néanmoins l'immatérialité de l'informatique entraîne de nombreuses difficultés dans la collecte de preuves. Pour combler ces difficultés, les Cours européennes emploient la notion du dommage « *probabiliste* » en utilisant

le verbe « *pouvoir* ». Ce verbe allège la preuve d'un réel dommage aux « *droits et libertés* » des personnes concernées pour se contenter de la forte probabilité de sa réalisation.

Les deux systèmes juridiques européens interviennent depuis longtemps pour fixer le cadre méthodologique qui permet de caractériser l'incertitude issue d'innovations ou de situations factuelles entraînant une menace à l'échelle de l'individu ou de la communauté. Ils constituent une source d'inspiration pour délimiter l'assiette des risques à prendre en considération lorsqu'un responsable de traitement réalise une analyse d'impact relative à la protection des données personnelles. Ici, le principe de précaution traduit une vision prudente du déploiement des innovations technologiques dans un contexte environnemental. La Convention des droits de l'homme est, ici, pertinente pour nous aider à définir l'étendue des « *droits et libertés* » afin de cerner l'identification des risques en amont d'une atteinte possible aux droits de l'homme (Section 1). Si les deux sources du droit fournissent, dans une certaine mesure, une appréciation de l'étendue des mesures à adopter afin d'atténuer les risques identifiés, le droit de l'Union européenne propose peu de solutions pouvant servir de cadre aux analyses d'impact relative à la protection des données. En revanche, le droit du Conseil de l'Europe fait preuve de pragmatisme en développant une appréciation circonstanciée en fonction des droits concernés et des moyens mis à disposition (Section 2, page 107).

Section 1. Les modes jurisprudentiels de calcul de la probabilité d'un risque dans le domaine des droits de l'homme

Afin d'appréhender les différentes formes d'appréciation du risque dans le domaine des droits de l'homme, nous aborderons dans un premier temps les analyses réalisées par la CJUE (1.1), pour ensuite présenter celles effectuées par la CEDH (Sous-Section 2, page 102).

Sous-Section 1. L'analyse du risque par la CJUE

L'analyse du risque par la CJUE se réalise dans deux domaines distincts : le droit de l'environnement, et le droit des données personnelles. Le droit de l'environnement s'appuie sur le principe de précaution incorporé par le Traité de Maastricht du 7 février 1992. Il a été ensuite codifié à l'article 191(2) par le Traité sur le Fonctionnement de l'Union Européenne (ci-après « TFUE ») adopté le 13 décembre 2007 (A, page 96). L'analyse du risque en matière de données personnelles a pour sa

part été développée au regard du principe de proportionnalité par l'arrêt Schrems en 2015[288], avant d'être précisée par la jurisprudence ultérieure. Cette jurisprudence prend en compte le caractère abstrait d'un risque (B, page 100).

A. L'analyse d'un risque potentiel au regard du principe de précaution

84 De manière générale, le principe de précaution se distingue du principe de prévention par le degré d'incertitude que présente un éventuel risque.

- L'application du *principe de prévention* a pour effet d'interdire la distribution d'un produit du fait de **la certitude** de la réalisation du dommage généré par ce produit.
- Le *principe de précaution* se concentre sur **l'incertitude** de la réalisation du dommage pour prononcer l'interdiction de commercialisation du produit[289].

De prime abord, l'étendue du principe de précaution, entendu comme un principe d'action, est limitée puisqu'il a vocation à s'appliquer dans des domaines spécifiques : la protection des consommateurs[290], l'environnement, la sécurité alimentaire[291] et les organismes génétiquement modifiés. La jurisprudence administrative française l'a étendu à la protection de la santé publique pour justifier, par exemple, l'interdiction d'implanter des lignes à haute tension ou des antennes relais dans certaines zones[292].

Sans préciser les conditions d'application, cette extension prétorienne des domaines concernés a donné lieu à de multiples critiques[293]. D'une part, à l'instar de l'analyse d'impact relative à la protection des données, le principe de précaution s'applique en amont de la commercialisation du produit éventuellement litigieux. La critique porte, d'autre part, sur la procédure applicable à l'appréciation du risque généré par le produit examinée par l'autorité compétente, procédure définie dans le cadre de plusieurs jurisprudences.

---

288 CJUE, 6 juil. 2015, C-362/14, SCHREMS.

289 Parlement européen, « *Le Principe de précaution – définitions, applications et gouvernance* », 2015, p. 29, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/573876/EPRS_IDA%282015%29573876_FR.pdf

290 C. BLUMANN C. et V. ADAM, « *La politique agricole commune dans la tourmente : la crise de la vache folle* », RTD eur., avril-juin 1997, p. 292.

291 Directive du Conseil 89/397/CEE du 14 juin 1989 relative au contrôle officiel des denrées alimentaires, JOCE. n° L 186 du 30 juin 1989, p. 23.

292 Voir dans ce sens, S. CAUDAL, « *Existe-t-il un principe de précaution appliqué par le juge administratif ?* », RFDA 2017, p. 1061 qui souligne l'interprétation large du principe de précaution pour des mesures qui ne relèvent pas directement du *ratione materiae* européen. Ainsi la santé publique a fondé en droit français l'interdiction de l'installation dans certaines zones géographiques de lignes à haute tension (CE 26 fév. 2014, Association Ban Asbestos France), de l'amiante (CE, 23 juil. 2014, Sté Maco Pharma) ou des antennes relais (CE 08 oct. 2012, Commune de Lunel).

293 Voir dans ce sens Commission européenne, « *Science for environment policy, future brief: the precautionary principle: decision-making under certainty* », iss. 18, 09/2017, p. 24, spéc. pp. 6-8 où les auteurs reprennent la plupart des critiques formulées à l'encontre de ce principe en axant principalement leurs arguments sur les effets négatifs en ce qui concerne l'innovation. Voir également le rapport du Parlement européen, « *Le Principe de précaution – définitions, applications et gouvernance* », p. 12-13, qui se positionne principalement sur les critiques arguant sur le caractère discrétionnaire des risques neutralisant tous fondements scientifiques légitimant l'application du principe de précaution.

Cette procédure débute par l'identification des dangers[294], puis se poursuit par une mise sous forme de probabilités d'un phénomène ou d'un événement en recourant à des descriptions qualitatives ou quantitatives des propriétés de l'agent chimique ou biologique problématique. Outre les critères de la gravité et de la vraisemblance, la CJUE peut prendre en compte les effets de la dissémination d'un produit ou d'un composé chimique ou biologique, comme le trichloréthylène, dans l'environnement[295]. Cette étape comprend, à l'instar de ce qui est prévu pour les AIPD, la détermination de la gravité et de la vraisemblance du risque sur la santé humaine[296].

La procédure d'examen se conclut par l'analyse du risque en tant que tel. Les résultats présentés aboutissent alors à l'autorisation, totale ou partielle, ou au refus de distribution du produit par les autorités nationales et / ou européennes compétentes.

La gestion du risque intervient, à ce niveau, par la prise en compte par le producteur des informations scientifiques en fonction de la gradation de la gravité et de la probabilité du risque à se réaliser. L'analyse scientifique permettant de déterminer la survenance du risque guidera l'interprétation des résultats de l'expertise scientifique pour les traduire en décision de gestion des risques. Les effets concrets de cette analyse du risque présentent cependant une différence avec les AIPD. En effet, bien que les deux types d'analyses soient réalisés par le producteur du produit ou le responsable du traitement de données personnelles, l'examen du produit par une autorité compétente est obligatoire dans le premier cas. De plus, même si la soumission est acceptée par cette première autorité, l'autorisation peut être remise en cause par une autorité d'un autre État membre, laquelle est éligible à soumettre le litige devant la CJUE. Dans le cas d'une analyse européenne d'un produit attentatoire à l'environnement, la Commission européenne, en tant qu'organe politique, est tenue de reconsidérer le résultat de l'analyse du risque[297]. La CJUE rappelle que « *l'évaluation scientifique des risques est communément définie, tant au niveau international qu'au niveau communautaire, comme un processus scientifique qui consiste à identifier et à caractériser un danger, à évaluer l'exposition et à caractériser le risque* ». Cette compétence européenne garantit que le principe de précaution ne peut être invoqué par un État membre pour justifier la prise de mesures discriminatoires qui viendraient limiter la circulation de marchandises provenant d'autres États membres sur son territoire.

85 Comme l'indiquent les lignes directrices de la Commission européenne relatives au principe de précaution[298], « *le recours (à ce principe) n'intervient que dans une hypothèse de risque potentiel, même si ce risque ne peut être entièrement démontré, son ampleur quantifiée ou ses effets*

---

294 Art. 3(14) du règlement général sur la nourriture FAO : « *Le danger est le potentiel d'une source identifiée, biologique, chimique ou physique qui peut causer un effet juridique défavorable* ». Voir dans ce sens, CJCE Commission c. Danemark, 23 sept. 2003, C-192/01, §51 : « *une application correcte du principe de précaution présuppose, en premier lieu, l'identification des conséquences potentiellement négatives pour la santé de l'adjonction proposée de substances nutritives, et, en second lieu, une évaluation compréhensive du risque pour la santé fondée sur des données scientifiques disponibles les plus fiables et des résultats les plus récents de la recherche internationale* ».

295 Ex : CJCE, 11 juil. 2000, C-473/08, Toolex, §41 : « *Le gouvernement suédois expose que le trichloréthylène affecte le système nerveux central, le foie et les reins. Sa très grande volatilité contribuerait à multiplier les situations d'exposition qui pourraient facilement avoir des effets négatifs sur la santé. Son inhalation pourrait provoquer de la fatigue, des maux de tête ainsi que des troubles de la mémoire et de la concentration* ».

296 CJCE, 02 avr. 2004, C-41/02, Commission c. Pays-Bas, §49 : « *Dans un tel contexte, l'évaluation du risque que l'État membre est tenu d'effectuer a pour objet l'appréciation du degré de probabilité des effets néfastes de l'adjonction de certaines substances nutritives aux denrées alimentaires pour la santé humaine et de la gravité de ces effets potentiels* ».

297 Voir dans ce sens TPICE, Pfizer, 11 sept. 2002, T-13/99, §156 qui reprend la décision CJCE, 05 déc. 2018, C-14/78, Denkavit v. Commission, §24 : « *l'assurance, dans l'ensemble de la communauté, que les institutions communautaires veillent avec vigilance à ce que la libre circulation des marchandises ne puisse avoir des effets de nature nocive à la santé humaine ou animale est un élément de nature à favoriser cette libre circulation* ».

298 Commission européenne, « *Communication sur le recours au principe de précaution* », 2000, p. 13, §5.1, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A52000DC0001.

déterminés en raison de l'insuffisance ou du caractère non concluant des données scientifiques ». Ainsi le caractère « *potentiel* » du risque – c'est-à-dire l'incertitude liée à la nocivité du produit – fonde la légitimité de son examen au regard du principe de précaution. Concrètement, cet examen aboutit à l'interdiction de distribution du produit sur le territoire d'un État membre ou de l'Union européenne.

86 Afin de quantifier l'incertitude, le principe de précaution s'appuie sur des évaluations scientifiques contradictoires pour tenter d'obtenir un avis impartial quant à l'existence d'un risque. Pour cela, « *les données scientifiques disponibles les plus fiables et des résultats les plus récents de la recherche internationale* »[299], voire « *une information suffisamment fiable et solide* »[300], sont constituées à titre probatoire. Les données scientifiques considérées par l'autorité compétente sont celles qui sont disponibles au moment de la prise de la mesure[301] ou lorsqu'une nouvelle preuve scientifique est disponible[302]. Autrement dit, il s'agit de prendre en compte de façon évolutive « *l'état des connaissances scientifiques* ». L'institution examinant la nocivité du produit doit alors réunir « *des indices sérieux et concluants, qui, sans écarter l'incertitude scientifique, permettent raisonnablement de douter de l'innocuité et/ou de l'efficacité du médicament* »[303]. Bien que la Cour de justice de l'Union européenne estime qu'il s'agit ici de procéder à une « *évaluation approfondie du risque* »[304], les critères devront être précisés. L'institution examinatrice peut être assistée par des services d'organismes scientifiques internationaux, communautaires, voire nationaux, dans l'appréciation approfondie du risque. L'évaluation scientifique étant considérée comme factuelle, l'avis scientifique qui en découle n'est donc soumis à aucun régime spécifique[305]. Ceci engendre deux conséquences. D'une part, cette « *simple* » preuve peut être combattue par toute preuve scientifique ultérieure. D'autre part, le faible caractère probatoire de la preuve scientifique illustre l'absence d'harmonisation dans l'application du principe de prévention. Les États membres peuvent ainsi rehausser le niveau de risque à prendre en compte dans le respect des grandes libertés européennes. La Cour rappelle que « *[c]ela signifie qu'une décision de gestion du risque relève de chaque partie contractante, qui dispose d'un pouvoir d'appréciation pour déterminer le niveau de risque qu'elle considère approprié. À ces conditions, une telle partie peut invoquer le principe de précaution, selon lequel il est suffisant de démontrer qu'il existe une incertitude scientifique*

---

299 CJCE, 11 juil. 2000, C-473/98, Kemikalieinspektionen contre Toolex Alpha AB : « *Compte tenu des derniers travaux de la recherche médicale en la matière, mais aussi des difficultés de détermination, en l'état actuel de cette recherche, du seuil critique à partir duquel l'exposition au trichloréthylène constituerait un risque sérieux pour la santé humaine, aucun élément du dossier ne permet à la Cour de constater qu'une réglementation nationale telle que celle en cause au principal va au-delà de ce qui est nécessaire pour atteindre le but visé* ».

300 TPICE, Pfizer, §162 : « *Malgré l'incertitude scientifique subsistante, cette évaluation scientifique doit permettre à l'autorité publique compétente d'apprécier, sur la base des meilleures données scientifiques disponibles et sur celle des résultats les plus récents de la recherche internationale, si le niveau de risque qu'elle juge acceptable pour la société est dépassé. C'est sur cette base que cette autorité doit décider si la prise de mesures préventives s'impose* ».

301 Id., §144 : « *Il résulte au contraire du principe de précaution, tel qu'interprété par le juge communautaire, qu'une mesure préventive ne saurait être prise que si le risque, sans que son existence et sa portée aient été démontrées «pleinement» par des données scientifiques concluantes, apparaît néanmoins suffisamment documenté sur la base des données scientifiques disponibles au moment de la prise de cette mesure* ».

302 TPICE, 26 nov. 2002, aff. jtes. T-74/00, T-76/00, T-83/00 à T-85/00, T-132/00, T-137/00 et T-141/00, Artegodan.

303 Id., §192 : « *Dans ce contexte, l'autorité compétente peut se limiter à fournir, conformément au régime commun du droit de la preuve, des indices sérieux et concluants, qui, sans écarter l'incertitude scientifique, permettent raisonnablement de douter de l'innocuité et/ou de l'efficacité du médicament* ».

304 CJCE, Commission c Danemark, note supra, §48 : « *Une décision d'interdire la commercialisation, qui constitue, d'ailleurs, l'entrave la plus restrictive aux échanges concernant les produits légalement fabriqués et commercialisés dans d'autres États membres, ne saurait être adoptée que si le risque réel allégué pour la santé publique apparaît comme suffisamment établi sur la base des données scientifiques les plus récentes qui sont disponibles à la date de l'adoption d'une telle décision. Dans un tel contexte, l'évaluation du risque que l'État membre est tenu d'effectuer a pour objet l'appréciation du degré de probabilité des effets néfastes de l'addition de certaines substances nutritives aux denrées alimentaires pour la santé humaine et de la gravité de ces effets potentiels* ».

305 Concl. avocat général J. Kokott dans CJUE, 8 juill. 2010, C-343/09, Afton Chemical, §34.

pertinente en ce qui concerne le risque en question. Ce pouvoir d'appréciation est, cependant, soumis au contrôle du juge »[306].

Un parallèle peut être effectué avec les articles 25[307] et 32[308] du RGPD, respectivement relatifs à la protection des données et à la sécurité, qui prévoient l'obligation du responsable du traitement de prendre en compte de « *l'état des connaissances* ». Cette notion est précisée par les Lignes directrices du CEPD relatives à la protection des données dès la conception et par défaut[309]. Incidente à l'obligation de réalisation de l'AIPD, l'obligation de respect des dispositions posées par l'article 25 relatif à la sécurité des données personnelles contraint le responsable du traitement à « *déterminer les mesures techniques et organisationnelles appropriées en prenant en compte les solutions technologiques disponibles sur le marché* ». Cette notion d'état des connaissances, reposant entre autres sur les certifications et autres standards[310], est donc une obligation de veille technologique. Néanmoins, la mise en œuvre des mesures technologiques résultant de cette veille est conditionnée par la prise en compte du coût de leur implémentation. Ainsi, le CEPD relativise cette veille en soulignant qu'une solution technique onéreuse n'est pas pour autant gage d'une efficacité absolue[311]. La jurisprudence relative au principe de précaution a été prise en compte par le législateur européen en rappelant que le coût de mise en œuvre n'est qu'un facteur à prendre en compte parmi d'autres. Ainsi, le refus d'implémentation d'une mesure technologique assurant le respect des droits et libertés ne saurait, à lui seul, être justifié par un coût déraisonnable. Le responsable du traitement est, selon le CEPD, tenu de prendre en compte les mesures techniques de protection des droits et libertés des personnes concernées dans le budget global du traitement projeté[312].

Les logiques inhérentes au droit des données personnelles et au principe de précaution, pris au sens large, divergent au regard du régime de la preuve de l'incertitude. Le droit des données personnelles repose sur le principe de responsabilité, ce qui correspond à une autoévaluation réalisée par le responsable de traitement lui-même, là où le droit de l'environnement repose sur la preuve produite par le producteur auprès du juge administratif dans le cadre d'un recours en excès de pouvoir dirigé à l'encontre d'une autorisation délivrée par un ministère[313] ou une autorité nationale, ou d'un recours auprès de la Commission européenne[314]. Cette preuve objective

---

306 CJCE, 01 avr. 2004, C-286/02, Bellio F.lli Srl v Prefettura di Treviso, §58.

307 Selon lequel : « ***Compte tenu de l'état des connaissances**, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées* ».

308 Selon lequel : « ***Compte tenu de l'état des connaissances**, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

309 CEPD, 20 oct. 2020, « *Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut* », https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_fr.

310 CEPD, Id., p. 8, §22.

311 CEPD, Id., p. 10, §24 : « *L'élément coût n'oblige pas le responsable du traitement à dépenser une quantité disproportionnée de ressources lorsqu'il existe d'autres mesures moins exigeantes en ressources, mais tout aussi efficaces* ».

312 CEPD, Id., p. 10, §26 : « *Les responsables du traitement devraient être en mesure de gérer les coûts globaux afin de mettre en œuvre tous les principes de façon effective et, par conséquent, de protéger les droits* ».

313 Dans ce sens, C.E., 25 sept. 1998, Greenpeace c. ministère de l'Agriculture.

314 A. STIRLING, « *Precaution in the governance of technology* », *in Oxford handbook of law, regulation and technology*, 2017, pp. 644-669, spéc. p. 648.

caractérise le risque « *potentiel* » ou l'« *incertain* »[315], c'est-à-dire « *une situation où les impacts d'une situation sur l'environnement et/ou la santé humaines sont probables mais où les probabilités sont inconnues* »[316]. De manière discrétionnaire, l'appréciation des risques par un responsable du traitement des données personnelles « *pour les droits et libertés* » des personnes concernées questionne les modalités de preuve. Généralement, celles-ci attestent de l'absence de risque liées à la mise en œuvre du traitement envisagé[317].

Bien que l'application du principe de précaution ait été étendue au-delà du droit de l'environnement, il ne s'applique pas de manière uniforme en matière de droits de l'homme. En matière de protection des données personnelles, la CJUE privilégie le recours au principe de proportionnalité[318].

B. La prise en compte du caractère abstrait d'un risque potentiel en matière de données personnelles

87 L'appréciation du risque par la CJUE dans le domaine des données personnelles porte sur des points particuliers étudiés au fil des affaires qui lui ont été soumises. Il s'agit d'une approche casuistique. En effet, la Cour se limite à des questions relatives à la sécurité informatique[319], aux données devant être protégées dans le cadre de l'application de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[320], à l'accessibilité des données par des acteurs tiers[321], ou encore aux garanties à fournir[322] pour démontrer le respect effectif de l'exercice des droits par les personnes concernées[323].

88 L'Avocat Général Yves BOT a souligné[324] dans ses conclusions dans la première affaire SCHREMS, que la charge de la preuve d'un dommage résultant d'une violation de données personnelles n'incombe pas au requérant. Dans cette affaire, le demandeur fait grief d'une atteinte à la protection de ses données personnelles par leur partage potentiel entre le responsable du traitement, Facebook, avec les services de renseignement étasunien. L'Avocat Général souligne tout d'abord, que « *la Commission [européenne] fait valoir que M. Schrems n'aurait pas avancé d'arguments spécifiques donnant à penser qu'il courrait un risque imminent de subir des dommages graves en raison du transfert de données entre Facebook Ireland et Facebook USA* », avant d'estimer qu' « *au contraire, en raison de leur nature abstraite et générale, les inquiétudes exprimées par M. Schrems à propos des programmes de surveillance mis en œuvre par les agences de sécurité américaines seraient identiques à celles qui ont conduit la Commission à entamer le réexamen de la décision 2000/520*[325] *(établissant l'accord de Safe Harbor)* ».

---

315 Rapport du Parlement européen, « *Le Principe de précaution – définitions, applications et gouvernance* » (note supra), p. 9.

316 Rapport du Parlement européen, « *Le Principe de précaution – définitions, applications et gouvernance* », p. 9.

317 Voir supra Partie 2, Chapitre 2.

318 F. SUDRE, « *La Cour européenne des droits de l'homme et le principe de précaution* », RFDA 2017, p. 1039.

319 CJUE, 10 juil. 2018, aff. C-25/17, Jehovan todistajat.

320 CJUE, 1er oct. 2017, aff. C-673/17, Planet 49.

321 CJUE, 6 juil. 2015, aff. C-362/14, Schrems.

322 CJUE, 8 avr. 2014, aff. C-293/12 et C-594/12, Digital Rights, et Schrems II (§176).

323 CJUE, 16 juil. 2020, C-311/18, Schrems II.

324 Voir dans ce sens le §59 des conclusions de l'Avocat Général BOT, dans l'affaire Schrems (I).

325 Décision de la Commission 2000/520/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, JOCE L 215 du 25.8.2000, p. 7–47.

De même, la CJUE prend en compte le « *caractère* » abstrait d'une violation. Autrement dit, l'absence de démonstration de la réalisation de cette violation ne fait pas obstacle à la caractérisation du risque et au prononcé de sanctions par la Cour[326]. Ce raisonnement est repris dans les affaires où le responsable du traitement de données personnelles est un État membre[327], par exemple l'Irlande dans l'arrêt Digital Rights, ou un État tiers à l'Union européenne, comme les États-Unis dans les affaires Schrems[328]. Dans les deux cas sont visés les « *risques d'abus contre tout accès et toute utilisation illicite des données* ». Cette perception prend également en compte le caractère massif des bases de données personnelles. Dans ces deux affaires, la surveillance régalienne entraîne un manquement à l'obligation de transparence relative à l'information à communiquer à la personne concernée. Les affaires Schrems sont plus symptomatiques, dans la mesure où la sécurité des supports communiquant les données personnelles est compromise par un État tiers à des fins d'intrusion dans la vie privée, lesquelles sont justifiées, à tort, par la recherche et l'identification d'éventuelles menaces qui seraient faites aux intérêts de l'État américain.

89 La CEDH rejoint partiellement la position retenue par la CJUE concernant l'appréciation des mesures visant à prévenir des dommages potentiels dans le cadre de l'utilisation des données personnelles. Si la CEDH quantifie le risque à partir de preuves issues de rapports internationaux ou des preuves fournies par les parties, la CJUE fait preuve de moins de rigueur. Dans l'arrêt Schrems II de 2020, la CJUE puise son argumentation dans ses décisions antérieures, les conclusions de l'Avocat Général et les allégations soutenues par l'association None Of Your Business (NOYB) pour invalider le second accord conclu entre la Commission européenne et la *Federal Trade Commission* appelé *Privacy Shield*, remplaçant « *l'accord de Safe Harbor* » annulée par l'arrêt Schrems I. L'utilisation répétitive du verbe « *pouvoir* » y illustre également l'incertitude factuelle[329]. Or, le *Privacy Shield*, remis en cause par l'action de NOYB auprès de la CJUE, était un accord conclu entre la Commission européenne et le Gouvernement Fédéral des États-Unis d'Amérique organisant le transfert des données personnelles à destination de ce dernier. Son désaveu par la CJUE assoit la prévalence et l'autonomie de la règle de droit. Incidemment, l'arrêt Schrems II renforce également la compétence des autorités nationales de contrôle, telles que la CNIL, en rappelant leur indépendance vis-à-vis de la Commission européenne. En matière de données personnelles, le fondement retenu par la CJUE semble tangible en raison de la prise en compte de probabilités. De son côté, la CEDH s'appuie sur des rapports objectifs et indépendants. Toutefois, dans les deux cas, la rigueur procédurale juridique est problématique du fait de la difficulté d'une réelle investigation juridique réalisée dans les locaux étasuniens où se trouvent les serveurs de Facebook par les autorités nationales de contrôle, ou bien de l'impossibilité de quantifier véritablement les atteintes aux données personnelles. L'impossibilité procédurale de réaliser des investigations dans des États tiers empêche l'examen de l'ampleur du traitement contrevenant aux dispositions du RGPD et donc l'appréciation de la réalité et de l'étendue de l'atteinte constituée. De même, bien qu'étant une organisation régionale liant ses États membres, la CEDH voit occasionnellement ses arrêts souffrir d'un manque d'efficacité, les États parties refusant d'exécuter ces arrêts[330]. Cette dernière raison

---

326 Voir infra Chapitre 2.

327 CJUE, Grande chambre, 8 avr. 2014, C-293/12 et C-594/12, Digital Rights, où était visée l'Irlande.

328 Dans les deux affaires Schrems, il s'agissait exclusivement des États-Unis.

329 CJUE, 16 juil. 2020, C-311/18, Schrems II, §196, « *ainsi que M. l'avocat général l'a souligné, au point 338 de ses conclusions, si le considérant 120 de la décision BPD (Décision du du 12 juillet 2016, conformément à la directive 95/46 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (JOUE 2016, L 207, p. 1) fait état d'un engagement du gouvernement américain à ce que la composante concernée des services de renseignement soit tenue de corriger toute violation des normes applicables détectée par le médiateur du bouclier de protection des données, ladite* ***décision ne comporte aucune indication selon laquelle ce médiateur serait habilité à prendre des décisions contraignantes à l'égard de ces services et ne fait pas non plus état de garanties légales dont serait assorti cet engagement et dont pourraient se prévaloir les personnes concernées*** ».

330 Sur ce sujet, voir A. KOVLER, « *La CEDH face à la souveraineté d'un État, L'Europe en formation* », 2013/2, n°368, p. 209-222, https://www.cairn.info/revue-l-europe-en-formation-2013-2-page-209.htm au sujet de l'arrêt CEDH, 18 déc. 1996, Loizidou c. Turquie, Req. N°15318/89, pour lequel la Turquie s'est opposée à la décision de la CEDH.

est l'une des raisons pour lesquelles les arrêts Big Brother[331] et Centrum[332] tolèrent des traitements de données personnelles attentatoires à la vie privée sur le fondement des intérêts vitaux des États membres au Conseil de l'Europe. Le juge PINTO DE ALBURQUEQUE de la CEDH souligne que ces mêmes traitements étaient auparavant censurés par la Cour comme une atteinte à la vie privée[333]. Les commentaires informels au lendemain de ces arrêts mettent en exergue une volonté des Cours européennes de ne pas brusquer les intérêts nationaux de ses États membres[334].

L'approche par les risques est appréhendée par les Cours européennes d'une façon probabiliste. Comme il a déjà été évoqué, la collecte de preuves face à des traitements de données personnelles opaques est rendue délicate qu'il s'agisse des systèmes d'interception massives de communications mises en place par les États ou des traitements de données personnelles effectuées par Facebook[335]. Bien que composés d'experts, ces cours ne traitent que du droit et non de la technique. Dans de telles conditions, les informations fournies par les parties en cause sont, par nature, incomplètes. Ce caractère incomplet invite le juge à ne prendre en considération que les pièces disponibles, ce qui le prive de l'exercice d'un contrôle approfondi. De plus, les méthodologies de contrôle varient en fonction des Cours saisies. Là où la CJUE effectue un contrôle *in concreto* de la compatibilité des traitements envisagés avec son bloc normatif, c'est-à-dire en prenant en compte la réalité du terrain avec les informations disponibles, la CEDH effectue un contrôle *in abstracto* par un simple examen du respect de la législation créant ces traitements avec les conditions posées par son interprétation de la Convention ESDH. Or ces deux mesures dépendent du bon vouloir des parties en cause. Ces dernières peuvent être, à l'instar des contentieux initiés par NOYD, tierces aux débats. D'autres parties peuvent être réticentes à fournir des informations complètes. Fondée sur des sources tierces, l'appréciation de la Cour n'est réalisée que façon parcellaire et matériellement incomplète[336].

Sous-Section 2. L'appréciation du risque de non-respect des droits de l'homme par la CEDH

90 La jurisprudence de la Cour européenne des droits de l'homme porte en matière de risque sur l'application des articles 2 (droit à la vie), 3 (interdiction de la torture) et 8 (droit au respect à la vie privée) de la Convention européenne de sauvegarde des droits de l'homme. Cette jurisprudence oscille entre deux approches pour apprécier un risque d'atteinte aux droits de l'homme.

