Pour une approche globale des risques dans le droit de la protection des données personnelles

Quelle est la nature du risque pour les droits et libertés des personnes physiques dans le règlement général sur la protection des données (RGPD) ? S'agit-il d'un risque de restriction des droits des personnes concernées, ou plutôt de ce qui pourrait mal tourner lors du traitement des données à caractère personnel dans un projet ? Une approche globale de ces risques permettrait une vision plus complète et cohérente des enjeux, tout en favorisant la conformité à la loi et à la protection des droits fondamentaux.

L'évaluation des risques pour les droits et les libertés des personnes physiques est l'une des étapes les plus complexes du processus d'analyse d'impact relative à la protection des données (AIPD)[1] (article 35, paragraphe 7, point c) du RGPD[2].

L'AIPD est un processus technico-juridique qui aide les organisations à prendre de meilleures décisions sur la façon de protéger les données personnelles et de se conformer à la loi. Dans certaines circonstances (article 35 du RGPD), ce processus est légalement requis. Pour chaque AIPD, les évaluateurs doivent d'abord s'interroger sur ce qu'est exactement un risque en matière de protection des données. La démarche consiste ensuite à évaluer conjointement la vraisemblance de survenance de ce risque et sa gravité, ce qui amène à le qualifier de « faible », « moyen » ou « élevé ». Ces informations permettent ensuite de recommander au responsable du traitement des mesures pour atténuer, éliminer, accepter ou transférer le risque. Mais quel type de risque doit

précisément être pris en considération lors de cette analyse ?

Dans un premier temps, il convient de s'interroger sur la portée de l'évaluation des risques pour les droits et libertés. Son objectif se limite-t-il simplement à déterminer la conformité d'un projet au RGPD et, dès lors, au droit à la vie privée ? Dans ce cas, il s'agira alors d'examiner, par exemple, dans quelle mesure le projet pourrait restreindre l'exercice des droits des personnes concernées, et si ces dernières risquent de perdre le contrôle de leurs données à caractère personnel. L'analyse vise-t-elle plutôt à évaluer la vraisemblance et la gravité de ce qui pourrait mal tourner lors du traitement des données à caractère personnel dans le cadre du projet ? Il s'agira alors, par exemple, d'observer si le projet présente un risque accru de fraudes, d'enlèvements, de chantage, de violences ou d'intimidations, notamment si le lieu de résidence des personnes concernées ou de leurs proches venait à être rendu public. Ou peut-être cette analyse vise-t-elle à évaluer ces deux types de risques ?

En second lieu, la question de l'étendue de l'AIPD mérite d'être posée. Doit-elle se limiter aux risques pour les personnes concernées ou doit-elle être élargie ? En effet, il est communément admis que le traitement des données à caractère personnel peut affecter non seulement les personnes concernées, mais également les responsables du traitement, les sous-traitants, les tiers, voire la société dans son ensemble.

Ces difficultés découlent du choix du législateur européen de baser le RGPD – comme de nombreux instruments récents de la législation européenne relative aux données et au numérique – à partir d'une approche fondée sur les risques, dont l'AIPD constitue une illustration emblématique. Cette approche impose aux responsables du traitement et aux sous-traitants d'adapter leurs obligations en fonction du niveau de risque pour les droits et libertés des personnes physiques. Malgré des objectifs clairement affichés visant à renforcer la protection des données, à concilier des intérêts parfois contradictoires et à offrir une plus grande flexibilité dans la mise en œuvre du RGPD, la compréhension et l'évaluation du risque en question soulèvent des enjeux tant conceptuels que pratiques. Afin de relever ces défis, une approche globale est nécessaire afin de clarifier la notion de risque dans ce contexte[3].

Les risques liés à la protection des données ne se limitent pas aux violations de la loi

Tout d'abord, le risque lié à la protection des données va bien au-delà de la simple violation de la loi. Autrement dit, ces risques ne se limitent pas uniquement à une infraction aux principes fondamentaux de protection des données tels que la minimisation ou la limitation de la conservation (article 6 du RGPD). Restreindre l'analyse à ces seules violations reviendrait à omettre des aspects importants en la matière. Plusieurs arrêts de la Cour de justice de l'Union européenne (CJUE) illustrent notre propos.

La CJUE évoque régulièrement le risque d'« *abus* » ou d'« *utilisation abusive* » des données à caractère personnel. Dans l'affaire *Schufa* (2023)[4], la Cour s'est prononcée sur l'usage des scores de crédit par les banques comme aide à la décision en matière de crédit à la consommation. Elle a souligné que les risques associés à la prise de décision automatisée sont « *susceptibles de peser sur les intérêts légitimes et les droits de la personne concernée, notamment compte tenu des effets discriminatoires potentiels à l'égard des personnes physiques* » (§ 59).