- La **première** approche mise en avant par L. SEMINARA, similaire à la **démarche qualitative**[337], est dite « **linguo-juridique** ». Pour être qualifiée de risque selon la CEDH, une situation exige **la réalité et l'immédiateté d'un événement dommageable pour démontrer l'existence de ce risque**.

---

331 CEDH, 25 mai 2021, Big Brother c. Royaume-Uni, Req. no58170/13, 62322/14 et 24960/15.

332 CEDH, 25 mai 2021, Centrum för Rattvisa c. Suède, Req. no35252/08.

333 Voir dans ce sens l'avis concurrent du juge PINTO DE ALBURQUEQUE sous l'arrêt Big Brother qui souligne ce décalage entre les visions antérieures et actuelles de la CEDH sur cette question.

334 Voir dans ce sens C.E., 21 avr. 2021, French Data Network, obs. T. DOUVILLE et H. GAUDIN, « *Un arrêt sous le signe de l'exceptionnel* », D. 2021, n°23, p. 1268, qui insistent sur la réserve permise par l'article 4-2°, troisième phrase du Traité sur le Fonctionnement de l'UE. prévoyant une réserve de souveraineté des États membres.

335 Voir dans ce sens l'avis concurrent du juge PINTO DE ALBURQUEQUE (note précédente) qui souligne le refus des États membres implémentant des systèmes d'interception massive de télécommunication de produire l'intégralité des informations relatives aux traitements des télécommunications interceptées. Dans le même sens, voir l'avis dissident de R. CHOPRA dans la transaction conclue entre Facebook et la FTC, https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf (in fine p. 9).

336 Telles que des rapports d'organisations internationales, d'observatoires publics, etc.

337 Distinction opérée par L. SEMINARA, « *Risk Regulation and the European Convention on Human Rights* », European Journal of Risk Regulation, 2016, pp. 733-749.

- La **seconde** approche, davantage proche de la **démarche quantitative**, est dite « **juridico-économique** ». Elle repose sur les critères traditionnels de la gestion des risques, à savoir **la gravité, la probabilité et l'acceptabilité** (A).

Après avoir présenté ces notions, nous exposerons les **différentes catégories de risques** définies par la CEDH (B).

A. L'application de critères classiques par la CEDH : gravité, probabilité et acceptabilité

91 Systématique, l'examen par la CEDH porte tout d'abord sur la gravité d'un risque considéré. Sa détermination permet d'apprécier la recevabilité du recours qui lui est soumis[338]. Contrairement aux dispositions des articles 32 et 35 du RGPD respectivement relatifs à la sécurité des données et à l'analyse d'impact relative à la protection des données, toute situation, même hypothétique, susceptible d'entraîner une violation de la Convention ESDH, est systématiquement caractérisée par la Cour comme une atteinte au droit en cause[339].

La jurisprudence et la doctrine s'accordent sur une hiérarchisation des droits consacrés par la Convention ESDH. Cet ordonnancement entend privilégier les droits contribuant au maintien d'une société démocratique, par exemple le droit à la liberté, à un jugement équitable ou le droit à la vie[340]. De plus, M. le Professeur SUDRE souligne[341] que les droits de l'homme de troisième génération, à savoir les droits collectifs, tels que notamment « *le droit à* » un environnement viable, « *le droit à* » la culture, amoindrissent le corpus juridique des droits individuels en diluant ceux-ci dans des droits collectifs. L'universitaire justifie cette vision en déclarant que « *l'introduction des droits de solidarité dans (…les) droits de l'homme fait perdre à celle-ci toute unité conceptuelle et toute cohérence intellectuelle et menace la notion même de droits de l'homme. (…) Les droits de l'homme deviennent « un ensemble flou » (…remettant en cause) les droits individuels. Le discours sur les « droits de solidarité » autorise un amalgame entre les droits positifs et de simples aspirations qui vise à priver les droits individuels de leur crédibilité, de leur positivité* »[342]. Dans ce contexte, la Cour range la protection des **droits de l'homme dits « secondaires » et de « solidarité »** dans la catégorie des droits en faveur du développement économique. À titre comparatif, et pour fonder la légitimité de leurs décisions, quelques arrêts rendus par la CJUE et des délibérations de la CNIL mettent en avant l'existence d'un « *dommage sociétal* »[343]. Néanmoins, ces arrêts et délibérations empruntent la voie de la sanction administrative, non celle de la réparation du préjudice.

---

338 Article 35, § 3, b), de la Convention ESDH qui pose le principe de l'irrecevabilité de la requête en cas d'absence de préjudice important sauf « *si le respect des droits de l'homme garantis par la Convention et ses protocoles exige un examen de la requête au fond et à condition de ne rejeter pour ce motif aucune affaire qui n'a pas été dûment examinée par un tribunal interne* ».

339 Voir les points 94 et 95 de l'arrêt Centrum : « *La Cour considère que la législation litigieuse sur le (renseignement) a instauré un dispositif de surveillance secrète susceptible de toucher, par exemple, tout usager de téléphonie mobile et d'internet, et ce sans notification. Par ailleurs, comme elle l'a constaté ci-dessus (paragraphe 84), il n'existe aucun recours interne qui permettrait à un demandeur soupçonnant que ses communications ont été interceptées d'obtenir une décision comportant une motivation détaillée. Dans ces circonstances, la Cour estime justifié l'examen in abstracto de la législation pertinente.95. La requérante est donc en droit de se prétendre victime d'une violation de la Convention bien qu'elle ne puisse alléguer à l'appui de sa requête avoir fait l'objet d'une mesure concrète d'interception. Pour les mêmes raisons, la simple existence de la législation incriminée constitue en soi une ingérence dans l'exercice par la requérante de ses droits découlant de l'article 8* ».

340 M. AFROUKH, «*Une hiérarchie des droits fondamentaux ? Le point de vue du droit européen* », RDLF, 2019, chr. 23, http://www.revuedlf.com/cedh/une-hierarchie-entre-droits-fondamentaux-le-point-de-vue-du-droit-europeen/

341 F. SUDRE, « *Droit européen et international des droits de l'homme* », PUF, 14e éd., p. 1013, spéc. p.100 et s..

342 F. SUDRE, p. 108, §65.

343 Voir dans ce sens les arrêts Schrems I et II (déjà cités), CNIL Délib. n°SAN-2019-001 du 21 janv. 2019 et Délib. de la formation restreinte n°SAN-2020-013 du 7 déc. 2020 concernant la société AMAZON EUROPE CORE.

92 La CEDH apprécie la **gravité du préjudice allégué en fonction des mesures prévues par l'État membre concerné pour prévenir la survenance de tout événement qui aurait pour effet la violation d'un droit de l'homme**. La Cour module son appréciation de la gravité en recourant à la notion de « *seuil de gravité* »[344] dont l'évaluation dépend des données de l'espèce, ce qui recouvre les éléments versés aux débats (éléments de preuve, expertises, etc …) et qu'elle a le loisir de se procurer d'office[345]. Ces éléments sont d'autant plus pris en compte lorsque la gravité de l'atteinte aux droits de l'homme se situe sur le territoire d'un État tiers[346]. La Cour prend ici en compte le droit positif en vigueur dans celui-ci, par exemple en cas d'extradition, le droit applicable dans l'État de destination[347].

93 Le critère de la **probabilité** est apprécié concomitamment à celui de la gravité. La méthode d'appréciation de la CEDH dépend du moment de la réalisation de la potentielle atteinte aux droits de l'homme. Lorsque l'événement considéré ne s'est pas encore réalisé, la Cour s'interroge sur la vraisemblance du risque. En cas de survenance de l'événement, elle écarte les critères de probabilité pour apprécier l'ensemble des mesures prises par l'État pour prévenir sa réalisation. À ce titre, MM. DANNER et SCHULMAN soulignent que **la Cour retient facilement la condition de vraisemblance**[348]. Ils estiment que « *cela conduit à une tolérance au risque du public post-accident bien inférieure à celle qui aurait été impliquée par la réticence antérieure à payer le coût nécessaire pour atténuer la probabilité ou les conséquences du risque* ». À cette fin, la CEDH apprécie *in concreto* les informations disponibles pour déterminer le degré de probabilité de la réalisation d'un événement grave. Ces informations proviennent de rapports relatifs au respect des droits de l'homme par un État qui ont été réalisés par des organisations internationales ou gouvernementales. En sus, les garanties diplomatiques fournies par les États, c'est-à-dire les engagements fournis par les États entre eux, peuvent également prendre en compte l'appréciation des probabilités d'une éventuelle violation. Des informations documentaires peuvent être puisées dans des rapports objectifs en lien avec l'affaire en cause. Par exemple, la CEDH a apprécié l'absence de mesures préventives suffisantes dans le cadre du suicide d'une personne, après plusieurs tentatives connues de tous, se trouvant sous la responsabilité directe de l'État[349].

Contrairement à l'approche de la CJUE en matière de données personnelles, le requérant auprès de la CEDH doit participer activement à l'élaboration de la conviction de la Cour. L'objectif ici ce n'est pas de démontrer la probabilité de la violation alléguée des droits de l'homme mais de produire une preuve crédible et substantielle de la survenance d'un risque[350].

94 **L'acceptabilité du risque** correspond aux situations dans lesquelles l'État ne prend pas en considération certains risques sans pour autant enfreindre la Convention ESDH. De jurisprudence constante, la Cour estime qu'il n'existe pas une obligation positive à la charge d'un État à prévenir

---

344 Voir dans ce sens pour l'article 8 Convention ESDH, CEDH, 10 février 2011, Dubetska et autres c. Ukraine, §105 ; CEDH, 09 juin 2005, Fadeïeva c. Russie, §§ 68 et 69.

345 CEDH, 6 mars 2001, Hilal c. Royaume-Uni, §60 repris dans CEDH, Grde Ch., 23 mars 2016, F.G. c. Suède, §112.

346 Voir CEDH, 07 juil. 1989, Soering c. Royaume-Uni.

347 Pour une violation relative à l'article 2 (droit à la vie) et à l'article 3 (interdiction de la torture), voir CEDH, 2 mars 2010, Al-Saadoon et Mufdhi c. Royaume-Uni, CEDH, 19 avr. 2018, A.S. c. France, §60, pour une méconnaissance de l'article 6 de la Convention ESDH, CEDH, 4 fév. 2005, Mamatkoulov et Askarov c. Turquie, §91.

348 C. DANNER et P. SCHULMAN, « *Rethinking Risk Assessment for Public Utility Safety Regulation* », Risk Analysis, 2019, pp. 1044-1059, p. 1048.

349 CEDH, 16 oct. 2008, Renolde c. France, §§ 87-89. Pour un comportement instable ou alarmant (CEDH, 07 juin 2005, Kilinç et autres c. Turquie, §45) ou encore la fourniture du dossier médical (CEDH, 24 avr. 2014, Perevedentsevy c. Russie, §98).

350 CEDH, 2 déc. 2002, KRS c. R.U., où la Cour exige la fourniture d'une preuve de la violation de la Convention ESDH par l'État destinataire, en l'espèce le Royaume-Uni.

l'ensemble des risques potentiels. En effet, **la prévention des risques « *ne doit pas être interprétée de manière à imposer aux autorités un fardeau insupportable ou excessif* »**, comme l'indique le refus d'un État d'être contraint à autoriser la diffusion audiovisuelle d'une publicité critiquant de façon véhémente les produits issus de l'abattage animal[351]. La Cour estime que l'État, disposant de moyens limités, doit fixer des **priorités**[352]. **L'imprévisibilité du comportement humain**[353] empêche l'anticipation de toutes les atteintes faites aux droits protégés par la Convention ESDH[354]. En outre, l'acceptabilité du risque par les requérants est présumée lorsque ceux-ci se placent volontairement dans une situation dangereuse en pleine connaissance du risque. Une telle situation est interprétée comme une tolérance de la part de la Cour pour exonérer l'État membre de sa responsabilité de ne pas avoir pris les mesures nécessaires à prévenir le dommage subi. Cette tolérance est limitée par la prise en compte de **l'information du risque délivrée à l'individu**[355] **et au regard de ses capacités, notamment financières, pour y faire face**[356]. Cette approche peut être transposée dans le cadre des données personnelles. La CNIL fait de nombreuses fois grief aux responsables du traitement de ne pas avoir suffisamment informé les personnes concernées des risques qu'elles sont susceptibles d'encourir lors de la mise en œuvre des traitements. Enfin, la CEDH souligne que l'article 2 de la Convention européenne des droits de l'homme relatif au droit à la vie « *ne doit pas être indûment altérée par des interprétations paternalistes, sachant que la notion d'autonomie personnelle est un principe important sous-tendant les garanties de la Convention, principalement celles qui concernent la vie privée* »[357]. Dans un arrêt relatif à une mort liée à des courses de voitures non autorisées, l'individu est réputé avoir accepté les conséquences de ses actes et avoir pleinement conscience du risque encouru.

Après avoir étudié les différents critères retenus par la CEDH pour définir le risque, il convient de présenter les différentes conceptions retenues par cette même Cour.

B. La conceptualisation de la typologie des risques par la CEDH

95 Dans sa jurisprudence, la Cour alterne entre les termes de « *risque réel* »[358], « *risque réel et immédiat* »[359], « *risque sérieux* », « *risque élevé* », « *risque important* »[360] ou de « *risque certain et imminent* »[361]. Cette variété se retrouve également dans les textes en anglais avec les notions de « *real risk* », « *real and immediate risk* », « *serious risk* », « *high risk* » et « *significant risk* ». Un auteur relève, qu'au sein d'une même décision, « *risk* » est traduit, en français, à la fois par les noms communs « *risque* » et « *danger* »[362]. Ainsi, la confusion entre un « *danger* », situation inhérente à certaines choses ou situations, et un « *risque* », danger dépendant de facteurs contextuels et

351 CEDH, Gr. Ch., 30 juin 2009, Verein gegen Tierfabrieken Schweiz (VgT) c. Suisse (No. 2), §81.

352 CEDH, 2 mars 2017, Talpis c. Italie, §101.

353 CEDH, Gr. Ch., 31 janv. 2019, Fernandes de Oliveira c. Portugal; CEDH, 3 nov. 2015, Olszewscy c. Pologne, §59.

354 C. HILSON, *Risk and the European Convention on Human Rights*, Cambridge Yearbook of Legal Studies, 2009, pp. 353-375.

355 CEDH, Gr. Ch., 30 nov. 2004, Öneryildiz c. Turquie, §105.

356 CEDH, 8 juil. 2003, Hatton et autres c. Royaume-Uni, §127.

357 CEDH, 26 fév. 2015, Prilutskiy c. Ukraine, §32.

358 CEDH, 28 oct. 1998, Osman c. Royaume-Uni, §116.

359 CEDH, 3 avr. 2001, Keenan, §93.

360 CEDH, 13 sept. 2016, A.Ş. c. Turquie, §49 ; CEDH, Grande ch., 24 mars 2011, Giuliani et Gaggio c. Italie, §248.

361 CEDH, 23 fév. 2012, Civek c. Turquie ; CEDH, 10 oct. 2000, Akkoc c. Turquie, §94.

362 CEDH, 31 janv. 2019, Rooman c. Belgique, §145.

comportementaux, floute davantage la qualification du risque opérée par la Cour européenne[363]. Le recours à ces différents adjectifs correspond à des situations dans lesquelles les obligations des États parties à la Convention ESDH varient.

96 Lorsque la Cour se réfère au **risque « simple »**, elle vise les actions étatiques ayant théoriquement conduit à une concertation préalable anticipant les conséquences des risques étudiés. Le risque simple est associé aux contentieux relevant principalement de **l'extradition**[364] ou de **mesure restrictive de liberté d'une personne**[365].

L'utilisation des adjectifs **« sérieux »**, **« important »**, **« élevé »** et **« certain »** renvoie à une **obligation de l'État à prévenir les violations découlant de ses propres décisions**[366]. Le recours à ces qualificatifs invite donc les États à prendre les mesures nécessaires pour éviter une atteinte à un droit fondamental[367].

97 Le risque **« réel et immédiat »** est, quant à lui, constitué dès lors qu'un État n'a pas pris de mesure adéquate pour prévenir la réalisation d'un risque réel et immédiat à l'encontre d'une personne identifiée[368]. Ce type d'hypothèse correspond à **un dommage infligé par un tiers mais qui aurait dû être prévenu par l'État**. Ainsi, dans l'arrêt Kavaklioğlu, le risque réel et immédiat est constitué par l'absence de mise en place de conditions pénitentiaires prévenant les violences physiques[369]. La Cour définit également les adjectifs « *réel* » et « *immédiat* » : le premier adjectif suggère une **vraisemblance certaine** dans la réalisation du dommage[370] ; le second renvoie à **l'imminence de la transformation du risque en dommage**[371] mais sans préjuger de la gravité de l'atteinte. La qualification ne diffère pas lorsque le risque réel et immédiat vise une personne individuelle, un groupe de personnes ou la société en général. La Cour n'examine alors pas la réalité et l'immédiateté du risque, mais se concentre davantage sur les mesures préventives de réduction du risque.

---

363 Dans ce sens voir F. BOUHON, « *Le risque et la Cour européenne des droits de l'homme – Premières esquisses d'une réflexion sur le risque à l'aune des droits fondamentaux* », 2019/46 http://www.revuedlf.com/droit-fondamentaux/le-risque-et-la-cour-europeenne-des-droits-de-lhomme-premieres-esquisses-dune-reflexion-sur-le-risque-a-laune-des-droits-fondamentaux/#_ftn5, dans le même sens voir H. BELVEZE, « *Lignes directrices pour l'application du principe de précaution* », NSS 9, p. 71-77, spéc. p. 71, https://www.nss-journal.org/articles/nss/pdf/1999/03/nss19990703p71.pdf.

364 CEDH, 14 fév. 2017, Allanazarova c. Russie, §99.

365 Pour la réincarcération d'un individu et le suivi psychologique afférant (CEDH, 22 déc. 2005, Balyemez c. Turquie, §96) ou son internement (CEDH, 31 mai 2016, Comoraşu c. Roumanie, §70) sans possibilité de voie de recours.

366 Voir dans ce sens l'extradition d'étranger (CEDH, 31 mai 2017, Comoraşu c. Roumanie, 31 mai 2016, §70) ou l'incarcération d'un ressortissant serbe dans une prison bosniaque (CEDH, 27 mai 2008, Rodić et autres c. Bosnie-Herzégovine, §§ 70 et 72) .

367 Voir par exemple le refus de l'invocation de l'article 8 pour un prisonnier mis en isolement en attente de son procès afin d'éviter la connivence avec d'autres accusés (CEDH, 6 oct. 2016, W.P. c. Allemagne, §62 ; CEDH, 2 juin 2016 Petschulies c. Allemagne, §80).

368 CEDH, 4 oct. 2016, Cevrioğlu c. Turquie, §50.

369 CEDH, 6 oct. 2015, Kavaklioğlu et autres c. Turquie, §174.

370 Dans ce sens voir CEDH, 09 juin 1998, L.C.B. c. Royaume-Uni qui rappelle l'exigence d'un lien de causalité entre le risque et le dommage (§38) avant de l'exclure au nom de l'état de la science (§39).

371 L'adjectif « *imminent* » est utilisé à titre subsidiaire dans les arrêts relatifs aux risques pour le droit à la vie dans un contexte pénitentiaire CEDH, 07 fév. 2019, Patsaki c. Grèce, §90 ; CEDH, 14 mars 2002, Paul et Audrey Edwards c. Royaume-Uni, §57 ; CEDH, 03 avr. 2001, Keenan c. Royaume, §93.

Section 2. Les modalités jurisprudentielles d'atténuation des risques

Les mesures d'atténuation des risques sont appréhendées par la CJUE et la CEDH sous le vocable des « *mesures de prévention* ». Ces dernières recourent au principe de proportionnalité pour apprécier soit la nécessité de la mesure d'interdiction de distribution d'un produit prise sur le fondement du principe de précaution au regard des données scientifiques disponibles (§1), soit la suffisance des mesures prises pour prévenir un dommage lié à une atteinte aux droits de l'homme (Sous-Section 2, page 108).

Sous-Section 1. L'approche de la CJUE relative à l'atténuation des risques liée à la distribution d'un produit

98 La CJUE ne définit pas ce qu'est une mesure adéquate pour réduire la réalisation du risque lié à la distribution d'un produit. Pour apprécier la pertinence de l'interdiction de distribution, outre les avis scientifiques sollicités par l'autorité compétente pour déterminer sa décision[372], elle actionne le principe de proportionnalité. Cette appréciation met en balance l'avantage sociétal résultant de l'utilisation du produit et les différentes atteintes générées par sa mise sur le marché et son utilisation par les usagers. Ainsi, **les « *préoccupations, considérations éthiques ou morales ou autres facteurs légitimes et principe de précaution* »[373] doivent être pris en compte**.

En la matière, la discrétion réglementaire est de mise. Dans les décisions de gestions des risques ayant un impact direct sur la santé des consommateurs[374], la CJUE a confirmé la compétence des autorités nationales pour apprécier la nécessité de prendre en considération certains facteurs locaux pour justifier l'interdiction de la présence de certains éléments, composés et produits, en l'espèce l'utilisation de farine de viande et d'os de mammifères pour nourrir les bovins. Ces facteurs locaux sont d'une importance telle qu'ils s'inscrivent dans la mise en œuvre des politiques d'ordre public menées par l'autorité, ainsi par exemple la Belgique qui refuse la vente de pain comprenant plus de 2 % de sel[375] ou encore l'Allemagne avec la bière sans additif[376]. L'appréciation de la proportionnalité, se positionnant entre l'atteinte à la santé des consommateurs /de l'environnement et les intérêts économiques en jeu, entraîne systématiquement une exigence de protection « *élevée* ». La volonté de préserver la vie humaine et l'environnement influence l'appréciation du risque rendue par les autorités évaluatrices[377].

99 L'analyse de la perte économique est réalisée *in concreto*[378]. Dans l'arrêt Pfizer[379], la Cour analyse la nécessité de l'administration d'un produit, en l'espèce un vaccin pour les porcs, au regard de l'analyse coût-bénéfice d'une telle vaccination dont les effets sont inconnus sur la santé humaine. Elle prend également en considération l'existence et la disponibilité des méthodes alternatives aux traitements traditionnels aux antibiotiques qui pourraient s'y substituer. Enfin, elle examine le coût et la durée de la décision de suspension de l'autorisation de distribution. Elle en conclut que, bien que **d'importantes conséquences économiques existent pour le producteur, ces**

---

372 G. SKOGSTAD, « *The WTO and Food Safety Regulatory Policy Innovation in the European Union* », in 39 Journal of Common Market Studies 485, 490 (2001), « *les avis scientifiques font autorité, mais pas exclusivement* ».

373 TPICE, 26 fév. 2003, T-344/00 et T-345/00, CEVA, §86.

374 CJCE, Ord, 15 déc. 1996, C-180/96, R.U. c. Commission, §89.

375 CJCE, 14 juil. 1994, C-17/93, Van der Velt.

376 CJCE, 12 mars 1987, C-178/84, Commission c. Allemagne.

377 CJCE, 5 mai 1998, C-157/96 et C-180/96, National Farmer's Union.

378 TPICE, 11 sep. 2002, T-13/99, Pfizer c. Commission, §456.

379 Id.

conséquences économiques ne sauraient entrer en compte face à l'intérêt supérieur de la santé publique[380].

100 L'application du principe de précaution est susceptible de constituer une restriction à la libre circulation des biens. En tant que vecteur de potentielles restrictions, son application doit être provisoire. Par conséquent, l'appréciation doit être revue dans un délai raisonnable en fonction des informations complémentaires qui pourraient être fournies. Ici, l'avis scientifique, caractérisant une preuve imparfaite, doit être qualifié : il ne doit pas être qu'une simple « *considération purement académique ou hypothétique* » mais constituer « *une évaluation du risque compréhensive basée sur les informations scientifiques les plus récentes* »[381]. Ainsi la démonstration d'une preuve scientifique contraire à l'avis rendu par les experts de l'autorité nationale ou compétente offre la possibilité pour l'acteur économique de se soustraire à l'interdiction formelle de la distribution de son produit.

Néanmoins, l'arrêt Alpharma réduit le seuil d'appréciation de risque pour établir une précaution *a priori*[382] laissant une large marge d'appréciation à l'autorité nationale compétente. Ainsi, « sauf à *vider le principe de précaution de son effet utile, l'impossibilité de réaliser une évaluation scientifique complète des risques ne saurait empêcher l'autorité publique compétente de prendre des mesures préventives, si nécessaire à très brève échéance, lorsque de telles mesures apparaissent indispensables eu égard au niveau de risque pour la santé humaine déterminé par cette autorité comme étant inacceptable pour la société* »[383].

En matière de données personnelles, hormis certaines hypothèses balisées, l'AIPD n'est qu'une preuve documentée par le responsable du traitement pour démonter le respect de la conformité du traitement aux obligations posées par le RGPD. En dehors des traitements régaliens soumis à une autorisation préalable de la CNIL, aucune référence doctrinale et d'actes juridictionnels ne fait état d'une soumission d'une AIPD à une autorité de contrôle préalable pour des risques résiduels, ni même d'une analyse de ceux-ci par un contrôle juridictionnel. Tant le contenu que la notation des risques restent soumis à la discrétion du responsable du traitement. Cette discrétion doit prendre en compte l'état des connaissances techniques et scientifiques[384]. En d'autres termes, l'exigence de conformité du traitement de données personnelles n'est, par essence, pas influencée par d'autres considérations que celle de la licéité de son fondement. En effet, l'opportunité d'un traitement respectueux du RGPD, néanmoins intrusif, sera davantage régulée par le marché que par la loi.

Sous-Section 2. La jurisprudence de la CEDH relatives aux mesures de protection devant être adoptées par les États

101 La jurisprudence de la CEDH fournit plusieurs éléments concernant les mesures de prévention à adopter par les États. Rappelons que cette jurisprudence sanctionne les États défaillants dans l'exercice de leurs fonctions régaliennes, mais également législatives ou judiciaires, au titre du règlement de litiges entre personnes de droit privé. Ces mesures préventives varient en fonction du rôle de l'État dans la réalisation potentielle du risque et l'appréciation du risque en cause.

Lorsque l'État reste passif et que le risque porte sur un droit contribuant au maintien d'une société démocratique[385], **les autorités publiques sont tenues de prendre des mesures « adaptées au**

---

380 Cour AELE, 05 avr. 2001, Aff. E-3/00, EFTA Surveillance Authority c. Norvège, §§ 27 et 28. et CJUE, 28 janv. 2010, C-333/08, Commission/France, §89.

381 Cour AELE, Efta Surveillance Authority c. Norvège, note supra.

382 TPICE, 11 sept. 2002, Aff. T-70/99, Alpharma v Conseil, §173.

383 Id. 174.

384 Voir supra §85, page 97.

385 Voir supra §91, page 103.

niveau de risque », en fournissant par exemple les informations disponibles sur la création d'une usine chimique voisine à un village[386]. Cette jurisprudence oblige les États à anticiper les risques lorsque la vie humaine est en jeu[387]. D'abord limitée à l'environnement, elle a été étendue aux catastrophes naturelles provoquées par des accidents industriels[388] et aux événements de la vie courante, comme l'absence de mesures restreignant efficacement la circulation d'armes à feu[389].

102 Ces obligations positives à la charge des États se subdivisent en deux catégories. D'une part, **l'État doit instaurer un cadre juridique assurant la protection de la vie et de la santé des habitants contre des « activités à caractère industriel, dangereuses par nature, telles que l'exploitation de sites de stockage de déchets »**[390]. Cette protection juridique prend en compte les modalités d'exploitation d'une déchetterie comme dans l'affaire Oneryildiz portant sur une explosion de méthane entraînant la mort de la famille du plaignant, ainsi que sa situation géographique au regard du lieu de situation des habitations[391]. La CEDH impose à l'État **l'obligation de prévenir efficacement** des dommages à l'environnement et à la vie humaine[392]. Cette obligation est fondée sur **le droit à la vie**[393] **et au respect de la vie privée**[394]. D'autre part, l'État doit prendre « *préventivement des mesures d'ordre pratique pour protéger l'individu dont la vie est menacée* »[395], comme le fait de procéder à un suivi psychologique pour un prisonnier suicidaire.

103 La Cour considère que le « **risque réel et immédiat** » est constitué dans des situations où le dommage a été réalisé par des tiers et que l'État n'a pas tenté de réduire le risque de survenance de ce dommage. L'exemple typique est la victime non protégée par les forces de l'ordre, nonobstant la menace constituée par des tiers identifiés[396]. **Le défaut de mesures préventives pour un risque réel et immédiat est également constaté dans des hypothèses où un individu se trouve sous la responsabilité directe de l'État**, comme le défaut de soutien psychologique qui aurait dû être apporté à un soldat identifié comme suicidaire[397]. Dans ces deux cas, l'État manque à ses obligations en raison de son inaction alors que la réalité du risque était constituée.

Les solutions dégagées par les arrêts récents de la Cour européenne des droits de l'homme[398] questionnent la façon dont les risques découlant d'une interception massive des données personnelles doivent être pris en compte par un État. Dans les arrêts Centrum et Big Brother relatifs aux interceptions massives et indifférenciées de communications à des fins de sécurité publique, la Cour relève un risque lié à un « *traitement des données à caractère personnel et à l'intégrité personnelle* » tout en se concentrant particulièrement sur le second risque[399]. Ainsi, la Cour assimile le profilage d'une personne à partir de ses données personnelles comme une atteinte à son intégrité physique. En outre, elle reconnaît l'existence d'un risque d'arbitraire des services

386 De jurisprudence constante CEDH, Grande chambre, 19 fév. 1998, Guerra et autres c. Italie.

387 CEDH, Grande chambre, 30 nov. 2004, Grd. Ch., Öneryildiz c. Turquie, §90.

388 CEDH, 20 mars 2008, Boudaïeva c. Russie, req. n°15339/02, 21166/02, 20058/02, 11673/02 et 15343/02, §132.

389 CEDH, 1er déc. 2016, Gerasimenko et autres c. Russie, req. n°5821/10 et 65523/12, §94 et CEDH, 19 avr. 2012, Sašo Gorgiev c. « L'Ex-République yougoslave de Macédoine », req. n°49382/06, §42.

390 CEDH, 30 nov. 2004, Oneryildiz c/ Turquie, req. n°48939/99, §71.

391 CEDH, 20 mars 2008, Budaïeva et a. c/ Russie, note supra.

392 CEDH, 27 janv. 2009, Tatar c/ Roumanie, req. n°67021/01, §88.

393 CEDH, Oneryildiz c/ Turquie, note supra, §90

394 CEDH, 9 déc. 1994, Lopez Ostra c/ Espagne, req. n°16798/90.

395 CEDH, 20 octobre 1998, Osman c/ Royaume-Uni, req. n°23452/94 §115.

396 CEDH, Osman c. Royaume-Uni, note précédente, §116.

397 CEDH, 1er juin 2017, Malik Babayev c. Azerbaidjan, §67.

398 CEDH, 25 mai 2021, Centrum för Rattvisa c. Suède, et CEDH, 25 mai 2021, Big Brother c. Royaume-Uni.

399 CEDH, Centrum, spéc. §54, voir références note précédente.

de renseignement en ce qui concerne la personne / le groupe de personnes à surveiller. Bien que retenant l'existence d'un risque avéré pour les droits des citoyens, les mesures d'atténuation et de contrôle proposées par les États membres sont, par principe, validées par la Cour Européenne des Droits de l'Homme dès lors que des procédures de contrôle préalables, par des autorités indépendantes, et postérieures, entre autres par la personne concernée, sont instituées.

	CJUE		CEDH	
	Principe de précaution	**Droits des données personnelles**	**Droits prévus par la CEDH**	**Données personnelles**
Domaine applicable	Protection des consommateurs, de l'environnement et la sécurité alimentaire	- Conformité du traitement - Exercice des droits par les personnes concernées - Prévention d'une utilisation illicite des données personnelles par des tiers non autorisés	Prioritairement : - droit à la vie - jugement équitable - société démocratique	- Surveillance généralisée - Droit au respect à la vie privée - Droit à la non discrimination
Analyste	- Autorité nationale compétente - Commission européenne	Responsable du traitement (principe de responsabilité)	États membres et participation active du demandeur	
Vraisemblance	Oui, sous le terme d'incertitude apprécié à partir des évaluations scientifiques	Voir partie 1 et 2	Systématiquement admise par une appréciation *in concreto* des informations disponibles pour déterminer le degré de probabilité de la réalisation d'un événement grave	
Gravité	L'évaluation scientifique des risques est communément définie, tant au niveau international qu'au niveau de l'Union européenne, comme un processus scientifique qui consiste à identifier et à caractériser un danger, à évaluer l'exposition et à caractériser le risque		La gravité du préjudice allégué est appréciée en fonction des mesures prévues par l'État membre concerné pour prévenir la survenance de tout événement qui aurait pour effet la violation d'un droit de l'homme	Respect des procédures d'information et d'opposition aux traitement de données personnelles

suite des caractéristiques page suivante

Correspondance avec les méthodologies	← PRIAM →
	← NIST →
	CNIL
	BSI

Tableau 14. Récapitulatif de l'appréciation des risques par la CJUE et par la CEDH et correspondance avec les méthodologies PRIAM, NIST, CNIL et BSI

	CJUE		CEDH	
	Principe de précaution	**Droits des données personnelles**	**Droits prévus par la CEDH**	**Données personnelles**

suite du tableau de la page précédente

Charge de la preuve	Demandeur	Responsable du traitement	L'État partie mis en accusation
Preuve	- État des connaissances (toutes les publications scientifiques sur ce sujet) - Assistance par des services d'organismes scientifiques internationaux, de l'Union européenne et nationaux	État des connaissances (toutes les publications scientifiques sur ce sujet) et l'état de l'art (mesure techniques et organisationnelles appropriées)	Les éléments versés aux débats (éléments de preuve, expertises, etc.), rapports relatifs au respect des droits de l'homme par l'État défendeur réalisés par des organisations internationales ou gouvernementales et pouvoir du juge de demander la production de pièces complémentaires
Force probante	Faible (l'état des connaissances peut être réfuté par une information récente)	Importante (la documentation réalisée par le responsable du traitement jouit d'une force probante)	Faible (appréciation du juge)
Source d'appréciation	Dynamique permettant une levée du principe de précaution en cas de preuve scientifique contraire	- Certification et standard - Documentation par le responsable du traitement - Examen *prima facie* par les autorités nationales de contrôle (CNIL)	Déclarations des États
Prise en compte de l'élément économique	Non		Oui (approche pragmatique de la Cour du risque)
Prise en compte de l'élément social	Oui (préoccupations, considérations éthiques ou morales ou autres facteurs légitimes et principe de précaution)	Non	Oui (approche politique de la Cour)
Correspondance avec les méthodologies	← PRIAM →		
	← NIST →		
		CNIL	
		BSI	

Chapitre 2 L'appréciation de la violation des données personnelles par le juge judiciaire

Chapitre 2

Chapitre 2 L'appréciation de la violation des données personnelles par le juge judiciaire

Les parties précédentes de ce rapport mentionnent des méthodologies intégrant la prise en compte de nouveaux risques engendrés par un traitement de données personnelles. Sur le plan juridique, ceux-ci peuvent être subdivisés en deux catégories : des risques immatériels propres à la personne concernée (ex : le dommage d'anxiété) et des risques propres au responsable du traitement (ex : les dommages financiers). La réparation de ces dommages s'effectue, conformément à l'article 80 du RGPD, principalement par la voie judiciaire. Cette voie ayant été explorée par le droit anglais et le droit étasunien, nous examinerons leurs jurisprudences, que nous comparerons avec les solutions découlant du droit des contrats et du droit de la responsabilité civile français.

Dans un premier temps, la notion de « *dommage* » au sens civiliste sera examinée pour souligner la difficile application du droit des contrats dans le cadre de l'obligation d'information prévue par le RGPD pour y préférer le droit de la responsabilité civile. À l'instar des droits anglophones, l'exigence de l'immédiateté du dommage est requise pour que l'atteinte aux droits et libertés de la personne concernée soit réparée. En effet, le droit français ne reconnaît pas la responsabilité du fait des choses immatérielles : un dommage physique, par exemple, ne peut être produit que par une chose purement matérielle. Si une telle vision neutralise l'analyse de certains risques telle que promue par certaines méthodologies, comme celle de la CNIL, une réserve interprétative peut néanmoins être formulée. Le RGPD octroie à la CJUE un pouvoir discrétionnaire d'interprétation de la notion de dommage. Une évolution jurisprudentielle reste donc possible.

Pour leur part, les droits étasunien et anglais reconnaissent un droit à la réparation en cas de dommage lié à une atteinte aux données personnelles. Une exigence de réalité et d'immédiateté du dommage avec le fait générateur est requise. C'est au niveau organique que ces deux droits divergent. En effet, l'absence d'un droit à la protection des données personnelles généraliste aux États-Unis d'Amérique invite le juge à employer les « *torts* », offrant des solutions alternatives à la simple réparation pécuniaire. Leur accueil diffère en fonction des différentes Cours d'appel fédérales. Le droit anglais recourt également au *tort*, et plus précisément au *tort* de « *misuse of private information* », pour faire droit à des réparation en cas de violation de données personnelles sur le fondement du droit au respect de la vie privée. Cependant, ce *tort* limite la réparation aux seuls dommages subis, excluant les dommages et intérêts punitifs.

Notre approche comparatiste s'intéressera, ensuite, aux modalités de calcul des dommages et intérêts. Les autorités nationales de contrôle étant soumises à la jurisprudence européenne en

matière de droit à un jugement équitable, l'adéquation de ce droit avec les lignes directrices sur l'application et la fixation des amendes administratives du Comité Européen de la Protection des Données seront étudiées pour déterminer les grandes lignes des méthodes de calcul en cas de violation au droit des données personnelles.

Enfin, les questions de la recevabilité et de la réparation d'un dommage collectif seront examinées. La transposition de l'article 80 du RGPD en droit français questionne de nombreux points de procédures. Notamment, l'éligibilité d'une action collective ou d'une action de groupe interroge respectivement l'étendue du mandat accordé à une association pour obtenir réparation de dommages moraux subis par ses mandants ou l'exigence d'un dommage équivalent pour constituer une action de groupe. Cette dernière problématique a longtemps servi de barrage procédural en droit anglo-saxon avant d'être assoupli et de faciliter l'accès à la justice.

104 Les méthodologies BSI et NIST invitent le responsable du traitement à prendre en compte le risque financier lié à une sanction pécuniaire en cas de litige. Cette sanction pécuniaire découle de la reconnaissance de la responsabilité judiciaire du responsable du traitement, telle que prévue par le chapitre 7 du RGPD. À titre liminaire, nous exposerons les questions purement procédurales découlant de la lettre du RGPD. Ainsi son considérant 147 dispose que « *lorsque le présent règlement prévoit des règles de compétence spécifiques, notamment en ce qui concerne les procédures relatives aux recours juridictionnels, y compris ceux qui visent à obtenir réparation, contre un responsable du traitement ou un sous-traitant, les règles de compétence générales, telles que celles prévues dans le règlement (UE) n°1215/2012, ne devraient pas porter préjudice à l'application de telles règles juridictionnelles spécifiques* ». Ce considérant fait écho aux dispositions de l'article 81 du RGPD ouvrant à la personne concernée le droit d'attraire le responsable du traitement devant une juridiction et renvoie au règlement n°1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale[400]. Il suggère que seuls les contentieux civils seraient concernés par cette disposition. Cette supposition est confirmée par l'article 82 du RGPD qui prévoit que « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi* ». Cette disposition est applicable dans le cadre d'un contentieux

400 Règlement (CE) n°1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, JOUE L 351, 20.12.2012, p. 1–32.

judiciaire prenant en compte des dommages matériel ou moral générés par une utilisation illicite ou malencontreuse des données personnelles par le responsable du traitement. Ainsi dans l'hypothèse d'une violation de données personnelles, la disponibilité incontrôlée des données personnelles est susceptible de créer des dommages dans plusieurs États membres. En fonction de la nature du lien établi entre le responsable du traitement et la personne concernée, la loi applicable au litige et la juridiction compétente pour le connaître varient.

105 Si ce lien est qualifié de relation contractuelle, le juge compétent est naturellement celui du contrat, et *a fortiori* est invocable le droit de la consommation. Le règlement n°1215/2012 offre à la victime le choix entre le juge du lieu de domicile de la partie professionnelle ou celui de son propre lieu de domicile[401]. La question de la loi applicable, en l'occurrence, se définit à partir de l'article 6 du règlement Rome 1[402] entraînant l'application de la loi du pays du consommateur. Il est important de noter que la CJUE a sanctionné toute clause attributive de juridiction imposée par le professionnel au consommateur[403]. La Cour estime en effet qu'est abusive la clause désignant « *la loi de l'État membre du siège de ce professionnel régit le contrat* » lorsqu'elle induit ce consommateur en erreur en lui donnant l'impression que seule la loi de cet État membre s'applique au contrat, sans l'informer au préalable du bénéfice de la protection assurée par les dispositions impératives du droit applicable en l'absence de cette clause[404]. Néanmoins, la jurisprudence européenne a atténué cette solution dans l'hypothèse d'une action de groupe comprenant une pluralité de demandeurs de nationalités différentes[405]. Ici, la CJUE estime que le mandat, correspond à la qualité à agir, accordé par un consommateur étranger[406] au mandataire d'une action de groupe devant une juridiction nationale d'un autre État membre que celui de son domicile n'offre pas, en matière de protection des données personnelles, « *les droits qu'il tire (personnellement) d'un contrat avec le défendeur* »[407]. Par cette décision, la CJUE empêche donc la création d'actions de groupe intra-européen et restreint l'interprétation de l'article 82 du RGPD aux demandeurs « *consommateurs* » à leur seul droit national.

106 Les relations délictuelles sont elles aussi régies par le règlement n°1215/2012 concernant la compétence judiciaire, ainsi que le règlement (CE) n°864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles[408]. La multiplication des lieux de dommages facilitée par le caractère immatériel des données personnelles est susceptible d'entraîner une cascade de contentieux. En effet les données personnelles peuvent être à la fois rattachées à la qualification de droit de la personnalité ou de droit patrimonial. Dans ces deux hypothèses, la jurisprudence européenne en matière de responsabilité délictuelle, initiée par l'arrêt Mines de Potasse d'Alsace de 1976[409] et étendue en droit de la personnalité par l'arrêt Fiona Shevill de 1995[410], offre au demandeur une règle de compétence en mosaïque permettant d'attraire le défendeur :

---

401 Art. 18 du règlement n°1215/2012 : « *L'action intentée par un consommateur contre l'autre partie au contrat peut être portée soit devant les juridictions de l'État membre sur le territoire duquel est domiciliée cette partie, soit, quel que soit le domicile de l'autre partie, devant la juridiction du lieu où le consommateur est domicilié* ».

402 Règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles, dit Rome I, JOCE L 177, 4.7.2008, p. 6–16.

403 CJUE, 28 juillet 2018, C-191/15, Verein für Konsumenteninformation c. Amazon EU Sarl.

404 CJUE, Verein für Konsumenteninformation, précité, §71.

405 CJUE, 25 janv. 2018, C-498/16, M. SCHREMS c. Facebook.

406 CJUE, Schrems II, précité, §38, c'est-à-dire une personne utilisant des services à des fins non professionnelles.

407 CJUE, Schrems II, précité, §47.

408 Règlement (CE) n°864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles, dit Rome II, JOCE L 199, 31.7.2007, p. 40–49.

409 CJCE, 30 nov. 1976, C-21-76, Handelskwekerij G. J. Bier BV contre Mines de potasse d'Alsace SA.

410 CJCE, 7 mars 1995, C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL.

- soit devant la juridiction du lieu du fait générateur (à savoir le lieu où les actes ont été commis) pour obtenir la réparation intégrale du dommage subi dans tous les États membres,
- soit devant le tribunal de chacun des lieux de matérialisation du dommage, afin d'obtenir réparation du seul dommage subi localement,
- soit devant le juge du « *centre des intérêts* » de la victime[411].

La CJUE éclaircit, dans son arrêt Bolagsupplysningen[412] de 2017, les règles de compétence juridictionnelle en matière de données personnelles en fonction des demandes propres à l'espèce. Suivant la solution développée par l'arrêt Google-Spain[413], le juge compétent pour toutes les demandes relatives à l'exercice des droits des personnes concernées est celui de l'État membre où est domicilié l'établissement du responsable de traitement. La question du juge compétent pour les dommages et intérêts relatifs à une collecte ou utilisation non autorisée de données personnelles ou à des fins non autorisées relève de la jurisprudence classique relative aux dommages immatériels. Il est traditionnellement admis que la preuve du dommage subi dépend de la loi procédurale, c'est-à-dire la loi du for du juge compétent. En d'autres termes, la juridiction civile compétente soumet les parties à son droit procédural local pour toutes les questions relatives à la preuve ainsi qu'à la fixation des dommages et intérêts.

107 Ces derniers sont consacrés par l'article 82 du RGPD portant sur le droit à la réparation, lequel dispose que « *Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi* ». Le considérant 145 précise cette stipulation en déclarant que « *le responsable du traitement ou le sous-traitant devrait réparer tout dommage qu'une personne peut subir du fait d'un traitement effectué en violation du présent règlement* ». En d'autres termes, la personne concernée peut engager la responsabilité civile du responsable du traitement dès lors qu'est prouvé et chiffré le dommage (le préjudice) lié à une absence de conformité du traitement de ses données personnelles. De surcroît, le même considérant 145 rappelle le pouvoir d'interprétation de la CJUE en soulignant que la « *notion de dommage doit être interprétée (…) à la lumière de la jurisprudence de la CJUE, d'une manière qui tienne pleinement compte des objectifs du (RGPD)* ». Le dommage matériel ou moral découlant d'une violation du droit aux données personnelles devient donc une notion autonome, c'est-à-dire susceptible de s'affranchir des droits nationaux et dépendante de l'interprétation de la CJUE. Cette évolution n'est toutefois pas contradictoire avec la possibilité pour les personnes concernées d'invoquer des moyens spécifiques au(x) droit(s) du/des juge(s) de(s) l'État(s) membre(s) saisi(s). En effet, le considérant 145 énonce que la réparation « *est sans préjudice de toute action en dommages-intérêts fondée sur une infraction à d'autres règles du droit de l'Union ou du droit d'un État membre* ». Le considérant 146 précise enfin que les personnes concernées sont en droit d'avoir une « *réparation complète et effective* » pour le « *dommage subi* ». Le principe de la réparation intégrale est donc reconnu par le RGPD, entraînant des questionnements quant à son application mais aussi sur la quotité du risque financier à anticiper dans les méthodologies NIST et BSI.

108 En outre, les articles 77, 78 et 79 du RGPD débutent tous les trois par l'anaphore « *Sans préjudice de tout autre recours administratif ou extrajudiciaire* ». Cette précision procédurale souligne ici que la voie judiciaire n'est pas exclusive et peut être une voie complémentaire à la saisine de l'autorité nationale de contrôle. Le « *recours extrajudiciaire* » renvoie quant à lui aux mesures alternatives de règlement des différends (MARDs) tels que la conciliation, la médiation ou la transaction. Bien que peu expérimentées en France en matière de données personnelles, les MARDS, spécifiquement la voie de la transaction extrajudiciaire, est une importation procédurale anglo-saxonne. Cette

411 Arrêt, 25 oct. 2011, C-509/09 et C-161/10, eDate Advertising GmbH e.a. contre X et Société MGN Ltd.

412 CJUE, 17 oct. 2017, C-194/16, Bolagsupplysningen c. Svesnks Handel AB.

413 CJUE, 13 mai 2014, C-131/112, Google Spain c/ AEPD.

voie transactionnelle interroge sur la quotité du risque financier. Ainsi le droit européen, au travers du RGPD et de la directive (UE) 2019/261 en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs[414], permet à tous les demandeurs « *d'introduire une plainte (…) auprès du centre compétent du réseau des Centres européens des consommateurs en fonction des parties concernées* ». En pratique, cette plainte est déposée sur la plateforme de règlement des litiges en ligne créée par le Règlement (UE) 524/2013 du Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation[415]. Cette plateforme concerne spécifiquement « *(l)es obligations contractuelles découlant de contrats de vente ou de service en ligne entre un consommateur résidant dans l'Union et un professionnel* »[416]. Cette procédure européenne de règlement amiable des litiges est éloignée des exigences légales françaises relatives aux transactions extrajudiciaires mettant fin à des litiges. En effet, contrairement aux dispositions de l'article 2044 du Code civil qui impose au juge français de contrôler les concessions réciproques accordées entre les parties, les textes européens n'abordent pas la question de cette vérification.

109 Ce contexte judiciaire européen invite à dresser un panorama des solutions judiciaires développées par les différents États dans le cadre des contentieux civils relatifs aux données personnelles pour ainsi en déduire les risques à prendre en compte dans les AIPD. Du fait de leur culture judiciaire, les Cours anglo-saxonnes ont été confrontées à de nombreuses questions encore inconnues du droit continental. L'arrêt VM Morrison Supermarket rendu par la Cour suprême anglaise en est une parfaite illustration. Les juges britanniques y questionnent l'étendue de la responsabilité du responsable du traitement lors d'une violation de données personnelles occasionnée par un salarié malveillant. Cette judiciarisation se traduit également par le recours aux accords transactionnels, à l'instar de la *Federal Trade Commission* (« FTC ») aux États-Unis, entre des responsables du traitement violant les dispositions des législations relatives à la protection des données personnelles. Elle questionne l'harmonisation des solutions dans le droit des États membres dans l'adaptation d'un domaine relevant pourtant du droit européen. En effet, le RGPD n'a pas vocation à harmoniser les régimes de responsabilité civile des différents États membres. Ainsi en Angleterre, par exemple, les juridictions reconnaissent, sur le fondement du risque, un droit à la réparation aux victimes d'une utilisation illicite d'informations tout en limitant cette réparation aux dispositions du *Personal Data Act*[417]. De plus, les nombreuses innovations par le RGPD interrogent la compatibilité du droit français. Pour examiner cette compatibilité, nous étudierons dans un premier temps la notion de dommage engendré par une gestion défaillante des données personnelles comme fondement à une réparation judiciaire, en comparant les analyses développées en droit français et en droits étasuniens et anglais (Section 1). Cette méthodologie comparative sera reproduite pour présenter les conditions du calcul des dommages et intérêts dans le cadre d'une action collective (Section 2, page 134).

---

414 Voir dans ce sens l'article 5 de la directive (UE) 2019/2161 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs (Texte présentant de l'intérêt pour l'EEE), JOUE L 328, 18.12.2019, p. 7–28. Nous noterons cependant que la transposition française par la loi n°2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière (JORF n°0293 du 4 déc. 2020) ne mentionne pas cette possibilité.

415 Règlement (UE) n°524/2013 du Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n°2006/2004 et la directive 2009/22/CE (règlement relatif au RLLC) JOUE L 165, 18.6.2013, p. 1–12.

416 Article 2 du règlement (UE) n°524/2013.

417 Infra Section 2, 1.2, B, page 132.

Section 1. La qualification de la notion de « dommage » en droit des données personnelles

La qualification de dommages en droit des données personnelles est appréhendée différemment en droit français (§1) et en droit de la *Common Law* (Sous-Section 2, page 128).

Sous-Section 1. La difficile élection d'un dommage lié au traitement de données personnelles en droit civil français

Les méthodologies PRIAM et CNIL invitent le responsable du traitement à prendre en compte le risque de dommage généré par un traitement de données personnelles. Pour ce faire, nous chercherons tout d'abord à qualifier le type de responsabilité applicable à une violation de données, pour en déduire l'application du droit de la responsabilité contractuelle (A). Dans un second temps, l'étude des divers fondements relatifs au droit de la responsabilité délictuelle démontrera la difficulté à retenir ce nouveau fondement de responsabilité (B, page 123).

A. La réduction du champ de la reconnaissance de la réparation d'un dommage lié à un traitement de données personnelles en droit français

1. *L'inadéquation du droit contractuel dans l'encadrement des relations entre le responsable du traitement et la personne concernée*

110 Le présent développement porte sur la question de l'appréciation de la conformité, seconde étape de l'AIPD. En droit français, le domaine de la réparation varie en fonction de la nature du lien de droit établi entre le responsable du traitement et la personne concernée. Ce lien peut être soit contractuel[418], soit délictuel[419]. Or, en cas de contentieux, la règle du non-cumul des actions délictuelles et contractuelles contraint la personne concernée à opter judiciairement pour un seul choix procédural[420]. Dans le cas pratique Biomem, les traitements de données personnelles réalisés dans le cadre de la voiture connectée se fondent principalement sur l'exécution du contrat, ou de façon subsidiaire sur le consentement. Dans un premier traitement de données personnelles basé sur l'exécution du contrat, la nature contractuelle du lien entre la personne concernée et le responsable du traitement ne fait aucunement débat. À l'inverse, dans l'hypothèse du fondement du consentement, la fourniture sincère[421] de toutes les informations permettant le recueil libre et éclairé de la personne concernée est indispensable. Le consentement, défini par le RGPD, se rapproche du consentement au sens civiliste du terme[422], et ce jusqu'à son retrait par la personne concernée ou jusqu'à sa difficile annulation par le juge judiciaire sur le fondement de la violation contractuelle[423].

---

418 C'est-à-dire que le traitement de données personnelles repose sur un contrat.

419 C'est-à-dire que le traitement de données personnelles est factuel. La personne concernée peut ne pas être informée, ni avoir consenti à ce traitement.

420 Depuis l'arrêt Cass. Civ., 11 janv. 1922, Pelletier c. Doderet. Sur la question des données personnelles, Voir A. DANIS-FATOME, « *Quelles actions judiciaires en cas de violation du RGPD ?* », CCE 2019, dossier 18, note 23.

421 Voir contra, CNIL, Délibération de la formation restreinte n°SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société X, ou encore TGI Paris, 12 fév. 2019, UFC Que Choisir c. Google.

422 Dans ce sens, E. NETTER, « *L'extinction du contrat et le sort des données personnelles* », AJ Contrat 2019, pp .416 et s. « *N'est-ce pas une forme de pollicitation ? Le consentement spécial envisagé par le RGPD n'est-il pas alors une acceptation ? La réponse nous semble positive, et le fruit de la rencontre des volontés s'annexe alors au contrat de base - il peut en être expurgé si le consentement à la finalité spécifique est repris, ce que l'on doit pouvoir faire sans conséquence, en principe, pour le contrat sous-jacent (Art. 7.4)* ».

423 Id. « *le droit civil ne nous semble pas disposer d'instruments permettant un examen aussi exigeant et pragmatique, d'une part de la clarté de l'offre, d'autre part de la netteté de l'acceptation, que celui mené par l'autorité administrative indépendante sur la base du RGPD* ».

111 Deux questions relatives au respect de la conformité restent en suspens. La première, primordiale, concerne l'indépendance des politiques de confidentialité du contrat régissant la prestation tierce. La CNIL exige que les politiques de confidentialité consenties par la personne concernée soient stipulées dans une annexe distincte et indépendante au contrat liant la personne concernée et le responsable du traitement[424]. Ainsi dans l'hypothèse de Biomem-Indé, l'application est utilisée pour établir une intermédiation entre le fournisseur de vidéos à la demande et le véhicule connecté. L'objet de son contrat est donc intimement lié au traitement des données personnelles. Toutefois, dans les hypothèses de Biomem-Constructeur et Biomem-VOD, le traitement de données personnelles est accessoire à la prestation de service fournie. La seconde question concerne la qualification d'un passager en tant que personne concernée. Ce dernier n'a pas directement consenti ou souscrit au service traitant ses données personnelles. Dans le cadre de Biomem, le titulaire du compte est distinct de l'utilisateur, transformant cet utilisateur en tiers dont le consentement peut ne pas être formellement recueilli du fait de sa simple présence dans le véhicule. La doctrine civiliste invite à considérer ce « faux tiers » comme une partie au contrat, car bénéficiant indirectement de la prestation[425]. La Cour de cassation désavoue cependant cette vision en jugeant que « ***le tiers à un contrat peut invoquer, sur le fondement de la responsabilité délictuelle, un manquement contractuel dès lors que ce manquement lui a causé un dommage*** »[426] et ce, nonobstant l'identité de la source des fondements délictuel et contractuel. Ainsi, le tiers n'ayant pas directement consenti à un traitement de données personnelles est en droit d'invoquer la responsabilité civile délictuelle.

112 Lorsque la qualification contractuelle est retenue, cette nature entraîne des responsabilités contractuelles en cas d'inexécution ou de violation du contrat. Dans l'hypothèse du fondement contractuel du traitement, les solutions définies par l'article 1217 du Code civil[427] relatives à la violation d'une clause ou d'une inexécution devraient trouver leur application dans l'AIPD lors de l'étape de la conformité prévoyant les modalités d'exercice des droits des personnes concernées. Ainsi, les cinq solutions définies par l'article 1217 du Code civil sont les suivantes :

1. Le refus d'exécuter la contrepartie ou la suspension de son exécution,
2. La poursuite de l'exécution forcée en nature de l'obligation,
3. L'obtention de la réduction du prix de la prestation,
4. La résolution du contrat,
5. La réparation des conséquences de l'inexécution.

Le législateur français a reconnu à la partie victime, demanderesse, la possibilité de cumuler chacune de ces options procédurales. Celles-ci peuvent avoir un impact direct dans l'étape de conformité de l'AIPD, telles que le fondement de licéité ou encore les modalités de l'exercice des droits des personnes concernées. Dans le cas de Biomem, la suspension de l'exécution peut être d'ores et déjà écartée. En effet, cette suspension peut juridiquement se manifester par le refus de la personne concernée à continuer de transmettre ses données personnelles au responsable du traitement. Une telle option procédurale entraîne *de facto* la quatrième option, c'est-à-dire **la résolution du contrat** puisque l'objet même de certaines applications logicielles repose exclusivement sur le traitement de données personnelles. **La réduction du prix** pourrait s'appliquer à Biomem-Indé, seule hypothèse prévoyant une mise à disposition onéreuse de l'application. **La poursuite de**

---

424 CNIL, Pack de conformité, Véhicules Connectés et données personnelles, note supra, spéc. p.14.

425 Voir dans ce sens depuis G. DURRY en 1969, RTD civ. p. 776 qui estime que le tiers demandeur partie à un contrat connexe à celui dont il invoque la violation fait partie du même groupe contractuel que le défendeur. Voir aussi G. VINEY, « *Introduction à la responsabilité* », 3e éd., LGDJ, 2008, p. 659 et s. qui promeut la fin de l'absolutisme de la distinction.

426 Cass., Ass. Plen., 06 oct. 2016 n°05-13.255.

427 Modifiée par l'ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035 du 11 février 2016.

l'exécution forcée en nature de l'obligation est, quant à elle, consacrée par l'article 37-III de la loi Informatique et Libertés par la possibilité d'exiger la cessation d'un manquement au RGPD ou à la loi Informatique et Libertés. Toutefois, nous voyons mal la substitution de la partie débitrice (le responsable du traitement) par un tiers mandaté par la partie créancière (le conducteur ou le passager) pour réaliser l'exécution de l'obligation défaillante aux dépens de la partie débitrice. En d'autres termes, l'exécution forcée de l'inexécution ou de la violation contractuelle ne peut être exigée que du responsable du traitement seul débiteur de cette obligation et dans l'hypothèse où un sous-traitant existe. Cette question invite à examiner l'existence d'une éventuelle obligation pour la victime de limiter son dommage en attendant les mesures réparatrices applicables par le responsable du traitement défaillant[428].