Dans l'affaire *Digital Rights Ireland* (2014)[5], la CJUE a déclaré invalide la directive sur la conservation des données à caractère personnel – et, plus précisément, les données techniques de connexion – à des fins d'enquête, de détection et de poursuite des infractions pénales graves. Pour cette raison, la Cour a souligné la nécessité de « *protéger efficacement* [les] *données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données* » (§ 54).

Dans l'affaire *Österreichischer Rundfunk* (2003)[6], relative à la mise à disposition publique des données personnelles sur les revenus des salariés d'entités publiques, la CJUE a estimé que, relativement à « *l'obligation pour les entités publiques soumises au contrôle du Rechnungshof de communiquer à ce dernier les traitements et pensions dépassant un certain niveau* [...] *ainsi que le nom des bénéficiaires, en vue de l'établissement d'un rapport annuel* [...] *mis à la disposition du grand public* », les personnes concernées peuvent « *être lésées du fait des répercussions négatives de la publicité attachée à leurs revenus*

professionnels, notamment sur les perspectives d'embauche qui s'ouvriraient à elles dans d'autres entreprises » (§ 2 et 89).

Dans l'affaire *Puškár* (2017)[7], la CJUE a examiné un recours visant à supprimer le nom d'une personne d'une liste de prête-noms liés à de la criminalité financière. La Cour a examiné si les autorités fiscales nationales « *ont le droit de tenir une liste confidentielle des personnes physiques qui exercent de manière fictive des fonctions de direction auprès de certaines personnes morales* » (conclusions de l'avocat général, § 1) à des fins de perception de l'impôt et de lutte contre la fraude fiscale. La Cour a estimé que – pour la personne concernée – une « *inscription sur cette liste pourrait nuire à sa réputation et affecter ses relations avec les autorités fiscales* » (§ 114).

Dans l'affaire *Latvijas Republikas Saeima* (2021)[8], relative à une législation prévoyant de rendre accessibles les points de pénalité imposés aux conducteurs ayant commis des infractions routières, la CJUE a statué que le RGPD s'y oppose. La Cour a considéré que « *la communication au public de données à caractère personnel relatives aux infractions routières, y compris les points de pénalité imposés pour leur commission,* [...] *peut provoquer la désapprobation de la société et entraîner la stigmatisation de la personne concernée* » (§ 74, 75 et 112). Un raisonnement similaire a été adopté dans l'arrêt *Endemol Shine Finland* (2024 ; § 54)[9], au sujet de la communication orale des données relatives à des condamnations pénales.

Enfin, dernier exemple, dans l'affaire *FT (Copies du dossier médical)* (2023)[10], la Cour a examiné le droit d'obtenir une copie intégrale d'un dossier médical. Elle a estimé qu'un « *simple résumé ou une compilation de ces données par le médecin, afin de les présenter sous une forme synthétique, pourrait créer le risque que certaines données pertinentes soient omises ou reproduites de manière incorrecte ou, en tout état de cause, que la vérification de leur exactitude et de leur exhaustivité ainsi que leur compréhension par le patient en soient rendues plus difficiles* » (§ 78).

Les risques liés à la protection des données ne se limitent pas aux personnes concernées

Le traitement des données à caractère personnel peut également générer des risques distincts, c'est-à-dire des risques qui ne s'appliquent pas exclusivement aux personnes concernées. Cette perspective impose parfois de prendre en compte des conséquences négatives allant au-delà de la portée stricte du RGPD, qui ne protège que les personnes concernées. Trois hypothèses doivent être distinguées.

Premièrement, des conséquences négatives peuvent affecter en particulier les personnes physiques : les personnes concernées mais plus largement d'autres personnes. Au sein de cette catégorie, il convient de distinguer les conséquences substantielles des conséquences formelles. Les conséquences substantielles incluent divers effets tels que les pertes financières, la discrimination ou l'atteinte à l'autonomie, notamment par des actes de manipulation ou de coercition. Elles peuvent également se manifester par des effets dissuasifs, des dommages psychologiques comme la détresse émotionnelle ou la perturbation, ainsi que par des atteintes à la réputation, telles que l'embarras, la honte ou le ridicule. Enfin, ces conséquences substantielles peuvent aller jusqu'à engendrer des dommages physiques, incluant des blessures corporelles, voire le décès. Les conséquences formelles, quant à elles, consistent en des violations des dispositions du RGPD sans qu'il y ait nécessairement un préjudice tangible ou intangible pour une personne physique. Elles incluent les infractions aux principes de protection des données, aux droits des personnes concernées ou aux règles relatives aux transferts internationaux.