La dernière option est la **réparation des conséquences de l'inexécution** renvoyant aux dispositions prévues aux articles 1231 à 1231 al. 7 du Code civil. Dans cette hypothèse, la partie demanderesse (la personne concernée) devra démontrer que **la violation du traitement (1)** reposant sur le fondement de licéité du contrat ou du consentement a entraîné **un dommage (2)** et qu'il existe **un lien de causalité (3)** entre ces deux éléments. Ces trois conditions rejoignent les dispositions prévues par l'article 1240 du Code civil instituant les conditions de la responsabilité délictuelle[429]. Enfin, il doit être rappelé que les clauses limitatives de responsabilité dans le cadre d'une relation contractuelle établie entre un professionnel et un consommateur sont exclues de plein droit[430]. En effet, la reconnaissance judiciaire des conditions générales d'utilisation et des politiques de confidentialité comme étant soumises au droit de la consommation entraîne l'application de l'article L 212-1 du Code de la Consommation. Cet article consacre l'exclusion des clauses limitatives de responsabilité aux contrats conclus entre professionnels et consommateurs[431].

2. *La réparation de la perte d'une chance*

113 La réparation de la **perte d'une chance** en défaveur de la personne concernée questionne l'éligibilité de la réparation d'un dommage futur subi par la personne concernée. Cette hypothèse se pose lors d'une violation de données personnelles, c'est-à-dire une « fuite » incontrôlée des données stockées sur les serveurs du responsable du traitement. L'examen de ce dommage délictuel[432] peut correspondre à un risque futur pour la personne concernée, devant être pris en compte par le responsable du traitement lors de la réalisation d'une AIPD. Toutefois, l'accueil des tribunaux judiciaires est mitigé sur la question des conséquences d'une éventuelle utilisation des données personnelles fuitées. En effet, la perte d'une chance implique un **préjudice futur certain** évaluable par le juge judiciaire[433]. Ainsi, la jurisprudence civile a très tôt statué en estimant que « *s'il n'est pas possible d'allouer des dommages-intérêts en réparation d'un préjudice purement éventuel, il en est autrement lorsque le préjudice, bien que futur, apparaît au juge du fait comme la prolongation certaine et directe d'un état de choses actuel et comme étant d'estimation immédiate* ». Ainsi la **distinction** judiciaire s'effectuera entre **le préjudice futur et le préjudice éventuel**, le premier étant le seul réparable. Le préjudice futur implique **le calcul de probabilités** pour apprécier la certitude du préjudice subi[434]. Ce caractère certain se manifeste tout d'abord par une **brève échéance des**

---

428 Voir infra §118, page 126.

429 Voir supra §110, page 119.

430 Voir supra §108, page 117 sur Schrems (II).

431 Voir dans ce sens, TGI Paris, 12 fév. 2019, UFC Que choisir contre Sté Google inc., N° RG: 14/07224, Voir X. DELPECH, « *Une recommandation de la Commission des clauses abusives sur les réseaux sociaux* », Dalloz Actu, 05 déc. 2014.

432 Comp. Cass. Civ. 2e, 19 oct. 1976 et Cass. Civ. 1ere, 17 nov. 1982, D. 1984, p.305.

433 Voir dans ce sens Cass. Crim., 01 juin 1932.

434 Voir dans ce sens Cass. Civ. 2e, 01 avril 1965.

effets générés par le dommage[435] qui se définit surtout par son caractère « **direct et certain** »[436]. Le calcul de la probabilité de la réalisation du dommage sert à déterminer l'opportunité d'un risque, inscriptible dans l'AIDP, mais également à fixer le montant de la réparation accordée à la victime. L'indemnisation a pour seul objet la réparation de la tentative de l'action empêchée par l'événement préjudiciable, les effets bénéfiques potentiels découlant de la chance en étant exclus[437]. La perte d'une chance est principalement utilisée pour assouplir les exigences relatives à la preuve du lien de causalité avec le dommage. À l'heure actuelle, les exigences posées pour la perte d'une chance en droit français semblent exclure ce fondement, du fait de l'incertitude du dommage et de son absence de connexité temporelle avec l'éventuel dommage ultérieur. À l'inverse, le droit étasunien commence à reconnaître ce fondement dans des contentieux relatifs à des usurpations d'identités découlant de fuites malveillantes de données[438]. Il n'est cependant pas impossible que la jurisprudence française évolue dans ce sens, des travaux européens sur la réforme de la responsabilité civile à « l'âge numérique » ayant récemment été initiés[439].

3. *La prise en compte civiliste des vulnérabilités organisationnelles*

114 Le détournement de données personnelles par un salarié correspond aux vulnérabilités organisationnelles étudiés lors des seconde et troisième étapes des méthodologies d'AIPD. Ici, l'étude des solutions applicables en droit français sur la responsabilité des commettants du fait de leurs préposés est nécessaire[440]. À cet égard, bien que la jurisprudence civile ait pu être fluctuante[441] dans la détermination de la faute détachable du service[442], elle reconnaît toutefois la responsabilité de l'employeur pour les fautes de son salarié, fautes commises dans le cadre d'un dommage fait aux tiers pendant l'exercice de ses fonctions ou dans le cadre d'un contrat avec un client. La doctrine civiliste voit en l'exonération du commettant le risque de négation de l'objet même du contrat liant le client avec le commettant. Le contrat, dépourvu de cause[443], n'aurait aucune valeur juridique, la faute du salarié permettant à l'entreprise de s'exonérer de toute obligation contractuelle.

---

435 Voir dans ce sens, Cass. Civ., 13 févr. 1923, GAJC, Tome 2, p. 290-293.

436 Cass. Civ. 1ere, 30 avril 2014.

437 GAJC, id.: « *Il ne s'agit pas, en effet, d'accorder à la victime l'avantage que la survenance de l'accident l'a irrémédiablement privée de la possibilité de briguer, car ce serait à supposer à coup sûr, le plaideur aurait gagné son procès, l'éleveur sa course, le candidat son examen* ».

438 S. N. JONES, « *Having An Affair May Shorten Your Life: The Ashley Madison Suicides* », 33 Ga. St. U. L. Rev. 455 (2017).

439 Voir l'appel à contribution de l'Union européenne, « *Civil liability – adapting liability rules to the digital age and artificial intelligence* », https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en.

440 Art. 1242 al. 5 du Code civil.

441 Ainsi dans la première partie du 20e siècle, la faute commise par le salarié, même en dehors du cadre normal de ses fonctions, entraînait la responsabilité de l'employeur (Cass. Crim. 20 juil. 1931). Jusqu'au troisième quart de ce même siècle, la faute commise en dehors des fonctions mais avec les moyens de l'employeur oscillait entre la responsabilité du salarié (Cass. Civ. 2e 24 juin 1957) et celle du commettant (Cass. Crim. 05 oct. 1961). L'arrêt rendu par l'Assemblée Plénière le 17 juin 1983 met un terme au débat en reconnaissant la responsabilité du seul salarié sous trois conditions : l'absence d'autorisation, la poursuite par le préposé d'une fin étrangère à ses attributions et le dépassement objectif des fonctions. Cette dernière condition disparaît avec l'arrêt de l'Assemblée plénière du 17 octobre 1985. La Cour de cassation se dédit avec un arrêt du 19 mai 1988, devenu droit constant, où elle déclare que le « *commettant ne s'exonère de sa responsabilité que si son préposé a agi en dehors des fonctions auxquelles il était employé, sans autorisation, et à des fins étrangères à ses attributions* ».

442 À l'instar du droit administratif dont l'arrêt fondateur a été rendu par le T.C. du 30 juillet 1873, Pelletier, entraînant des myriades de distinction entre la faute du service et la faute personnelle commise en dehors du service (CE, 12 mars 1975, Pothier), dans ou à l'occasion de l'exercice du service (T.C., 9 juil. 1953, Dame Vve Bernadas). Ce principe a été amoindri en 1918 (C.E., 26 juillet 1918, Époux Lemonnier) où a été a reconnu le cumul de responsabilité d'une faute personnelle avec une faute de service pour une faute unique.

443 Ancien article 1118 du Code civil, remplacé par l'article 1168 du Code civil par l'ordonnance du 10 février 2016, JORF n°0035 du 11 février 2016.

Ici la reconnaissance de la responsabilité du commettant, sous réserve d'une faute totalement détachable du préposé, entraîne une garantie de l'employeur dans la réalisation, de bonne foi, de l'exécution du contrat. Cette solution française semble diverger de la jurisprudence issue de l'arrêt Morrison rendu par la Cour suprême du Royaume-Uni, lequel entraîne une exonération de la responsabilité de l'employeur des faits de son salarié. Ce risque de négation de l'objet du contrat se rapproche du principe de responsabilité posé par le RGPD. Le responsable du traitement est en effet tenu de documenter toutes les mesures prises pour identifier et réduire les risques. Parmi ceux-ci se trouvent les vulnérabilités « *organisationnelles* » supposées être encadrées par des mesures de restriction des accès logiques et administratifs.

115 Il convient également de porter attention aux vulnérabilités organisationnelles lors de l'acquisition de sociétés par le responsable du traitement. L'arrêt du 25 novembre 2020 rendu par la chambre criminelle de la Cour de cassation invite à la vigilance. En effet, dans cette espèce, une société, absorbée par la suite par une autre société, a été tenue pour responsable des faits de destructions involontaires par incendie. Contrairement à sa jurisprudence antérieure[444], la chambre criminelle pose trois conditions cumulatives pour transférer la responsabilité de la société absorbée à la société absorbante :

- sont seulement concernées les sociétés anonymes ou des sociétés par actions simplifiées visées par la directive relative à la fusion des sociétés anonymes[445] ;
- la portée de la sanction est limitée pour la société absorbante aux peines d'amende et de confiscation ;
- les droits de la défense sont transférés à la société absorbante qui pourra se substituer sur tous les moyens à la société absorbée.

Les infractions n'étant pas explicitement définies, le dispositif de sanction prévu par la loi Informatique et Libertés peut engager la responsabilité pénale de la société absorbante. Dans une telle mesure, la société souhaitant réaliser une acquisition devra procéder en amont à un audit complet de la licéité des traitements réalisés par la société en voie d'absorption pour s'assurer de ne pas être exposée à une sanction pénale sur le fondement des infractions antérieures à l'absorption.

B. Les conditions de prise en compte du dommage matériel découlant d'une violation de données personnelles et de son aggravation

116 Le considérant 75 du RGPD invite à considérer les dommages physiques ou matériels dans l'appréciation des risques découlant d'un mauvais traitement des données personnelles[446]. L'inclusion de tels dommages dans les risques à prendre en compte distend le lien de responsabilité entre le fait générateur et le dommage subi. En effet, un lien de causalité est présupposé entre ces deux événements. Le considérant 75 du RGPD s'affranchit des règles classiques de la responsabilité civile en utilisant la notion de « *risque* » pour associer tout dommage à un traitement de données personnelles, que celui-ci soit ou non le fait générateur. Cette rédaction textuelle est d'autant plus soutenue que le considérant 146 du RGPD dispose que « *la notion de dommage devrait être interprétée au sens large, à la lumière de la jurisprudence de la Cour de justice, d'une manière qui tienne pleinement compte des objectifs du présent règlement* ». **Ainsi la CJUE dispose d'un**

444 Voir dans ce sens, Cass. Crim., 20 juin 2000, n°99-86.742, Cass. Crim., 13 oct. 2003, n°02-86.375 ou Cass. Crim., 18 fév. 2014, n 12-85.807.

445 Directive 78/855/CEE du Conseil du 9 octobre 1978 relative à la fusion des sociétés anonymes, codifiée en dernier lieu par la directive (UE) 2017/1132 du Parlement européen et du Conseil du 14 juin 2017, JOCE, 30 juin 2017, L 169/46.

446 Selon le considérant 75, « *Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier* ».

pouvoir discrétionnaire pour interpréter la notion de dommage. Autrement dit, la compétence juridictionnelle de la Cour européenne lui permet de créer de nouvelles catégories de dommages sans qu'il n'y ait un lien direct avec le traitement. Ce pouvoir discrétionnaire invite le juge français à recourir à la théorie **dite de l'équivalence des conditions**. Cette dernière **intègre dans le lien de causalité tous les éléments ayant concourus à la réalisation du dommage**. Cette théorie entraîne donc une répartition des dommages et intérêts pour chacun des acteurs ayant concouru à la réalisation du dommage, même si celui-ci est distant du fait générateur[447]. Cette approche est toutefois problématique dans l'hypothèse d'une violation de données personnelles où le responsable du traitement / le sous-traitant est / sont responsable(s) du défaut de sécurité des données personnelles mais pas de l'utilisation malfaisante subséquente réalisée par des tiers.

Ainsi, les différentes AIPD invitent le responsable du traitement à atténuer les « *dommages matériels* », c'est-à-dire les atteintes à l'intégrité physique ou aux biens des personnes concernées. Mais, traditionnellement, le droit français rejette la responsabilité du fait des choses immatérielles[448] de la responsabilité civile. M. le Professeur André LUCAS soutient qu'**une chose immatérielle ne peut générer que des dommages uniquement immatériels**. Reposant sur la **théorie de la causalité adéquate**, le **lien de causalité** se trouvant entre **le fait générateur** (le mésusage d'une donnée personnelle) et **le dommage** (un préjudice physique découlant de ce mésusage) n'est pas directement établi. En effet, **la doctrine estime que l'information seule ne peut pas être un élément générant un dommage mais que cette information nécessite une transmutation matérielle pour que ce dommage puisse être généré**. Ainsi par exemple, la divulgation d'une donnée personnelle sensible (sexualité, santé) n'est pas constitutive d'un dommage matériel direct. Elle est indéniablement constitutive d'un dommage moral mais pour que le dommage matériel soit constitué, le responsable du traitement, le sous-traitant ou toute partie intéressée doit occasionner un dommage matériel à la personne concernée victime à partir de cette information. Cette théorie de l'irresponsabilité du dommage matériel du fait des choses immatérielles est actualisée par le Professeur TRICOIRE[449]. Celui-ci insiste sur la limitation du dommage immatériel aux seules choses immatérielles en citant les exemples d'atteintes au respect à la vie privée et de la réputation des personnes morales. Dans ce sens, la CJUE dans son arrêt Krone[450] estime que le suivi par un lecteur d'un conseil de santé erroné, publié dans un article de journal imprimé, entraînant un dommage corporel ne peut pas engager la responsabilité de l'éditeur sur le fondement de la responsabilité des produits défectueux. Cette décision maintient donc l'impossibilité juridique de retenir la responsabilité du fait d'une chose immatérielle.

La Cour de cassation, de son côté, se refuse depuis un certain nombre d'années à se positionner sur la théorie du lien de causalité la plus adaptée. En effet, les juges du fond[451] recourent à la théorie de l'équivalence des conditions lorsque la détermination exacte du fait générateur est difficilement déterminable. Dans son arrêt rendu le 27 mars 2003, la Cour de cassation estime que « *si des fautes successives imputables à des auteurs différents ont pu jouer un rôle causal sur ce poste de préjudice, (…), cette pluralité des causes (…) n'est pas de nature à faire obstacle à l'indemnisation de l'entier dommage par l'auteur initial par application du principe de l'équivalence des causes*

---

447 Se rapprochant donc des dispositions prévues à l'article 79 du RGPD.

448 Voir dans ce sens, A. LUCAS, « *La responsabilité du fait des choses immatérielles* », MELANGES CATALA, Litec, 2001, p. 1023, spéc. p. 817.

449 E. TRICOIRE, « *La responsabilité du fait des choses immatérielles* », MELANGES LE TOURNEAU, Dalloz, 2008, p. 1083, spéc. p. 983.

450 CJUE, 10 juin 2021, C-65/20, Krone-Verlag.

451 Voir dans ce sens, Cass. Crim, 20 oct. 2020, n°19-84.641, « *Il résulte de ces textes que lorsque plusieurs fautes ont concouru à la production du dommage, la responsabilité de leurs auteurs se trouve engagée dans une mesure dont l'appréciation appartient souverainement aux juges du fond* ».

dans la production d'un même dommage »[452]. Ainsi cette théorie est régulièrement utilisée pour créer une présomption de causalité pour les produits de santé défectueux facilitant la réparation du préjudice subi par les patients victimes d'un dommage médical[453]. Néanmoins, en contrepartie, la juridiction suprême diminue la condamnation du responsable en assimilant à la faute de la victime l'obligation pour celle-ci de prendre toutes les mesures raisonnables pour empêcher la réalisation du dommage[454] ou réduire ses effets[455].

1. *L'obligation pour la victime de prévenir l'aggravation du dommage*

117 L'obligation pour la victime de mettre en place des mesures raisonnables prévenant l'aggravation du dommage correspond aux mesures correctives et préventives applicables postérieurement à la réalisation d'un dommage. Il est possible de lier cette future obligation à la mise en place de mesures d'atténuation en matière de données personnelles, postérieurement à la réalisation du risque. Cette obligation peut être interprétée en deux temps. Le premier temps peut amener à la diminution de la responsabilité civile du responsable du traitement, voire à son exonération. Cette hypothèse est probable si le responsable du traitement fournit la preuve de la conformité du traitement au RGPD, en soulignant le respect de l'état des connaissances par l'instauration de mesures d'atténuations du risque adéquates, conformes à la veille, et que celles-ci sont documentées. Cette obligation de documentation fait partie des obligations exigées par l'article 30 du RGPD relatif au registre des activités du traitement. Elle permet également à la réalisation d'une actualisation de l'AIPD prescrite par les méthodologies CNIL et PRIAM. La violation des données personnelles peut être considérée comme un cas de force majeure[456]. Le second temps peut néanmoins tempérer ce raisonnement. Les effets du dommage peuvent se révéler ultérieurement à un jugement civil. Concrètement, l'exonération du responsable du traitement à un moment défini pour une violation de données personnelles ne prohibe pas l'octroi de dommages et intérêts ultérieurs au nom des dommages subséquents. La jurisprudence civile exclut la révision de l'autorité de chose jugée dans la seule hypothèse où la réévaluation des dommages et intérêts entraîne leur diminution[457]. Ainsi, le juge peut réévaluer les dommages et intérêts lorsque le préjudice est aggravé[458], la prescription de l'action en réparation ne commençant qu'à compter de la manifestation de cette aggravation[459]. Cette aggravation peut correspondre, par exemple, à l'absence de diligence d'un responsable de traitement à implémenter des mesures de garanties adaptées suite à la mise à jour de son AIPD ou suite à une violation de données personnelles. En effet, au nom de la réparation intégrale, la victime est en droit d'obtenir réparation en cas de variation de son dommage depuis le jour de l'accident. Ainsi, dans l'hypothèse d'une réutilisation illicite des données personnelles ultérieure à la violation de données ayant permis leur divulgation, le responsable du traitement peut, nonobstant une première condamnation civile ou une exonération judiciaire, être pourtant tenu responsable pour tous les préjudices subis ultérieurement par la / les personne(s) concernée(s) victime(s). Cette vision relativise ainsi les effets de la limitation de la jurisprudence pour la perte d'une chance dans le domaine des données personnelles mais cette vision entraîne dans le même temps une augmentation de l'assiette du risque à prendre en compte dans l'AIPD.

---

452 Voir dans ce sens, Cass. Civ. 2e, 27 mars 2003, n°01-00.850

453 Voir par exemple, Cass. Civ. 1ère, 5 avr. 2005, n°02-11.947 et n°02-12.065.

454 Voir dans ce sens, Cass. Crim., 20 oct. 2020 *in fine* : « *Est de nature à constituer une telle faute le fait, pour la victime, de ne pas avoir pris les précautions utiles pour éviter le dommage* ».

455 A. LUCAS, *La responsabilité du fait des choses immatérielles*, note supra.

456 Article 82-3° du RGPD : « *Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable* ».

457 Cass. Civ., 30 déc. 1946 et Cass. Civ. 2e, 12 oct. 1972.

458 Cass. Civ. 2e, 06 mai 1960 et Cass. Civ. 2e, 14 janv. 1979.

459 Cass. Civ. 2e, 15 nov. 2001.

118 L'obligation pour la personne concernée d'atténuer les effets du dommage résultant de données personnelles en attendant la prononciation judiciaire de mesures est prépondérante dans cette matière, des actions correctives pouvant réduire l'intensité du dommage subi. Ces dernières doivent être anticipées lors de la quatrième étape de l'AIPD. Le considérant 86 du RGPD invite le responsable du traitement à prévenir la personne concernée dans les « *plus brefs délais* » dans l'hypothèse d'une violation des données pour que « *celle-ci puisse prendre les précautions qui s'imposent* ». Une telle disposition invite donc la personne concernée, informée de cette violation, à limiter le dommage potentiel découlant de la violation de données personnelles. Or, le droit français s'oppose traditionnellement à cette obligation[460]. Ce positionnement est perçu comme un particularisme juridique en droit comparé. L'article 1263 du projet de réforme du Code civil de 2017[461] propose de le supprimer en créant un « *devoir d'atténuation* »[462]. Une partie de la doctrine déclare cette évolution nécessaire en estimant que la « *faute lucrative traduit un comportement répréhensible que n'aurait pas le* bonus pater familias*, et (qui) est l'expression d'une déloyauté manifeste (… du…) fait de la victime* »[463]. Le juge de cassation reconnaît cette déloyauté de la victime en soutenant les rejets des juges du fond, depuis 2018[464]. Dans ce cas de figure, la personne concernée n'est pas fondée à se prévaloir de ses propres lacunes pour engager la responsabilité du responsable de traitement pour les dommages ultérieurs du fait des données personnelles fuitées. Ce principe souffre de l'exception des traitements de données biométriques, ces dernières ne pouvant faire l'objet d'une mesure d'atténuation du fait de leur unicité. Pour être traitées, le responsable de traitement doit chiffrer ces dernières informations dès leur collecte, pendant toute la durée de leur traitement jusqu'à leur effacement définitif[465]. De plus, et de façon optimale, la CNIL l'invite à conserver ces données sur un support indépendant et sécurisé restant sous le contrôle exclusif de la personne concernée[466].

2. *Le dommage d'anxiété*

119 La question d'un dommage d'anxiété provoqué par une utilisation non autorisée de données personnelles ultérieure à une violation de données personnelles doit être écartée en droit français. En effet, cette notion a été développée en matière de données personnelles par la doctrine étasunienne pour fonder la réparation de ce nouveau type de préjudice[467]. Un tel dommage « *psychologique* » trouve un écho dans la méthodologie PRIAM. Bien qu'il ait été reconnu en droit français par la Cour de cassation, son existence est limitée au seul domaine du droit du travail et spécifiquement lorsque

---

460 Dont l'arrêt de la Cass. Civ . 2e, 19 juin 2003 (D. 2004, somm. p.1346, D. MAZEAUD ou JCP 2004, I, 101, n°9, G. VINEY) qui pose clairement le principe en tant que principe général du droit civil en statuant « *que l'auteur d'un accident doit en réparer toutes les conséquences dommageables ; que la victime n'est pas tenue de limiter son préjudice dans l'intérêt du responsable* ». Voir auparavant Cass. Civ. 2e, 13 janv. 1966, ou Cass. Crim. 30 oct. 1975.

461 Projet de réforme de la responsabilité civile, mars 2017, http://www.justice.gouv.fr/publication/Projet_de_reforme_de_la_responsabilite_civile_13032017.pdf.

462 Voir dans ce sens, H. MUIR WATT, « *La modération des dommages en droit anglo-américain* », LPA, 20 nov. 2002, p.45, voir plus récemment G. DE MONTCUIT, « *L'incidence de l'obligation de ne pas aggraver son dommage sur l'action privée en réparation du dommage concurrentiel* », LPA, 18 janv. 2019, n°14, p. 9.

463 D. GENCY-TRANDONNET, « *L'obligation de modérer le dommage dans la responsabilité extra-contractuelle* », G.P. 06 mai 2004.

464 Voir dans ce sens, Cass. Civ. 3e, 21 juin 2018, n°17-15.897 et Cass. Civ. 3e, 12 avr. 2018, n°17-26.906, note H. BARBIER, RTD civ. 2018, p. 900.

465 Voir supra §20, page 25 et §21, page 25.

466 Voir dans ce sens, CNIL, délibération n°2016-212 du 7 juillet 2016 autorisant l'association Natural Security Alliance à mettre en œuvre un système d'authentification biométrique basé sur la détention d'un ordiphone ou d'un support individuel contenant une application, placé sous le contrôle des personnes concernées, aux fins d'accès à des services.

467 Voir infra §123, page 130.

les conditions de travail exposent le salarié à des substances toxiques, telle que l'amiante[468]. Pour être éligible à l'*Allocation de cessation anticipée d'activité des travailleurs de l'amiante* (ACAATA), le salarié doit alors (1) fournir la preuve de son travail dans un établissement de fabrication de matériaux contenant de l'amiante[469] et (2) se « *trouver dans une situation d'inquiétude permanente face au risque de déclaration à tout moment d'une maladie liée à l'amiante* »[470]. Il doit également (3) produire l'attestation de cette inquiétude par des contrôles médicaux et examens médicaux, la jurisprudence ayant tendance à progressivement éliminer cette condition. Ce préjudice d'anxiété peut être ainsi défini comme « *une situation d'inquiétude permanente face au risque de déclaration à tout moment d'une maladie liée à l'exposition à une substance dangereuse (…), lorsque cette inquiétude est directement causée par une politique lacunaire de prévention des risques. À l'inverse si l'employeur a mis en œuvre toutes les mesures de prévention nécessaires, alors l'inquiétude subie par ses salariés ne lui sera pas directement imputable* »[471]. Ce préjudice d'anxiété rend la victime éligible à des préjudices extra-patrimoniaux. La pratique judiciaire française limite la réparation de ce type de préjudice aux circonstances relatives au travail dans des conditions périlleuses, c'est-à-dire à des risques incertains situés dans le monde matériel où le dommage est « palpable ». Les requérants peuvent alléguer des préjudices extra-patrimoniaux, c'est-à-dire des dommages moraux, sur le fondement de l'anxiété dès lors que ces derniers sont attestés par des preuves objectives[472]. Or ce raisonnement est difficilement transposable dans un contexte immatériel, et particulièrement de traitement de données personnelles.

En effet, la démonstration d'un tel préjudice serait difficile en droit des données personnelles. Le dommage moral du fait d'une chose immatérielle est, certes, pris en compte par le juge civil mais ses effets sont limités. Le dommage immatériel provenant des données personnelles peut être ultérieur à la réalisation de la violation, abandonnant les victimes dans « *une situation d'inquiétude permanente face au risque de déclaration à tout moment* » d'un préjudice. Toutefois, ce préjudice doit être « *directement causé par une politique lacunaire de prévention des risques* »[473]. En outre, la question de la valeur probatoire des constatations de la CNIL face aux politiques lacunaires devant le juge judiciaire se pose et sera abordée ultérieurement au §135, page 141. Les manquements du responsable du traitement relèvent des preuves factuelles, c'est-à-dire démontrables par tout moyen. C'est à ce niveau que la troisième condition relative à la production de l'attestation de l'inquiétude suscitée par des recherches sur l'utilisation des données personnelles fuitées serait utile pour souligner l'existence d'un préjudice. En effet, la personne concernée victime d'une utilisation non autorisée de ses données provenant d'une violation de données personnelles pourrait apporter la preuve de son temps de recherches aux débats démontrant le caractère chronophage de ceux-ci. Toutefois, la prise en compte du barème Dinthillac, standard judiciaire pour fixer le montant des réparations, quantifie ces réparations en deçà du préjudice moral réellement subi.

---

468 Voir dans ce sens, L. de MONTVALON, « *Extension du préjudice d'anxiété* », D. Act. 18 sept. 2019, note sous Cass. Soc. 11 sept. 2019, voir W. FRAISSE, « *Amiante : la preuve du préjudice d'anxiété* », D. Act. 02 mai 2014 qui dresse un panorama de la jurisprudence antérieure.

469 Dont la liste est établie par la loi n°98-113 du 23 décembre 1998 relative au financement de la sécurité sociale pour 1999 modifiée par la loi n° 016-1827 du 23 décembre 2016 de financement de la sécurité sociale pour 2017, JORF n°0299 du 24 décembre 2016.

470 Cass. Soc., 11 mai 2010, n°09-42.241.

471 W. FRAISSE, note supra.

472 Voir dans ce sens CEDH, 25 juin 1997, Halford c. Royaume-Uni, où la demanderesse obtient une réparation pour un préjudice d'angoisse sur le fondement de l'atteinte au droit au respect à la vie privée. Cette atteinte est soutenue par des attestations médicales. Toutefois, une analyse de l'arrêt démontre que la Cour a fait droit aux demandes de réparation pour le préjudice moral pour sanctionner les écoutes illégales tout en relativisant le lien entre lesdites écoutes et le dommage allégué.

473 W. FRAISSE, note supra.

Sous-Section 2. L'éligibilité d'un dommage du fait d'une gestion défaillante des données personnelles en droits étasunien et anglais

Dans un premier temps, nous aborderons le droit étasunien des données personnelles pour souligner les limites inhérentes à la réparation d'un préjudice subi du fait de la gestion défaillante des données personnelles (A) avant d'examiner l'évolution de la jurisprudence anglaise en la matière (B, page 132).

A. La difficile reconnaissance du fondement du préjudice basé sur une violation des données personnelles en droit étasunien

120 Le droit étasunien ne disposant pas d'une législation *omnibus* générale au niveau fédéral, la protection des données personnelles est assurée par divers textes[474] ou une interprétation extensive de certains *privacy torts*, tels que reconnus par le droit coutumier[475]. Cette diversité amenuise la protection des données personnelles, et ce d'autant plus que les Cours fédérales n'ont pas dégagé de consensus pour les affaires relatives à ce type de droit, généralement portées par des actions de groupe. Les affaires les plus emblématiques aboutissent généralement à des transactions judiciaires[476], à l'instar de l'accord historique conclu en 2019 entre Facebook et la FTC où le réseau social a accepté une amende administrative record de 5 milliards de dollars[477]. En effet, la FTC préfère la voie transactionnelle à un probable échec judiciaire, les jugements aboutissant généralement à une exonération du responsable du traitement[478]. Les transactions étant des actes privés conclus entre la Commission et l'entreprise défaillante, elles permettent d'imposer des obligations contractuelles allant au-delà des obligations légales et coutumières issues des *torts*.

121 Afin de constituer une action de classe, les victimes d'une atteinte au droit à la protection des données personnelles doivent respecter les dispositions du *Class Action Fairness Act*[479]. À l'instar du droit anglais et du droit français, cette disposition articule le procès en deux temps :

- la permission de constituer un groupe ayant subi un préjudice identique,
- puis le procès en lui-même, comprenant les débats et le jugement.

Lors de la première étape, le demandeur doit démontrer la généralisation de son préjudice à des tiers et la réalité du préjudice[480] (*hurdle of standing*). Une fois ces conditions validées par le juge,

---

474 Citons pour l'exemple le *Child Online Protection Act* [COPA] (1998) qui sera utilisé dans le cadre de la transaction conclue avec Youtube de septembre 2019 ou encore le *Health Insurance Portability and Accountability Act* [HIPAA] (1996).

475 Voir infra B, page 132.

476 Voir dans ce sens la transaction conclue entre la FTC et Facebook du 24 juillet 2019 ou celle conclue entre la FTC et Youtube du 4 septembre 2019. Il est également possible de citer la transaction conclue entre Google avec des plaignants pour 13 millions de dollars le 22 août 2017, relative à la localisation des réseaux wifi lors des cartographies effectuées par Google map, https://static.reuters.com/resources/media/editorial/20200122/In%20re%20Google%20Referrer%20Header%20Privacy%20Litigation.pdf, ou encore une transaction à 7.5 millions de dollars regroupant plusieurs contentieux pour une violation de données de Google+, https://www.googleplusdatalitigation.com/.

477 FTC - Facebook, Stipulated order for civil penaly, monetary judgement and injunctive relief, 24 juillet 2019, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

478 Voir dans ce sens les réserves effectuées par les commissaires R. SHOPRA (https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf) et S. SLAUGHTER (https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf) qui, après avoir rappelé l'impossibilité d'avoir une assurance que le jugement soit défavorable à Facebook, soulignent qu'il existait suffisamment de preuves pour obtenir une réelle condamnation. Dans ce sens voir R. CHOPRA, *Dissenting opinion* (note supra).

479 U.S. Class Action Fairness Act of 2005, 28 U.S.C. Sections 1332, 1453, and 1711–1715, Pub.L. 109–2.

480 Voir dans ce sens, l'interprétation faite par la Cour d'Appel fédérale du 9e circuit dans l'affaire Wolin c. Jaguar, 617 F. 3d 1168, 2010.

le demandeur est en droit d'ouvrir une procédure d'*opt in* pour que les victimes se trouvant dans une situation analogue puissent se joindre à cette action. C'est à ce niveau que la grande majorité des demandes de constitution d'action de classe est rejetée, les parties n'étant pas en mesure de produire la preuve d'un dommage « *concret* »[481]. En effet, la majorité des affaires reposent sur des demandes de réparation de « *dommage intangible* », c'est-à-dire immatériel, voire sur un « *risque* » de dommage. Cependant, la jurisprudence étasunienne est actuellement en pleine évolution, comme en attestent les arrêts **Clapper** de 2013 et **Spokeo** de 2016 de la Cour suprême des États-Unis d'Amérique[482]. Dans l'affaire **Clapper c. Amnesty International**, relative à des présomptions d'activités d'espionnage réalisées par les services secrets étasunien sur le fondement du *Foreign Intelligence Surveillance Act*[483], des avocats, des journalistes et des militants des droits de l'homme estiment que leur droit au respect à leur vie privée était violé par l'examen des métadonnées de leurs communications avec des contacts situés à l'étranger. Bien que reconnaissant l'existence d'un « *préjudice factuel* » (« *injury in fact* »), la Cour suprême retient l'absence de preuve de la réalité d'une atteinte par la surveillance. Ainsi, la violation du droit de la *privacy* doit être démontrée par des preuves tangibles d'une réelle atteinte.

122 L'arrêt Clapper ouvre la voie à des débats ultérieurs portant sur l'**imminence du risque** dans des contentieux relatifs aux violations de données par des pirates informatiques. La criticité d'une donnée personnelle divulguée est alors prise en compte pour apprécier un risque. Dans ce contexte, la jurisprudence ultérieure admet le risque de fraude ou d'usurpation d'identité découlant d'un vol de données personnelles comme fondement à une action judiciaire. Ainsi certaines Cours fédérales étasuniennes[484] reçoivent ce moyen en estimant que la motivation du piratage, **à savoir l'accès à des données personnelles afin de les valoriser**[485], constitue un **dommage réel et non hypothétique**. Cette approche se retrouve dans la méthodologie PRIAM qui prend en compte la motivation du pirate informatique à accéder à une donnée critique dans son analyse de la vraisemblance d'un risque. Cependant, la majorité des Cours soulève l'absence d'**imminence du dommage** pour rejeter cet argument[486]. La Cour suprême se saisit de l'occasion présentée par l'affaire **Spokeo, Inc. v. Robins**[487] pour régler cette divergence jurisprudentielle. En se fondant sur le *Fair Credit Reporting Act federal*, le plaignant, chômeur peu qualifié de longue durée, reproche au moteur de recherches de référencer des informations erronées à son sujet à partir d'un rapport de solvabilité concernant un cadre supérieur. Le demandeur soutient que ces erreurs diminuent ses chances d'obtenir un travail. Le juge du premier degré rejette sa demande, contrairement à la Cour suprême. Cette dernière donne pour instruction à la Cour d'Appel fédérale de qualifier le dommage de « *réel* » dès lors qu'un « *dommage immatériel* », voire un « *risque* » de dommage, est « *dans une relation proche d'un dommage qui aurait traditionnellement été regardé comme fournissant un fondement devant les Cours anglaises ou américaines* ». Les dommages immatériels non imminents sont reconnus comme fondement d'un *tort* pour la formation de l'action de groupe qui doivent être pris en compte dans la définition des risques pour les données personnelles.

---

481 Voir dans ce sens, l'arrêt de la Cour suprême des États-Unis, Spokeo v. Robins, 138 CT 1540 (2016).

482 Cour suprême des États-Unis, Clapper c. Amnesty international USA, 568, US (2013).

483 *Foreign Intelligence Surveillance Act* de 1978 amendée par *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008*, autorisant les programmes de surveillance contestés dans l'arrêt Schrems I.

484 Principalement les Cours d'appels fédérales du 6e, 7e et 9e circuit.

485 Voir dans ce sens, Cour d'appel fédérale du troisième circuit, Reilly v. Ceridian, 664 D. 3d 37,2011, Cour d'appel fédérale du troisième circuit In re Horizon Healthcare Servs., 846, F.3D 625, 2017 et Cour d'Appel du South District du Texas, Peter v. St Joseph Servs. Corp 74 F. supp. 3d. 847.

486 Voir dans ce sens, Cour fédérale de Louisiane, Eastern District, Green c. eBay, E.D. 4, 2015 : « *the mere increased risk of identity thef or identity fraud alone does not constitute a cognizable injury* ».

487 Voir note supra, Spokeo inc. c. Robins.

À partir de ces deux arrêts, un **mouvement doctrinal**[488], initié par D. K. CITRON et D. SOLOVE, **plaide** pour la prise en compte d'**un dommage sur le fondement de l'anxiété** et l'existence d'**un dommage pour risque**.

123 Ces deux auteurs invitent à la reconnaissance du « *risque d'anxiété* » comme fondement juridique d'un dommage dans le cadre d'une violation de données personnelles. Se basant sur les effets psychologiques que peut revêtir un vol d'identité par les pirates informatiques[489], ils invitent à considérer les dépenses engagées par la victime pour atténuer les risques de réutilisation des données violées ou pour surveiller leur potentielle utilisation illicite[490]. Les deux auteurs comparent la jurisprudence applicable au droit médical[491] et au droit de l'environnement[492] pour justifier de *précédents* **qualifiant de dommage des risques futurs**. Ces risques sont des **préjudices probabilistes, éthérés**[493] reposant sur des *torts* développés par la *Common Law*[494]. Ces dommages se caractérisent par la destruction d'une opportunité future et la perte d'un espoir, c'est-à-dire la forte probabilité de la réalisation d'un risque. Ainsi, à la différence du droit français[495], ces types de dommages basés sur leur réalisation à long terme ne sont pas pour autant soumis à l'attente de leur réalisation[496]. Au lendemain de la violation des données, les victimes, personnes concernées, engagent des frais pour prévenir la réalisation de ces risques, démontrant l'existence de la probabilité de ces risques. Les auteurs rappellent que l'arrêt Spokeo reconnaît que le préjudice immatériel informationnel constitue une base suffisante pour engager une action collective sur le fondement de la *Common Law*. Dans ce cas, plusieurs **facteurs d'appréciation** doivent être pris en compte dans le calcul des dommages et intérêts :

- **le calcul de la vraisemblance et de la magnitude du préjudice subi**[497] s'apprécie en fonction de la criticité des données par rapport à la protection technique accordée. Après avoir souligné que le risque futur[498] est un risque difficilement qualifiable, les auteurs proposent de larges préconisations qui pourraient être reprises par les Cours pour l'appréciation d'un risque futur[499] ;

---

488 Voir dans ce sens, D. SOLOVE, D. K. CITRON, « *Risk and anxiety: a theory of data breach harms* », Texas Law review, 2018, pp. 737-768, spéc. p. 744 : « *Clapper and Spokeo have led to confusion about how harms involving personal data should be conceptualized. To many judges and policymakers, recognizing data-breach harms is akin to attempting to tap dance on quicksand, with the safest approach bieng to retreat to the safety of the most traditional notions of harm* ».

489 Id. p. 757, où les auteurs listent les effets négatifs en précisant le vol d'identité entraînant des prêts ou des dépenses faites par les pirates informatiques.

490 Id. p. 758 : « *In cases involving privacy violations and inadequate data security, consumers bear the lion's share of these costs because courts view them as too attenuated to recognize as harms* ».

491 Cour suprême du Connecticut, Petriello c. Kalman, 576 A. 2d 475 (Con. 1990).

492 Id. p. 762.

493 Pour reprendre le qualificatif de N. LEVIT, « *Ethereal torts* », 61 Geo. Wash. L. Rev. (1992) qui les définit comme étant « *cause of action of expectancy or reliance interests* » (p. 139) soulignant ainsi leur côté non immédiat.

494 Id. p. 761 où les auteurs évoquent les *torts* de risque accru de blessure (« *increased risk of injury* ») que l'on pourrait rapprocher du dommage d'anxiété en droit français, de la perte d'une chance et de la peur d'une maladie.

495 Voir supra §113, page 121, sur la perte d'une chance en droit français.

496 D. SOLOVE, D. K. CITRON, « *Risk and anxiety : a theory of data breach harms* », spéc. p. 763.

497 Id. p. 774-775.

498 Id. p. 775 : « *in many cases, it can be challenging to assess the likelihood and magnitude of future injury with any degree of scientific precision. This is because the potential uses of the data are vast* ».

499 Id. p. 775 : « *Nonetheless, there are factors that suggest the likelihood and magnitude of future injury. Courts can assess how different types of data have been misused in the aftermath of similar data breaches. Courts can look at the means and methods used to exploit different types of data involved in data breaches. Courts should examine the extent that breached data can be aggregated with other available data and the harms that result from the use of the aggregated data* ».

- **le caractère sensible de la donnée et son exposition** s'apprécie en fonction de la publicité du caractère intime et/ou confidentiel de la donnée, qui peut créer un risque substantiel, découlant par exemple d'une fraude ou d'une usurpation d'identité ;
- **les actions d'atténuation instaurées**, comme par exemple en cas de divulgation des numéros de carte de crédit, le remboursement des frais de remplacements de la carte ;
- **les mesures préventives implémentées par le responsable du traitement**, lesquelles correspondent aux moyens concrets et raisonnables visant à prévenir la réalisation de ces risques.

En somme, ces facteurs correspondent à diverses étapes réalisées lors d'une analyse d'impact relative à la protection des données telle que prévue par le RGPD. Les professeurs SOLOVE et CITRON se concentrent sur le dommage sur le fondement de **l'anxiété** en estimant la crainte suscitée par les effets futurs de la violation des données personnelles. L'anxiété est décrite comme « *une forme de détresse émotionnelle qui est un terme générique regroupant une large gamme de sentiments négatifs et perturbants tels que la tristesse, l'embarras* »[500]. À titre d'exemple, M. JONES souligne la corrélation entre les suicides et la divulgation de la base de données des membres pratiquant l'adultère[501]. Ainsi un parallèle peut être établi avec la catégorie de « dommages psychologiques » définies par la méthodologie PRIAM, catégorie qui est décrite par le professeur CALO comme « *un* tort d'assault – *où le dommage est une émotion de la peur* »[502]. De plus, la divulgation incontrôlée des données personnelles révèle des détails de l'intimité de la vie privée, que la personne peut vouloir légitimement dissimuler au regard du public. Cette divulgation recoupe le droit coutumier au respect de la vie privée étasunien[503], qui lui-même, englobe la réparation de la détresse émotionnelle[504]. Ainsi, D. SOLOVE et D. K. CITRON dressent la liste des différents « *privacy torts* » rendant le préjudice d'anxiété éligible à la qualification de dommage réparable. Parmi ces *privacy torts* se trouvent :

- la détresse émotionnelle (*emotional distress tort*) correspond, par exemple, à la publication d'une photographie d'une femme politique en sous-vêtements[505] ;
- la perturbation émotionnelle (*emotional disturbance tort*) découle de certains types de comportement, dans des conditions spécifiques, qui peuvent être profondément offensants et psychologiquement dommageables pour d'autres personnes, même en l'absence de menace de dommage physique imminent[506] ;
- le délit d'intrusion dans la vie privée (*tort of intrusion upon seclusion*) est constitué par exemple dans l'hypothèse d'une surveillance accrue de salariés syndiqués par des employeurs[507] ;
- le délit de violation de la confidentialité (*breach of confidentiality tort*) sanctionne la divulgation d'informations confiées par la victime à une profession régulée[508].

---

500 Citant, p. 764, l'exemple du piratage de la base de données d'Ashley Madison.

501 S. N. JONES, « *Having An Affair May Shorten Your Life: The Ashley Madison Suicides* », 33 Ga.St.U. L. Rev.455 (2017).

502 Voir R. CALO, « *Privacy Harm Exceptionalism* », 12 Colo. Tech. L. J. 361 (2014).

503 S. WARREN, L. BRANDEIS, « *The right to privacy* », 4 harv. L. Rev., 193 (1890).

504 Cour suprême de Californie, Molien v. Kaiser Foundation Hospitals, 27 Cal. 3d 916, (1980) et Cour suprême de l'Ohio, Schultz v. Barberton Glass Co, 447 N.E.2d 109 (Ohio 1983), 82-316.

505 Cour fédérale du Colorado. Doe v. Hofstetter No. 11-cv-02209-DME-MJW, 2012 WL 3398316, (D. Colo. Aug. 14, 2012) et Cour suprême d'Alabama, Daily Times Democrat v. Graham - 276 Ala. 380, 162 So. 2d 474 (1964).

506 Cour suprême du Massachusetts, George v. Jordan Marsh Co. - 359 Mass. 244, 268 N.E.2d 915 (1971).

507 Qui reconnaît la détresse mentale. Voir dans ce sens Cour fédérale du Southern District de l'État de New-York, Socialist Workers Party v. Attorney General of US, 642 F. Supp. 1357 (S.D.N.Y. 1986).

508 Cour d'appel de l'État du Kentucky, Douglas v. Stokes ,149 S.W. 849 (Ky.App. 1912), plus limitée que les propositions doctrinales (voir par exemple, le professeur LITMAN qui proposait un « *tort-based —breach of trust approach for data privacy protection because —[a] relational approach (. ..) carries significant intuitive appeal‖ and —its scope can easily be limited by confining the definition of a qualifying relationshi* », in J. LITMAN, « *Information Privacy/Information property* », 52 Stan.L. Rev. (2000)).

Les *torts* définis par la *Common Law* permettent au juge de recourir aux *remedies*[509] comme moyen de réparation du dommage. En raison de leur caractère informel, ces *remedies* sont des solutions plus souples que les règles légales.

B. Le droit à réparation pour une mauvaise utilisation d'une information privée en droit anglais

1. *Le* misuse of private information*, fondement à un préjudice découlant d'un traitement défaillant de données personnelles*

124 Le droit anglais oscillait entre deux fondements pour reconnaître un droit à la personne concernée d'obtenir réparation pour un préjudice découlant de l'utilisation non autorisée de ses données personnelles. Ainsi, les différentes Cours d'appels d'Angleterre et d'Écosse se basaient soit sur l'application du *Misuse of Private Information* (MPI), soit sur la section 13(1) du *Data Protection Act* relative au droit à la réparation d'un dommage découlant de la violation du droit à la protection des données personnelles. L'arrêt **Lloyd v. Google**[510] **de la Cour d'appel d'Angleterre et d'Écosse** unifie les deux régimes pour accorder une indemnisation au seul titre de la réparation du préjudice subi par la personne concernée.

Le MPI est un *tort* consacré par l'arrêt **Gulati v. MGN Ltd**[511] sur la base de l'article 8 de la Charte des Droits fondamentaux de l'Union européenne. Cette solution reconnaît un droit de réparation à la personne concernée en cas d'utilisation illicite de ses données personnelles par un responsable du traitement non autorisé l**orsque l'information privée a été divulguée sans son consentement**. Le principe de la réparation est accepté sans exiger la production d'une preuve démontrant une perte pécuniaire ou un dommage moral. La divulgation de l'information fonde seule l'indemnisation. Ainsi une vulnérabilité organisationnelle conduisant à la divulgation de données personnelles par le responsable du traitement peut engager la responsabilité civile de ce dernier. De nombreuses actions de groupe anglo-saxonne illustrent ce moyen. À l'instar du droit étasunien, la procédure anglaise comprend deux étapes : l'acceptation de la formation d'une action de classe respectant les conditions posées par l'article 19.6. du *Civil Procedure Rules*, puis les débats et le jugement en lui-même.

En parallèle à cette vision favorable à la personne concernée basée sur le MPI, une approche plus restrictive est adoptée par d'autres juges d'appel sur le fondement de la section 13 du *Data Protection Act* relative à l'indemnisation d'un dommage découlant d'une utilisation illicite des données personnelles. Bien que reconnaissant l'existence d'un MPI, l'arrêt **Vidal-Hall v. Google**[512] conditionne ainsi le droit à réparation à la production de la preuve d'un préjudice de détresse (« *distress* ») lié soit à un dommage subi par la personne en raison de la violation par le responsable de traitement de l'une des exigence du *Data Protection Act* (Section 13 §2a), soit à une infraction concernant le traitement de données personnelles à des fins particulières (Section 13 §2b)[513].

---

509 C'est-à-dire des mesures d'exécution jugées arbitrairement par le juge permettant, par exemple, de restreindre la diffusion de photographies (in Doe v. Hofstetter, D. colo. 13 juin 2012).

510 Lloyd v. Google [2019] EWCA civ 1599, https://www.judiciary.uk/wp-content/uploads/2019/10/Google.finaldraftjudgment.approved-2-10-19.pdf.

511 Cour d'appel d'Angleterre et du Pays de Galles, Gulati v. MGN LTD [2015] EWHC 1482.

512 Vidal-Hall v. Google [2014] EWHC 13 (QB), https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf.

513 Ainsi, selon la Section 13 : « *(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage. (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if— (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes* ».

125 En 2019, l'affaire **Lloyd v. Google**[514] du 2 octobre 2019 reprend en partie les solutions antérieures. Dans un premier temps, l'arrêt Gulati est invoqué pour rappeler que la personne concernée est libre de définir les modalités de partage de ses données. Ainsi, les arguments de Google arguant de l'indifférence de certaines personnes à partager leurs données personnelles sont rejetées, le juge soulignant que la valorisation des données par Google entraîne un droit de réparation en cas d'utilisation non autorisée des données personnelles. En assimilant ainsi les mésusages d'une information privée au droit des données personnelles, le juge souligne le droit des personnes concernées à être indemnisées en cas de divulgation et de réutilisation non autorisée de leurs données personnelles. Mais dans un second temps, la référence à l'affaire Vidal-Hall permet au juge de restreindre l'indemnisation accordée à la personne concernée. En effet, le juge rappelle que les précédents se situent dans **une logique de réparation et non de dommages et intérêts punitifs, limitant ainsi l'étendue des dommages et intérêts**. Le juge d'appel renverse cette solution en étendant les préjudices prévus par l'article 13 du *Data Personal Act* aux dispositions de l'article 23 de la Directive 95/46 CE, prévoyant la possibilité d'une réparation en cas de « *dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions (…) de la présente directive* ». L'article 23 de la directive 95/46/CE est ici interprété de façon large, le juge se référant également au considérant 85 du RGPD.

2. *L'exonération de la responsabilité de l'employeur en cas de traitement illicite de données personnelles réalisé à son insu par son salarié en droit anglais*

126 L'apport de l'arrêt **Morrison**[515] rendu le 1er avril 2020 par la Cour suprême d'Angleterre se situe dans la seconde étape d'une action de classe. En l'espèce, une violation de données personnelles de ressources humaines a été commise par un salarié mécontent. Pour s'exonérer de sa responsabilité de plein droit, l'employeur démontre que le salarié est seul fautif et que ses actions ont été volontairement réalisées dans une intention de nuire à son employeur. Les victimes estiment quant à elles que l'employeur est responsable des agissements de son préposé. Leur argumentaire souligne que le *Data Protection Act* ne prévoit pas le type d'exonération avancé par le défendeur. Ainsi après avoir rappelé que le *Data Protection Act* a pour but de transposer la directive 95/46/CE, remplacée depuis par le RGPD, le juge fait droit aux arguments de l'employeur, l'exonérant de l'intégralité de sa responsabilité. L'argumentation du défendeur repose sur l'invocation d'une combinaison de jurisprudences. Parmi celles-ci, l'arrêt Fashion ID[516] dans lequel la CJUE décrit les principes de responsabilité conjointe par une lecture littérale de la définition de la notion de responsable du traitement tel que posée par l'article 4 du RGPD. Le responsable du traitement étant la personne qui « *détermine les finalités et les moyens du traitement* », le salarié est éligible à cette qualification dès lors qu'il traite des données personnelles sans l'autorisation de son employeur. Cette absence d'autorisation permet à l'employeur de se fonder sur le précédent Majrowski[517] précisant, qu'en l'absence d'une norme législative contraire, la responsabilité du fait de l'employeur est exclue. Le RGPD ne précisant pas que le responsable de traitement doit être tenu responsable des agissements de son salarié, la Cour juge qu'un salarié mal intentionné décidant de partager des données personnelles collectées par un responsable du traitement n'engage pas la responsabilité civile de ce dernier. Cette solution est, comme nous l'avons vu, difficilement transposable en droit français.

---

514 Cour d'appel d'Angleterre et du Pays de Galles, Lloyd v. Googlr [2019] EWCA civ 1599, https://www.judiciary.uk/wp-content/uploads/2019/10/Google.finaldraftjudgment.approved-2-10-19.pdf.

515 Cour suprême du Royaume-Uni, WM Morrisons Supermarkets plc (Appellant) c. Various Claimants [2020] UKSC 12.

516 CJUE, 29 juil. 2019, C-40/17, Fashion Id Gmbh & Co.

517 House of Lords, Majrowski (2007), 1. AC 224.

Section 2. Les amendes administratives et dommages-intérêts issus d'un préjudice lié à une violation des données personnelles

L'article 82 du RGPD consacre le droit des personnes concernées « *ayant subi un dommage similaire* » à intenter des actions de groupe à l'encontre d'un/des responsable(s) du traitement. La présente analyse mettra en exergue l'appréciation d'un risque collectif, devant faire l'objet d'une analyse d'impact selon la méthodologie PRIAM, et d'un risque financier, également envisagé par la méthodologie BSI. En la matière, le droit européen comme le droit français n'apportent aucune réponse procédurale précise sur le calcul des dommages-intérêts liés à un risque collectif ou financier (Sous-Section 1). Pour leur part, les droits étasuniens et anglais posent certaines limitations à la réparation d'un dommage collectif causé par un fait générateur unique (Sous-Section 2, page 142).

Sous-Section 1. Les modalités de calcul des dommages et intérêts lié à un risque collectif ou financier en droit européen et français

Tout d'abord, les grands principes du droit européen seront examinés pour déterminer les modalités de calcul du montant d'une amende administrative (A). Il en ressort qu'une amende administrative peut aussi être qualifiée d'amende pénale, qualification qui n'est pas sans conséquences sur les modalités procédurales devant être observées par le juge judiciaire (B, page 140).

A. Les modalités de calcul du montant d'une amende administrative en droit européen

127 La jurisprudence de la CEDH a reconnu en 2013 le principe de la « *satisfaction équitable* »[518]. Ce principe a un impact direct sur la réparation accordée aux personnes concernées par les tribunaux judiciaires, car il va au-delà du principe de réparation intégrale en contraignant le juge à se préoccuper de la réparation des dommages moraux. Ainsi, l'arrêt Trevalec manifeste la volonté réelle de la CEDH de faire évoluer le droit[519]. Bien que fortement critiquée[520] et limitée à une décision, la Cour européenne des droits de l'homme invite à ne pas considérer cette jurisprudence comme un arrêt d'espèce[521]. Les faits sont les suivants : un journaliste français, demandeur, accompagne une opération policière belge, durant laquelle il est touché par deux balles tirées par des policiers. Le journaliste obtient des Cours belges une réparation limitée, tout en recevant une réparation complémentaire de la Commission d'indemnisation des victimes d'infractions (CIVI) française. Le requérant estime que ces réparations ne couvrent que partiellement son préjudice moral et conteste la compétence de l'autorité française, État qui est certes de sa nationalité mais qui n'est pas l'État ayant commis la violation. La CEDH fait droit à ces arguments. Tout en rappelant que l'État français n'a pas vocation à être garant des intérêts belges, la Cour accepte le moyen soutenant l'existence d'un préjudice moral issu du dommage corporel de la victime. Cette reconnaissance du dommage corporel n'est cependant que très peu motivée. L'opinion concordante du Juge PINTO ALBURQUERQUE souligne que l'objectif ici est de sanctionner l'absence de mesures prises par les autorités belges à l'encontre des policiers. La Cour applique le principe de la satisfaction

---

518 Voir dans ce sens l'arrêt CEDH, Trevalec c. Belgique, 25/06/2013, req. 30812/077.

519 Voir dans ce sens l'opinion concordante du juge ALBUQUERQUE, dans l'arrêt CEDH Big Brother p. 12 : « *Le temps est donc venu pour la Cour d'assumer, en termes clairs, le bien fondé de ce principe émergent, qui offre un instrument crucial d'application du droit européen des droits de l'homme et de renforcement du système de protection de ces droits. Ce faisant, elle contribuera aussi à l'évolution du droit de responsabilité internationale de l'État et fera ainsi avancer la légalité internationale face aux gouvernements, autorités publiques et représentants de l'État non respectueux des droits de l'homme* ».

520 Voir dans ce sens P.-Y. GAUTIER, « *La CEDH poursuit la révolution normative* », D. 2013, p. 2106 et O. SABARD, note D. 2013, p. 2139.

521 Voir dans ce sens, C. QUÉZEL-AMBRUNAZ, « *Des dommages et intérêts octroyés par la Cour européenne des droits de l'homme* », RDLF 2014, Chron. n°5.

équitable dès lors que le droit interne n'offre pas une réparation efficace des conséquences d'une violation[522]. Ce principe de la satisfaction équitable invite dépasse le principe de la réparation intégrale limitée au seul préjudice subi, en y intégrant la réparation des préjudices moraux. Les instructions de la CEDH invitent les juridictions des États membres à mieux prendre en compte, dans un but d'indemnisation[523], la réparation du préjudice moral[524]. Ce préjudice peut être accordé sur le fondement de l'article 8 de la Convention ESDH à un demandeur lors d'un contentieux relatif aux données personnelles.

128 Le principe de la « *satisfaction équitable* » est d'autant plus susceptible de s'appliquer que les Lignes directrices du Comité européen de la protection des données sur l'application et la fixation des amendes administratives[525] sont soumises au droit de la Convention ESDH. Les amendes administratives étant considérées comme relevant de la matière pénale, l'article 6 de la Convention ESDH relatif au droit à un jugement équitable est applicable. L'assiette de risques aux droits et libertés des personnes concernées doit être également élargie. En effet, l'anticipation des amendes administratives correspond, à la fois, à des obligations légales[526] et à des risques financiers à prendre en compte par les méthodologies BSI et NIST[527]. Or les Lignes directrices du CEPD sont imprécises quant à la pondération des différents facteurs dans le calcul et donc la détermination des amendes administratives. Cette imprécision est renforcée par sept renvois explicites aux législations internes. Toutefois, et hormis l'applicabilité des garanties fournies par les contrats d'assurance, l'éligibilité de ces amendes à la qualification de l'amende en matière pénale entraîne de nombreuses questions procédurales judiciaires[528]. En effet, les modalités de calcul de l'amende administrative telles que décrites ci-dessous suggèrent une amende au sens pénal du terme. L'arrêt **Jussila** rendu par la Grande chambre de la CEDH[529] définit les conditions d'éligibilité d'une procédure à la qualification pénale entraînant l'application des articles 4 et 6 de la Convention ESDH[530]. À cet égard, trois conditions doivent être remplies :

- **l'acte d'accusation** qui désigne « *la notification officielle* », servant de point de départ à une enquête ou à une procédure, doit « *éman(er) d'une autorité compétente, (formulant le) reproche d'avoir accompli une infraction pénale* » impliquant « *des répercussions importantes sur la situation du suspect* »[531]. « *L'acte d'accusation* »[532] comprend également les enquêtes administratives établissant les faits servant de point de départ aux poursuites administratives.