Deuxièmement, des conséquences négatives peuvent également atteindre la société tout entière, notamment des groupes, des collectifs ou des communautés. On peut identifier, d'une part, des conséquences pour la démocratie, comprenant des atteintes aux droits et à la justice, aux médias, à l'information et au débat public, ainsi qu'au processus électoral avec un traitement des données dans le but de manipuler, de désinformer ou de discréditer. D'autre part, des conséquences peuvent également être observées dans des domaines particuliers tels que la santé publique, l'environnement et l'économie, comme un traitement des données qui entraînerait un avantage concurrentiel déloyal.

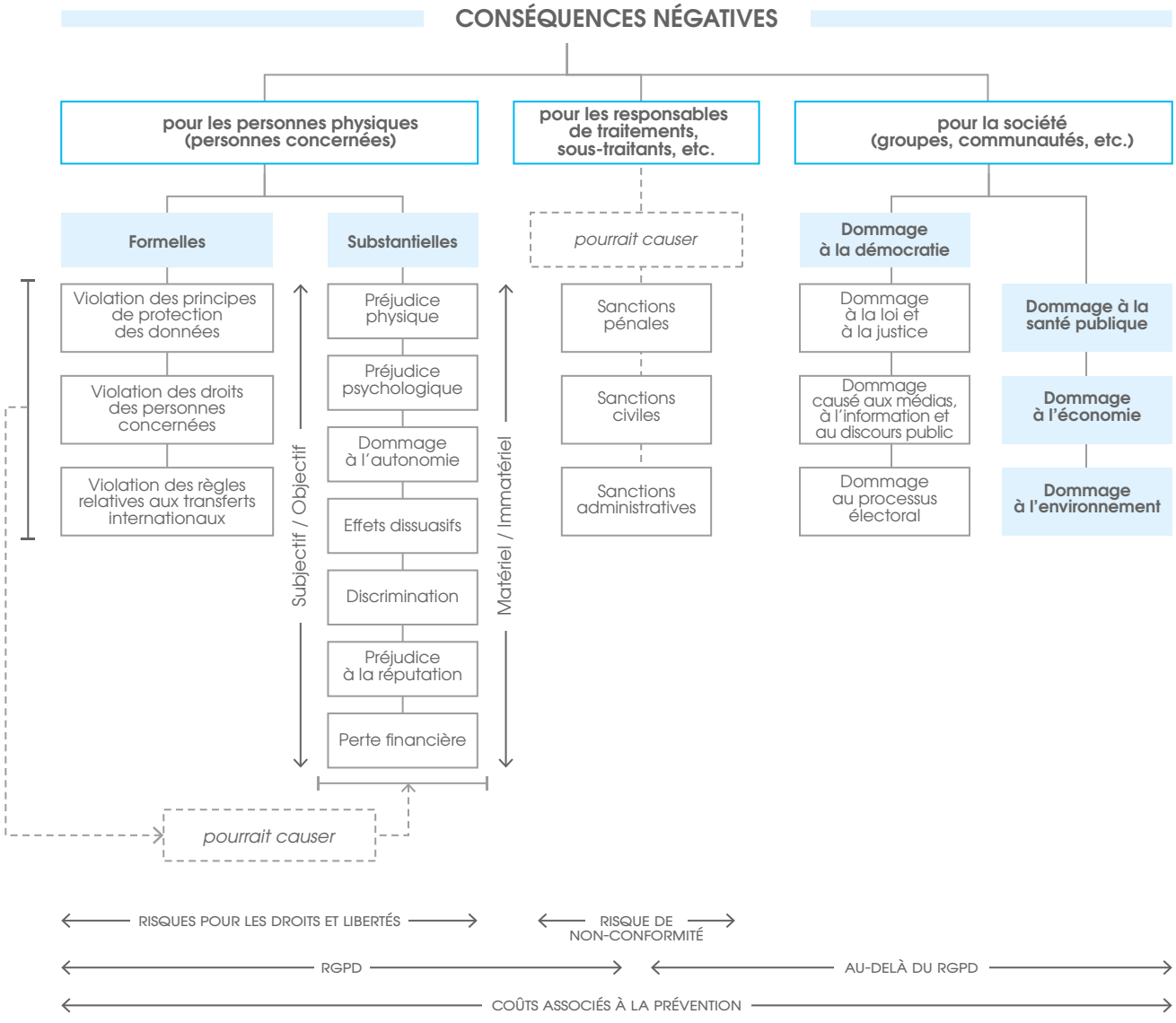
Troisièmement, les conséquences négatives peuvent s'appliquer aux personnes qui traitent les données à caractère personnel d'autrui – principalement les responsables du traitement, les sous-traitants, les destinataires et les tiers.