---

522 Voir dans ce sens CEDH, « *Demandes de satisfaction équitable, instructions pratiques* », https://www.echr.coe.int/Documents/PD_satisfaction_claims_FRA.pdf.

523 Dans ce sens S. CARVAL, « *La responsabilité civile dans sa fonction de peine privée* », LGDJ, 1995, T. 250 n°189 : « *les dommages et intérêts ainsi alloués sont bel et bien des « peines privées » qui viennent sanctionner, à l'instar de la sanction pénale à laquelle ils s'ajoutent, un comportement répréhensible* ».

524 Que l'on retrouve dans la méthodologie PRIAM sous la nomenclature d' « *atteinte psychologique* ».

525 CEPD, Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 du 3 octobre 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

526 Voir supra §76, page 87, sur le *Sorbane Oaxley Act* étasunien.

527 Voir dans ce sens la méthodologie BSI qui invite à prendre en compte les sanctions. Outre ce risque, la méthodologie NIST requiert également le coût de régularisation des traitements de données en cas de condamnation.

528 Voir infra §133, page 140, et suivants.

529 CEDH, Grde ch., 23 nov. 2006, Jussila c. Finlande, Req n°73053/01.

530 Respectivement le principe *non bis in idem*, c'est-à-dire l'interdiction de deux jugements pour les mêmes faits, et le principe d'un procès équitable.

531 CEDH, 28 juin 1976, König c. RFA.

532 CEDH, 17 déc. 1996, Saunders c. Royaume-Uni.

- **la nature du fait ou du comportement transgresseur** est « *un élément d'appréciation d'un plus (grand) poids* »[533] qui se subdivise en sous-critères comprenant la protection de l'ordre public, la protection de la norme plutôt que celle d'un groupe particulier[534] avec pour objectif d'être « *à la fois dissuasif et répressif et pas seulement réparateur* »[535].
- **la nature et le degré de la sanction prononcée ou exécutée**, la sévérité étant analysée en fonction du but, de la nature et des modalités d'exécution de la sanction. Le critère dissuasif de cette sanction conduit à la qualifier de sanction pénale[536].

L'arrêt **Jussila** de la CEDH rappelle que ces critères sont alternatifs. Cependant, le juge européen se focalise en priorité sur le deuxième critère pour définir la matière pénale, c'est-à-dire l'atteinte à l'ordre public. L'arrêt **A et B c. Norvège**[537] étend, en 2016, cette solution aux contentieux traités par les autorités nationales de contrôle[538]. En pratique, il importe donc de lire attentivement les délibérations de la CNIL pour en déduire si cette dernière prononce ou non des sanctions pénales. Dans l'affirmative, il est alors possible d'apprécier l'étendu de la responsabilité pénale à laquelle s'expose le responsable du traitement. Deux conséquences peuvent être concrètement reliées aux AIPD. Les sanctions pénales permettront pour les méthodologies CNIL et PRIAM d'affiner en priorité les risques au regard des droits et libertés des personnes concernées et pour les méthodologies BSI et NIST de mieux prendre en compte l'ensemble des risques encourus par les responsables du traitement grâce aux métriques déduites à partir des délibérations de la CNIL.

129 Ces délibérations, à caractère pénal, se conforment aux lignes directrices du Comité européen de protection des données relatives aux amendes administratives. Celles-ci poursuivent deux objectifs.

Tout d'abord, le respect du besoin d'« **équivalence** » des sanctions est souligné afin d'assurer une protection uniforme des données personnelles dans l'Union européenne et ainsi d'éviter de créer une distorsion de concurrence.

Le second objectif est de conférer un **caractère répressif** aux mesures correctives imposées par les autorités nationales de contrôle. Ces mesures se décomposent en deux catégories : les amendes administratives sur le fondement de l'article 83 du RGPD et les injonctions en nature qui peuvent être prononcées sur le fondement de l'article 58-2° du RGPD. Selon cet article, chaque autorité de contrôle dispose du pouvoir :

a) d'avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ;
b) de rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement ;
c) d'ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement ;
d) d'ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ;

---

533 CEDH, 24 sept. 2007, Irfan Bayrak c. Turquie, Req. n°39429/98.

534 Id.

535 CEDH, 21 févr. 1994, Bendemoun.

536 CEDH, 8 juin 1976, Cour plénière, Engel c. Pays-Bas req. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72.

537 CEDH, 15 nov. 2016, A et B c. Norvège.

538 Voir C.E. 12 mars 2014, Société pages jaunes Groupe, sur la soumission de la CNIL aux dispositions de l'article 6 de la Convention ESDH.

e) *d'ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel ;*
f) *d'imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;*
g) *d'ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19 ;*
h) *de retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;*
i) *d'imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas ;*
j) *d'ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.*

Parmi ces différentes prérogatives juridictionnelles, des résonnances avec les AIPD peuvent être trouvées. Le point (a) permet à l'autorité de contrôle d'avertir le responsable du traitement de la survenance d'un risque. Les points (c) et (e) offrent la possibilité de régulariser les risques de non-conformité du traitement. Enfin, le point (g) fait écho à la seconde étape de l'AIPD, c'est-à-dire l'étape de la conformité, ainsi qu'aux principes de *Data Protection by design and by default* en rappelant l'obligation pour le responsable du traitement de contrôler le flux des données personnelles. Soulignons que ces différentes mesures peuvent se cumuler pour s'assurer que la violation du RGPD soit atténuée au maximum tout en réparant dans les meilleures conditions l'atteinte à l'ordre public occasionnée. Le rappel à l'ordre prévu par le point (b), par exemple, peut concerner des « *violations mineures* » mentionnées par le considérant 148 du RGDP[539]. Ces dernières renvoient à des violations pouvant être rapidement régularisées[540]. En ce qui concerne les violations dites « *majeures* », le droit européen pourrait s'inspirer du droit étasunien en important les solutions développées dans le cadre du mécanisme de la transaction extra-judiciaire. Ces solutions contractuelles, employées par la FTC, présentent une plus grande modularité. Notamment, les autorités de contrôle européennes pourraient contraindre le responsable du traitement défaillant à instaurer des garanties appropriées au sein de la gouvernance de son entreprise, comme la création d'un comité indépendant chargé de surveiller la conformité des traitements de données personnelles accompagné d'une obligation de *reporting* auprès de ces mêmes autorités. Cependant, l'imposition de ce type de mesures nous semble difficilement transposable car l'article 58-2 du RGPD relatif aux mesures correctives que peuvent imposer les autorités nationales de contrôle est, de par sa nature pénale, d'application stricte. La révision du RGPD devrait selon nous permettre aux autorités de contrôle de recourir à la transaction extra-judiciaire.

130 Les modalités de fixation des amendes administratives prévues par l'article 83 du RGPD sont également précisées par les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement du Comité européen de protection des données. Ces modalités, exposées ci-dessous, peuvent être utilisées pour déterminer le risque financier auquel le responsable du traitement s'expose. Ici le principe des mesures et *a fortiori* des amendes administratives, est de « *répondre de manière adéquate à la nature, à la gravité et aux conséquences de la violation* » *tout en respectant un « caractère effectif, proportionné et dissuasif (…) en considération (de) l'objectif poursuivi (…) à savoir de restaurer le respect des règles ou de sanctionner un comportement illicite*

539 Selon le considérant 148 du RGPD : « *En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende* ».

540 Voir dans ce sens Cour suprême du Royaume-Uni, Lloyd c. Google, §55. « *That threshold would undoubtedly exclude, for example, a claim for damages for an accidental one-off data breach that was quickly remedied* ».

(ou les deux) ». Les lignes directrices précisent ces conditions tout en soulignant la nécessité pour l'autorité de contrôle de prendre en compte la spécificité de chaque affaire et de déterminer s'il s'agit d'une violation « *mineure* »[541] ou d'une violation « *majeure* ». La première catégorie correspond à une « *violation (qui) n'engendre pas un risque important pour les droits des personnes concernées* »[542]. La seconde catégorie repose sur une appréciation portant sur « *la nature, la portée ou la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi* »[543]. Les variations entre les différents types de « *violations* » peuvent être mis en parallèle avec les risques. En effet, cette disparité invite, à l'instar des préconisations de la méthodologie CNIL, à l'implémentation en priorité les mesures permettant de réduire les risques graves, et donc de retarder la mise en œuvre des mesures relatives aux violations mineures.

Le CEPD prend en compte dans le calcul de l'amende administrative l'évaluation du nombre de personnes victimes de la violation, pour en déterminer son étendue. Cette détermination se fait par exemple par le calcul « *(du) nombre total de déclarants dans la base de données en cause, (du) nombre d'utilisateurs d'un service, (du) nombre de clients ou à la population du pays* »[544]. La pratique des autorités nationales de contrôle, et de la CNIL en particulier, révèle néanmoins une évaluation floue quant à la définition du nombre de victimes[545]. Il pourrait être intéressant de voir si cette imprécision dans une délibération de la CNIL peut constituer un fondement recevable d'appel.

Les Lignes directrices rappellent que les autorités de contrôle nationale doivent également vérifier l'application du principe de la spécificité des **finalités** et de l'utilisation compatible des données. Une mauvaise application de ce principe doit être pris en compte dans l'évaluation de l'amende administrative.

Les Lignes directrices précisent également l'application du considérant 75 du RGPD[546] qui définit largement le critère du dommage subi par les personnes concernées. Dans le cas spécifique

---

541 Voir supra §120, page 128 sur les mesures alternatives, et voir CEPD, Lignes directrices sur l'application et la fixation des amendes administratives, p. 9-10.

542 Où l'on retrouve le principe de *minimis* posé par la CEDH (supra Chapitre 1, Section 2, page 107).

543 Article 83-2°-a du RGPD.

544 Voir CEPD, Lignes directrices sur l'application et la fixation des amendes administratives p. 11.

545 Voir dans ce sens CNIL, **Délibération de la formation restreinte n°SAN-2020-012 du 7 décembre 2020 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED**, §125 : « *Elle souligne que le moteur de recherche Google Search comptabilisant au moins 47 millions d'utilisateurs en France, ce qui correspond à 70% de la population française, le nombre de personnes concernées par le traitement est extrêmement important* », puis §137 « *Elle souligne qu'en raison de la portée du moteur de recherche Google Search en France ces pratiques ont affecté près de cinquante millions d'utilisateurs résidant en France* », CJUE, Grande chambre, 06 oct. 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner, §78. « *Il convient de constater que, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, du nombre important de personnes dont les droits fondamentaux sont susceptibles d'être violés* ».

546 Selon le considérant 75 du RGPD : « *Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées* ».

de l'amende administrative, l'imposition d'une telle amende : « *ne dépend pas de la capacité de l'autorité de contrôle à établir un lien de cause à effet entre la violation et le préjudice matériel* »[547]. Ainsi, l'autorité de contrôle est tenue uniquement de prouver l'existence de la violation.

À cet égard, elle doit apprécier la **durée** de la violation en cas :

- D'acte intentionnel,
- D'omission de prise des mesures préventives appropriées, ou
- D'incapacité de mettre en place les mesures techniques[548].

De cette durée est déduite l'**intention**, pour considérer un éventuel caractère atténuant ou aggravant à partir d'« *éléments objectifs de comportement déduits des faits de l'espèce* ». Ce critère d'intention est utilisé pour calculer l'amende administrative.

En pratique, les autorités nationales de contrôle ne se basent pas sur l'ensemble des critères que nous venons d'énoncer. Ainsi, la délibération de la CNIL prononçant à l'encontre de Google une amende de 60 millions d'euros se contente de constater la seule violation au RGPD et à la directive ePrivacy[549].

131 La première incidence pratique du caractère pénal de l'amende administrative concerne la possibilité de bénéficier de la garantie offerte par un contrat d'assurance. Si une amende administrative est prononcée à l'encontre du responsable du traitement, la réserve prévue par l'article L 113-1 alinéa 2 du Code des assurances s'applique. Cet article interdit le bénéfice du contrat d'assurance en s'appuyant sur le principe de l'exclusion des « *fautes intentionnelles* », parmi lesquelles figurent les infractions pénales reconnues par un tribunal. Ne constitue pas une telle faute, selon les lignes directrices du CEPD sur l'application et la fixation des amendes administratives[550], l'absence de caractère intentionnel comme dans l'hypothèse du piratage d'une base de données personnelles répondant aux bonnes pratiques en matière de sécurité informatique. Par ailleurs, les praticiens[551] distinguent les amendes à but dissuasives des amendes prononcées à des fins de régularisation, couvertes par les garanties prévues par les contrats d'assurance.

L'impossibilité de souscrire une assurance couvrant à la fois les amendes administratives et les dommages et intérêts accordés, à titre individuel ou collectif, aux personnes concernées victimes n'est pas sans impacter les situations où un traitement de données personnelles est effectué par une filiale d'une entité européenne. En effet, le *Sarbane Oxley Act* étasunien impose au responsable du traitement soit de prendre une assurance équivalente à toute amende potentiellement applicable à une société exerçant aux États-Unis[552], soit d'anticiper les dommages et intérêts en provisionnant une somme d'argent équivalente en cas de sanctions judiciaires ou administratives. Pour ce faire, il peut être utile d'utiliser les méthodologies NIST et BSI qui proposent de chiffrer les risques financiers liés à une mauvaise gestion de données personnelles.

---

547 CEPD, Lignes directrices sur l'application et la fixation des amendes administratives, p. 12.

548 CEPD, Lignes directrices sur l'application et la fixation des amendes administratives, p. 12.

549 CNIL, Délibération n°SAN-2020-12 du 7 déc. 2020.

550 CEPD, 3 oct. 2017, Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

551 N. HELENON, C. HESLAUT, « *Données personnelles : l'assurabilité des sanctions administratives* », Expertises, 2017, n°424 p. 180-184.

552 Sur ce sujet voir C. FERTE, R. LABAT, « *L'alerte professionnelle et la loi Sapin 2* », Option droit et affaires, 2017, n°371, p. 10-11.

132 La seconde problématique découlant du caractère pénal de l'amende porte sur la hiérarchisation des procédures contentieuses pouvant être invoquées par la personne concernée. En effet, les articles 80 et suivants du RGPD ne posent aucun critère à ce sujet. Si en France, la CNIL est considérée comme une autorité répressive, l'article 4 du Code de procédure pénale codifiant le principe du pénal tenant le civil en l'état, s'applique dans l'hypothèse d'une action à but répressif[553]. Cette application suspend alors toute action engagée devant le juge civil, notamment l'impossibilité pour le juge d'apprécier la responsabilité du responsable du traitement en cas d'actions collectives[554]. Celui-ci, tenu par la décision de la CNIL réunie en section du contentieux, n'a plus que pour seule compétence résiduelle la prononciation des dommages et intérêts accordés aux personnes concernées victimes.

B. Le régime des dommages et intérêts dans les actions de groupe

133 La possibilité pour les personnes concernées d'engager des actions de groupe constitue une évolution juridique majeure impactant directement l'appréciation des risques. Ainsi, la méthodologie CNIL effectue une lecture stricte des lignes directrices du CEPD sur l'analyse d'impact relative à la protection des données en ne prenant en compte que les risques individuels, c'est-à-dire du point de vue d'une seule personne concernée. À l'inverse, les méthodologies NIST et PRIAM invitent à considérer les risques collectifs et sociétaux, c'est-à-dire une atteinte touchant un groupe de personnes ou la société dans son ensemble[555]. L'article 80 du RGPD adopte une approche similaire en créant des procédures d'intérêt à agir collectif.

Plus précisément, l'**article 80**-1° du RGPD porte sur l'**action de groupe**. Il permet à un organisme spécialisé dûment mandaté (une association à but non lucratif qui a été valablement constituée conformément au droit national) par une ou plusieurs personne(s) concernée(s) d'introduire une réclamation en son nom devant les juridictions judiciaires ou administratives pour faire cesser ou sanctionner les traitements problématiques d'un responsable du traitement et d'exercer son droit à réparation. En d'autres termes, cette voie procédurale agrège en une seule action les demandes des personnes concernées pour leur permettre d'obtenir une réparation. Pour sa part, l'article 80-2° du RGPD porte sur l'**action collective**. Il offre la possibilité à tout organisme visé au paragraphe 1, indépendamment de tout mandat confié par la personne concernée, d'introduire une réclamation auprès d'une autorité nationale de contrôle et d'exercer un recours juridictionnel contre cette même autorité, ou contre un responsable du traitement ou un sous-traitant afin d'obtenir une somme forfaitaire symbolique. La finalité de cette procédure est de permettre la sanction d'un acte contraire à l'intérêt général.

Soulignons ici que l'action de groupe et l'action collective ne sont pas totalement inconnues du droit français. La loi pour une République Numérique du 7 octobre 2016[556], et la loi de modernisation de la justice du 18 novembre 2016[557] ont en effet organisé la possibilité de tels recours pour les consommateurs, antérieurement à a loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

134 Toutefois, l'article 25 de la loi pour la protection des données personnelles transposant l'article 80-1° vise explicitement notre matière. Cette action de groupe prévoit une procédure subdivisée en deux temps.

---

553 Voir supra §130, page 137.

554 Voir infra §138, page 144.

555 Lors de nos entretiens, Daniel LE METAYER cite l'exemple de Cambridge Analytica pour illustrer ce risque.

556 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016. https://www.legifrance.gouv.fr/jorf/jo/2016/10/08/0235.

557 Art. 60 à 92 de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, JORF n°0269 du 19 novembre 2016, Texte 1.

La première partie de la procédure porte sur la reconnaissance par le juge administratif ou judiciaire d'un fait générateur ayant entraîné un dommage individuel à une pluralité de personnes concernées. Comme nous le verrons, à la différence du juge étasunien et anglais, cette reconnaissance permet aux personnes concernées d'obtenir la réparation de leur préjudice individuel. La seconde étape de la procédure porte sur la détermination de la réparation en tant que telle. La problématique judiciaire est ici de déterminer si le juge doit prendre en compte le préjudice propre à chaque partie et en déduire un montant adapté à chaque personne concerne ou s'il doit prononcer un montant fixe et forfaire, ou encore si les deux options se cumulent. À cet égard, la loi de modernisation de la justice du XXIe siècle éclaircit peu ou pas ce point. De son côté, la Chambre criminelle de la Cour de cassation a jugé de l'absence de confusion des préjudices subis au titre de l'intérêt des consommateurs avec ceux subis individuellement[558]. En d'autres termes, les dommages et intérêts auxquels est éligible l'association mandatée sont différents de ceux des victimes, mandataires.

135 Le montant des dommages et intérêts alloués par le juge judiciaire dans les contentieux de presse n'est pas une chose aisée à déterminer. D'une part, les montants prononcés dans le cadre des contentieux relatifs à la protection de la vie privée fondée sur l'article 9 du Code civil, connexe au droit des données personnelles, sont souvent faibles. Le préjudice s'apprécie au moment de la publication[559] des informations relatives à l'intimité de la victime sans prendre en compte un éventuel préjudice ultérieur ; seule la notoriété de la victime permet d'accorder des dommages et intérêts élevés. D'autre part, les juges sont invités à refuser de prendre en compte les profits réalisés par le responsable via une atteinte à la vie privée, les profits réalisés devant « *rester étrangers à l'évaluation des dommages et intérêts qui n'ont pas pour objet de sanctionner un comportement ou d'avoir (…) un effet dissuasif mais doivent être évalués en fonction du seul dommage subi par la victime conformément aux principes généraux du droit de la responsabilité* »[560]. Cependant la souveraineté des juridictions dans l'appréciation des faits leur permet d'inclure un « *accent punitif* »[561]. Enfin, le juge doit justifier le montant de la réparation du préjudice moral[562], interdisant le recours à la « *condamnation symbolique* »[563].

En la matière, le Professeur LE TOURNEAU souligne l'imprécision de l'appréciation des juges dans les contentieux relatifs à la protection de la vie privée qui distinguent les « *faits relevant in abstracto de la sphère privée (de ceux) d'atteinte à la vie privée* »[564]. Le Professeur MOLFESSIS compare cette souveraineté peu motivée à l'avènement de dommages et intérêts punitifs dissimulés sous

---

558 Voir dans ce sens Cass. Crim., 20 mai 1985, n°84-91606.

559 A. LEPAGE, « *Précisions sur les modes de réparation du préjudice en matière d'atteintes à la vie privée et à l'image* », D. 2003, p. 1542.

560 C.A. Toulouse, 25 mai 2004, CCE 2005, n°17, note A. LEPAGE, Droit à l'image. Également, TGI Toulouse, 24 mai 2004, « *les profits réalisés par le journal doivent en effet rester étrangers à l'évaluation des dommages et intérêts qui n'ont pas pour objet de sanctionner un comportement ou d'avoir pour la presse un effet dissuasif mais doivent être évalués en fonction du seul dommage subi par la victime conformément aux principes généraux du droit de la responsabilité civile* », de jurisprudence constante depuis Cass. Civ. 2e, 8 mai 1964, JCP 1965, IIL 131140 note P. ESMEIN.

561 P. LE TOURNEAU, « *Droit de la responsabilité et des contrats* », Dalloz Action, 2019, p. 2702.

562 Voir dans ce sens J. KNETSCH, « *La désintégration du préjudice moral* », D. 2015 p. 443, « *Le dénominateur commun de l'ensemble des chefs de préjudice extrapatrimoniaux reconnus par le droit français est le lien intime avec la personnalité de la victime. Que ce soit le préjudice esthétique, le* pretium doloris*, le préjudice d'établissement ou le préjudice d'affection, les conséquences non économiques du dommage corporel visent à appréhender les souffrances et relèvent donc exclusivement du ressenti de la victime et non de son patrimoine.* » L'auteur critique l'inadéquation de la nomenclature Dinthillac pour les préjudices moraux.

563 Cass. Crim., 14 janv. 1997, n°96-82.264.

564 P. LE TOURNEAU, Droit de la responsabilité et des contrats, spéc. p. 597, § 2125.261 citant l'arrêt de la Cass. Civ. 1ère du 3 avr. 2002, n°99-19.852, où la Cour qualifie la diffusion de certaines informations relevant de la vie intime de personnes publiques comme n'étant pas « *caractéris(ées) comme une atteinte au respect de la vie privée* ».

la réparation du préjudice moral[565], plus aisément accordé en complément à un dommage matériel principal qu'en tant que chef de préjudice autonome[566]. Ainsi, le recours aux préjudices moraux demeure une piste potentielle pour obtenir une réparation. Le rôle des conseils du responsable du traitement sera donc de contrebalancer la jurisprudence de la Cour de cassation, en exigeant que la victime produise une attestation démontrant l'existence d'un préjudice individuel.

Sous-Section 2. Les critères de calcul des dommages et intérêts en droit de la *Common Law*

Tout d'abord, la méthodologie de calcul des dommages et intérêts de la *Federal Trade Commission* sera explorée (A), avant d'aborder la jurisprudence anglo-saxonne (B, page 143).

A. L'invitation au calcul des dommages et intérêts de violation de données personnelles par la FTC

136 Dans l'hypothèse d'une action administrative réalisée sur le fondement de l'article 5 du *FTC act*, la Commission fédérale du commerce se réfère à une grille de lecture minimale pour condamner la société violatrice de données personnelles[567]. S'affranchissant de tout barème préalable, cette grille de lecture comprend cinq critères :

1. l'appréciation de la bonne foi du défendeur ;
2. l'atteinte au public ;
3. la capacité de payer l'amende ;
4. l'élimination des bénéfices subséquents à la violation ;
5. la nécessité d'affirmer l'autorité de la FTC.

Deux objectifs cumulables[568] sont poursuivis par la FTC lorsque celle-ci prononce une amende administrative. Tout d'abord, l'amende doit être « équitable » pour sanctionner la violation de la loi et permettre, si possible, le remboursement des personnes concernées victimes. Le second objectif relève davantage d'une politique pénale. Le quatrième critère (*l'élimination des bénéfices subséquents à la violation*) impose donc que la sanction à un enrichissement sans cause soit supérieure au gain réalisé indûment par le responsable du traitement. Cette exigence se cumule avec le troisième critère (*la capacité de payer l'amende*). Notons que ce dernier point fait l'objet d'une absence de consensus au sein de la FTC. La minorité des Commissaires critique le quantum à prendre en compte. La où la majorité des Commissaire semble se contenter de l'effet publicitaire lié au prononcé d'amendes importants, la minorité incite à prendre en compte la réalité financière du groupe à sanctionner[569]. Selon l'espèce et l'attitude de la société mise en examen, la FTC peut décider de recourir aux *civil penalties* pour sanctionner les agissements prohibés de l'auteur de l'infraction en se fondant sur le premier critère (*l'appréciation de la bonne foi du défendeur*). Dans l'affaire Facebook, le Commissaire CHOPRA souligne l'absence de diligence du réseau social à produire certains actes. L'étendue de l'atteinte au public est la condition la plus

---

565 Note supra p. 412 et 413, spéc. §27.

566 Voir dans ce sens par exemple C.A. Agen, 23 déc. 2020, n°18/00794 où le préjudice extrapatrimonial de déficit permanent est accordé après une agression, ou Cass. Civ. 2e 20 mai 2020 n°19-10.717 pour un accident de judo à l'université, ou encore Crim. 2 avr. 2019, n°18-81.917, F-P+B+I, note P. JOURDAIN, RTD Civ. 2019, p. 341, pour les victimes par ricochet d'un préjudice d'affectation pour un motard percuté par un automobiliste. La preuve du préjudice dans cette dernière espèce n'était pas fournie, là où dans les précédentes le préjudice était prouvée par diverses attestations.

567 Posée par l'arrêt United States v. Reader's Digest Ass'n, 662 F.2d 955, 967 (3d Cir. 1981).

568 Voir dans ce sens l'avis dissident de R. CHOPRA in re Facebook, https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf spéc. p. 15 .

569 Voir dans ce sens l'avis dissent de R. CHOPRA in re Facebook, p. 17 et dans l'avis dissident de Youtube, https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf, p. 6. Voir surtout l'avis dissident de S. SLAUGHTER in re Facebook, https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf, p. 8.

contestée mais aussi la plus déterminante des condamnations[570]. En effet, le caractère collectif des dommages est difficilement appréciable et, ce d'autant que dans les transactions Facebook et Youtube, les Commissaires dissidents établissent des parallèles avec des manipulations électorales suggérant des risques sociétaux tels que prévus par la méthodologie PRIAM. Enfin, le Commissaire CHOPRA estime que les résultats obtenus à partir des données, en l'espèce l'enrichissement de l'algorithme de *machine learning* ayant utilisé ces données, devraient être inclus dans le calcul de l'amende[571]. Les Commissaires soulignent leur volonté de recourir à l'accord transactionnel, même si celui-ci peut se relever désavantageux sur bien des aspects, plutôt que de prendre le risque d'une procédure judiciaire hasardeuse[572]. En outre, l'opinion majoritaire dans l'affaire Facebook souligne que la transaction de 5 milliards de dollars est sans commune mesure avec les indemnisations accordés sur le fondement du RGPD[573] ou par une action judiciaire réalisée devant un tribunal civil[574].

B. La réparation de l'atteinte aux droits des données personnelles en droit anglais

137 Le juge anglais se réfère à l'arrêt **Halford** rendu par la CEDH[575] en 1997 pour justifier le droit de réparation des victimes d'une intrusion dans leur vie privée. Sur ce fondement, l'arrêt **Gulati** concernant des affaires de *misuse of private information* (MPI), offre une réparation de plein de droit des victimes[576] sans exiger aucune autre condition supplémentaire qu'une utilisation non autorisée de ces informations privées. L'arrêt **Halliday**[577] tempère cette indemnisation en soulignant que le *Data Protection Act* limite la réparation au seul « *nominal damages* »[578], c'est-à-dire des dommages ayant pour objectif de revenir à un *statu quo ante*.

---

570 Que l'on retrouve en droit français avec la délibération de la CNIL contre Google, n°SAN-2019-001 du 21 janv. 2019 et en droit européen avec l'arrêt Schrems III du 16 juil. 2020, C-311/18.

571 Voir dans ce sens R. CHOPRA https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

572 Voir l'avis majoritaire de la FTC, https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf, p.8, spéc. pp. 4-6 « *The $5 billion penalty assessed against Facebook today is orders of magnitude greater than in any other privacy case, and also represents almost double the greatest percentage of profits a court has ever awarded as a penalty in an FTC case* ».

573 Voir l'avis majoritaire de la FTC, note supra, pp. 1-2 « *For purposes of comparison, the EU's General Data Protection Regulation (GDPR) is touted as the high-water mark for comprehensive privacy legislation, and the penalty the Commission has negotiated is over20 times greater than the largest GDPR fine to date. This penalty is also one of the largest civil penalties in U.S. history—alongside only cases involving enormous environmental damage and massive financial fraud. The magnitude of this penalty resets the baseline for privacy cases—including for any future violation by Facebook—and sends a strong message to every company in America that collects consumers' data: where the FTC has the authority to seek penalties, it will use that authority aggressively* ».

574 Id. p. 6 « *The Order's innovative, far-reaching conduct relief—imposing affirmative obligations and corporate governance reforms—extends well beyond the typical relief historically awarded by the courts in consumer protection cases involving legitimate companies. Even assuming the FTC would prevail in litigation, a court would not give the Commission carte blanche to reorganize Facebook's governance structures and business operations as we deem fit* ».

575 CEDH, 25 juin 1997, Halford c. R.-U., n°20605/92.

576 Voir dans ce sens AAA v. Associated Newsparpers ltd EWHC, 2013, Weller v. Associated newspaper ltd, EMLR (2014) 24.

577 Cour d'appel d'Angleterre et d'Écosse, Halliday v. Creation Consumer Finance Limited (2013) civ. 33.

578 C'est-à-dire des dommages et intérêts accordés lorsqu'une faute a été commise, mais sans engendrer de dommages indirects. Leur fonctionnement est la réparation du seul droit violé.

Les dommages et intérêts sont uniquement accordés pour réparer le préjudice subi par les personnes concernées, sans aucune volonté judiciaire[579], ou de fondement juridique[580], de sanctionner le responsable du traitement excluant ainsi les dommages et intérêts punitifs. Le juge judiciaire anglais apprécie le droit à réparation du préjudice moral subi en se référant au précédent **One Step**[581]. Dans cet arrêt relatif à une cession de parts sociales d'une société, la Cour souligne que la réparation du préjudice ne repose pas sur une simple comparaison des situations patrimoniales antérieures et postérieures au dommage mais se définit par la démonstration de la preuve du quantum du préjudice subi, en l'espèce un manque lié au prix d'acquisition des parts sociales et leur valeur réelle[582]. Cette estimation subjective contraint le juge à une estimation hasardeuse[583].

138 L'un des refus les plus courants pour accorder le « *standing* », c'est-à-dire l'autorisation de la constitution de l'action collective, demeure le risque d'avoir un passager clandestin bénéficiant indûment des dommages et intérêts accordés au titre de la réparation. Antérieurement à l'arrêt Lloyd-Google[584], la jurisprudence exigeait une identité du préjudice pour tous les membres de l'action de classe afin d'éviter une condamnation disproportionnée du défendeur. Prévue par l'article 19.6 du *Civil Procedure Rules*, cette exigence devint alors un seuil nécessaire pour l'élaboration d'une action de classe imposant l'identité du préjudice pour chaque membre du groupe. L'arrêt Lloyd assouplit cette interprétation. Tout d'abord, le juge d'appel estime qu'une telle restriction empêche toute action collective en matière de données personnelles. Pour justifier son raisonnement, le magistrat recourt au précédent[585] rendant éligible tout demandeur ayant un « *intérêt commun et une peine commune recherchant un secours qui par nature serait bénéfique à tous* »[586]. Cependant pour échapper à une éventuelle censure de la Cour suprême, le juge atténue ce revirement en précisant que les dommages et intérêts accordés à chaque membre de l'action de groupe doivent être appréciés à l'aune des préjudices individuels. Ce revirement est important, dans la mesure où une appréciation individuelle du préjudice empêche la définition d'une somme unique et forfaitaire reversée à chacun des demandeurs.

---

579 Voir dans ce sens Lloyd v. Google, §§62-63 où le juge refuse l'application de la jurisprudence antérieure (Walumba Lumba v Secretary of State for the Home Department, [2011] UKSC 12), applicable au tort de *false imprisonment* réalisé par les pouvoirs publics, en estimant que l'assimilation était impossible du fait que Google est une personne morale de droit privé.

580 Voir dans ce sens Lloyd v. Google, §§62-63 où le juge rappelle que la jurisprudence applicable (Shaw v. Kovac [2017] 1 WLR 4773) au dommage physique occasionné lors d'une opération médicale sans consentement préalable de la victime ne peut faire l'objet d'une analogie avec les litiges relatifs à la vie privée et donc entraîner des dommages et intérêts punitifs.

581 Cour suprême du Royaume-Uni, Morris-Garner c. One Step, 18 avr. 2018, [2018] UKSC 20.

582 Id. §96 : « *le demandeur avait le droit de choisir la manière dont ses dommages devaient être évalués. Il s'est trompé en supposant que la difficulté de quantifier son préjudice financier, tel qu'il était, justifiait l'abandon de toute tentative de quantification et l'octroi, à la place, d'une réparation qui ne pouvait être considérée comme compensatoire au sens propre du terme* ».

583 Citant Chitty on contracts, 3nd ed. (2015), « *where it is clear that claimant has suffered substantial loss, but the evidence does not enable it to be precisely quantified, the court will assess damages as best it can on the available evidence* ».

584 Voir dans ce sens l'arrêt Cours d'appel du Royaume-Uni, Murray v. express Newspapers [2007] EwHC 1908.

585 Cour d'Appel d'Angleterre et d'Écosse, Duke of Bedford [1901] AC 1.

586 Id. §8. « *common interest and a common grievance (…) relief sought (is) in antrue beneficial to all* ».

<table>
<tr><th></th><th></th><th colspan="5">Recevabilité en droit…</th></tr>
<tr><th>Risque</th><th>Méthodologie</th><th>de l'UE</th><th>de la CEDH</th><th>français</th><th>étasunien</th><th>anglais</th></tr>
<tr><td>Préjudice individuel</td><td>CNIL PRIAM NIST BSI</td><td colspan="5">oui</td></tr>
<tr><td>Préjudice collectif</td><td>PRIAM NIST</td><td colspan="2">oui

(mais seulement par groupe de demandeurs de même catégorie)</td><td>Droit en cours d'élaboration</td><td>Si preuve d'un dommage provenant du même fait générateur</td><td>Si identité du dommage provenant du même fait générateur</td></tr>
<tr><td>Préjudice sociétal</td><td>PRIAM</td><td colspan="3">oui

(indirectement pour qualifier une infraction)</td><td>oui

(l'importance de certaines bases de données personnelles a amené la FTC à reconnaître l'existence d'un dommage sociétal)</td><td>non

(la démonstration de la preuve d'un préjudice sociétal a été réfutée)</td></tr>
<tr><td>Préjudice physique</td><td rowspan="4">CNIL PRIAM NIST BSI</td><td colspan="2">non

(mais possible par le pouvoir normateur du juge européen)</td><td>non

(impossibilité pour une chose immatérielle d'engendrer un dommage matériel)</td><td colspan="2" rowspan="2">non

(mais possible par le biais des torts)</td></tr>
<tr><td>Préjudice moral</td><td>non

(mais possible par le pouvoir normateur du juge européen)</td><td>non

(mais possible par le principe de la satisfaction équitable)</td><td>non

(le dommage purement immatériel est difficilement démontrable)</td></tr>
<tr><td>Préjudice psychologique</td><td colspan="2">non

(mais possible par le pouvoir normateur du juge européen)</td><td>non

(démonstration de la preuve difficile)</td><td colspan="2">oui

(par le biais des torts)</td></tr>
<tr><td>Préjudice d'anxiété</td><td>non

(limité à des cas spécifiques)</td><td>non

(mais promu par une doctrine importante)</td><td>non

(exigence d'immédiateté du préjudice)</td></tr>
</table>

Exemples de type de préjudice subi par la personne concernée engendré par une mauvaise utilisation de ses données :

- Préjudice sociétal : la mauvaise utilisation des données personnelles engendre indirectement un dommage à la personne concernée par son caractère collectif (ex : truquage d'une élection)
- Préjudice physique : la mauvaise utilisation des données personnelles engendre un dommage physique à la personne concernée (ex : des données personnelles erronées conduisant à un mauvais diagnostic médical)
- Préjudice moral : la mauvaise utilisation des données engendre directement un dommage moral à la personne concernée (ex : une diffamation)
- Préjudice psychologique : la mauvaise utilisation des données personnelles engendre un dommage psychologique à la personne concernée (ex : une discrimination)
- Préjudice d'anxiété : la mauvaise utilisation des données personnelles engendre un préjudice d'anxiété à la personne concernée (ex : la crainte d'une usurpation d'identité)

suite du tableau page suivante

Tableau 15. Récapitulatif des types de préjudices pris en compte par les différents ordres juridiques

Risque	Méthodologie	Recevabilité en droit… de l'UE	de la CEDH	français	étasunien	anglais

suite du tableau de la page précédente

Atteinte au droit au respect de la vie privée	CNIL PRIAM	oui (indirectement pour des affaires relevant du droit des données personnelles)	oui (à titre principal)	non (mais la CNIL le mentionne dans ses délibérations)	oui (comme fondement spécifique)	
Défaut organisationnel imputable à un responsable du traitement conjoint / sous-traitant	CNIL PRIAM NIST BSI	oui (qualification souveraine du juge de l'Union européenne)	non (la CEDH ignore cette question pourtant soulevée)	oui (par ricochet de l'interprétation du juge européen) et non (par l'application du droit du travail)	oui (par un contrôle accru de la FTC)	non (un salarié du responsable du traitement utilisant les données personnelles à des fins étrangères devient responsable du traitement, exonérant son employeur de toute responsabilité)
Violation des données personnelles		non (mais possible par le pouvoir normateur du juge européen)	non (la CEDH n'a pas été interrogée sur cette question)	oui (mais faiblement et uniquement en cas de mauvaise foi du responsable du traitement)	Un tel préjudice n'est pas encore retenu mais le droit des torts trouverait à s'appliquer	

- Atteinte au droit au respect de la vie privée : l'utilisation des données personnelles entraîne un risque de discrimination / isolation / intrusion

Conclusion

Conclusion

Conclusion de la troisième partie

L'étude du contentieux relatif au droit des données personnelles permet de dresser le panorama des risques à considérer lors de la réalisation d'une analyse d'impact relative aux données personnelles (AIPD).

Tout d'abord, 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 non pas comme un contrat conclu entre le responsable du traitement et la personne concernée mais comme une simple formalité à respecter. Le droit des contrats, et donc la responsabilité contractuelle du responsable du traitement, n'a donc pas à être pris en compte lors de la réalisation d'une AIPD.

Du point de vue de la responsabilité extracontractuelle, l'étude du droit comparé 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. Le juge exclut, par principe, les dommages matériels, comme l'atteinte à l'intégrité physique de la personne concernée suite à la violation de ses données personnelles. 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 occasionnés lors d'une fuite de données personnelles 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. Mais pour l'instant, lors de la réalisation d'une AIPD, seuls les dommages moraux immédiats doivent être analysés.

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 au §80, page 90, les risques organisationnels analysés lors de l'AIPD peuvent être significativement réduits via des dispositions adéquates insérées dans des chartes informatiques ou dans des contrats de sous-traitance.

Enfin, les critères permettant la réparation d'un préjudice subi par la personne concernée, tels que fixés par le « *Chapitre VIII du RGPD relatif aux voies de recours, responsabilité et sanctions* » conduisent en pratique à limiter la réparation accordée aux victimes par les juridictions civiles françaises.

Inspiré des droits étasunien et britannique, le RGPD permet désormais d'engager des actions de groupe. Cependant, 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.

Conclusion générale

Bien que manifestation du principe clé de responsabilité (ou *accountability* en anglais), la réalisation d'une analyse d'impact relative à la protection des données (AIPD) telle qu'imposée dans certaines circonstances par l'article 35 du règlement général sur la protection des données (RGPD), rencontre de nombreux obstacles pour identifier, puis atténuer les risques pour les droits et les libertés des personnes concernées. 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 qu'il a bien documenté par écrit toutes les mesures garantissant que les traitements de données personnelles effectués sont conformes à la réglementation en vigueur. Si les lignes directrices relative à l'AIPD du Comité européen de la protection des données fournissent des précisions importantes, elles sont loin de répondre à toutes les questions opérationnelles que se pose le praticien. La principale difficulté réside dans l'absence de détermination précise du risque dans toutes ses dimensions (assiette, occurrence ou probabilité, échelle de gravité). Pourtant, l'AIPD est l'un des éléments centraux du RGPD. Elle contribue notamment au respect du principe de protection des données dès la conception et par défaut (*Data Protection by design and by default*).

Concrètement, il n'existe pas de méthodologie unique pour réaliser une AIPD. Le responsable de traitement reste libre de procéder comme il l'entend, de choisir 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 dans lequel une application téléchargeable sur un dispositif d'infodivertissement est installée dans un véhicule connecté, démontre, à cet égard, que chaque outil présente des avantages et des inconvénients.

Notamment, les méthodologies françaises CNIL et PRIAM de chercheurs de l'INRIA spécialisés en ingénierie informatique offrent un niveau de granularité reflétant parfaitement le cycle de vie des données personnelles ; 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 seuls aspects de sécurité informatique. Les méthodologies *Bundesamt für Sicherheit in der Informationstechnik* (BSI) allemand et *National Institute of Standards and Technology* (NIST) étasunien 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, car elles s'avèrent moins efficaces du point de vue de la conformité au RGPD.

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 de l'AIPD, correspondant respectivement à la description des flux de données personnelles et à l'appréciation des risques, peuvent s'inspirer directement de la méthodologie PRIAM qui permet de détailler finement le cycle de vie des données personnelles. Cette méthodologie est particulièrement adaptée aux traitements de données complexes et multipartites. La troisième étape peut également intégrer l'étude des « nouveaux » risques proposés par les méthodologies BSI et NIST afin d'y 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 différentes garanties organisationnelles et techniques adéquates préconisées. Enfin, lorsque l'analyste souhaite s'assurer d'une identification des risques pour la protection des données aussi complète que possible, nous l'encourageons à recourir à la méthodologie de modélisation des menaces pour la vie privée LINDDUN (pour « *Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of*

information, Unawareness, and Non-compliance ») proposée par des chercheurs de l'université belge, KU Leuven belge.

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 solutions retenues par les Cours et tribunaux, en particulier la jurisprudence européenne développée par la Cour européenne des droits de l'homme du Conseil de l'Europe et par la Cour de justice de l'Union européenne, démontrent que l'« *état des connaissances* » exclue 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. Outre les dommages futurs, conformément à la jurisprudence étudiée, les dommages du fait des choses immatérielles ne doivent eux aussi pas être pris en compte. Les risques liés à des dommages moraux s'en trouvent d'autant plus réduits.

La prise en compte des types de dommages pouvant découler du non-respect des « *droits et libertés* » des personnes concernées doit donc être relativisée. Elle conduit à considérer la seule vraisemblance à des risques immédiats, l'analyste ne devant prendre en compte que le risque de sécurité informatique, l'obligation d'information préalable et l'exercice des droits par la personne concernée. Dans les cas pertinents, l'analyse des risques financiers découlant d'une éventuelle sanction prononcée par une autorité nationale de contrôle ou une juridiction civile peut s'avérer pertinente. À cet égard, il pourrait être envisagé d'établir une grille de lecture basés sur les critères conduisant au prononcé d'une sanction. Néanmoins, cette grille de lecture est difficile à établir du fait de l'absence de motivations suffisantes. Les lignes directrices sur l'application et la fixation des amendes administratives du Comité européen de la protection des données permettent difficilement de prévoir le montant de l'amende administrative encouru par le responsable du traitement.

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.

Annexes

Annexes

Annexe 1 Article 35 du RGPD : Analyse d'impact relative à la protection des données

1 Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

2 Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au DPO, si un tel délégué a été désigné.

3 L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants :

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou
c) la surveillance systématique à grande échelle d'une zone accessible au public.

4 L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

5 L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

6 Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

7 L’analyse contient au moins :

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l’intérêt légitime poursuivi par le responsable du traitement ;
b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et
d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

8 Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l’article 40 est dûment pris en compte lors de l’évaluation de l’impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d’une analyse d’impact relative à la protection des données.

9 Le cas échéant, le responsable du traitement demande l’avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

10 Lorsque le traitement effectué en application de l’article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l’Union ou dans le droit de l’État membre auquel le responsable du traitement est soumis, que ce droit réglemente l’opération de traitement spécifique ou l’ensemble des opérations de traitement en question et qu’une analyse d’impact relative à la protection des données a déjà été effectuée dans le cadre d’une analyse d’impact générale réalisée dans le cadre de l’adoption de la base juridique en question, les paragraphes 1 à 7 ne s’appliquent pas, à moins que les États membres n’estiment qu’il est nécessaire d’effectuer une telle analyse avant les activités de traitement.

11 Si nécessaire, le responsable du traitement procède à un examen afin d’évaluer si le traitement est effectué conformément à l’analyse d’impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Annexe 2 Lignes directrices AIPD du Comité européen de la protection des données, Annexe 2

Annexe 2 (« Critères d'acceptabilité d'une AIPD ») des « 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 », p. 26-27, https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

Les critères suivants proposés par le Groupe de travail de l'article 29 peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD considérée est suffisamment complète aux fins du respect des exigences du RGPD :

- une description systématique du traitement est fournie [article 35, paragraphe 7, point a)] :
  - la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90) ;
  - les données à caractère personnel concernées, les destinataires et la durée pendant laquelle les données à caractère personnel seront conservées sont précisés ;
  - une description fonctionnelle de l'opération de traitement est fournie ;
  - les actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier) sont identifiés ;
  - le respect de codes de conduite approuvés est pris en compte (article 35, paragraphe 8) ;
- la nécessité et la proportionnalité sont évaluées [article 35, paragraphe 7, point b)] :
  - les mesures envisagées pour assurer la conformité au règlement sont déterminées [article 35, paragraphe 7, point d), et considérant 90], avec prise en compte :
    - de mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement, fondées sur les exigences suivantes :
      - finalités déterminées, explicites et légitimes (article 5, paragraphe 1, point b)] ;
      - licéité du traitement (article 6) ;
      - données adéquates, pertinentes et limitées à ce qui est nécessaire [article 5, paragraphe 1, point c)] ;
      - durée de conservation limitée [article 5, paragraphe 1, point e)] ;
    - de mesures contribuant aux droits des personnes concernées :
      - informations fournies à la personne concernée (articles 12, 13 et 14) ;
      - droit d'accès et droit à la portabilité des données (articles 15 et 20) ;
      - droit de rectification et droit à l'effacement (articles 16, 17 et 19) ;
      - droit d'opposition et droit à la limitation du traitement (articles 18, 19 et 21) ;
      - relations avec les sous-traitants (article 28) ;
      - garanties entourant le ou les transferts internationaux (chapitre V) ;
      - consultation préalable (article 36) ;

- les risques pour les droits et libertés des personnes concernées sont gérés [article 35, paragraphe 7, point c)] :

  - l'origine, la nature, la particularité et la gravité des risques sont évalués (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime aux données, modification non désirée des données, disparition des données) du point de vue des personnes concernées :

    - les sources de risques sont prises en compte (considérant 90) ;
    - les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements tels qu'un accès illégitime aux données, une modification non désirée de celles-ci ou leur disparition ;
    - les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition sont identifiées ;
    - la probabilité et la gravité sont évaluées (considérant 90) ;

  - les mesures envisagées pour faire face à ces risques sont déterminées [article 35, paragraphe 7, point d), et considérant 90] ;

- les parties intéressées sont impliquées:

  - l'avis du DPD est recueilli (article 35, paragraphe 2) ;
  - le point de vue des personnes concernées ou de leurs représentants est recueilli, le cas échéant (article 35, paragraphe 9).

Annexe 3 Questionnaire pour les entretiens menés auprès des professionnels

Choix méthodologique

- Quelles méthodologies utilisez-vous ?
- Vous servez-vous des lignes directrices :
  - du CEPD ?
  - de la CNIL ?
  - de l'ISO ?
- Utilisez vous des méthodologies de définition du risque telles que :
  - EBIOS ?
  - LINDDUN ?
  - NIST ?

Sur l'appréciation de la méthodologie

- En êtes-vous satisfait(e) ?
- Pensez-vous qu'elle soit adéquate ?
- Répond-elle à vos besoins ?
- La réalisation de l'AIPD est-elle effectuée :
  - en amont de l'implémentation d'un nouveau traitement ?
  - en aval d'un nouveau traitement à des fins de régularisation de la conformité ?

Sur les parties prenantes

- La réalisez-vous seul(e) ?
  - Vous faites-vous accompagner par une société de conseil ?
  - Si oui, l'avez-vous choisie pour :
    - son expertise métier ?
    - pour sa réputation ?
    - pour son assurance ?
  - si non, pourquoi ?
- Combien de temps dure en moyenne la réalisation d'une AIPD ?
- Quels sont les services que vous associez à sa réalisation ?
  - Quel est leur degré d'implication ?
  - Quel est leur degré de disponibilité ?
- Est-il prévu de les solliciter de nouveau ?
  - Si oui, l'actualisation est-elle prévue de façon interne avec un moment prédéfini :
    - un moment fixe,
    - une période variable,
    - y a-t-il une validation interne / un process spécifique ?
  - Si oui, l'actualisation est-elle soumise à une circonstance externe :
    - un changement de prestataire technique,
    - une innovation technologique,
    - une évolution jurisprudentielle ?
- Y a-t-il une veille technologique dédiée au traitement examiné ?
  - Si oui, dispose-t-elle de moyen d'implémenter de nouvelles technologies dans le traitement ?
    - Une nouvelle AIPD est-elle réalisée ?
    - L'ancienne AIPD est-elle implémentée ?
    - Si équipe il y a, est-elle intégralement sollicitée à nouveau ?

- Disposez-vous d'un « budget » particulier dédié à la réalisation d'une AIPD pour solliciter d'autres services ?
- Faites-vous participer des tiers à la réalisation de l'AIPD ?
  - Si oui, est ce que ces tiers sont des cocontractants (sous-traitants) ?
    - Quel est leur apport ?
    - Participent-t-ils activement ?
  - Si oui, avez-vous sollicité la CNIL ?
    - Si non, souhaitez-vous le faire ?
  - Si oui, sollicitez-vous le public ?
    - Si oui, comment le choisissez-vous ?
    - Si oui, comment appréciez-vous leur retour ?

Sur l'application de la méthodologie

- Dans quel domaine avez-vous réalisé une AIPD ?
  - Si vous avez utilisé le fondement basé sur une obligation légale :
    - L'AIPD est-elle plus simple ?
    - Comment réalisez-vous l'exercice des droits et les obligations d'information ?
    - Communiquez-vous avec l'autorité policière compétente dans la réalisation de l'AIPD ?
    - Prenez-vous en compte les articles 24 et 25 du RGPD relatifs au *Privacy by design / by default* ?
  - Si vous avez utilisé le fondement basé sur l'intérêt légitime :
    - L'AIPD est-elle plus simple ?
    - Comment réalisez-vous l'exercice des droits et les obligations d'information ?
- Comment avez-vous apprécié les risques ?
  - Comment les avez-vous définis ?
    - De quel point de vue vous placez-vous ?
    - Quels sont les risques qui mériteraient d'être retenus ?
    - Analysez-vous les risques à la seule vue :
      - de votre entreprise / client ?
      - des personnes concernées ?
  - Utilisez-vous les évaluations de cybersécurité pour prendre en compte les risques ?
  - Avez-vous écarté certains risques ?
    - Si oui, pour quel fondement ?
    - Si oui, les avez-vous tout de même documentés ?
    - Si oui, sont-ils mis à jour ?
- L'accès / modification / disparition des données sont-ils les seules sources de risque que vous prenez en compte ?
- Publiez / communiquez-vous les résultats de votre AIPD ?
  - Dans l'hypothèse d'une obligation légale, transférez-vous l'AIPD aux forces de l'ordre ?
  - Faites-vous un résumé de votre AIPD et le placez-vous sur Internet ?

Références internes

Références internes

Table des matières détaillée

Paragraphes numérotés

Partie 3

Chapitre 1

Chapitre 2

Table des illustrations

Liste des abréviations

§	Paragraphe. Au sein de ce rapport, **§** fait référence à un paragraphe numéroté dans le rapport, tandis que § fait référence à un paragraphe du document cité.

A

ACN :	Autorité Nationale de Contrôle
AELE :	Association Européenne de Libre-Échange
AFCDP :	Association Française des Correspondants à la protection des Données Personnelles
Aff. :	Affaire
AFNOR :	Association Française de Normalisation
AIPD :	Analyse d'Impact relative à la Protection des Données
AJ :	Actualités Juridiques
Al. :	Alinéa
ACAATA. :	Allocation de Cessation Anticipée d'Activité des Travailleurs de l'Amiante
ANSSI :	Agence Nationale de la Sécurité des Systèmes d'Information
Art. :	Article
Ass. Plen. :	Assemblée plénière

B

B. :	bulletin
BSI :	*Bundesamt für Sicherheit in der Informationstechnik*

C

C. ou c./ :	contre
CA :	Cour d'Appel
Cass. :	Cour de cassation
CDFUE :	Charte des Droits Fondamentaux de l'Union Européenne
C.E. :	Conseil d'État
CEDH :	Cour Européenne des Droits de l'Homme
CEPD :	Comité Européen de la Protection des Données (*European Data Protection Board, EDPB*). À ne pas confondre avec le Contrôleur européen de la protection des données, cf. EDPS ci-dessous. Dans ce rapport, CEPD est réservé au Comité, tandis que le Contrôleur est désigné par EDPS.
CGU :	Conditions Générales d'Utilisation
CIL :	Correspondant Informatique et Libertés
CIPL :	*Centre for Information Policy Leadership*
Civ. :	Chambre civile de la Cour de Cassation
CIVI :	Commission d'Indemnisation des Victimes d'Infractions
Circ. :	Circuit de cour d'appel fédéral
CJCE :	Cour de Justice des Communautés Européennes (devenue CJUE le 1er décembre 2009)
CJUE :	Cour de Justice de l'Union Européenne
Cf. :	Confer
CNIL :	Commission Nationale de l'Information et des Libertés
coll. :	collection
Colo. Tech. L. J. :	*Colorado Technology Law Journal*
Comm. Com. Elect. :	Communication commerce électronique
Convention ESDH :	Convention européenne de sauvegarde des droits de l'homme
Crim. :	Chambre criminelle

D

D. :	Dalloz
D. Act. :	Dalloz Actualité
D. IP/IT :	*Dalloz Intellectual Property / Information Technology*
déc. :	Décision
Délib. :	Délibération
Dir. :	Sous la direction de
DPA :	*Data Protection Act*
DPbDD :	*Data Protection by Design and by Default*
DPIA :	*Data Protection Impact Assessment*
DPO :	Délégué à la Protection des Données
DSI :	Directeur de la Sécurité Informatique

E

éd. :	édition
EDPB :	*European Data Protection Board* (Comité Européen de la Protection des Données, cf. entrée CEPD ci-dessus) https://edpb.europa.eu/
EDPS :	*European Data Protection Supervisor* (Contrôleur Européen de la Protection des Données) https://edps.europa.eu/
EEE :	Espace économique européen
EIA :	*Ethic Impact Assessment*
eIDAS :	*Electronic IDentification And trust Services*
EIVP :	Évaluation d'Impact de la Vie Privée
Eur. Data Pro. L. Rev . :	*European Data Protection Law Review*
EMLR :	*European Market Law Review*
EWCA :	*England and Wales Court of Appeal*.
EWCH :	*England and Wales High Court*
Ex. :	exemple

F

FTC :	*Federal Trade Commission*
F.3d :	Cour d'appel fédérale du troisième circuit

G

G29 :	Groupe Article 29
GA. St. U. L Rev. :	*Georgia State University Law Review*
GAJC :	Grands Arrêts de la Jurisprudence Civile
G.P. :	Gazette du Palais
Gr. Ch. :	Grande Chambre

H

harv. L. Rev. :	*Harvard Law Review*
HSE :	*Health and Safety Executive*

I

ICO :	*Information Commissioner's Office*
Id. :	Idem
IdO / IOT :	Internet des Objets
IDPL :	*International Data Privacy Law*
ISO :	*International Organization for Standardization*

J

JCP :	Semaine juridique
JOCE :	Journal Officiel de la Communauté Européenne
JORF :	Journal Officiel de la République Française
JOUE :	Journal Officiel de l'Union Européenne

L

LCEN :	Loi pour la Confiance dans l'Économie Numérique
LIL :	Loi Informatique et Libertés
LINDDUN :	*Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance*
LPA :	Les Petites Affiches

M

MARD :	Mesures Alternatives de Règlement des Différents
MED :	Mise En Demeure
MPI :	*Misuse of Private Information*

N

n° / no / num :	numéro
NIST :	*National Institute of Standards and Technology*
NSS :	Nature Science Société

P

p. :	page/pages (pour les références en français)
pp. :	pages (pour les références en anglais)
PIA :	*Privacy Impact Assessment*
PUF. :	Presses universitaires de France

R

req. :	requête
Règlement eIDAS :	Règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
RGPD :	Règlement Général sur la Protection des Données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données)
RLDI :	Revue Lamy Droit de l'Immatériel
RTD Civ. :	Revue Trimestrielle de Droit civil
RTD eur. :	Revue Trimestrielle de Droit européen
RFDA :	Revue Française de Droit Administratif
RDLF :	Revue des Droits et Libertés Fondamentaux

S

s. (« et s.») :	et suivantes
SAN :	Sanction
Soc. :	Chambre sociale de la Cour de Cassation
spéc. :	spécialement
Stan.L. Rev. :	*Standford Law Review*

T

T.C. :	Tribunal des Conflits
TFUE :	Traité pour le Fonctionnement de l'Union Européenne
TGI :	Tribunal de Grande Instance
TPICE :	Tribunal de Première Instance des Communautés Européennes

U

UE :	Union Européenne
ULB :	Université Libre de Bruxelles

V

v. :	versus
VOD :	*Video On Demand*

W

Wash. L. Rev. :	*Washington Law Review*

Index

A

B

C

D

E

F

G

H

I

J

S

T

V

Y

Bibliographie

1. Législation

1.1. Législation européenne

Directive 78/855/CEE du Conseil du 9 octobre 1978 relative à la fusion des sociétés anonymes, codifiée en dernier lieu par la directive 2017/1132 du Parlement européen et du Conseil du 14 juin 2017, JOCE L 169 du 30.06.2017.

Décision de la Commission 2000/520/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, JOCE L 215 du 25.8.2000, p. 7–47.

Règlement (CE) n°864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles dit Rome II, JOCE L 199 du 31.7.2007, p. 40–49.

Règlement (CE) n°593/2008 du Parlement européen et du Conseil du 17 juin 2008sur la loi applicable aux obligations contractuelles, dit Rome I, JOCE L 177 du 4.7.2008, p. 6–16.

Directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence des équipements terminaux de télécommunication, L162/20, 21 juin 2008, JOCE L 162 du 21.06.2008, p. 20–26.