On peut distinguer, d'une part, les conséquences qui découlent de leur non-respect du RGPD et, d'autre part, les conséquences qui portent préjudice à des personnes physiques ou à la société par le traitement fautif des données à caractère personnel, notamment le risque de non-conformité. Les conséquences sont alors de nature civile, pénale ou administrative. Il pourra s'agir d'une amende infligée par une autorité de protection des données ou encore de dommages et intérêts versés à la personne concernée.

En outre, le coût associé à la prévention ou à la réparation de ces conséquences, qu'il s'agisse de temps, de ressources financières ou humaines, constitue une méta-conséquence pour tous les types de conséquences négatives identifiés.

Vers une typologie des conséquences négatives

Afin de faciliter l'identification des risques liés à la protection des données à caractère personnel, nous proposons une classification des conséquences négatives possibles du traitement des données à caractère personnel telle qu'établie dans le graphique suivant :



Le concept de données à caractère personnel restant ouvert et les évolutions technologiques, économiques et sociétales étant constantes, d'autres conséquences négatives émergeront inévitablement avec le temps.

Cet effort en vaut-il la peine ?

Adopter une approche globale des risques liés à la protection des données (conséquences négatives) permet de dresser un tableau précis et complet des traitements envisagés, tout en contribuant à un niveau élevé de protection des droits fondamentaux. Pour un responsable du traitement, cette approche témoigne d'une diligence raisonnable, réduisant notamment les risques de non-conformité et d'atteinte à la réputation. Par conséquent, un effort supplémentaire – dans le cadre d'une AIPD et chaque fois que le risque pour les droits et des libertés des personnes physiques doit être évalué – apparaît non seulement pertinent, mais également bénéfique à long terme.

Dariusz Kloza, Thibaut D'hulst, Malik Aouadi [11]

Une version antérieure de ce texte a été publiée en juin 2025 par le blog de droit public du CIRC (Centre interdisciplinaire de recherches en droit constitutionnel et administratif, UCLouvain Saint-Louis Bruxelles)[12]*, que nous remercions pour cette aimable autorisation de reproduction.*

1 Voir, par exemple, Kloza Dariusz, van Dijk Niels, Casiraghi Simone, Vazquez Maymir Sergi, Tanas Alessia, « The Concept of Impact Assessment », *in* Burgess J. Peter, Kloza Dariusz (eds), *Border control and new technologies. Addressing integrated impact assessment*, Bruxelles, ASP, 2021, p. 31-48.

2 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO 2016, L 119, p. 1-88.

3 Voir Kloza Dariusz, D'hulst Thibaut, Aouadi Malik, « What could possibly go wrong? On risks to the rights and freedoms of natural persons in EU data protection law, their typologies and their identification », *Technology and Regulation*, 2024, p. 309-329.

4 CJUE, 1re ch., *OQ c./ Land Hessen en présence de SCHUFA Holding AG*, nº C-634/21, 7 décembre 2023.

5 CJUE, GC, *Digital Rights Ireland Ltd et autres*, affaires jointes nº C-293/12 et C-594/12, 8 avril 2014.

6 CJUE, ass. plén., *Österreichischer Rundfunk et autres*, affaires jointes nº C-465/00, C-138/01 et C-139/01, 20 mai 2003.

7 CJUE, 2e ch., *Peter Puškár c./ Finančné riaditeľstvo Slovenskej republiky et autres*, nº C-73/16, 27 septembre 2017.

8 CJUE, GC, *B en présence de Latvijas Republikas Saeima*, nº C-439/19, 22 juin 2021.

9 CJUE, 6e ch., *Endemol Shine Finland* Oy, nº C-740/22, 7 mars 2024.

10 CJUE, 1re ch., *FT c./ DW*, nº C-307/22, 7 mars 2024.

11 Le présent propos n'engage toutefois que ses auteurs.

12 Kloza Dariusz, D'hulst Thibaut, Aouadi Malik, « Et si ça tournait mal ? Des conséquences négatives du traitement des données personnelle en droit européen », CIRC (Centre interdisciplinaire de recherches en droit constitutionnel et administratif, UCLouvain Saint-Louis Bruxelles), 17 juin 2025.