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JOCE L 337 du 18.12.2009, p. 11–36.

Règlement (CE) n°1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, JOCE L 351 du 20.12.2012, p. 1–32

Règlement (UE) n 524/2013 du Parlement européen et du Conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 2009/22/CE (règlement relatif au RLLC) JOUE L 165 du 18.6.2013, p. 1–12.

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (Article 27), JOUE L 119 du 4.5.2016, p. 89–131.

Règlement UE 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (Article 39), JOUE L 295 du 21.11.2018, p. 39–98.

Directive (UE) 2019/2161 du Parlement européen et du Conseil du 27 novembre 2019 modifiant la directive 93/13/CEE du Conseil et les directives 98/6/CE, 2005/29/CE et 2011/83/UE du Parlement européen et du Conseil en ce qui concerne une meilleure application et une modernisation des règles de l'Union en matière de protection des consommateurs (Texte présentant de l'intérêt pour l'EEE), JOUE L 328 du18.12.2019, p. 7–28.

Règlement UE (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) no 78/2009, (CE) no 79/2009 et (CE) no 661/2009 du Parlement européen et du Conseil et les règlements (CE) no 631/2009, (UE) no 406/2010, (UE) no 672/2010, (UE) no 1003/2010, (UE) no 1005/2010, (UE) no 1008/2010, (UE) no 1009/2010, (UE) no 19/2011, (UE) no 109/2011, (UE) no 458/2011, (UE) no 65/2012, (UE) no 130/2012, (UE) no 347/2012, (UE) no 351/2012, (UE) no 1230/2012 et (UE) 2015/166 de la Commission (Texte présentant de l'intérêt pour l'EEE), JOUE L 325 du 16.12.2019, p. 1–40.

Proposition de règlement du Parlement européen et du Conseil du 21 avril 2021 établissant des règles harmonisées concernant l'Intelligence Artificielle, COM (2021) 206 final, Bruxelles, 21.04.2021.

1.2. Législation française

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.
https://www.legifrance.gouv.fr/jorf/jo/2016/10/08/0235
Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.
https://www.legifrance.gouv.fr/jorf/jo/2016/02/11/0035
Ordonnance du 10 février 2016, JORF n°0035 du 11 février 2016.

2. Jurisprudence

2.1. Jurisprudence européenne

2.1.1. *Jurisprudence de la Cour de justice de l'Union européenne et du Tribunal de première instance*

CJCE, 30 nov.1976, C-21/76, Handelskwekerij G. J. Bier BV c. Mines de potasse d'Alsace SA.
CJCE, 12 mars 1987, C-178/84, Commission c. Allemagne.
CJCE, 14 juillet 1994, C-17/93, Van der Velt.
CJCE, 7 mars 1995, C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL.
CJCE, 15 décembre 1996, C-180/96, R.U. c. Commission.
CJCE, 5 mai 1998, C-157/96 et C-180/96, National Farmer's Union.
CJCE, 11 juillet 2000, C-473/98, Kemikalieinspektionen c. Toolex Alpha AB.
TPICE, 11 septembre 2002, T-13/99, Pfizer c. Commission.
TPICE, 26 novembre 2002, T-74/00, T-76/00, T-83/00 à T-85/00, T-132/00, T-137/00 et T-141/00, Artegodan.
CJCE, 23 septembre 2003, C-192/01, Commission c. Danemark.
CJCE, 02 avril 2004, C-41/02, Commission c. Pays-Bas.
CJUE, 28 janvier 2010, C-333/08, Commission c. France.
CJUE, 8 juillet 2010, C-343/09, Afton Chemical.
CJUE, 25 octobre 2011, C-509/09 et C-161/10, eDate Advertising GmbH e.a. c. X et Société MGN Ltd.
CJUE, 8 avril 2014, C-293/12 et C-594/12, Digital Rights c. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.la.
CJUE, 13 mai 2014, C-131/112, Google Spain c. AEPD.

CJUE (grande chambre), 6 octobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner.
CJUE, 1er octobre 2017, C-673/17, Planet 49.
CJUE, 17 octobre 2017, C-194/16, Bolagsupplysningen c. Svesnks Handel AB.
CJUE, 25 janvier 2018, C-498/16, M. SCHREMS c. Facebook.
CJUE, 05 juin 2018, C-210/16, Wirtschaftsakademie.
CJUE, 10 juillet 2018, C-25/17, Jehovan todistajat.
CJUE, 28 juillet 2018, C-191/15, Verein für Konsumenteninformation c. Amazon EU Sàrl.
CJCE, 05 décembre 2018, C-14/78, Denkavit c. Commission.
CJUE, 29 juillet 2019, C-40/17, Fashion ID Gmbh & Co.
CJUE, 16 juillet 2020, C-311/18 Data Protection Commissioner/Maximillian Schrems c. Facebook Ireland.
CJUE, 10 juin 2021, C-65/20, Krone-Verlag.

2.1.2. *Jurisprudence de la Cour de justice de l'Association européenne de libre-échange*

Cour AELE, 05 avril 2001, E-3/00, EFTA Surveillance Authority c. Norvège.

2.1.3. *Jurisprudence de la Cour européenne des droits de l'homme*

CEDH, 8 juin 1976, Cour plénière, Engel c. Pays-Bas.
CEDH, 28 juin 1976, König c. République Fédérale d'Allemagne.
CEDH, 21 février 1994, Bendemoun c. France.
CEDH, 9 décembre 1994, Lopez Ostra c. Espagne.
CEDH, 17 décembre 1996, Saunders c. Royaume Uni.
CEDH, 18 décembre 1996, Loizidou c. Turquie.
CEDH (Grande Chambre), 19 février 1998, Guerra et autres c. Italie.
CEDH, 09 juin 1998, L.C.B. c. Royaume-Uni.
CEDH, 20 octobre 1998, Osman c. Royaume-Uni,
CEDH, 10 octobre 2000, Akkoc c. Turquie.
CEDH, 6 mars 2001, Hilal c. Royaume-Uni.
CEDH, 3 avril 2001, Keenan c. Royaume-Uni.
CEDH, 14 mars 2002, Paul et Audrey Edwards c. Royaume-Uni.
CEDH, 2 décembre 2002, KRS c. Royaume-Uni.
CEDH, 8 juillet 2003, Hatton et autres c. Royaume-Uni.
CEDH (Grande Chambre), 30 novembre 2004, Öneryildiz c. Turquie.
CEDH, 4 févier 2005, Mamatkoulov et Askarov c. Turquie.
CEDH, 07 juin 2005, Kilinç et autres c. Turquie.
CEDH, 09 juin 2005, Fadeïeva c. Russie.
CEDH, 22 décembre 2005, Balyemez c. Turquie.
CEDH (Grande Chambre), 23 novembre 2006, Jussila c. Finlande.
CEDH, 24 septembre 2007, Irfan Bayrak c. Turquie.
CEDH, 20 mars 2008, Boudaïeva c. Russie.
CEDH, 27 mai 2008, Rodić et autres c. Bosnie-Herzégovine.
CEDH, 16 octobre 2008, Renolde c. France.
CEDH, 27 janvier 2009, Tatar c. Roumanie.
CEDH (Grande Chambre), 30 juin 2009, Verein gegen Tierfabrieken Schweiz (VgT) c. Suisse (No. 2).
CEDH, 2 mars 2010, Al-Saadoon et Mufdhi c. Royaume-Uni.
CEDH, 10 février 2011, Dubetska et autres c. Ukraine.
CEDH (Grande Chambre), 24 mars 2011, Giuliani et Gaggio c. Italie.
CEDH, 23 février 2012, Civek c. Turquie.
CEDH, 19 avril 2012, Sašo Gorgiev c. « L'Ex-République yougoslave de Macédoine ».
CEDH, 25 juin 2013, Trevalec c. Belgique.
CEDH, 24 avril 2014, Perevedentsevy c. Russie.
CEDH, 26 février 2015, Prilutskiy c. Ukraine.

CEDH, 6 octobre 2015, Kavaklioğlu et autres c. Turquie.
CEDH, 3 novembre 2015, Olszewscy c. Pologne.
CEDH (Grande Chambre), 23 mars 2016, F.G. c. Suède.
CEDH, 31 mai 2016, Comoraşu c. Roumanie.
CEDH, 2 juin 2016 Petschulies c. Allemagne.
CEDH, 13 septembre 2016, A.Ş. c. Turquie.
CEDH, 4 octobre 2016, Cevrioğlu c. Turquie.
CEDH, 6 octobre 2016, W.P. c. Allemagne.
CEDH, 15 novembre 2016, A et B c. Norvège.
CEDH, 1er décembre 2016, Gerasimenko et autres c. Russie.
CEDH, 14 février 2017, Allanazarova c. Russie.
CEDH, 2 mars 2017, Talpis c. Italie.
CEDH, 31 mai 2017, Comoraşu c. Roumanie.
CEDH, 1er juin 2017, Malik Babayev c. Azerbaidjan.
CEDH, 31 janvier 2019, Rooman c. Belgique.
CEDH, 07 février 2019, Patsaki c. Grèce.
CEDH, 25 mai 2021, Big Brother c. Royaume-Uni.
CEDH, 25 mai 2021, Centrum för Rattvisa c. Suède.

2.2. Jurisprudence française

2.2.1. *Tribunal des conflits*

T.C. 30 juillet 1873, Pelletier.
T. C. 9 juillet 1953, Dame Veuve Bernadas.

2.2.2. *Ordre administratif*

Conseil d'État

C.E., 26 juillet 1918, Époux Lemonnier.
C.E., 12 mars 1975 Pothier.
C.E., 25 septembre 1998 Greenpeace c. Ministère de l'Agriculture.
C.E., 26 février 2014, Association Ban Asbestos France.
C.E., 12 mars 2014, Société pages jaunes Groupe.
C.E., 23 juillet 2014, Sté Maco Pharma.
C.E., assemblée section contentieux, 21 avril 2021, French Data Network.

CNIL

Délibération Autorisation, 2016-212 du 7 juillet 2016, Natural Security Alliance.
Délibération n°SAN-2019-001 du 21 janvier 2019, Google.
Délibération n°MED-2018-042 du 30 octobre 2018, Vectaury.
Délibération n°MED-2020-015 du 15 juillet 2020, Stop Covid.
Délibération n°SAN-2020-003 du 28 juillet 2020, Spartoo.
Délibération n°MEDP-2020-003 du 16 juillet 2020, Ministère des Solidarités et de la Santé.
Délibération n°SAN-2020-013 du 7 décembre 2020, Amazon Europe Core.

2.2.3. *Ordre judiciaire*

Tribunal judiciaire

TGI Toulouse, 24 mai 2004.
TGI de Paris, 12 février 2019 (UFC-Que choisir Google) et du 9 avril 2019, UFC-Que Choisir /Facebook Inc.

Cour d'appel

Cour d'appel Toulouse, 25 mai 2004.
Cour d'appel Agen, 23 décembre 2020.

Cour de cassation

Cass. Civ., 11 janv.1922.
Cass. Civ., 13 février 1923.
Cass. Crim., 20 juillet 1931.
Cass. Crim., 01 juin 1932.
Cass. Crim., 05 octobre 1961.
Cass. Civ. 2e, 8 mai 1964.
Cass. Civ. 2e, 01 avril. 1965.
Cass. Civ. 2e, 19 octobre 1976.
Cass. Civ. 1ère, 17 novembre 1982.
Cass. Crim., 8 juillet 1975.
Assemblée Plénière, 17 juin 1983.
Cass. Crim., 20 mai 1985.
Cass, Assemblée plénière, 17 octobre 1985.
Cass. Crim., 20 juin 2000.
Cass. Civ. 1ère, 3 avril 2002.
Cass. Crim., 13 octobre 2003.
Cassation, Assemblée Plénière, 06 octobre 2006.
Cass. Crim., 18 février 2014.
Cass. Civ., 1ère, 30 avril 2014.
Cass. Crim., 2 avril 2019.
Cass. Civ. 2e, 20 mai 2020.

2.3. **Jurisprudence étrangère**

2.3.1. *Jurisprudence du Royaume-Uni*

Cour suprême du Royaume-Uni

Walumba Lumba c. Secretary of State for the Home Department, [2011] UKSC 12.
Morris-Garner c. One Step, [2018] UKSC 2.

Cours d'appel du Royaume-Uni

Duke of Bedford [1901] AC 1.
Murray v. express Newspapers [2007] EwHC 1908.
Halliday v. Creation Consumer Finance Limited [2013] civ. 33.
AAA v. Associated Newsparpers ltd EWHC [2013].
Weller v. Associated newspaper ltd EMLR [2014] 24.

Vidal-Hall v. Google [2014] EWHC 13 (QB).
Gulati v. MGN LIMITED [2015] EWHC.
Shaw v. Kovac [2017] 1 WLR 4773.
Lloyd v. GOOGLE [2019] EWCA civ 1599.
R (Bridges) v. CC South Wales [2020] EWCA Civ 1058.

2.3.2. *Jurisprudence étasunienne*

Jurisprudence fédérale des États-Unis d'Amérique

Cour suprême des États-Unis d'Amérique

Clapper c. Amnesty international USA, 568, US (2013).
Spokeo v. Robins, 136 CT 1540 (2016).

Cour d'appel fédérale des États-Unis d'Amérique

Petriello v. Kalma, 576 A. 2d 475 (Com 1990).
Cour d'appel du troisième circuit, Reilly v. Ceridian, 664 D. 3d 37, 2011.
Remijas v. Neiman Marcus, 794 F.3D. 2015.
Cour d'Appel du South District du Texas, Peter v. St Joseph Servs. Corp 74 F. supp. 3d. 847.
Cour d'appel du troisième circuit In re Horizon Healthcare Servs., 846, F.3D 625, 2017.
Green v. Ebay, E.D. 4, 2015.

Federal Trade Commission

FTC - Facebook, Stipulated order for civil penaly, monetary judgement and injunctive relief, 24 juillet 2019.
https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

Avis dissident de R. CHOPRA dans la transaction conclue entre Facebook et la FTC.
https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf.

Avis dissident de S. SLAUGHTER dans la transaction conclue entre Facebook et la FTC.
https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf.

Jurisprudence des Cours étatiques des États-Unis d'Amérique

Douglas v. Stokes, 149 S.W. 849, 850 (Ky. 1912).
Daily times Democrat v. Graham (Ala. 1964).
George v. Jordan Marsh Company, 268 NE 2d 915 (Mass. 1971).
Molien v. Kaiser Found. Hosps., 616 P.2d, 813 (Cal. 1980).
Schultz v. Barberton Glass Co. 477 Ne, 2d , 109 (Ohio 1983).
Doe v. Hofstetter, D. colo. (2012).
Doe v. Hofstetter (D. colo. 13 juin 2020).

3. Rapports et lignes directrices

3.1. Rapports de l'Union européenne

Commission européenne, Communication sur le recours au principe de précaution, 2000.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A52000DC0001

Commission européenne, Science for environment policy, future brief: the precautionary principle: decision-making under certainty, iss. 18, 09/2017.
https://ec.europa.eu/environment/integration/research/newsalert/pdf/precautionary_principle_decision_making_under_uncertainty_FB18_en.pdf

Parlement européen, « le Principe de précaution – définitions, applications et gouvernance ».
https://www.europarl.europa.eu/thinktank/fr/document.html?reference=EPRS_IDA%282015%29573876

3.2. Lignes directrices du Comité européen pour la protection des données (CEPD), antérieurement Groupe de l'article 29l

Groupe de l'article 29, 10 juillet 2010, Avis n°3/2010 sur le principe de responsabilité.
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf

Groupe de l'article 29, 10 avril 2014, Avis n°5/2014 sur les techniques d'anonymisation.
https://www.dataprotection.ro/servlet/ViewDocument?id=1288

Groupe de l'article 29, 16 septembre 2014, Avis n°8/2014 sur les développements récents sur l'internet des objets, 14/EN.
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

CEPD, 3 oct. 2017, Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679.
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

CEPD, 25 septembre 2018, Avis n°9/2018 sur le projet de liste établi par l'autorité de contrôle compétence de la France concernant les opérations pour lesquelles une AIPD est requise (article 35°4 du RGPD).
https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-pinion_2018_art._64_fr_sas_dpia_list_fr.pdf

CEPD, 28 janvier 2020, Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité, v.1.0.
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

CEPD, 20 octobre 2020, Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut.
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_fr

CEPD, 09 mars 2021, Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité, v.2.0.
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

3.3. Documents du Contrôleur européen de la protection des données (EDPS)

EDPS, 3 juillet 2019, Accountability on the ground Part I : Records, registers and when to do Data protection impact Assessment, v.1.3.

https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf

EDPS, 6 juillet 2020, Survey on Data Protection Impact Assessments under Article 39 of the Regulation.
https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en

3.4. Lignes directrices de la Cour européenne des droits de l'homme

CEDH, Demandes de satisfaction équitable, instructions pratiques.
https://www.echr.coe.int/Documents/PD_satisfaction_claims_FRA.pdf

4. Doctrine

4.1. Ouvrages de droit français

S. CARVAL, *La responsabilité civile dans sa fonction de peine privée*, LGDJ, 1995, T. 250, n°189.

P. LE TOURNEAU, « *Droit de la responsabilité et des contrats* », Dalloz Action, 2019, p. 2702

A. LUCAS, « *La responsabilité du fait des choses immatérielles* », MELANGES CATALA, Litec, 2001.

L. PAILLIER, *Les outils technologiques, la compliance by design et le RGPD : la protection des données dès la conception*, in M.-A. FRISON-ROCHE (dir.), Les outils de la Compliance, série «Régulations & Compliance ». Journal of Regulation & Compliance et Dalloz, 2021, p. 279–286

A. STIRLING, *Precaution in the governance of technology*, in Oxford handbook of law, regulation and technology, 2017, p. 644-669.

F. SUDRE, « *Droit européen et international des droits de l'homme* », PUF, 14e éd..

E. TRICOIRE, « *La responsabilité du fait des choses immatérielles* », MELANGES LE

TOURNEAU, Dalloz, 2008.

G. VINEY, *Introduction à la responsabilité*, 3e éd., LGDJ, 2008.

4.2. Articles publiés dans des revues françaises

M. AFROUKH, « *Une hiérarchie des droits fondamentaux ? Le point de vue du droit européen* », RDLF, 2019, chr. 23.
http://www.revuedlf.com/cedh/une-hierarchie-entre-droits-fondamentaux-le-point-de-vue-du-droit-europeen/

H. BARBIER, Commentaire de l'arrêt Civ. 3e, 12 avril 2018, n°17-26.906, RTD civ. 2018, p. 900.

H. BELVEZE, « *Lignes directrices pour l'application du principe de précaution* », NSS 9, p. 71-77.
https://www.nss-journal.org/articles/nss/pdf/1999/03/nss19990703p71.pdf

C. BLUMANN C. et V. ADAM, « *La politique agricole commune dans la tourmente : la crise de la vache folle* », RTD eur., avril-juin 1997, p. 292.

F. BOUHON, « *Le risque et la Cour européenne des droits de l'homme – Premières esquisses d'une réflexion sur le risque à l'aune des droits fondamentaux* », RLDF, 2019/46.

http://www.revuedlf.com/droit-fondamentaux/le-risque-et-la-cour-europeenne-des-droits-de-lhomme-premieres-esquisses-dune-reflexion-sur-le-risque-a-laune-des-droits-fondamentaux/

C. CASTELLUCCIA, D. LE MÉTAYER, « *Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode* », INRIA, 2019.
https://hal.inria.fr/hal-02373093/document

S. CAUDAL, « *Existe-t-il un principe de précaution appliqué par le juge administratif ?* », RFDA 2017, p. 1061.

A. DANIS-FATOME, « *Quelles actions judiciaires en cas de violation du RGPD ?* », Comm. Com. Elect. 2019, dossier 18, note 23.

X. DELPECH, « *Une recommandation de la Commission des clauses abusives sur les réseaux sociaux* », Dalloz Actu, 05 déc. 2014.

T. DOUVILLE et H. GAUDIN, « *Un arrêt sous le signe de l'exceptionnel* », D. 2021, n°23, p. 1268.

C. FERTE, R. LABAT, « *L'alerte professionnelle et la loi Sapin 2* », Option droit et affaires, 2017, n°371, pp. 10-11.

W. FRAISSE, « *Amiante : la preuve du préjudice d'anxiété* », Dalloz Actu, 02 mai 2014.

P.-Y. GAUTIER, « *La CEDH poursuit la révolution normative* », D. 2013, p. 2106 et O. SABARD, note D. 2013, p. 2139.

D. GENCY-TRANDONNET, « *L'obligation de modérer le dommage dans la responsabilité extracontractuelle* », G.P. 06 mai 2004.

N. HELENON, C. HESLAUT, « *Données personnelles : l'assurabilité des sanctions administratives* », Expertises, 2017, n°424 pp. 180-184.

J. KNETSCH, « *La désintégration du préjudice moral* », D. 2015 p. 445.

A. KOVLER, « *La CEDH face à la souveraineté d'un État* », L'Europe en formation, 2013/2, n°368, pp. 209-222.
https://www.cairn.info/revue-l-europe-en-formation-2013-2-page-209.htm

A. LEPAGE, « *Précisions sur les modes de réparation du préjudice en matière d'atteintes à la vie privée et à l'image* », D. 2003, p. 1542.

X. MAGNON, « *La doctrine, la QPC et le Conseil constitutionnel : quelle distance ? Quelle expertise ?* », Colloque du 14 juin 2013 à l'Université de Toulouse 1 Capitole.
https://www.dailymotion.com/video/xvfuy0

W. MAXWELL, S. TAIEB, « *L'accountability, symbole d'une influence américaine sur le RGPD* », D. IP/IT, 2016, p. 123.

D. MAZEAUD, Commentaire de l'arrêt Civ. 2e du 19 juin 2003, D. 2004, somm. p. 1346.

N. METALLINOS, « *Le principe d'accountability : des formalités préalables aux études d'impact sur la vie privée* », Comm. Com. Elect. 2018, dossier 18.

G. DE MONTCUIT, « *L'incidence de l'obligation de ne pas aggraver son dommage sur l'action privée en réparation du dommage concurrentiel* », LPA 18 janvier 2019, N°14, p. 9.

L. de MONTVALON, « *Extension du préjudice d'anxiété* », Dalloz actu 18 septembre 2019, note sous Cass.Soc. 11 septembre 2019.

H. MUIR WATT, « *La modération des dommages en droit anglo-américain* », LPA 20 novembre 2002, p. 45.

E. NETTER, « *L'extinction du contrat et le sort des données personnelles* », AJ Contrat 2019, p. 416.

C. Quézel-Ambrunaz, « *Des dommages et intérêts octroyés par la Cour européenne des droits de l'homme* », RDLF 2014, Chron. n°5.

F. SUDRE, « *La Cour européenne des droits de l'homme et le principe de précaution* », RFDA 2017, p. 1039.

G. VINEY, Commentaire de l'arrêt Civ. 2e du 19 juin 2003, JCP 2004, I, 101, n° 945.

4.3. Articles publiés dans des revues étrangères

U. BECK, *Risk Society: Towards a New Modernity*, Sage pub., 1992, p. 260.

CIPL (Center for Information Policy Leadership), *Risk, high risk, risk assessment and DPIA under the GDPR*, 2016.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

R. CALO, *Privacy Harm Exceptionalism*, 12 Colo. Tech. L. J. 361 (2014).

R. CLARKE, *An evaluation of PIA guidance documents*, IDPL, 2011, Vol.1, n°2, p. 111–120.

C. DANNER et P. SCHULMAN, *Rethinking Risk Assessment for Public Utility Safety Regulation*, Risk Analysis, 2019, p. 1044-1059.

P. DE HERT, *A human right perspective on privacy and DPIA*, in Privacy Impact Assessment, Springer, 2012

K. DEMETZOU, *Data protection impact assessment, and the unclarified concept of « high risk» in the GDPR*, Computer Law & Security Review 35 (2019) 105342.

R. GELLERT, *Understanding the notion of risk in the general data protection regulation*, Computer Law & Security Review 34 (2018), p. 279–288.

C. HILSON, *Risk and the European Convention on Human Rights*, Cambridge Yearbook of Legal Studies, 2009, p. 353–375.

S. JONES, *Having An Affair May Shorten Your Life: The Ashley Madison Suicides*, 33 Ga. St. U. L. Rev. 455 (2017).

D. LANDOLL, *The security risk Assessment handbook*, CRCP Press, 2011.

J. LITMAN, *Information Privacy/Information property*, 52 Stan.L. Rev. (2000).

N. LEVIT, *Ethereal torts*, 61 Geo. Wash. L. Rev. (1992).

SATORI, A common framework for ethical impact assessment, Annex 1 A reasoned proposal for a set of share ethical values, principles and approaches for ethics assessment in the European Context, Delivrable D4.1., p. 79.
https://satoriproject.eu/media/D4.1_Annex_1_EIA_Proposal.pdf

L. SEMINARA, *Risk Regulation and the European Convention on Human Rights*, European Journal of Risk Regulation, 2016, p. 733–749.

G. SKOGSTAD, *The WTO and Food Safety Regulatory Policy Innovation in the European Union*, in 39 Journal of Common Market Studies 485, 490 (2001).

D. SOLOVE, *A taxonomy of privacy, University of Pennsylvania Law Review*, Vol. 154 n°3, 2006, p. 477.

D. SOLOVE, D. K. CITRON, *Risk and anxiety: a theory of data breach harms*, Texas Law review, 2018, p. 737.

S. WARREN & L. BRANDEIS, *The right to privacy*, 4 harv. L. Rev., 193 (1890).

K. WUYTS & W. JOOSER, LINDDUN, *A privacy threat modelling: a tutorial*, 2015, p. 38.

5. Méthodologies d'analyse d'impact relatives aux données personnelles

CNIL

CNIL, *Managing Privacy Risks-Methodology*.
https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

CNIL, *Privacy Impact Assessment*.
https://www.cnil.fr/en/privacy-impact-assessment-pia

DPIA Lab

DPIA Lab de l'Université Libre de Bruxelles, *Data protection impact assessment in the European Union: developing a template for a report from the assessment process*, 2020.
https://dpialab.wordpress.com/publications/

EBIOS

ANSSI, *EBIOS Risk Manager*, 2019.
https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

PRIAM

D. LE METAYER et S. JOYEE DE, *Priam: a privacy risk methodology*, 2016.
https://hal.inria.fr/hal-01302541/document

LINDDUN

Linkabiliy, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance.

https://www.linddun.org/

NIST

NIST Privacy Risk Assessment Methodology (PRAM).

https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/riskassessment/

Analyse d'impact relatives aux données personnelles réalisées

Ministère de la Justice néerlandais, DPIA Office 365 for the Web and mobile Office apps, 20 juin 2020.

https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps

Health Service Executive, DPIA Covid Tracker App, 26 juin 2020.

https://github.com/HSEIreland/covidtracker-documentation/blob/master/documentation/privacy/Data%20Protection%20Impact%20Assessment%20for%20the%20COVID%20Tracker%20App%20-%2026.06.2020.pdf

Auteurs

Claire Levallois-Barth

Enseignante-chercheuse en droit à l'Institut Mines-Télécom/Télécom Paris, et chercheuse de l'Institut Interdisciplinaire de l'Innovation (I3), unité mixte du CNRS, Claire Levallois-Barth est par ailleurs Coordinatrice de la Chaire Valeurs et Politiques des Informations Personnelles de l'IMT. Elle est responsable de l'axe 5 « Protection des données personnelles impliquées dans le véhicule connecté » de la Chaire *Connected Cars & Cyber Security* de Télécom Paris. Elle est également membre du Comité pilote d'éthique du numérique, éditeur associé des *Annals of Telecommunications*, membre du comité scientifique du Forum International de la Cybersécurité (FIC), membre du *Data Privacy Expert* Panel d'AXA, membre du Comité d'éthique sur l'intelligence artificielle de Pôle Emploi et membre du Comité éthique de la Data et de l'IA d'Orange.

Contact : claire.levallois@imt.fr

Jonathan Keller

Ingénieur de recherches dans la Chaire de Télécom Paris *Connected Car and Cybersecurity* (C3S) et chercheur associé à la Chaire de l'IMT Valeurs et Politiques des Informations Personnelles (VP-IP), Jonathan Keller est docteur en droit public spécialisé dans les questions du numérique.

Contact : jonathan.keller@telecom-paris.fr

La responsabilité des partenaires des Chaires C3S et VP-IP ne peut en aucun cas être mise en cause en raison du contenu de la présente publication, qui n'engage que ses deux auteurs.

Remerciements

Les auteurs remercient tout particulièrement M. Bruno LALANDE (Renault) pour sa très grande implication dans la relecture des différentes étapes de rédaction ainsi que tous les partenaires ayant participé à cette recherche :

Nokia	Renault	Valéo	Wavestone
Florian Damas	Estée Artis Christelle Dardant Lionel Ferrieres Frank Serrieres	Christophe Jouvray	Raphaël Brun François Luquet

En savoir plus

https://chairec3s.wp.imt.fr/

https://www.informations-personnelles.org/
YouTube youtube.www.informations-personnelles.org
@CVPIP

Ilustration de couverture

Renault Mégane E-Tech Electric. Groupe Renault – Direction Design. Juin 2021.

Nepeys – www.nereys.fr – RCS 499438505

FONDATION Mines-Télécom
La Fondation de l'IMT

CHAIRE CONNECTED CARS & CYBER SECURITY

CHAIRE VP-IP
VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES
DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

Partenaires de la Chaire C3S

Valeo — SMART TECHNOLOGY FOR SMARTER CARS

WAVESTONE

NOKIA

THALES

Partenaires de la Chaire VP-IP

IN GROUPE

BNP PARIBAS

orange™

DASSAULT SYSTEMES

Experts associés

SÉCURITÉ ROUTIÈRE VIVRE, ENSEMBLE.

Partenaire qualifié

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS