The CDSL Working Paper Series

WP3/2021

CYBER & DATA SECURITY LAB

L'obligation de sécurité des données personnelles : vers un standard de « diligence digitale » ?

Franck Dumortier[1]

[1] Franck Dumortier is a researcher at the Cyber and Data Security Lab and a member of the Research Group on Law, Science, Technology & Society (LSTS) at VUB. This contribution was written in the context of the project "Search and Rescue" which is funded by the European Union's Horizon 2020 research and innovation program under grant agreement no. 882897.

Abstract

The effectivity of the fundamental rights protecting privacy and personal data depends to a large extent on the measures put in place to ensure data security. As early as 2008, in the case of I. v. Finland , the European Court of Human Rights found that the lack of appropriate safeguards to secure data against unauthorized use constituted a violation of the positive obligation to ensure respect for the right to privacy enshrined in Article 8 of the European Convention on Human Rights. It is therefore quite logical that the GDPR now places the principle of personal data security on the same level as the traditional principles of data quality (lawfulness, fairness, transparency, purpose limitation, data minimization, data accuracy and limitation of data retention). According to this "new" principle, data must be processed in such a way as to ensure appropriate security, "including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organizational measures".

The purpose of this contribution is to analyze the duty of security as imposed by the GDPR in light of the recent interpretative work of the data protection authorities and of the European courts. After having recalled the basic concepts and definitions of the GDPR, this paper clarifies the objectives, the nature and the debtors of duty of security, details the methodology of risk analysis and the factors to be taken into account in order to determine appropriate measures, analyzes some of the security measures favored by data protection authorities and, finally, briefly recalls the applicable obligations in case of a data breach.

Table of contents

Introduction

L'effectivité des droits fondamentaux à la vie privée et à la protection des données à caractère personnel dépend considérablement des mesures mises en place pour assurer la sécurité de celles-ci. Déjà en 2008, dans l'affaire *I. c. Finlande* [2], la Cour européenne des droits de l'Homme avait estimé que le défaut de garanties appropriées relatives à la sécurisation des données contre des usages non-autorisés constituait une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'article 8 de la Convention européenne des Droits de l'Homme (ci-après « CEDH »). C'est donc très logiquement que le RGPD[3] érige désormais le principe de sécurité des données à caractère personnel au même rang que les traditionnels principes de qualité de celles-ci (licéité, loyauté, transparence, finalité, minimisation, exactitude et limitation de la conservation des données)[4]. Selon ce « nouveau » principe, les données doivent être traitées de façon à garantir une sécurité appropriée, « y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées »[5].

L'objet de la présente contribution est d'analyser l'obligation de sécurité telle qu'imposée par le RGPD à la lumière de l'œuvre interprétative des autorités de protection des données ainsi que des instances et juridictions européennes[6]. Dans celle-ci, après avoir rappelé les notions et définitions de base du RGPD, nous précisons les objectifs, la nature et les débiteurs de l'obligation de sécurité, clarifions la méthodologie d'analyse de risques ainsi que les facteurs à prendre en compte pour déterminer des mesures appropriées, analysons

[2] Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*, req. n° 20511/03. Dans cette affaire, la requérante infirmière dénonce la consultation illégale de son dossier médical confidentiel par ses collègues de travail. Dans son arrêt, la Cour conclut, à l'unanimité, qu'il y a eu violation de l'article 8, les autorités internes n'ayant pas, au moment des faits, mis les données médicales de la requérante à l'abri d'un accès non autorisé.

[3] 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).

[4] Les principes relatifs au traitement des données à caractère personnel sont listés à l'article 5 du RGPD. Cet article érige la sécurité des données personnelles au rang de principe – ce qui démontre son importance accrue – alors qu'elle n'était pas reprise à l'article 6 de la 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, abrogée par l'entrée en application du RGPD.

[5] Article 5.1, f) du RGPD.

[6] Ne font pas l'objet de la présente contribution les traitements de données tombant hors du champ d'application du RGPD, par exemple parce qu'ils sont soumis à 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. Ne sont pas non plus analysées les obligations de sécurité découlant de l'application d'autres instruments législatifs comme, par exemples, la Directive (UE) 2016/1148 du Parlement Européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ; ou encore le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (Règlement sur la cybersécurité).

quelques mesures de sécurité plébiscitées par les autorités de protection des données et, enfin, rappelons brièvement les obligations applicables en cas de violation de données.

I. Notions et définitions

1. L'interprétation large de la notion de donnée à caractère personnel

Dans un avis[7] datant de 2007, le Groupe 29[8] insistait déjà sur l'interprétation large de la notion de « données à caractère personnel »[9] en analysant les quatre grands éléments constitutifs de la définition, à savoir « toute information », « concernant », « une personne physique », « identifiée ou identifiable ».

Du point de vue de la nature des informations, le concept de données à caractère personnel englobe toutes sortes de renseignements, corrects ou non, à propos d'une personne physique[10]. Il peut s'agir d'informations « objectives » tels les revenus d'une personne concernée ou d'informations « subjectives » sous forme d'avis ou d'appréciations[11]. Du point de vue du contenu des informations, la notion couvre les informations touchant à la vie privée et familiale d'une personne physique, *stricto sensu*, mais également les informations relatives à ses activités, quelles qu'elles soient, tout comme celles concernant ses relations de travail ainsi que son comportement économique ou social indépendamment de sa situation ou de sa qualité (en tant que consommateur, patient, employé, client, etc.).[12] Enfin, s'agissant du format des informations ou du support utilisé pour celles-ci, le concept couvre les informations disponibles sous n'importe quelle forme, qu'elles soient alphabétiques, numériques, graphiques, photographiques ou acoustiques.[13]

---

[7] Groupe 29, WP136, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, p.4.
[8] Le Groupe de travail « Article 29 » (ci-après « Groupe 29 ») est le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du RGPD). Depuis lors, il a été remplacé par le Comité européen de la protection des données (ci-après « EDPB »).
[9] Le concept de « données à caractère personnel » est défini par l'article 4, 1) du RGPD comme étant « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».
[10] La protection conférée par le Règlement s'applique aux personnes physiques mais ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales. Voy. considérant 14 du RGPD.
[11] Dans l'arrêt Nowak, la CJUE énonce clairement que la notion de données à caractère personnel couvre tant les données qui résultent d'éléments objectifs, vérifiables et contestables que des données subjectives qui contiennent une évaluation ou un jugement porté sur la personne concernée. Voy. CJUE, arrêt *Nowak*, 20 décembre 2017, C-434/16.
[12] Cour eur. D. H., 16 février 2000, *Amann c. Suisse*, req. n° 27798/95, point 65: «[…]le terme «vie privée» ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de «vie privée» (arrêts Niemietz/Allemagne du 16 décembre 1992, série A n° 251-B, pp. 33-34, § 29 et Halford précité, pp. 1015-1016, § 42). Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 […] ».
[13] Groupe 29, WP136, *op.cit.*, p.6 à 9.

Afin de considérer que les données « concernent » une personne physique, la présence d'un élément de « contenu », de « finalité » ou de « résultat » est indispensable[14]. L'élément de « contenu » est présent lorsque des informations ont trait à une personne. A titre purement illustratif, l'Autorité de Protection des Données (ci-après « APD ») nationale a récemment considéré qu'une photo/vidéo d'une cheminée en tant que telle n'est pas une donnée à caractère personnel auquel s'applique le RGPD, « mais qu'il est par contre bien question d'un traitement de données à caractère personnel dès lors que la vidéo est publiée avec le nom et l'adresse de la personne concernée »[15]. L'élément de « finalité » est, quant à lui, considéré comme réalisé lorsque des données sont utilisées ou susceptibles d'être utilisées afin d'évaluer, de traiter d'une certaine manière ou d'influer sur le statut ou le comportement d'une personne physique. Enfin, l'élément de « résultat » est matérialisé lorsque des données sont susceptibles d'avoir un impact sur certains des droits et intérêts d'une personne, compte tenu de l'ensemble des circonstances du cas d'espèce. A cet égard, il convient de relever qu'il n'est pas nécessaire que le résultat potentiel ait un impact majeur. Il suffit qu'une personne physique puisse être traitée différemment par rapport à d'autres personnes à la suite du traitement de ses données.[16]

Une personne physique est considérée comme « identifiée » lorsque, au sein d'un groupe de personnes, elle se « distingue » de tous les autres membres de ce groupe. Elle est « identifiable » lorsque, même sans avoir encore été identifiée, il est possible de le faire (comme l'exprime le suffixe « -able »)[17]. En principe, l'identification est possible au moyen d'informations spécifiques que l'on peut appeler « identifiants » directs – dont le nom de la personne est évidemment le plus courant − ou indirects par le biais du phénomène des « combinaisons uniques » qui permettent de distinguer quelqu'un parmi d'autres. Par exemple, les fichiers informatiques peuvent attribuer un identifiant spécifique aux personnes enregistrées pour éviter toute confusion entre deux personnes se trouvant dans un même fichier, sans même s'enquérir du nom et de l'adresse des sujets[18]. La Cour de justice de l'Union européenne (ci-après « CJUE ») a également précisé que pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel », il n'est pas requis que toutes les

[14] Ces trois éléments (contenu, finalité, résultat) sont à considérer comme des conditions alternatives, et non cumulatives.
[15] APD, Chambre contentieuse, Décision quant au fond 71/2020 du 30 octobre 2020, p.20.
[16] A titre indicatif, le considérant 26 du GDPR considère les données utilisées à des fins de « ciblage » comme étant couvertes par la notion. Un exemple type est l'activité de publicité ciblée : « the ad network does not need to know who the person that visited a website is, it is enough to know that this person is the same person who earlier visited sites A and B and sometimes clicks on ads for product C ». Voy. EDRI, Key aspects of the proposed General Data Protection Regulation explained, disponible à l'adresse https://edri.org/files/GDPR-key-issues-explained.pdf..
[17] Le considérant 30 du RGPD indique que « les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes ».
[18] Groupe 29, WP136, *op.cit.*, pp. 14-15.

informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne[19]. Pour déterminer si une personne physique est identifiable, il convient donc de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement. Afin d'établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il faut prendre en compte l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci[20].

Le critère des moyens « susceptibles d'être raisonnablement mis en œuvre » à des fins d'identification (soit par le responsable du traitement, soit par un tiers) est extrêmement important puisqu'il est celui qui permet de distinguer les données à caractère personnel des données anonymes auxquelles la législation européenne sur la protection des données ne s'applique plus.

2. Le régime applicable aux données anonym(isé)es

Sont exclues du champ d'application du Règlement, les données anonymes − c'est-à-dire les informations ne concernant pas une personne physique identifiée ou identifiable − et les données anonymisées, soit celles rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable[21]. L'anonymisation peut donc être le résultat du traitement de données à caractère personnel dans le but d'empêcher irréversiblement l'identification de la personne concernée[22]. Attention toutefois, le processus d'anonymisation en lui-même constitue un traitement de données à caractère personnel ; et à ce titre, il est soumis aux exigences du Règlement jusqu'au moment où les données sont effectivement rendues anonymes[23].

Pour apprécier si le procédé d'anonymisation est suffisamment fiable, c'est-à-dire si l'identification est devenue « raisonnablement » impossible, le critère des « moyens susceptibles d'être raisonnablement mis en œuvre » doit être appliqué[24]. A cet égard, il s'agit d'être particulièrement attentif puisque, selon le Groupe 29, les deux grandes familles de techniques d'anonymisation – la randomisation[25] et la généralisation[26] des

[19] CJUE, 19 octobre 2016, arrêt *Breyer*, C-582/14, point 43.
[20] Considérant 26 du RGPD.
[21] *Ibidem.*
[22] Groupe 29, Avis 05/2014 sur les techniques d'anonymisation, WP216, adopté le 10 avril 2014, p.7.
[23] *Ibid.*, p.3.
[24] *Ibid.*, p.9.
[25] *Ibid*, p.13. Selon le Groupe 29, « La randomisation est une famille de techniques qui altèrent la véracité des données afin d'affaiblir le lien entre les données et l'individu. Si les données sont suffisamment incertaines, elles ne peuvent plus être rattachées à un individu en particulier. En elle-même, la randomisation ne réduira pas la singularité de chaque enregistrement, qui sera toujours dérivé d'une seule personne concernée, mais elle peut apporter une protection contre les attaques/risques relevant de l'inférence et peut être combinée avec des techniques de généralisation pour offrir de meilleures garanties de respect de la vie privée ».
[26] *Ibid*, p.18. Selon le Groupe 29, « La généralisation constitue la seconde famille de techniques d'anonymisation. Cette approche consiste à généraliser, ou diluer, les attributs des personnes concernées en modifiant leur échelle ou leur ordre de grandeur respectif

données – présentent des lacunes, même si chacune d'elles peut être appropriée, selon les circonstances et le contexte[27]. Lors du choix d'appliquer une technique donnée, trois risques essentiels en matière d'anonymisation doivent être pris en compte : 1) l'individualisation, qui correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données; 2) la corrélation, qui consiste dans 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) ; 3) l'inférence, qui est 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[28]. D'après le Groupe 29, la solution optimale devrait être choisie au cas par cas. Une solution (c'est-à-dire un processus d'anonymisation complet) répondant aux trois critères susmentionnés résisterait aux tentatives d'identification utilisant les moyens les plus susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement des données ou par des tiers. Lorsqu'un des critères n'est pas rempli par une proposition, il convient de procéder à une évaluation approfondie des risques d'identification, et le cas échéant d'opter pour une combinaison de techniques en vue de renforcer la fiabilité du résultat[29].

Une fois la technique/ la combinaison de techniques appliquée, le processus d'anonymisation « devrait être, dans l'état actuel de la technologie, aussi permanent qu'un effacement, c'est-à-dire qu'il devrait rendre impossible tout traitement de données à caractère personnel »[30]. En effet, les données « ne perdent leur qualification de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat »[31]. En pratique, cela signifie qu'un processus d'anonymisation robuste vise à réduire le risque de réidentification en dessous d'un certain seuil qui dépendra de plusieurs facteurs tels que la nature des données originales, les mécanismes de contrôle en place (y compris les mesures de sécurité restreignant l'accès aux ensembles de données), la taille de l'échantillon (aspects quantitatifs), la disponibilité de ressources d'informations publiques (sur lesquelles peuvent s'appuyer les destinataires), la communication envisagée de données à des

(par exemple, une région plutôt qu'une ville, un mois plutôt qu'une semaine). Si la généralisation peut être efficace pour empêcher l'individualisation, elle ne garantit pas une anonymisation effective dans tous les cas; en particulier, elle requiert des approches quantitatives spécifiques et sophistiquées afin de prévenir la corrélation et l'inférence ».

[27] *Ibid*., p.11. Parmi les éléments contextuels à prendre en considération, le Groupe cite « par exemple, la nature des données originales, les mécanismes de contrôle en place (y compris les mesures de sécurité restreignant l'accès aux ensembles de données), la taille de l'échantillon (aspects quantitatifs), la disponibilité de ressources d'informations publiques (sur lesquelles peuvent s'appuyer les destinataires), la communication envisagée de données à des tiers (limitée ou illimitée, par exemple sur l'internet, etc.) ».

[28] *Ibid*., p. 13.

[29] *Ibid*. pp. 26-27.

[30] *Ibid*., p.6.

[31] Exposé des motifs de la loi du 11 décembre 1998, Doc. Parl., Chambre, sess. ord. 1997-1998, n° 1566/1, p. 12.

tiers (limitée ou illimitée, par exemple sur l'internet, etc.)[32]. Bien qu'une anonymisation à 100 % soit l'objectif le plus souhaitable, un risque résiduel de réidentification doit donc souvent être pris en compte[33]. Par conséquent, une bonne pratique est de documenter la ou les techniques d'anonymisation mise(s) en œuvre et de réexaminer régulièrement les risques de réidentification au vu des développements techniques et des possibilités de croisement des données.

Afin d'éviter certains écueils et idées fausses, il est également important de rappeler que la pseudonymisation[34] n'est pas une méthode d'anonymisation. Le pseudonymat n'est pas de nature à empêcher qu'une personne concernée soit identifiable et reste donc dans le champ d'application du régime juridique de la protection des données. Cette technique réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne et constitue par conséquent une mesure de sécurité utile que nous analysons plus loin.

3. Les traitements régis par le RGPD

Pour que le RGPD soit d'application, il doit y avoir « traitement » de données à caractère personnel. L'article 4, 2) du RGPD définit le « traitement » comme étant « 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 ».

Le RGPD s'applique dès que les opérations effectuées sur des données personnelles se réalisent par des moyens automatisés. Le règlement s'applique donc, par exemple, à une base de données informatique où sont enregistrés les clients ou les fournisseurs d'une société, au système de vidéosurveillance d'une société, à la liste électronique des opérations effectuées sur un compte en banque, au fichier informatisé du personnel d'une entreprise ou des enfants inscrits dans une école.[35]

---

[32] Groupe 29, WP136, *op.cit.*, pp. 27-28.

[33] AEPD-EDPS joint paper on 10 misunderstandings related to anonymization, avril 2021, p. 5, disponible à l'adresse https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf

[34] L'article 4(5) du RGPD définit la pseudonymisation comme étant « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

[35] Dans le contexte du COVID-19, l'APD nationale a eu l'occasion de rappeler que l'utilisation de scanners de fièvre numériques perfectionnés, de caméras thermiques ou d'autres systèmes automatisés qui mesurent le niveau de température corporelle constitue en soi un traitement de données à caractère personnel, même en l'absence d'enregistrement des données. Voy. APD, Lignes

Afin d'éviter de créer un risque grave de contournement et d'être neutre sur le plan technologique, la définition s'applique non seulement aux traitements effectués à l'aide de procédés automatisés mais également aux traitements manuels si les données à caractère personnel sont contenues ou destinées à être contenues dans un « fichier. »[36] Par « fichier », le RGPD vise « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».[37] A contrario, les dossiers ou ensembles de dossiers de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne relèvent pas du champ d'application du règlement.[38]

La règle générale est donc que le Règlement s'applique à la plupart des situations. À notre époque, le stockage non automatisé (et non structuré) de données est devenu si rare qu'il est presque devenu introuvable et limité à des situations très spécifiques.[39]

Une exception importante mérite toutefois d'être relevée : le RGPD ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Sont par exemple considérées comme activités personnelles ou domestiques l'échange de correspondance et la tenue d'un carnet d'adresses ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités.[40] Cette exception est néanmoins toute relative dans le cyberespace. En effet, l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs

directrices relatives aux contrôles de température, 4 février 2021, disponibles à l'adresse https://www.autoriteprotectiondonnees.be/citoyen/themes/covid-19/prise-de-temperature

[36] Considérant 15 du RGPD.

[37] Article 4, 6) du RGPD.

[38] Prenons, par exemple, l'enregistrement de la température dans un contexte scolaire. Même si la température lue proprement dite n'est pas enregistrée, mais qu'une remarque est inscrite dans le dossier de l'élève pour indiquer une absence ou une maladie, il s'agit évidemment d'un traitement de données à caractère personnel

[39] Pensons, par exemple à des dossiers manuels qui sont conservés sans le moindre archivage structuré, comme un recueil non classé d'articles de presse dans des archives.

[40] Considérant 18 du RGPD. Notons néanmoins que « les activités de certains utilisateurs de services de réseaux sociaux (ci-après « SRS ») peuvent dépasser une activité purement personnelle ou domestique, quand, par exemple, le SRS est utilisé comme une plate-forme de collaboration pour une association ou une entreprise. L'exemption ne s'applique pas si un utilisateur de SRS agit au nom d'une entreprise ou d'une association ou qu'il utilise le SRS principalement comme une plate-forme à des fins commerciales, politiques ou sociales ». Dans la même logique, « lorsque l'accès aux informations du profil va au-delà des contacts choisis, notamment quand tous les membres appartenant au SRS peuvent accéder à un profil ou que les données sont indexables par les moteurs de recherche, l'accès dépasse la sphère personnelle ou domestique. De même, si un utilisateur décide, en parfaite connaissance de cause, d'élargir l'accès au-delà des « amis » choisis, il endosse les responsabilités d'un responsable du traitement des données ». Groupe 29, Avis 5/2009 sur les réseaux sociaux en ligne, 12 juin 2009, p. 6.

conditions de travail et à leurs passe-temps, a été considéré comme étant soumise au régime de protection des données.[41]

II. Les objectifs, la nature et les débiteurs de l'obligation de sécurité

1. Les objectifs de l'obligation de sécurité

Sous l'empire du RGPD, l'obligation de sécurité a pour but de prévenir toute violation de données à caractère personnel, c'est-à-dire toute violation de la sécurité « entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »[42]. Dans ses lignes directrices, le Groupe 29 catégorise les violations de données selon les trois objectifs classiques[43] de la sécurité de l'information, à savoir la confidentialité, l'intégrité et la disponibilité des données : une « violation de la confidentialité » entraîne la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel ; une « violation de l'intégrité » génère l'altération non autorisée ou accidentelle des données ; et enfin, une « violation de la disponibilité » a pour conséquence la destruction ou la perte accidentelles ou non autorisées de l'accès aux données[44].

L'APD nationale définit la propriété de confidentialité comme étant celle d'une information « de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à des personnes, entités ou processus autorisés »[45]. L'obligation qui en découle d'accorder un accès sélectif aux informations doit être assurée tout au long du traitement, notamment au cours de la collecte, de la conservation, et de la communication des données. A titre illustratif, dans une décision récente, l'APD nationale a condamné un responsable du traitement ayant négligé de mettre en œuvre des mesures techniques et organisationnelles adéquates pour éviter des consultations illicites, par l'un de ses employés, dans la Centrale de Crédits aux Particuliers[46]. Dans une autre décision, l'APD considère que l'envoi d'un email, dont tous les destinataires placés en copie sont visibles, a favorisé la diffusion non sollicitée de l'adresse électronique du plaignant à des

[41] CJCE, arrêt du 6 novembre 2003, arrêt *Bodil Lindqvist*, C-101/01.
[42] Article 4(12) du RGPD.
[43] L'ISO 27000 insiste particulièrement sur le triptyque « Disponibilité – Intégrité – Confidentialité ». Les normes ISO sont établies par l'organisation internationale de normalisation. La famille de normes ISO 27xxx (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems - Overview and vocabulary) en matière de gestion de la sécurité de l'information (ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (second edition) et de diverses implémentations (ISO 27002 – ISO 27017 – ISO 27018…) est considérée comme une véritable référence dans le domaine.
[44] Groupe 29, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, version révisée et adoptée le 6 février 2018, WP250rev.01, p.8.
[45] Voy. la note de l'APD relative à la sécurité des donnée à caractère personnel, p.1, , disponible à l'adresse https://www.autoriteprotectiondonnees.be/publications/note-relative-a-la-securite-des-donnees-a-caractere-personnel.pdf
[46] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021.

tierces personnes[47]. Un dernier exemple d'atteinte à la confidentialité, cité par l'EDPB, est celui d'une exfiltration de données − qu'une agence de recrutement avait collectées par le biais de formulaires de candidature en ligne − suite au placement d'un code malveillant sur le site web de celle-ci[48].

En ce qui concerne la propriété d'intégrité, le Groupe 29 considère que celle-ci peut se définir comme « la qualité en vertu de laquelle les données sont authentiques et n'ont pas été modifiées par mégarde ou malveillance pendant le traitement, le stockage ou la transmission. La notion d'intégrité peut s'étendre aux systèmes informatiques et exige que le traitement des données à caractère personnel sur ces systèmes reste inaltéré »[49]. En guise d'exemple, en juin 2021, l'APD norvégienne eut à se prononcer sur une fusion de systèmes informatiques contenant les dossiers médicaux de deux municipalités lors de laquelle plusieurs erreurs se sont produites. Certaines personnes ont notamment été enregistrées comme ayant reçu des vaccins, alors qu'en réalité elles n'en avaient pas reçu, et d'autres ont été enregistrées à tort comme n'ayant pas reçu de vaccin, alors qu'elles en avaient reçu[50].

Enfin, pour ce qui est de la propriété de disponibilité, l'APD nationale la définit comme étant « la propriété des informations, systèmes et processus d'être accessibles et utilisables sur demande d'une entité autorisée »[51]. Dans la même ligne, le Groupe 29 affirme qu'assurer la disponibilité, « c'est garantir un accès fiable et en temps opportun aux données à caractère personnel »[52]. En guise d'illustration, en janvier 2021, l'APD italienne eut à connaître d'un cas de vol de disque dur externe dans une administration[53]. Ce dernier était connecté à un serveur installé dans une pièce à laquelle tous les employés avaient accès. Le disque dur en question contenait, entre autres, des documents de travail ainsi des données concernant les travailleurs. Etant donné que les opérations de backup n'avaient pas pu aboutir, les données ont presque toutes été irrémédiablement perdues. Par conséquent, le responsable du traitement fut condamné, notamment, pour n'avoir pas mis en œuvre de

[47] APD, Chambre contentieuse, Décision quant au fond 53/2020 du 1er septembre 2020.
[48] EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 January 2021, p.14.
[49] Groupe 29, Avis 05/2012 sur l'informatique en nuage, adopté le 1er juillet 2012, WP196, p.18. Dans la même ligne, l'APD nationale considère que la propriété d'intégrité couvre deux aspects différents : l'intégrité des informations et l'intégrité des systèmes et processus. Selon celle-ci, « l'intégrité d'une information est la propriété de ne pas être altérée ou détruite de manière non autorisée, volontairement ou accidentellement. L'intégrité d'un système ou d'un processus est la propriété de réaliser la fonction désirée de façon complète et selon les attentes, sans être altérée par une intervention non autorisée, volontaire ou accidentelle ». Voy. la note de l'APD relative à la sécurité des donnée à caractère personnel, *op.cit.*, p.2.
[50] Datatilsynet, Vedtak om overtredelsesgebyr – Moss commune, 20/10671-12- INAN, 4 juin 2021.
[51] APD, note relative à la sécurité des données à caractère personnel, *op.cit*, p.2.
[52] Groupe 29, Avis 05/2012 sur l'informatique en nuage, *op.cit.*, p. 17. Le Groupe ajoute, en outre, que la notion de « violation de la disponibilité » englobe, non seulement la destruction et la perte accidentelles ou illicites de données à caractère personnel, mais également la perte d'accès accidentelle ou non-autorisée à celles-ci. De plus, il précise qu'une perte de disponibilité temporaire des données à caractère personnel doit aussi être considérée comme une violation. Voy. Groupe 29, WP250rev01, *op.cit*., pp. 8-9.
[53] Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Agenzia regionale protezione ambientale Campania (ARPAC), n°9538748, 14 janvier 2021.

mesures nécessaires pour permettre la continuité, sur une base permanente, et le rétablissement de la disponibilité des données personnelles volées.

Il convient également de noter qu'en fonction des circonstances, une violation peut concerner à la fois la confidentialité, l'intégrité et la disponibilité de données à caractère personnel ou une combinaison de ces éléments. Ainsi, dans notre dernier exemple, le vol du disque dur externe a potentiellement pu porter atteinte à la confidentialité des données en sus de leur disponibilité.

En outre, les trois propriétés de sécurité susmentionnées doivent être comprises comme étant « des finalités de base auxquelles s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité) ».[54] En effet, vu le nombre d'intervenants, d'équipements et de processus impliqués dans les environnements numériques, des mesures permettant d'imputer adéquatement les responsabilités en cas d'incident s'avèrent extrêmement utiles afin d'en identifier l'origine ainsi que pour permettre aux personnes lésées d'exercer leurs droits en cas de dommage. Pour ces raisons, les principaux standards internationaux en matière de sécurité informationnelle − dont la suite ISO 27xxx[55] − considèrent qu'outre les trois critères de sécurité classiques s'ajoutent d'autres propriétés, parmi lesquelles l'imputabilité « qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) »[56]. A cet égard dans deux décisions récentes, l'APD nationale a rappelé que « l'imputabilité s'exprime notamment de façon concrète par la tenue d'un registre des log files selon le principe de journalisation des accès »[57].

[54] S. GHERNAOUTI, *Sécurité informatique et réseaux*, Dunod, 2013., p. 1.
[55] Les normes ISO sont établies par l'organisation internationale de normalisation. La famille de normes ISO 27xxx (ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems - Overview and vocabulary) en matière de gestion de la sécurité de l'information (ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (second edition) et de diverses implémentations (ISO 27002 – ISO 27017 – ISO 27018…) est considérée comme une véritable référence dans le domaine.
[56] APD, « note relative à la sécurité des données à caractère personnel », *op.cit.*, p.2.
[57] Voy. APD, Chambre contentieuse, Décision quant au fond 15/2021, *op.cit.*, p.20 et Décision quant au fond 56/2021, *op.cit.*, p.17.

2. *Une obligation de sécurité liée au principe d'accountability*

En vertu du principe de responsabilité, ou d'*accountability*[58], énoncé par les articles 5.2 et 24 du RGPD, c'est au responsable du traitement[59] − c'est-à-dire à l'entité qui décide de certains éléments clés du traitement − qu'il appartient de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué en conformité avec le Règlement, y compris avec le principe de sécurisation des données prescrit par l'article 5.1, f). Il doit, par conséquent, être à même de démontrer l'efficacité[60] des mesures, lesquelles doivent être réexaminées et actualisées si nécessaire[61] et comprendre la mise en œuvre de politiques appropriées[62] permettant, en cas de contrôle, d'apporter la preuve des garanties appliquées.

Afin d'identifier le responsable du traitement, « on partira du principe qu'une société ou un organisme public est responsable en tant que tel des opérations de traitement qui se déroulent dans son domaine d'activités et de risques »[63], et non une personne physique en son sein. Etant donné que c'est au responsable du traitement que les personnes concernées s'adresseront lorsqu'elles désireront exercer les droits que leur confère le régime de protection des données, la désignation d'une entité stable et fiable est effectivement préférable.

Une analyse distincte s'impose toutefois si une personne physique agissant au sein d'une personne morale utilise des données à des fins personnelles, en dehors du cadre et de l'éventuel contrôle des activités de la personne morale. Dans la mesure où un employé traite des données à caractère personnel pour ses propres finalités, distinctes de celles de son employeur, il doit être considéré comme responsable du traitement et assumer toutes les conséquences et responsabilités qui en découlent[64]. Néanmoins, comme le rappelle la CJUE

---

[58] Selon le Groupe 29, « En français, le texte du RGPD utilise le terme « responsabilité ». En anglais, on utilise le terme « accountability », issu du monde anglo-saxon où il est d'usage courant et où il existe un vaste consensus sur le sens à lui donner – bien qu'il soit difficile d'en définir avec précision le sens dans la pratique. Globalement, on peut toutefois dire qu'il met l'accent sur la manière dont la responsabilité (responsability) est assumée et sur la manière de le vérifier. En anglais, les termes « responsibility » et « accountability » sont comme l'avers et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (responsability) est efficacement assumée dans la pratique ». Groupe 29, Avis n° 3/2010 sur le principe de la responsabilité, WP173, 13 juillet 2010, p.8.

[59] Le responsable du traitement est défini par l'article 4(7) du RGPD comme étant « 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 […] ».

[60] Considérant 74 du RGPD.

[61] Article 24.1 du RGPD.

[62] Article 24.2 du RGPD.

[63] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP169, p. 17. Selon le groupe, « parfois, les sociétés et les organismes publics désignent une personne précise pour être responsable de l'exécution des opérations de traitement. Cependant, même lorsqu'une personne physique est désignée pour veiller au respect des principes de protection des données ou pour traiter des données à caractère personnel, elle n'est pas responsable du traitement mais agit pour le compte de la personne morale (société ou organisme public), qui demeure responsable en cas de violation des principes, en sa qualité de responsable du traitement ».

[64] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, p. 27.

dans son arrêt *Wirtschaftsakademie* du 5 juin 2018, « la notion de responsable du traitement ne renvoie pas nécessairement à un organisme unique et peut concerner plusieurs acteurs »[65]. Par conséquent, le responsable du traitement initial pourrait conserver une certaine part de responsabilité si le nouveau traitement a eu lieu du fait d'une insuffisance des mesures de sécurité[66]. C'est en suivant ce raisonnement que, dans une décision d'avril 2021[67], l'APD nationale opère la distinction suivante : d'une part, un employé indélicat doit être considéré comme responsable du traitement spécifiquement pour ses consultations abusives ; de l'autre, il revient au responsable de traitement initial d'implémenter des mesures techniques et organisationnelles appropriées pour éviter de tels traitements abusifs. Et pour cause, « si 'employeur devait être exempté de toute responsabilité de sécurité pour les traitements irréguliers de ses employés effectués dans le cadre de leurs fonctions, même à des fins propres, ceci enlèverait une partie de son effet utile du RGPD »[68]. En application des dispositions relatives à la protection des données dès la conception et par défaut[69], le responsable du traitement initial doit donc intégrer le nécessaire respect du Règlement en amont de ses actes et procédures, en adoptant des règles internes[70] – utilement documentées dans la politique de sécurité de l'information – en vue, entre autres[71], de limiter l'accès aux données aux seules personnes qui en justifient le besoin par l'exercice de leurs fonctions ou du service[72]. Afin de pouvoir démontrer l'efficacité desdites mesures, un responsable diligent veillera également à pouvoir justifier l'exécution d'audits internes et/ou externes réguliers[73].

En outre, il s'agit de distinguer la question de l'employé indélicat de la situation dans laquelle le responsable du traitement fait appel à un sous-traitant[74]. Ainsi que le précise l'APD nationale, « l'existence de la sous-traitance dépend du responsable de traitement qui doit avoir décidé de ne pas réaliser lui-même le traitement dont il maitrise la ou les finalités et/ou moyens mais d'en déléguer tout ou une partie des opérations à une autre personne ou organisation extérieure que la sienne. Cette autre personne doit être juridiquement distincte de l'organisation du responsable de traitement et doit réaliser les opérations de traitement de données à caractère personnel déléguées pour le compte de ce dernier et conformément à ses instructions documentées

[65] CJUE, arrêt *Wirtschaftsakademie*, C-210/16, 5 juin 2018, §29.
[66] Groupe 29, WP169, *op.cit.*, p.17.
[67] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021.
[68] Ibid., p.14.
[69] Article 25 du RGPD.
[70] Considérant 78 du RGPD.
[71] Dans son WP173 précité, le Groupe 29 reprend une liste non exhaustive de « mesures de responsabilité » telles que l'instauration de procédures internes, la mise en place de politiques de protection des données écrites et contraignantes, la désignation d'un délégué à la protection des données, l'élaboration de procédures internes pour une gestion et une déclaration efficaces des infractions.
[72] Voy. la note de l'APD relative à la sécurité des donnée à caractère personnel, *op.cit.*, p.4.
[73] Groupe 29, WP173, *op.cit.*, pp.16-17.
[74] Le sous-traitant est défini par l'article 4(8) du RGPD comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

»[75]. Dans ce cas, l'obligation d'*accountability* du responsable s'étend aux traitements réalisés, pour son compte, par le sous-traitant[76]. C'est à ce titre que le premier doit d'assurer au préalable que le second présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées[77]. C'est dans cette optique également que l'article 28.3 du RGPD requiert qu'un contrat ou un acte juridique contraignant régisse les relations entre les deux parties. Cette convention doit revêtir la forme écrite aux fins de preuve[78] et, en principe être signée par chacune des parties[79]. Elle doit, en outre, contenir un certain nombre de clauses obligatoires[80], prévoyant notamment que le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable, qu'il doit prendre toutes les mesures requises pour sécuriser les données et veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité. Le contrat de sous-traitance doit également obligatoirement prévoir que le sous-traitant aide le responsable du traitement à garantir sa propre obligation de sécurité[81] et qu'il mette à la disposition du responsable du traitement toutes les informations nécessaires pour en démontrer le respect, ainsi que pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et qu'il contribue à ces audits[82]. Pour le surplus, il convient d'indiquer qu'outre les mentions imposées par l'article 28.3 du RGPD, rien n'empêche le contrat de sous-traitance de contenir des instructions additionnelles en matière de sécurité informationnelle auxquelles le sous-traitant devra se conformer. A l'inverse, le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne peut pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données[83].

En pratique, il s'agit également d'être attentif au fait que non seulement plusieurs parties peuvent intervenir en tant que sous-traitants mais qu'il est également habituel que des sous-traitants confient des activités à des sous-traitants de second rang. Dans ce cas, le RGPD prévoit que le sous-traitant ne peut pas recruter un autre

[75] Note de l'APD "Le point sur les notions de responsable de traitement / sous-traitant au regard du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats", septembre 2018, p 2.
[76] Considérant 74 du RGPD.
[77] Article 28.1 et considérant 81 du RGPD.
[78] Groupe 29, WP169, *op.cit.*, p.28.
[79] Dans une récente décision, l'APD admet toutefois une entente entre les parties au sujet de ce contrat de sous-traitance. Dans le cas d'espèce, ce contrat avait été établi par le responsable du traitement avant l'entrée en vigueur du RGPD mais n'avait pas encore été signé par lui. Il avait par contre déjà été signé par le sous-traitant. Voy. APD, Chambre Contentieuse, Décision quant au fond 22/2020 du 8 mai 2020.
[80] Celles-ci sont énumérées à l'article 28.3 du RGPD.
[81] Article 28.3, f), du RGPD.
[82] Article 28.3, f) et h), du RGPD.
[83] Groupe 29, WP169, *op.cit.*, p.28.

sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement[84]. De plus, le contrat régissant les relations entre le sous-traitant et le sous-traitant de second rang doit contenir les mêmes obligations en matière de protection de données que celles fixées dans le contrat entre le responsable du traitement et le sous-traitant, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées[85]. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant principal demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations[86].

3. *La nature de l'obligation de sécurité et ses débiteurs*

L'article 32 du RGPD considère non seulement le responsable du traitement mais également le sous-traitant comme débiteurs de l'obligation de sécurité. Tous deux doivent mettre en œuvre des mesures de sécurité appropriées pour garantir un niveau de sécurité adapté aux « risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[87] tout en prenant en compte l'état des connaissances, les coûts de mise en œuvre ainsi que la nature, la portée, le contexte et les finalités du traitement. Autrement dit, l'exigence de sécurité est « modalisable en fonction de la nature des données, des circonstances qui entourent leur traitement et des risques que celui-ci fait courir aux personnes concernées »[88]. Par conséquent, l'obligation légale de sécurisation doit être interprétée comme étant une obligation de moyens[89] ne mettant en jeu la responsabilité de ses débiteurs que s'il est démontré que ces derniers ont commis une faute en n'utilisant pas les moyens nécessaires pour l'éviter. Une telle qualification s'impose, d'une part, parce que l'utopie du risque nul est un mythe[90], et, d'autre part, parce que le RGPD laisse à ses débiteurs le soin d'évaluer les risques de leurs traitements afin de choisir les mesures appropriées pour les atténuer. Il en résulte qu'en cas de violation de sécurité, la charge de la preuve quant au caractère inapproprié des mesures mises en place échoit au créancier qui devra établir que le débiteur n'a pas été suffisamment prudent ou diligent dans la mise en œuvre de moyens qui auraient été nécessaires pour l'éviter. Une affirmation qui mérite néanmoins d'être

[84] Article 28.2 du RGPD. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.
[85] Article 28.4 du RGPD.
[86] *Ibidem.*
[87] Art. 32.1 du RGPD.
[88] C. DE TERWANGNE, « La réforme de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » in *Quelle protection des données personnelles en Europe ?*, Larcier, 2015, p. 113.
[89] « On se situe d'ailleurs pour l'essentiel dans le cadre d'obligations de moyens et ne seront nécessaires que les mesures dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent ». Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Doc. Parl., Ch. repr., Sess. ord. 1990- 1991, doc. 1610/1, 6 mai 1991, p.21.
[90] APD, « Note relative à la sécurité des données à caractère personnel », *op.cit.*, p.8.

fortement nuancée puisque que l'exigence d'*accountability*[91] a pour effet de renforcer cette obligation de moyens en imposant au responsable du traitement d'être en mesure de démontrer l'opportunité du choix des mesures de sécurité et leur efficacité sur demande de l'autorité de contrôle.

En cas de manquement, la responsabilité solidaire du responsable du traitement et du sous-traitant pourra être éventuellement engagée conformément aux articles 82 et 83 du Règlement. Sur le plan administratif, la répartition des éventuelles amendes dépendra notamment de leur degré de responsabilité respectif dans la violation de l'obligation, compte tenu des mesures techniques et organisationnelles qu'ils ont chacun mises en œuvre[92]. En guise d'exemple, dans une récente décision[93], la CNIL[94] a prononcé deux amendes distinctes : 150 000 euros à l'encontre du responsable de traitement et 75 000 euros à l'encontre du sous-traitant. Dans le cas d'espèce, l'autorité a souligné que « le responsable de traitement doit décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant. Mais le sous-traitant doit aussi rechercher les solutions techniques et organisationnelles les plus appropriées pour assurer la sécurité des données personnelles, et les proposer au responsable de traitement »[95]. Sur le plan civil, la personne lésée pourra, au choix, demander réparation du préjudice subi à l'un ou à l'autre[96], lequel pourra ensuite se retourner contre le partenaire contractuel en ce qui concerne sa part de responsabilité dans le dommage[97].

Au vu des règles précitées, dans les relations entre le responsable du traitement et le sous-traitant, il est utile de souligner que le principe de convention-loi ne s'oppose pas à ce que le contrat régissant leurs rapports contienne des obligations additionnelles de résultat en matière de sécurité informationnelle (par exemple en imposant un contrôle des accès physiques et logiques, la journalisation, la mise en œuvre de techniques cryptographiques spécifiques, l'interdiction du BYOD[98], etc.). De telles dispositions conventionnelles détaillées en matière de sécurité permettront, par exemple, à l'un ou l'autre acteur la possibilité de prouver

[91] Art. 5.2 et 24 du RGPD.
[92] Article 83.2, d) du RGPD.
[93] CNIL, Décision non publiée, 27 janvier 2021. Voy. « Credential stuffing : la CNIL sanctionne un responsable de traitement et son sous-traitant », disponible à l'adresse https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant
[94] La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'Autorité de protection des données en France.
[95] CNIL, Décision non publiée, 27 janvier 2021, *op.cit.*
[96] Article 82.1 du RGPD.
[97] Article 82.5 du RGPD.
[98] Le Bring Your Own Device (BYOD)est une pratique consistant à autoriser les employés à utiliser, dans un contexte professionnel, leurs propres terminaux personnels. Les smartphones en sont l'exemple le plus commun, mais le BYOD peut également recouvrir les tablettes, les ordinateurs portables, ou encore les clés USB. Groupe 29, Avis 2/2017 sur le traitement des données sur le lieu de travail, WP249, 8 juin 2017, p.16.

que le fait qui a provoqué la violation de données à caractère personnel lui est partiellement ou nullement imputable et ainsi être exonéré de responsabilité, en tout ou en partie[99].

III. Une obligation de sécurité axée autour des risques pour les personnes concernées

L'approche du RGPD fondée sur les risques (« risk-based approach ») a pour but de promouvoir une « approche évolutive et proportionnelle »[100] sans dispenser du respect des principes fondamentaux[101]. L'obligation de sécurité étant essentiellement une obligation de moyens, cette approche implique que ses débiteurs doivent prendre des mesures appropriées en fonction de l'évaluation du niveau de risque identifié.

1. La notion de « risque » dans le RGPD

Le considérant 4 du RGPD rappelle que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité ». Il est donc logique que l'obligation de sécurité soit principalement axée autour de la notion de « risques pour les droits et libertés des personnes physiques » [102]. Contrairement à la gestion de risques dans d'autres domaines − comme par exemple la sécurité de l'information qui est généralement orientée sur les intérêts et les finalités de l'organisation elle-même −, le RGPD se place sous l'angle du risque pour les droits et libertés des personnes concernées afin de déterminer le niveau de sécurité approprié.

Pour ce qui est de la nature des droits à prendre en compte, le Groupe 29 indique que la référence aux « droits et libertés » des personnes concernées ne renvoie pas uniquement au droit à la vie privée ou au droit à la protection des données, « mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion » [103].

Quant à la source des risques pour ces droits et libertés, « il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite » [104]. En d'autres mots,

[99] Article 82.3 du RGPD.
[100] En anglais: « a scalable and proportionate approach to compliance ». Voy. Groupe 29, Statement on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014, WP218, p. 2.
[101] *Ibidem.* Ainsi, les principes en matière de qualité des données et les droits des personnes concernées doivent toujours être respectés, quels que soient les risques qu'un traitement déterminé engendre.
[102] Considérant 75 du RGPD.
[103] Groupe 29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017, WP248rev01, p.7.
[104] Article 32.2 et considérant 83 du RGPD.

il s'agit de prendre en considération les risques d'atteintes à la confidentialité, à l'intégrité et à la disponibilité des données.

Un « risque » est donc une possibilité que survienne une conséquence négative pour lesdits droits et libertés des personnes physiques, résultant d'un traitement accidentel ou illicite de données à caractère personnel[105]. En guise d'illustration, dans une décision de mai 2021, l'APD nationale a estimé qu' « en attribuant le numéro de téléphone du plaignant à un tiers, on expose le plaignant au risque que des actes frauduleux soient effectués en son nom, en utilisant son numéro de téléphone. Le risque existe également […] que des données sensibles (telles que des données de santé) tombent entre les mains de tiers »[106].

Afin de procéder à l'évaluation des risques, l'article 32 du RGPD précise explicitement que leur « degré de probabilité et de gravité varie ». De même, le Groupe 29 définit le « risque » comme « un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité »[107] L'on comprend donc que le risque doit être analysé au regard de deux variables : sa probabilité, d'une part, et sa gravité de l'autre[108].

En ce qui concerne l'analyse de la première variable, évaluer la probabilité d'un risque revient à l'idée de statistiquement analyser la récurrence potentielle d'un événement possible qui n'est peut-être encore jamais intervenu. Néanmoins, dans son « Handbook on Security of Personal Data Processing »[109], rédigé en collaboration avec les APD hellénique et italienne, l'ENISA[110] propose, entre autres, une méthodologie destinée à évaluer la probabilité de la matérialisation d'un risque. Selon cette approche, les quatre dimensions principales suivantes doivent faire l'objet d'un examen scrupuleux afin de déterminer la probabilité d'un incident : les ressources techniques et de réseau (hardware et software) ; les processus et procédures régissant le traitement ; les différents destinataires externes et internes impliqués dans le traitement ; et enfin, le secteur concerné ainsi que l'échelle du traitement.

Quant à l'analyse de la gravité d'un risque, le considérant 75 du RGPD donne plusieurs exemples non limitatifs de conséquences négatives pour les droits et libertés des personnes physiques, à savoir « la discrimination, un vol ou une usurpation d'identité, des pertes financières, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel, la suppression non autorisée de la pseudonymisation, la

[105] *Ibidem*.
[106] APD, Chambre contentieuse, Décision quant au fond 05/2021 du 22 janvier 2021.
[107] *Ibidem.*
[108] Voir également ISO, "Risk management – Vocabulary", ISO Guide 73:2009 ("un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance").
[109] ENISA, "Handbook on Security of Personal Data Processing", décembre 2017, disponible à l'adresse https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing
[110] L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe.

situation où des personnes concernées ne peuvent pas exercer leurs droits et libertés ou sont empêchées d'exercer le contrôle sur leurs données à caractère personnel et, enfin, tout autre dommage économique ou social important ». L'APD nationale cite également comme exemples de conséquences négatives potentielles pour les droits et libertés des personnes concernées « la perte d'une opportunité, l'atteinte portée à la tranquillité ou au bien-être, la stigmatisation ou le stéréotypage, le refus ou la limitation d'accès à des lieux ou événements qui sont d'habitude accessibles au public, le traitement déloyal (par exemple fixation des prix différenciée), la manipulation (par exemple l'exploitation d'émotions), l'adaptation de comportement (par exemple autocensure) ou encore l'atteinte portée à l'intégrité physique ou morale » [111].

Le risque étant par nature un événement dont la survenance n'est pas certaine mais qui peut potentiellement entraîner des « dommages physiques, matériels ou un préjudice moral »[112] pour les personnes concernées, sa gravité est évidemment liée aux dommages potentiels qu'il peut engendrer. Il va de soi que le dommage physique repose, par définition, sur le principe de l'inviolabilité du corps humain. Quant au dommage matériel, celui-ci se définit comme le résultat d'une atteinte aux biens d'une personne, ou encore à ses possibilités d'en acquérir, de les accroître ou de les gérer.[113] Enfin, le « dommage moral », dans son acception la plus large, comprend « les souffrances morales (sentiment de diminution et d'inquiétude face à l'avenir), les souffrances physiques (appelées également *quantum doloris* ou *pretium doloris*), le préjudice psychologique, le préjudice d'agrément, le préjudice esthétique, le préjudice sexuel ou encore le préjudice d'affection, etc. » [114].

2. La méthodologie de l'évaluation des risques

Le considérant 83 du RGPD indique qu'afin « de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents […] ». Afin d'appliquer ce précepte, une distinction préalable entre le risque « inhérent » et le risque « résiduel » doit être opérée. Selon l'APD, « le risque "inhérent" renvoie à la probabilité qu'un impact négatif se produise lorsqu'aucune mesure de protection n'est prise. Le risque "résiduel" renvoie au contraire à la

[111] APD, Recommandation d'initiative n° 01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable, 28 février 2018, p.21.
[112] Considérant 75 du RGPD.
[113] Y. POULLET, « La sécurité informatique, entre technique et droit », *Cahiers du CRID*, n° 14, 1998, p.20. Ainsi que le souligne l'auteur, les trois types de dommages que nous citons peuvent bien entendu apparaître séparément ou simultanément à cause de la réalisation d'un risque. L'auteur ajoute « *a priori*, le dommage immatériel paraît le plus bénin, et le dommage "physique" le plus grave, mais il ne nous paraît pas souhaitable d'établir une véritable gradation de ces dommages. En effet, une "échelle" des dommages est toujours sujette à controverses et risque, en outre, de conduire à diminuer la prévention des dommages jugés moins graves. Or, cela ne semble pas entrer dans les intentions du législateur européen, qui vise à protéger les "libertés et droits fondamentaux des personnes", indépendamment du type de dommage éventuellement subi »
[114] C.T. Mons (10e ch.), 16 décembre 2015, RG n°2015/AM/313.

probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent) » [115].

Ayant clarifié ces notions, l'analyse des risques inhérents engloberait « l'ensemble du processus : d'identification des risques, d'analyse des risques et d'évaluation des risques »[116]. D'après l'autorité nationale, « l'identification des risques reviendrait à examiner, reconnaître et décrire les risques ; l'analyse du risque au processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. Enfin, l'évaluation du risque viserait le processus de comparaison des résultats de l'analyse du risque avec les critères de risque préétablis afin de déterminer si le risque (et/ou son importance) est (sont) acceptable(s) ou tolérable(s) »[117].

Afin de se livrer à l'exercice d'évaluation du risque, les débiteurs de l'obligation de sécurité peuvent choisir librement la méthode qu'ils souhaitent appliquer, à condition qu'elle soit objective et que le choix de l'une ou l'autre méthode puisse être justifié, compte tenu de la nature, du champ d'application, du contexte et des finalités du traitement[118]. Néanmoins, dans le but d'éviter qu'une situation d'insécurité juridique ne survienne, l'APD nationale a formulé plusieurs caractéristiques minimales d'une bonne gestion des risques[119].

Outre le fait que la gestion des risques doit, entres autres, être étayée méthodologiquement[120], être adaptée sur mesure au contexte et au profil du débiteur de l'obligation de sécurité, elle doit également être structurée de manière à contenir notamment la définition du contexte pertinent[121] ; l'identification, analyse et évaluation des risques[122] ; et l'identification de mesures d'atténuation des risques appropriées[123]

De plus, la méthode de gestion de risques doit être suffisamment nuancée et « comporter suffisamment d'échelles afin de permettre une évaluation nuancée des risques identifiés. Ne prévoir que trois échelles (bas, moyen, élevé) pour apprécier les risques n'est pas toujours suffisant pour donner lieu à une appréciation

[115] APD, Recommandation n° 01/2018, *op.cit*., p. 20.
[116] ISO, "Risk management – Vocabulary", ISO Guide 73:2009. Lors de l'identification des risques, le responsable du traitement doit faire preuve de la prudence nécessaire et anticiper les risques potentiels, même si la nature du risque n'est pas connue à l'avance. L'évaluation du niveau de risque n'a en effet lieu que lors de l'analyse ultérieure des risques identifiés.
[117] APD, Recommandation n° 01/2018, *op.cit.*, p.19.
[118] *Ibid.*, p.23.
[119] *Ibid.*, « Annexe 1 : Caractéristiques minimales d'une bonne gestion des risques », pp.39 à 41.
[120] En outre, l'APD recommande vivement « de se baser sur des méthodes déjà existantes en matière de gestion des risques. L'utilisation de normes internationales, telles que celles développées par l'Organisation internationale de normalisation (ISO). En particulier la norme ISO 31000 (Risk management). ISO 27005 (Information security risk management) et ISO/IEC 29134 (Guidelines for privacy impact assessment). L'adhésion à des codes de conduite élaborés ou agréés au niveau européen, est particulièrement importante dans ce cadre également ». APD, Recommandation n° 01/2018, *op.cit*., p. 23.
[121] Cette étape doit inclure une description de l'objet de l'analyse de risque, une définition des critères servant à évaluer les risques pour les droits et libertés des personnes physiques et la définition de valeurs de risques (in)acceptables).
[122] Y compris l'identification des vulnérabilités, des menaces et l'attribution d'une valeur de risque.
[123] C'est-à-dire les mesures techniques, organisationnelles qui sont nécessaires pour ramener le risque à un niveau acceptable.

correcte. Une description claire des critères utilisés pour évaluer le risque est quoi qu'il en soit indispensable »[124].

Pour le surplus, relevons que lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données (ci-après « AIPD ») pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque[125]. En d'autres mots, lorsque l'évaluation des risques inhérents conclu à l'existence d'un risque élevé, le responsable du traitement est soumis à une exigence documentaire supplémentaire, à savoir la réalisation d'une AIPD, laquelle est « est un processus dont l'objet est de décrire le traitement de données à caractère personnel, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques qui y sont liés en les évaluant et en déterminant les mesures nécessaires pour y faire face »[126]. En somme, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve[127]. Lorsqu'une AIPD est requise, les principes de privacy-by-design[128] et de privacy-by-default[129] imposent au responsable du traitement de la réaliser avant le traitement[130].

La notion de « risque élevé » n'est pas définie en détail dans le RGPD[131], toutefois le paragraphe 3 de l'article 35 précise qu'une AIPD est, en particulier, requise dans certains cas y énumérés[132]. Comme le laissent entendre les mots « en particulier » dans la phrase introductive de l'article 35.3 du RGPD, il s'agit là d'une liste non exhaustive. Même si elles ne figurent pas dans cette énumération, d'autres opérations de traitement peuvent

[124] APD, Recommandation n° 01/2018, *op.cit*, p.41.
[125] Article 35 et considérant 84 du RGPD.
[126] Groupe 29, WP248rev01, *op.cit.*, p. 4.
[127] *Ibidem*.
[128] Art. 25.1 du RGPD.
[129] Art. 25.2 du RGPD.
[130] Selon le Groupe 29, une telle analyse est toutefois « un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements. La réalisation d'une AIPD relève d'un processus continu et n'est pas un exercice ponctuel ». Groupe 29, WP248rev01, *op.cit.*, p. 17.
[131] Selon l'APD, de manière générale, la notion de « risque élevé » renverrait aux traitements de données qui « sont ou pourront être susceptibles d'avoir des incidences négatives sensibles pour les libertés et droits fondamentaux des personnes physiques. L'expression "susceptible de" ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées : la probabilité qu'elles soient sensiblement affectées suffit pour répondre à ce critère. Une "conséquence négative sensible" signifie que, dans le cas où le risque inhérent se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux ». Voy. APD, Recommandation n° 01/2018, *op.cit.*, p.8
[132] Ces cas sont les 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 9.1, 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.

néanmoins présenter un risque inhérent aussi élevé. Afin de déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque élevé – et donc qu'une AIPD doit être réalisée − les lignes directrices élaborées par le Groupe 29 sont particulièrement importantes[133]. Dans celles-ci, sont identifiés neuf critères que les responsables du traitement doivent prendre en considération dans leur analyse déterminant si un traitement envisagé est ou non susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Ces critères fournissent un socle commun permettant d'assurer la cohérence au sein de l'Union, puisque conformément à l'article 35.4 du RGPD, chaque Autorité nationale de Protection des données est tenue d'établir et de publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise[134].

Dans le cas où la conduite d'une AIPD n'est pas considérée comme étant nécessaire du fait qu'un risque inhérent n'est pas identifié comme étant « élevé », il faudra pourtant logiquement procéder à une analyse de risques afin de motiver et de documenter la raison pour laquelle le responsable du traitement est parvenu à cette conclusion[135]. Autrement dit, une analyse des risques inhérents doit être réalisée qu'il y'ait ou non une obligation de procéder à une AIPD. En effet, le fait de ne pas réaliser une AIPD ne dispense pas les responsables de traitements et les sous-traitants de leur obligation générale de prendre des mesures pour gérer de manière appropriée tous les risques pour les droits et libertés des personnes concernées conformément à l'article 32 du RGPD.

IV. Le caractère « approprié » des mesures de sécurité

Outre les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, l'article 32.1 du RGPD énumère trois facteurs supplémentaires qui doivent être pris en compte pour assurer la mise en œuvre de mesures de sécurité appropriées, à savoir 1) la nature, la portée, le contexte et les finalités du traitement, 2) l'état des connaissances, et 3) les coûts de mise en œuvre[136]. Aucune hiérarchisation de ces critères n'est établie par le Règlement, de sorte qu'aucun de ceux-ci n'a expressément de primauté sur l'autre. Dans les sections qui suivent, nous analysons ces différents éléments afin de clarifier la manière de les appliquer dans le processus de sécurisation.

[133] Groupe 29, WP 248, *op.cit.*.
[134] En Belgique, voy. APD, Décision du Secrétariat Général n° 01/2019, Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données (CO-A-2018-001), 16 janvier 2019.
[135] APD, Recommandation n° 01/2018, *op.cit.*, p.11.
[136] Voy. également le considérant 74 du RGPD.

1. La nature, la portée, le contexte et les finalités du traitement

Les débiteurs de l'obligation de sécurité doivent prendre en considération des facteurs tels que la nature, la portée, le contexte et la finalité du traitement lorsqu'ils déterminent les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Parmi les éléments pertinents pour déterminer la nature, la portée, le contexte et les finalités des traitements, l'APD cite « les catégories de personnes concernées, l'échelle du traitement de données, l'origine des données, la relation entre le responsable du traitement et les personnes concernées, les éventuelles conséquences pour les personnes concernées et le degré de facilité avec lequel on peut identifier ces dernières »[137]. L'EDPB résume ces critères comme suit : « la notion de nature peut être comprise comme les caractéristiques inhérentes au traitement. La portée se réfère à la taille et à l'échelle du traitement. Le contexte se rapporte aux circonstances du traitement, qui peuvent influencer les attentes de la personne concernée, tandis que la finalité a trait aux objectifs du traitement »[138].

En guise d'exemple de prise en compte de ces facteurs dans l'évaluation des mesures de sécurité, dans une décision récente, l'APD nationale a considéré que « dans la mesure où la consultation des données personnelles relatives aux crédits des personnes concernées constitue un traitement invasif de données financières sensibles, […] les mesures mises en place doivent être d'autant plus adaptées que les risques pour les droits fondamentaux des personnes concernées sont élevés »[139]. Dans la même logique, l'APD néerlandaise a estimé qu'un hôpital « traite des données à caractère personnel (catégories particulières de données) à grande échelle et il s'agit (souvent) de données de santé extrêmement sensibles. Cela impose des exigences plus élevées en matière de sécurité de ces données »[140].

Afin de matérialiser l'exigence d'étayer méthodologiquement la nature, la portée, le contexte et les finalités des traitements envisagés, l'article 30 du RGPD met à charge des responsables de traitement et des sous-traitants l'obligation de tenir un registre des activités de traitement (ci-après « Registre »)[141]. Ce Registre,

[137] APD, Recommandation n° 01/2018, *op.cit*., p.17.
[138] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on 13 November 2019, p.9.
[139] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021.
[140] Autoriteit persoonsgegevens, Stichting OLVG – boetebesluit, 26 november 2020.
[141] L'obligation de tenir un Registre comporte une exception pour les « entreprises ou organisations comptant moins de 250 employés ». Cette exception est néanmoins toute relative puisque les entreprises visées devront tout de même tenir un Registre lorsqu'elles se trouvent dans l'une des 4 hypothèses suivantes : le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et libertés des personnes concernées; le traitement qu'elles effectuent n'est pas occasionnel ; le traitement qu'elles effectuent porte sur des données sensibles ; le traitement qu'elles effectuent porte sur des données judiciaires. Etant donné que la « cartographie » des traitements de données opérés par les débiteurs de l'obligation de sécurité est essentielle à ceux-ci pour disposer d'une vue d'ensemble des traitements à sécuriser, l'APD recommande à tous les responsables de traitement et sous-traitants d'établir ce Registre, qu'ils soient ou non tenus de le maintenir aux termes du RGPD. Voy. APD, Recommandation n° 06/2017 relative au Registre des activités de traitements (article 30 du RGPD), 14 juin 2017, p.7.

écrit, et disponible en version électronique, doit notamment contenir les informations suivantes : la finalité de chaque traitement énoncée clairement et avec précision[142] ; une description des catégories de personnes concernées[143] et des catégories de données personnelles traitées[144]; les catégories de destinataires[145] auxquels les données ont été ou seront communiquées; le cas échéant les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, l'existence de garanties appropriées; et, dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données[146]. Relevons également que rien ne s'oppose à ce que le Registre contienne davantage d'informations que celles explicitement énumérées à l'article 30 du

[142] De manière générale, il faut veiller à ce que les finalités du traitement soient décrites avec la précision nécessaire. Il faut éviter un renvoi à des finalités générales, décrites au sens large (comme par ex. "améliorer l'expérience d'utilisateur", "sécurité IT", « analyse »). La description de la finalité doit donner à celui qui consulte le Registre − en ce compris l'autorité de contrôle − une idée claire des traitements de données opérés.

[143] On pense évidemment aux employés, aux clients, aux fournisseurs, aux prestataires externes. De plus, le Groupe 29 estime qu'il s'agit également d'identifier les catégories de personnes considérées comme étant vulnérables « en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits ». Peuvent être considérés comme des personnes concernées vulnérables, « les enfants (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié ». Groupe 29, WP248rev01, *op.cit*, p.12.

[144] L'identification des catégories de données traitées revient bien sûr à procéder à une description des données à caractère personnel qui font l'objet du traitement. Par ailleurs, il est recommandé d'opérer une classification desdites données. Il s'agit, tout d'abord, d'énumérer les données à caractère personnel traitées selon le traitement envisagé. Il convient également d'identifier les catégories de données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux, et qui, par conséquent, méritent une protection spécifique car elles peuvent « engendrer des risques importants pour ces libertés et droits ». Il s'agit des catégories particulières de données à caractère personnel (en vertu de l'article 9) ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions (en vertu de l'article 10). Enfin, le Groupe 29 suggère qu'il y a lieu d'énumérer les catégories de « données à caractère hautement personnel » en considérant « qu'au-delà des dispositions du RGPD, certaines catégories de données peuvent être considérées comme augmentant le risque possible pour les droits et libertés des personnes. Ces données à caractère personnel sont considérées comme sensibles (au sens commun du terme) dans la mesure où elles sont liées à des activités domestiques et privées (communications électroniques dont la confidentialité doit être protégée, par exemple), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte met en cause la liberté de circulation, par exemple) ou dans la mesure où leur violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple) ». Groupe 29, WP248rev01, *op.cit.*, p.11.

[145] La notion de destinataire est définie à l'article 4, 9) du RGPD comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ». Sont donc visés, tant d'éventuels destinataires internes (tels les employés) qu'externes (tels les sous-traitants ou des tiers), y compris les destinataires dans des pays tiers à l'Union européenne ou des organisations internationales, au regard de chacune des finalités identifiées. De plus, l'obligation de tenir un Registre des traitements étant une obligation dynamique, « le responsable du traitement et le sous-traitant veilleront à le tenir à jour en ajoutant par exemple tout nouveau destinataire qu'ils n'auraient pas pu envisager lors de la rédaction originelle du Registre (ex : inspection fiscale, nouveau partenaire commercial…) ». APD, Recommandation 06/2017, *op.cit.*, p.14.

[146] Cet élément d'information rejoint le principe selon lequel les données ne peuvent être conservées sous une forme permettant l'identification des personnes que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. « Par durée de conservation, il ne faut pas nécessairement comprendre une durée en jours, mois, années, soit une évaluation quantitative. La durée de conservation peut également faire référence à des paramètres tels que le temps nécessaire à la réalisation de la finalité concrète poursuivie ainsi qu'à la gestion du contentieux éventuel y relatif, l'expiration d'un délai de prescription, une durée d'archivage légal après la fin du traitement, etc. ». APD, Recommandation 06/2017, *op.cit.*, p.15.

RGPD. Dans la mesure du possible, le Registre contiendra donc utilement des informations additionnelles telles que la mention du fondement de licéité du traitement ; la mention qu'il s'agit de traitements qui imposent de procéder à une AIPD; la taille et le statut[147] du débiteur de l'obligation de sécurité ; l'échelle du traitement : volume (par catégorie) de données traitées et nombre (par catégorie) de personnes concernées[148] ; l'origine des données[149] ; les supports des données[150] ou encore les moyens du traitement[151].

Sans aucun doute, le Registre est un outil important pour l'évaluation des mesures de sécurité à mettre en œuvre[152] à l'aune de la nature, de la portée, du contexte et des finalités du traitement. Compte tenu de la variété

[147] De manière générale, le RGPD ne prévoit pas d'exception en fonction de la taille des responsables de traitement et sous-traitants, pour les Petites et Moyennes Entreprises par exemple (ci-après PME) : « l'approche par le risque reflétée dans une série d'obligations du RGPD s'accommode mal de ce type d'exceptions. Il serait à tout le moins incohérent de considérer qu'en toutes hypothèses, la taille d'un responsable de traitement ou d'un sous-traitant signifie une absence de risque ou un risque faible pour les droits et libertés des individus ». APD, Recommandation 06/2017, *op.cit.*, p.4. Néanmoins, le Groupe 29 considère que « les mesures attendues […] devraient être modulables et prendre en compte, entre autres critères, le type de la société (sa taille, son statut de société à responsabilité limitée) ». Groupe 29, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP168, 1er décembre 2009, p.23. De même, dans son vade-mecum à destination des PME, l'APD estime que « l'approche basée sur les risques signifie que les obligations qui découlent du RGPD varient en fonction du risque lié à l'activité de traitement. Le RGPD crée donc une marge pour parvenir à une solution sur mesure pour chaque PME ». APD, « RGPD vade-mecum pour les PME : Un guide pour préparer les petites et moyennes entreprises (PME) au Règlement général sur la protection des données », janvier 2018, p.5. En ce qui concerne plus particulièrement les mesures de sécurité que devraient prendre en compte les PME, l'ENISA a publié des « Guidelines for SMEs on the security of personal data processing » afin d'aider celles-ci dans leur approche. ENISA, Guidelines for SMEs on the security of personal data processing », décembre 2016. Ces invitations de « prise en compte » ne permettent cependant pas de dérogations nouvelles. APD, Recommandation 06/2017, *op.cit.*, p.5.

[148] Evaluer l'échelle du traitement est également utile pour déterminer la nature de celui-ci étant donné que le traitement de données traitées à grande échelle constitue un des critères pouvant entraîner un risque inhérent élevé et une éventuelle obligation de conduire une AIPD.

[149] Lorsqu'un traitement a lieu pour une fin autre que celle pour laquelle les données ont été collectées initialement et n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre, l'article 6, §4, b) requiert que l'analyse de la compatibilité de cette finalité ultérieure tienne compte du « contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ». Le Groupe 29 va dans le même sens en affirmant qu'il s'agit d'analyser « the specific context in which the data were collected and the reasonable expectations of the data subjects as to their further use based on that context. In other words, the issue here is what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection ». Voy. Groupe 29, Opinion 03/2013 on purpose limitation, WP203, 2 avril 2013, p.24.

[150] Selon la CNIL, il est également utile de recenser les supports sur lesquels reposent les traitements de données à caractère personnel, notamment : les matériels (ex : serveurs, ordinateurs portables, disques durs) ; les logiciels (ex : système d'exploitation, logiciel métier) ; les canaux de communication (ex : fibre optique, Wi-Fi, Internet) ; les supports papier (ex : document imprimé, photocopie). CNIL, La sécurité des données personnelles, in *Les guides de la CNIL*, 2018, p.4.

[151] L'APD recommande de décrire de manière suffisamment détaillée et claire les moyens techniques et opérationnels du traitement. Une visualisation de ces moyens peut contribuer à favoriser une approche systématique pour déterminer précisément la finalité de celui-ci. APD, Recommandation n° 01/2018, *op.cit.*, p.17.

[152] Selon l'article 30 du RGPD, le Registre doit d'ailleurs également contenir « dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles ».

des situations, il n'existe pas de canevas-type unique du Registre. Toutefois, des modèles de Registres ont été mis à disposition, par exemple, par l'APD nationale[153] et par la CNIL[154].

2. *L'état des connaissances*

Un second facteur à prendre en compte lors du choix des mesures de sécurité appropriées à mettre en œuvre est « l'état des connaissances », un concept déjà présent dans divers acquis de l'UE, par exemple en matière de protection de l'environnement et de sécurité des produits. Selon l'EDPB, la décision *Kalkar* de la Cour constitutionnelle fédérale allemande[155] peut servir de base pour une définition objective du concept : « le niveau technologique de "l'état des connaissances" serait identifié entre le niveau technologique des "connaissances et recherches scientifiques existantes" et les "règles technologiques généralement acceptées", plus établies. L'"état des connaissances" peut donc être identifié comme le niveau technologique d'un service, d'une technologie ou d'un produit qui existe sur le marché et qui est le plus efficace pour atteindre les objectifs identifiés » [156]. Dans la même logique, le Conseil de l'Europe recommande que « les mesures de sécurité devraient prendre en considération les méthodes et techniques *de pointe* en matière de sécurité des données dans le cadre du traitement de données »[157].

Par conséquent, la référence à l'état des connaissances imposerait aux débiteurs de l'obligation de sécurité, lorsqu'ils déterminent les mesures techniques et organisationnelles appropriées, de tenir compte de l'évolution actuelle des technologies disponibles sur le marché[158]. Selon l'EDPB, cela signifie que les responsables du traitement et les sous-traitants « doivent connaître et se tenir au courant des progrès technologiques, de la manière dont la technologie peut présenter des risques pour la protection des données dans le cadre du traitement, et de la manière de mettre en œuvre les mesures appropriées »[159].

Il découle de ce qui précède que l'état des connaissances est un concept dynamique qui ne peut être défini de manière statique à un moment donné, mais doit être évalué en permanence dans le contexte des progrès technologiques. Le fait de négliger de se tenir à jour avec les changements technologiques pourrait donc entraîner un manque de conformité avec l'article 32. En outre, il s'agit d'être attentif au fait que le critère de

[153]Le modèle de Registre de l'APD est disponible à l'adresse https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/registre-des-activites-de-traitement/comment-etablir-un-registre-
[154]Le modèle de Registre de la CNIL est disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx
[155] Cour constitutionnelle allemande, BVerfGE 49, 89 – Kalkar I, 1978
[156] EDPB, Guidelines 4/2019, *op.cit.*, p.7
[157] Conseil de l'Europe, Projet de rapport explicatif de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 2016, p.11
[158] La doctrine insiste sur le fait que ces techniques doivent être présentes sur le marché comme produits déjà commercialisés et non encore à l'état de prototypes et donc difficilement disponibles. Voy. Y. POULLET, *op.cit.*, p.43.
[159] EDPB, Guidelines 4/2019, *op.cit.*, p.8.

l'état des connaissances ne s'applique pas seulement aux mesures technologiques, mais aussi aux mesures organisationnelles. En effet, « l'absence de mesures organisationnelles adéquates peut diminuer, voire annuler complètement l'efficacité d'une technologie choisie »[160].

Plus concrètement, en 2019, l'ENISA et TeleTrusT – une association allemande en matière de sécurité informatique – ont publié conjointement des lignes directrices afin de fournir aux responsables de traitements et aux sous-traitants une assistance pour interpréter « l'état des connaissances » au sens du RGPD[161]. Selon ces lignes directrices, la mise en œuvre de mesures de sécurité envisagées devrait toujours intégrer les suivantes : authentification à deux facteurs, authentification mutuelle, chiffrement de la communication pendant le transport, chiffrement des données (par exemple pendant le stockage), protection de la clé privée contre la copie non autorisée, utilisation de processus de démarrage sécurisés, administration logicielle sécurisée, y compris la gestion des correctifs, administration sécurisée des utilisateurs avec option de verrouillage actif , cartographie sécurisée des zones réseau pour une protection supplémentaire au niveau du réseau, communication de données sécurisée entre différentes zones du réseau, navigation Internet sécurisée, réalisation du principe « need-to-know »[162], réalisation de l'approche minimale (y compris le « hardening »[163]), implémentation de systèmes de journalisation, de surveillance, de reporting et de gestion d'incidents, protection contre les logiciels malveillants, utilisation de systèmes de sauvegarde sécurisés pour prévenir la perte de données et, enfin, plusieurs configurations de système pour la mise en œuvre de haute disponibilité[164].

A la lecture de récentes décisions des autorités de protection des données, il ressort que le critère de « l'état des connaissances » exige également la prise en compte des diverses recommandations et avis de ces autorités. Ainsi, dans une décision d'avril 2021[165], l'APD nationale estime qu'elle « indiquait déjà dans ses Lignes

[160] *Ibidem.*
[161] ENISA et TeleTrusT, IT Security Act (Germany) and EU General Data Protection Regulation – Guideline "State of the art" – Technical and organizational measures, juin 2019. Les mesures techniques décrites au chapitre 3.2 de ce guide ont été évaluées à l'aide d'une méthode pratique axée autour du « degré de reconnaissance » et du « degré d'efficacité dans la pratique ».
[162] Le principe de « need-to-know » implique que, même si quelqu'un possède les habilitations officielles nécessaires, l'accès à ce type d'information ne peut lui être attribué qu'uniquement lorsqu'il a le besoin spécifique de la connaître.
[163] En informatique, le hardening est une démarche qui consiste principalement à réduire à l'indispensable les objets (logiciels, bibliothèques logicielles, outils) installés sur le système, ainsi qu'à éliminer les utilisateurs et les droits non indispensables, tout en conservant les fonctionnalités requises. Le principe sous-jacent est la réduction de la surface d'attaque possible, en considérant que tout objet installé est potentiellement une source de vulnérabilité (exploit). La réduction du nombre d'objets installés réduit donc le nombre de failles possibles, pour un système donné.
[164] L'ENISA a également publié des recommandations en matière de « privacy-by-default », ayant pour objet de clarifier la signification du principe de protection des données par défaut dans le design des technologies de l'information. Dans ce document, l'agence présente certaines des meilleures pratiques en matière d'application concrète de la protection des données par défaut et propose une liste de questions d'auto-évaluation pouvant être utiles aux responsables de traitements et aux sous-traitants. Voy. ENISA, Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default, 28 janvier 2019.
[165] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021, pp.17-18.

directrices pour la sécurité de l'information de données à caractère personnel ainsi que dans sa Recommandation aux villes et communes concernant les registres de logs IT que la journalisation constitue un élément incontournable de toute politique de sécurité de l'information, en ce qu'elle permet la traçabilité des accès aux systèmes informatiques »[166]. De même, dans une décision de la CNIL, l'APD française fait référence à sa délibération n° 2017-012[167] pour juger de la robustesse d'une méthode d'authentification par mot de passe[168]. Dans une autre délibération, la CNIL fait référence à son guide « La sécurité des données personnelles »[169] pour considérer qu'un responsable du traitement « a failli à deux principes élémentaires en matière de sécurité informatique, à savoir la protection du réseau informatique interne par la limitation des flux réseau au strict nécessaire et le chiffrement des données à caractère personnel »[170].

Autant dire que les débiteurs de l'obligation de sécurité ont tout intérêt à prendre en considération les consignes des autorités lors du choix et de l'implémentation de leurs mesures. A cet égard, dans un très récent avis datant de janvier 2021[171], l'EDPB énumère, de manière non-exhaustive, les mesures appropriées pour prévenir les attaques par ransomware et par exfiltration ainsi que pour mitiger les sources de risques humains internes, la perte et vol d'équipement ou encore l'envoi d'e-mails à de mauvais destinataires.

3. Les coûts de mise en œuvre

En ce qui concerne le critère des coûts, l'EDPB estime que celui-ci « ne s'entend pas seulement en termes d'argent ou d'avantage économique. Le coût, dans ce contexte, fait référence aux ressources en général, y compris le temps et les ressources humaines. L'EDPB rappelle au lecteur que le coût de la mise en œuvre de la protection des données dans le traitement fait partie des coûts de l'entreprise […]. La mise en œuvre et le maintien de "l'état de l'art" peuvent également être importants lors de l'examen du coût de la mise en œuvre »[172].

En gardant à l'esprit l'objectif d'une mise en œuvre de mesures appropriées par rapport aux risques pour les droits et libertés des personnes physiques, les débiteurs de l'obligation de sécurité doivent prévoir et engager

[166] Les « Lignes directrices pour la sécurité de l'information de données à caractère personnel » de l'APD sont disponibles à l'adresse https://www.autoriteprotectiondonnees.be/publications/lignes-directrices-pour-la-securite-de-l-information.pdf. Voy également CPVP, Recommandation aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national par les membres de leur personnel (CO-AR-2017-013), 30 août 2017. A propos de cette dernière recommandation, dans la décisions susmentionnée, l'APD considère que « Bien que cette recommandation s'adresse aux communes et villes, le raisonnement s'applique aux autres types de traitements de données, à fortiori lorsqu'il s'agit de données sensibles ».
[167] CNIL, Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.
[168] CNIL, Délibération de la formation restreinte n°SAN-2021-008 du 14 juin 2021, point 68.
[169] CNIL, La sécurité des données personnelles, *op.cit*.
[170] CNIL, Délibération de la formation restreinte no SAN-2020-014 du 7 décembre 2020.
[171] EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, *op.cit.*
[172] EDPB, Guidelines 4/2019, *op.cit.*, p.8.

les coûts nécessaires à la mise en œuvre effective de ces mesures[173]. L'incapacité à supporter les coûts n'est donc pas une excuse pour ne pas se conformer à leur obligation[174]. Dans la même logique, l'APD nationale considère que « le coût des mesures envisagées ne peut pas en soi constituer une raison de réaliser un traitement sans garanties suffisantes. Si le responsable du traitement n'est pas en mesure de prévoir des garanties suffisantes et de ramener le risque à un niveau acceptable, au vu de la technologie disponible et des frais d'exécution, il doit le cas échéant soit renoncer au traitement, soit réaliser une consultation préalable de l'autorité de contrôle » [175].

Toutefois, « la mise en œuvre effective des principes ne doit pas nécessairement entraîner une augmentation des coûts. Dépenser davantage en technologie ne conduit pas nécessairement à une mise en œuvre plus efficace des principes. Dans certains cas, il peut y avoir des solutions simples et peu coûteuses qui peuvent être tout aussi efficaces, voire plus, que leurs homologues coûteux »[176].

V. Analyse de quelques mesures de sécurité

Après avoir pris en compte les différents facteurs examinés dans les sections précédentes, les débiteurs de l'obligation de sécurité doivent mettre en œuvre des mesures appropriées afin de garantir un niveau de sécurité adapté au risque. Le RGPD en distingue deux types : d'une part, les mesures techniques, d'autre part les mesures organisationnelles[177], dont en guise d'illustrations, l'article 32 en énumère un certain nombre[178].

Dans les pages suivantes, sans prétention d'exhaustivité, nous analysons certaines mesures de sécurité ayant été plébiscitées par les autorités de protection des données dans leurs récentes décisions.

---

[173] La doctrine insiste sur le fait que le niveau de sécurité « ne peut se concevoir en fonction des ressources financières du responsable du traitement. Les frais doivent être suffisants et raisonnables compte tenu des précédents critères. Il serait inacceptable qu'un responsable des traitements limite la sécurité de son système d'information nonobstant les risques encourus pour les personnes concernées au seul motif que les techniques disponibles sont trop onéreuses au regard de ses ressources financières ». Voy. Y. POULLET, *op.cit.*, p.43

[174] EDPB, Guidelines 4/2019, *op.cit.*, p.8.

[175] APD, Recommandation n° 01/2018, *op.cit.*, p.25.

[176] EDPB, Guidelines 4/2019, *op.cit.*, p.8.

[177] En 1990, la Commission européenne précisait déjà le contour de ces notions: « technical measures of data security include: safety measures for access to data processing and storage locations, identification codes for persons entitled to enter such locations, informational safeguards such as the use of passwords for access to electronically processed files, the enciphering of data and monitoring of hacking and other unusual activities. Through organizational measures, the controller of the file adopts certain procedural stops within the hierarchy of his public authority or business enterprise, e.g. by establishing authority levels with regard to access to the data ». Voy. Commission communication on the protection of individuals on relation to the processing of personal data in the Community and Information security, COM (90) 314 final, 13 September 1990, p.37.

[178] L' article 32 énumère, de manière non-exhaustive, la pseudonymisation et le chiffrement des données à caractère personnel; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; et, une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

1. La pseudonymisation

La pseudonymisation[179] consiste à remplacer un attribut (généralement un attribut unique) par un autre dans un enregistrement afin de réduire le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée qui reste, par conséquent, toujours susceptible d'être identifiée indirectement[180]. Le résultat de la pseudonymisation peut être indépendant de la valeur initiale (comme dans le cas d'un numéro aléatoire généré par le responsable du traitement ou d'un nom choisi par la personne concernée) ou il peut être dérivé des valeurs originales d'un attribut ou d'un ensemble d'attributs, par exemple au moyen d'une fonction de hachage ou d'un système de chiffrement[181]. Certaines techniques de pseudonymisation ont été décrites et analysées par l'ENISA[182].

Par définition, le données pseudonymisées[183] sont des données à caractère personnel, du fait que le lien entre le pseudonyme et les données d'identification (par exemple, nom, prénom, adresse postale, adresse IP...) est disponible pour l'organisation collectant l'information ou une tierce partie[184]. L'intérêt de procéder à la pseudonymisation n'est donc pas de déroger à la l'application du RGPD mais de réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de sécurité des données. A titre d'exemple, dans une délibération de 2020 concernant l'application StopCovid, la CNIL a souligné que « la pseudonymisation est un élément important pour préserver la vie privée des personnes qui utiliseront ce dispositif »[185].

Notons toutefois que l'introduction explicite de la pseudonymisation dans le RGPD ne vise pas à exclure d'autres mesures de sécurité des données comme, par exemple, le chiffrement[186].

---

[179] Telle que définie à l'article 4(5) du RGPD.
[180] Groupe 29, WP216, *op.cit.*, p.22.
[181] *Ibidem.*
[182] ENISA, Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymization, 2018. Voy. également ENISA, Pseudonymisation techniques and best practices - Recommendations on shaping technology according to data protection and privacy provisions, 2019 et
[183] Les données pseudonymisées sont parfois désignées sous l'appellation de « données codées ». Celles-ci étaient définies comme étant « des données à caractère personnel qui ne peuvent être mises en relation avec une personne identifiée ou identifiable qu'au moyen d'un code ». Doivent également être considérées comme données à caractère personnel « les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne ». Voy. Exposé des motifs de la loi du 11 décembre 1998, Doc. Parl., Chambre, sess. ord. 1997-1998, n° 1566/1.
[184] Le considérant 26 du RGPD indique expressément que « les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable ».
[185] CNIL, Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid ».
[186] Considérant 28 du RGPD.

2. Le chiffrement

Le RGPD fait explicitement référence au chiffrement sans toutefois le définir. Néanmoins, en Belgique, son usage est régulé par l'article 48 du la loi du 13 juin 2005 qui dispose que « l'emploi de la cryptographie est libre » [187]. Dans ce contexte, la notion y est définie comme « l'ensemble des services mettant en œuvre les principes, moyens et méthodes de transformation de données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée » [188].

Selon le Groupe 29, « le cryptage peut contribuer de manière significative à la confidentialité des données à caractère personnel s'il est utilisé correctement, bien qu'il ne rende pas les données à caractère personnel irréversiblement anonymes ». Le Groupe 29 accorde une importance essentielle au chiffrement puisque celui-ci estime que « le cryptage des données à caractère personnel devrait être systématique pour les données "en transit" et être utilisé lorsque c'est possible pour les données "au repos" » [189]. Le Groupe recommande également de stocker les mots de passe « de manière sécurisée (par exemple, par salage ou à l'aide d'une fonction de hachage à clé cryptographique) »[190].

En guise d'illustrations, dans une décision de 2019, la CNIL a considéré que « l'accès aux images vidéo des caméras par la connexion au logiciel de gestion de la société repose sur une connexion non chiffrée, qui permet la lecture en clair des flux contenant des données personnelles transmis entre l'utilisateur et le serveur hébergeant le site. La mise en place d'un protocole de chiffrement [https] est donc destinée à assurer la sécurité des données personnelles lors des flux transmis entre l'utilisateur et le serveur hébergeant le site. L'ensemble de ces faits constitue un manquement aux obligations de l'article 32 du Règlement »[191]. Dans une délibération de 2020, après avoir constaté l'accès libre à des serveurs informatiques permettant la consultation et le téléchargement d'images médicales (IRM, radios, scanners, etc…) suivies notamment des nom, prénoms, date

[187] Article 48 de la loi du 13 juin 2005 relative aux communications électroniques. Néanmoins, le même article précise que « la fourniture au public de services de cryptographie que le Roi détermine, après avis de l'Institut [IBPT], est soumise à une déclaration préalable auprès de l'Institut. Le Roi arrête, après avis de l'Institut, le contenu et la forme de cette déclaration ». A notre connaissance, un arrêté royal n'a pas encore été adopté à ce sujet.

[188] Article 2, 40° de la loi du 13 juin 2005 relative aux communications électroniques. A cet égard, l'OCDE souligne que « l'utilisation de la cryptographie pour garantir l'intégrité des données, y compris les mécanismes d'authentification et de non-répudiation, peut être distinguée de son utilisation pour garantir la confidentialité des données, et que chacune de ces utilisations pose des problèmes différents ». OCDE, Recommandation du conseil relative aux lignes directrices régissant la politique de cryptographie, 22 mars 1997, p.4.

[189] Groupe 29, WP196, *op.cit.*, p.18.

[190] Groupe 29, Avis 03/2014 sur la notification des violations de données à caractère personnel, adopté le 25 mars 2014, WP213, p.10.

[191]. CNIL, Décision n° MED 2019-025 du 5 novembre 2019.

de naissance et date de consultation des patients[192], la CNIL rappelle que « que la protection du réseau informatique interne et le chiffrement des données à caractère personnel font partie des exigences élémentaires en matière de sécurité informatique, qui incombent à tout responsable de traitement »[193]. La CNIL s'est également exprimée au sujet de l'état des connaissances en matière cryptographique en rappelant « que le recours à la fonction de hachage MD5 par la société n'est plus considérée depuis 2004 comme à l'état de l'art et son utilisation en cryptographie ou en sécurité est proscrite. Ainsi, l'utilisation de cet algorithme permettrait à une personne ayant connaissance du mot de passe haché de déchiffrer celui-ci sans difficulté en un temps très court (par exemple, au moyen de sites internet librement accessibles qui permettent de retrouver la valeur correspondante au hash du mot de passe) »[194].

3. Classification, séparation des rôles et sécurisation logique des accès

Afin d'assurer la confidentialité, l'intégrité et la disponibilité des données, les débiteurs de l'obligation de sécurité doivent « limiter l'accès aux données aux seules personnes qui en justifient le besoin par l'exercice de leurs fonctions ou du service »[195]. En premier lieu, il importe donc de mettre en place des procédures de classification de l'information permettant d'inventorier et de localiser toutes les données à caractère personnel traitées, et ce, quel qu'en soit le support, ainsi que de maintenir à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction). Ce principe (plus communément nommé sous son acronyme anglais, *SoD*, c'est-à-dire *Segregation of Duties*) consiste à compartimenter les responsabilités des différents acteurs en leur assignant des rôles permettant de définir *qui peut faire quoi* ou encore *qui a accès à quoi*. Assez fortement liée au principe précédent, la limitation des privilèges consiste à limiter les droits selon les différents rôles. En effet, trop de privilèges sur les systèmes d'information peut conduire à des fraudes ou à des erreurs. A titre illustratif, dans une décision de 2020, l'APD nationale indique que, parmi les mesures de sécurité adaptées destinées à garantir la confidentialité des données, il s'agit de « s'assurer que les données à caractère personnel ne sont accessibles qu'aux personnes et aux applications qui en ont explicitement l'autorisation. ll convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître. Ces personnes devraient

[192] Dans ce dossier, la CNIL a auditionné le médecin responsable du traitement qui a indiqué que « pour pouvoir accéder à distance aux images médicales hébergées dans le disque dur de l'ordinateur fixe de son domicile, il a ouvert les ports de la LiveBox utilisée à son domicile en activant le mode DMZ de cette dernière, dans l'objectif de faire fonctionner le VPN ». Voy. CNIL, Délibération de la formation restreinte no SAN-2020-014 du 7 décembre 2020.
[193] *Ibidem.*
[194] CNIL, Délibération SAN-2021-008 du 14 juin 2021. Dans cette délibération, la CNIL relève néanmoins que, « dans le cadre de la procédure de sanction, la société a justifié avoir mis en œuvre un système de hachage satisfaisant, en SHA256, de l'ensemble des mots de passe des utilisateurs ».
[195] APD, « Note relative à la sécurité des données à caractère personnel », *op.cit.*, p.4.

uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues et ce, dans le respect du principe de finalité ».[196]

Afin d'assurer le respect de ces règles, il est recommandé de compléter l'identification des intervenants par une procédure d'authentification. Ainsi, selon la CNIL, « pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens informatiques »[197]. Par conséquent, dans une décision de 2021, l'autorité française considère que "l'attribution d'un identifiant unique par utilisateur et l'interdiction des comptes partagés figurent parmi les précautions indispensables afin de garantir une traçabilité effective des accès à une base de données. En l'espèce, le partage du compte permettant d'accéder à la copie de la base de données de production par quatre salariés ne permet pas de garantir une authentification correcte des utilisateurs et, par conséquent, une gestion effective des habilitations et une traçabilité correcte des accès. Une telle absence de traçabilité des accès ne permet ainsi pas d'identifier un accès frauduleux ou l'auteur d'une éventuelle détérioration ou d'une suppression des données à caractère personnel Dans ces conditions, la formation restreinte considère que l'utilisation d'un compte générique ne permet pas de garantir la sécurité des données, au sens de l'article 32 du RGPD »[198].

4. Les mots de passe

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, en 2017, la CNIL a adopté une recommandation fixant les mesures minimales à mettre en œuvre[199].

Mettant ses recommandations en pratique, dans une décision de 2019, après avoir constaté que les mots de passe et identifiant des comptes génériques et individuels étaient pré-enregistrés et automatiquement complétés, la CNIL observe que « tout utilisateur peut donc accéder aux postes informatiques et à la connexion au logiciel de gestion de la société sans authentification préalable, le pré-enregistrement des mots de passe et identifiants équivalant à une absence de mot de passe et d'identifiants. Par conséquent, l'authentification des utilisateurs n'est pas assurée ce qui peut conduire des tiers non autorisés à accéder à des données personnelles

[196] APD, Chambre contentieuse, Décision quant au fond 19/2020 du 29 avril 2020, p. 10. De même, dans une décision de 2019, la CNIL a constaté que « que l'ensemble des salariés peut, à partir de la connexion au logiciel de gestion de la société, accéder aux images filmées des caméras en direct. Tous les salariés peuvent ainsi accéder aux images vidéo alors que l'accès à ces données n'est pas strictement nécessaire à l'accomplissement de leurs missions. Or la société doit définir des profils d'habilitation afin de limiter les accès des utilisateurs aux seules données dont ils ont besoin, l'ensemble des salariés n'ayant pas à accéder aux images vidéo en temps réel. », voy. CNIL, Décision MED-2019-025 du 5 novembre 2019.
[197] CNIL, « La sécurité des données personnelles », *op.cit*., p.9.
[198] CNIL, Délibération SAN-2021-008 du 14 juin 2021.
[199] CNIL, Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

»[200]. Dans une autre délibération de 2021, l'autorité française s'intéresse à la robustesse des mots de passe, indiquant que « la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. […] À titre d'éclairage, la formation restreinte rappelle que pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, la CNIL recommande, dans sa délibération n° 2017-012 du 19 janvier 2017, que le mot de passe comporte au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou alors comporte au moins huit caractères - contenant trois de ces quatre catégories de caractères - s'il est accompagné d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (comme un captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses »[201]. Dans la même décision, la CNIL rappelle que « le fait de stocker les mots de passe d'accès aux bases de données en clair dans un fichier texte contenu dans un ordinateur de la société n'est pas une solution de gestion sécurisée des mots de passe. En effet, une authentification reposant sur l'utilisation d'un mot de passe court ou simple peut conduire à des attaques par des tiers non autorisés, telles que des attaques par force brute qui consistent à tester successivement et de façon systématique de nombreux mots de passe et permettre, ainsi, une compromission des comptes associés et des données qu'ils contiennent. Dans ces conditions, la formation restreinte considère que la politique de gestion des mots de passe de la société mise en cause n'était pas suffisamment robuste et contraignante pour garantir la sécurité des données, au sens de l'article 32 du RGPD »[202].

5. Journalisation, traçage et analyse des accès

Ainsi que nous l'avons déjà rappelé, les critères de sécurité classiques, tels que préconisés par la suite ISO27xxx, sont la confidentialité des données, leur intégrité et leur disponibilité. A ceux-ci s'ajoute la notion d'imputabilité, « qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) »[203]. De manière pragmatique, c'est l'activité de journalisation qui concrétise cette propriété d'imputabilité. Celle-ci consiste en l'enregistrement des informations pertinentes concernant les évènements d'un système informatique (accès au système ou à un de ses dossiers, modification d'un fichier, transfert de

[200] CNIL, Décision MED-2019-025 du 5 novembre 2019.
[201] CNIL, Délibération SAN-2021-008 du 14 juin 2021.
[202] *Ibidem.*
[203] APD, « note relative à la sécurité des données à caractère personnel », *op.cit.*, p.2.

données…) dans des fichiers appelés « log files »[204]. Les informations reprises sont entre autres les données consultées, la date, le type d'évènement, les données permettant d'identifier l'auteur de l'évènement, ainsi que le motif de cet accès. Ceci permet notamment d'identifier toute consultation des données personnelles abusive ou pour une finalité non légitime, ou encore de déterminer l'origine d'un accident.[205]

Bien que la journalisation ne soit pas expressément mentionnée dans le RGPD[206], la tenue d'un journal des log files constitue une mesure technique et organisationnelle envisagée dans l'article 32 du Règlement[207]. Dans une décision de 2021, l'APD nationale affirme que la journalisation « constitue une bonne pratique, recommandée par la Chambre Contentieuse à tout responsable de traitement. Ces mesures doivent être adaptées aux risques »[208]. En l'espèce, « un employé de la défenderesse a pu procéder à 20 reprises à des consultations illicites de ces données financières sensibles, sur une période s'étalant d'avril 2016 à août 2018. Ceci, combiné à l'absence de tenue d'un registre journal des accès ou d'un quelconque contrôle des accès par les cadres (dont faisait partie l'ex-mari) aux registres de la BNB par la défenderesse avant l'incident, démontre l'insuffisance des mesures dans le chef de la défenderesse »[209]. Selon l'autorité, cette absence de journalisation « empêche aussi la plaignante de pouvoir exercer son droit d'accès concernant les traitements illicites effectués par son ex-mari, employé de la défenderesse, puisque la défenderesse n'en conserve aucune trace ». Par conséquent, la Chambre Contentieuse « constate que la défenderesse était et demeure en défaut de mettre en œuvre les mesures techniques et organisationnelles adéquates requises par l'article 24.1 et 32 du RGPD pour garantir non seulement la sécurité des données en évitant des consultations illicites, mais aussi un exercice effectif des droits des personnes concernées telles la plaignante en l'absence de journalisation »[210].

Dans une autre décision de 2021, l'APD examine l'étendue du droit d'accès d'un plaignant « aux logs IT le concernant »[211]. Dans le cas d'espèce, la défenderesse justifie son refus de donner droit à la demande d'accès par deux arguments. Elle souligne, dans un premier argument, le droit à la vie privée des auteurs des logs IT comme raison pour refuser le droit d'accès du plaignant. Cet argument est rejeté par la Chambre contentieuse au motif que « le fait de rendre illisible les données à caractère personnel concernant les tiers avant de permettre l'exercice de son droit d'accès à la personne concernée satisfait l'exigence de l'article 15.4 RGPD

[204] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021, p.17.
[205] *Ibidem.*
[206] A l'inverse, la Directive (UE) 2016/680, déjà citée, accorde une importance particulière à la consultation et la divulgation (traitements les plus courants) et impose l'identification de l'auteur du traitement ainsi que celle des destinataires en cas de divulgation, le moment exact, ainsi que la justification du traitement.
[207] A ce sujet, lire F. DUMORTIER, « Chapitre 4 - Cybersécurité, vie privée, imputabilité, journalisation et log files » in Les obligations légales de cybersécurité et de notifications d'incidents, Bruxelles, Politeia, 2019.
[208] APD, Chambre contentieuse, Décision quant au fond 56/2021 du 26 avril 2021, p.17.
[209] *Ibid*., pp. 19-20.
[210] *Ibidem*.
[211] APD, Chambre contentieuse, Décision quant au fond 15/2021 du 09 février 2021, p.22.

de ne pas porter atteinte aux droits des tiers »[212]. Quant au second argument de la défenderesse liée à la charge de travail disproportionnée que représenterait une fouille systématique de tous les logs IT concernant le plaignant, l'APD suit la défenderesse dans son raisonnement : « faire droit à cette demande du plaignant lui imposerait une obligation disproportionnée à l'intérêt du plaignant à exercer son droit à la protection des données. Il n'y a dès lors pas de violation dans le chef de la défenderesse du droit d'accès quant aux logs IT concernant le plaignant »[213].

Pour le surplus, relevons que la CNIL a récemment publié un projet de recommandation relative à la journalisation[214], dans laquelle elle préconise notamment de « conserver ces données pendant une durée comprise entre six mois et un an. Elle estime en effet que cette durée est suffisante, dans la plupart des cas, afin d'assurer un équilibre entre, d'une part, la nécessité de disposer de données de journalisation permettant d'identifier les atteintes au système de traitement et, d'autre part, la nécessité de ne pas conserver un volume de données trop important pouvant faire l'objet d'attaques ou de détournements de finalité »[215].

6. L'effacement des données à caractère personnel

Le RGPD prévoit que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[216]. Quand cette durée est dépassée, le responsable du traitement doit donc anonymiser ces données ou les détruire de manière définitive. Lorsqu'il est fait usage de la seconde option, il est important de s'assurer que le processus est effectif au risque d'entraîner une divulgation non autorisée des données. Confrontée à de nombreuses questions relatives l'élimination « sécurisée » de données ou de supports de données, l'APD nationale a récemment publié une recommandation pour y répondre[217]. Dans celle-ci l'autorité présente les différentes techniques de « nettoyage » existantes pour différents types de supports (HD, SSD, papier, etc.) qui, soit rendent l'accès aux données impossible sur un support préservé (effacement sans possibilité de reconstitution et chiffrement), soit aboutissent à la destruction du support (sans possibilité de reconstruction). Trois niveaux de confidentialité associés à trois classes de techniques sont

[212] *Ibidem.*
[213] *Ibidem.*
[214] CNIL, Projet de recommandation relative à la journalisation soumise à consultation publique, 29 avril 2021, disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/projet_de_recommandation_-_journalisation.pdf
[215] *Ibid.*, p.3.
[216] Article 5.1, e) du RGPD.
[217] APD, Recommandation relative aux techniques de nettoyage de données et de destruction de supports de données, 2021.

distinguées : clear[218] (nettoyer), purge[219] (purger) et destroy[220] (détruire). La recommandation aborde aussi ce traitement (nettoyage et destruction) d'une manière plus large en détaillant ses différents aspects, tant légaux (que techniques ou organisationnels et examine le traitement dès avant l'achat des supports jusqu'aux étapes de vérification et d'enregistrement des résultats.

VI. Les obligations de notification et de communication d'incidents

Le Groupe 29 souligne qu'un des éléments clés de toute politique de sécurité des données est d'être en mesure de prévenir toute violation dans la mesure du possible et, lorsqu'une telle violation se produit malgré tout, d'y réagir dans les meilleurs délais.[221] Ainsi que déjà mentionné, le concept de « violation de données à caractère personnel » tel que défini à l'article 4, 12) du RGPD couvre tant les violations d'intégrité, de confidentialité que celles de disponibilité des données, mêmes si ces dernières sont seulement temporaires. Evidemment, ces différents types de violations de données peuvent avoir lieu séparément ou de manière cumulative[222].

Dès lors qu'une telle violation se produit, les débiteurs de l'obligation de sécurité sont soumis à un ou plusieurs devoirs selon les risques encourus.

1. Le registre des violations

Quelle que soit la gravité de la violation, le responsable du traitement est tenu de la documenter « en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier »[223]. Outre ces informations, le Groupe29 recommande que le responsable du traitement documente également le raisonnement justifiant les décisions prises en réaction à la violation. En particulier, lorsqu'une violation n'est pas notifiée à l'APD, la justification de cette décision devrait être documentée. Cette

[218] Selon l'APD, « les techniques de niveau « clear » visent à empêcher une récupération des données effectuée à l'aide d'un logiciel. Elles offrent une confidentialité modérée (certaines données pourront être récupérées si l'on dispose du temps, des connaissances et des compétences nécessaires). Il s'agit de techniques purement logiques. Exemples : la réécriture (partielle) à l'aide de commandes standards (read and write) et la réinitialisation de l'appareil ou du support (état 'sortie usine' - souvent conseillé pour les appareils mobiles et les routeurs/commutateurs). », *Ibid*., p.20.

[219] Selon l'APD, « Les techniques de niveau « purge » visent à empêcher une récupération des données effectuée à l'aide de techniques de laboratoire avancées. Elles offrent un niveau de confidentialité plus élevé et sont appropriées quand le support est destiné à être réutilisé dans un contexte de sécurité/confidentialité différent du contexte initial. Il s'agit de techniques logiques et physiques. Exemples : la réécriture à l'aide de commandes dédiées, la démagnétisation et l'effacement cryptographique. », *Ibid*., p.20.

[220] Selon l'APD, « les techniques de type « destroy » offrent le niveau le plus élevé de confidentialité/sécurité. La récupération des données est en effet impossible, même à l'aide de techniques de laboratoire de pointe. Elles reposent sur la destruction physique et sont donc incompatibles avec une réutilisation du support. Notons qu'une technique rendant le support inutilisable, n'atteindra pas le niveau destroy si certaines données restent néanmoins récupérables. Exemples : l'incinération, le déchiquetage et le broyage », *Ibid*., p.21.

[221] Groupe 29, WP250rev01, *op.cit*., p.7. Voy. également le considérant 87 du RGPD.

[222] *Ibid*., p.8.

[223] Article 33.5 du RGPD

justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus. Si le responsable du traitement considère que l'une des conditions visées à l'article 34.3, est remplie pour ne pas procéder à une communication, il devrait également pouvoir fournir des éléments de preuve appropriés à cet égard[224].

Le RGPD ne définit pas la période de conservation d'une telle documentation. Lorsque de tels registres contiennent des données à caractère personnel, il incombera au responsable du traitement de déterminer la période de conservation appropriée conformément aux principes liés au traitement de données à caractère personnel. De toute évidence, si les registres en eux-mêmes ne contiennent pas de données à caractère personnel, le principe de limitation de la conservation ne s'applique pas[225].

Cette exigence de tenir un registre des violations, qu'elles soient sujettes à notification ou non, est liée au principe d'*accountability*. Le responsable du traitement devra conserver cette documentation dès lors que l'autorité de contrôle pourrait la réclamer à titre de preuve du respect du RGPD. En cas de manquement à cette obligation de documenter correctement une violation, l'autorité de contrôle pourrait exercer ses pouvoirs au titre de l'article 58 et/ou imposer une amende administrative conformément à l'article 83.

2. La notification des violations à l'APD

A moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, l'article 33.1 du RGPD prévoit que le responsable du traitement est tenu de la notifier à l'APD dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance[226]. Dans le cas où la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est doit être accompagnée des motifs du retard.

Le Groupe 29 considère que le moment de prise de connaissance d'une violation de données est celui où il existe un « degré raisonnable de certitude » qu'un incident a eu lieu et que les données sont compromises[227]. Même si le moment concret de prise de connaissance dépend des circonstances, le Groupe estime que l'accent doit être mis « sur une intervention et une enquête rapide visant à déterminer s'il y a effectivement eu violation

[224] Groupe 29, WP250rev01, *op.cit*., pp.30-31
[225] *Ibidem*
[226] L'article 33.4 du RGPD prévoit que la notification à l'autorité de contrôle doit contenir, à tout le moins la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ; la communication, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; la description des conséquences probables de la violation de données à caractère personnel ; la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
[227] Groupe 29, WP250rev01, *op. cit*, p.11.

de données à caractère personnel »[228]. Après avoir pris connaissance d'un incident, et si celui -ci est *susceptible d'engendrer un risque,* le responsable du traitement devra le notifier dans les meilleurs délais, et, si possible, dans les 72 heures[229]. Pendant cette période de 72 heures, « le responsable du traitement devrait évaluer le risque probable pour les personnes concernées afin de déterminer si l'obligation de notification s'applique et quelle ou quelles mesures doivent être prises afin de remédier à cette violation »[230]. Afin d'évaluer le risque pour les personnes physiques résultant d'une violation de données, et par conséquent, pour savoir si une notification est requise, les exemples énumérés dans les lignes directrices du Groupe 29 et de l'EDPB sont particulièrement utiles[231]. A titre illustratif, « une violation qui ne nécessiterait aucune notification à l'autorité de contrôle serait la perte d'un appareil mobile crypté de façon sécurisée et utilisé par le responsable du traitement et son personnel. Si la clé de cryptage reste en la possession du responsable du traitement et que les données à caractère personnel affectées ne constituent pas une copie unique, celles-ci seraient inaccessibles à tout pirate »[232].

Quant au sous-traitant, le second paragraphe de l'article 33 du RGPD précise qu'il doit notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Il convient de noter que le sous-traitant ne doit pas évaluer la probabilité qu'un risque découle d'une violation avant de la notifier au responsable du traitement : il appartient au responsable du traitement d'effectuer cette évaluation après avoir pris connaissance de la violation[233]. L'obligation faite au sous-traitant de notifier la violation au responsable du traitement permet à ce dernier de déterminer s'il est nécessaire d'avertir l'autorité de contrôle conformément à l'article 33.1.

---

[228] *Ibid.,* p12.

[229] Selon le Groupe 29, « Le RGPD reconnaît que les responsables du traitement ne disposeront pas toujours de toutes les informations nécessaires concernant une violation dans les 72 heures après en avoir pris connaissance, dès lors que l'ensemble des détails de l'incident peuvent ne pas être systématiquement disponibles au cours de cette période initiale. Il autorise donc une notification échelonnée. Une telle notification interviendra plus probablement dans le cas de violations plus complexes, telles que certains types d'incidents de cybersécurité nécessitant par exemple une enquête approfondie et détaillée afin d'établir pleinement la nature de la violation et la mesure dans laquelle des données à caractère personnel ont été compromises ».

[230] *Ibid.,* p.13.

[231] Groupe 29, WP250rev01, *op. cit* et EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, *op.cit.*

[232] Groupe 29, WP250rev01, *op. cit*, pp.21-22. Toutefois, selon le Groupe, « Si, par la suite, il devient évident que la clé de cryptage a été compromise ou que le logiciel ou algorithme de cryptage est vulnérable, le risque pour les droits et libertés des personnes physiques s'en verra affecté et une notification pourra alors être nécessaire ».

[233] La raison pour laquelle le sous-traitant doit simplement établir si une violation s'est produite puis la notifier au responsable du traitement, sans évaluer les risques au préalable, est que le sous-traitant pourrait ne pas connaître tous les éléments pertinents liés à la violation. Il pourrait par exemple ne pas savoir si le responsable du traitement conserve toujours une copie ou une sauvegarde des données à caractère personnel détruites ou perdues par le sous-traitant. Ces éléments pourraient avoir une incidence sur l'obligation de notification du responsable du traitement. Autant dire qu'en cas de sous-traitance, une clause contractuelle précisant un délai plus précis de notification au responsable du traitement est fortement recommandée au risque pour ce dernier de ne pouvoir se conformer au délai « maximum » de 72 heures.

3. La communication des violations aux personnes concernées

En sus de l'obligation de notification à l'APD, l'article 34.1 du RGPD prévoit que lorsqu'une violation de données à caractère personnel est *susceptible d'engendrer un risque élevé* pour les droits et libertés d'une personne physique, le responsable du traitement doit également communiquer ladite violation à la personne concernée dans les meilleurs délais[234]. Le seuil à atteindre est par conséquent plus élevé pour la communication aux personnes concernées que pour la notification à l'autorité de contrôle. Pour évaluer si une violation est susceptible de constituer un risque élevé pour les droits et libertés des personnes physiques, il convient de tenir compte de la réponse à la question de savoir si la violation peut entraîner des dommages physiques, matériels ou immatériels pour les personnes dont les données font l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière et une atteinte à la réputation.[235]

En pratique, afin de savoir si une communication est requise ou non, il s'agit tout d'abord d'avoir égard aux trois conditions énumérées par le paragraphe 3 de l'article 34 dans lesquelles la communication aux personnes concernées n'est pas nécessaire[236]. En outre, l'annexe B des lignes directrices du Groupe 29 fournit une liste non exhaustive d'exemples de cas où une violation pourrait être susceptible d'engendrer un risque élevé pour les personnes concernées et, partant, de cas où un responsable du traitement devra communiquer une violation aux personnes concernées[237]. Enfin, tout récemment, l'EDPB a également énuméré un certain nombre d'exemples supplémentaires dans ses lignes directrices destinées à compléter celles du Groupe 29 afin d'aider les responsables lors de l'évaluation des risques[238]. A titre illustratif, dans une décision de 2021 l'APD nationale a estimé qu'une communication était requise car « en attribuant le numéro de téléphone du plaignant à un tiers, [le fournisseur] expose le plaignant au risque que des actes frauduleux soient effectués en son nom,

[234] Lorsque la communication aux personnes concernées est requise, celle-ci doit contenir décrire « en des termes clairs et simples » au moins les informations suivantes : la nature de la violation de données à caractère personnel ; la communication, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; la description des conséquences probables de la violation de données à caractère personnel ; la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

[235] Groupe 29, WP250rev01, *op. cit*., p.26.

[236] La communication à la personne concernée n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie: a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement; b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser; c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

[237] Groupe 29, WP250rev01, *op. cit*, pp. 35-38.

[238] EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification, *op.cit.*

en utilisant son numéro de téléphone. Le risque existe également - contrairement à ce que semble affirmer le défendeur - que des données sensibles (telles que des données de santé) tombent entre les mains de tiers »[239].

L'objectif principal de la communication est de permettre aux personnes concernées de « prendre les précautions qui s'imposent »[240]. Il s'agit donc de « formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels »[241]. Par exemple, dès lors que des mots de passe sont compromis, « le responsable du traitement devrait obliger les personnes concernées à créer un nouveau mot de passe, en mode sécurisé, afin de garantir que tous les nouveaux mots de passe soient utilisés par des utilisateurs légitimes, et non par des tiers qui ont obtenu les données d'identification. Dans la pratique, cela peut correspondre à la procédure sécurisée de renouvellement d'un mot de passe perdu et des informations justifiant le renouvellement du mot de passe devraient être incluses. Dans la notification adressée à l'utilisateur, il convient également de recommander à ce dernier de ne pas réutiliser l'ancien mot de passe ou un mot de passe similaire et de changer les mots de passe compromis pour tous les comptes où le même mot de passe était utilisé »[242].

Conclusion

Dans cette contribution, nous nous sommes efforcés à détailler les différents facteurs que les débiteurs de l'obligation de sécurité doivent prendre en compte afin de déterminer les mesures appropriées à mettre en œuvre pour sécuriser leurs traitements de données à caractère personnel. Parmi les éléments à prendre en considération figurent l'analyse des risques pour les droits et libertés des personnes physiques et l'état des connaissances technologiques. Ces deux paramètres ont en commun d'exiger une attention continue qui ne peut se limiter à un exercice ponctuel. En effet, l'analyse de la probabilité et de la gravité des risques nécessite une évaluation permanente pour maintenir à niveau la sécurité dans un environnement qui change au fil du temps. Quant à la prise en compte de l'état des connaissances, celle-ci impose aux responsables du traitement et aux sous-traitants un devoir de diligence digitale puisque ceux-ci doivent sans cesse être au courant des progrès technologiques, tant en termes de menaces potentielles que de mesures appropriées pour y faire face. Négliger de se tenir à jour avec les changements technologiques peut effectivement entraîner un manque de conformité avec l'article 32 du RGPD. A cet égard, il est utile de maintenir une veille des diverses recommandations et décisions des autorités de contrôle en la matière qui préconisent notamment la mise en place de politiques d'authentification, de gestion des accès logiques, de journalisation, de chiffrement et de

[239] APD, Chambre contentieuse, Décision quant au fond 05/2021 du 22 janvier 2021.
[240] Considérant 86 du RGPD.
[241] *Ibidem.*
[242] Groupe 29, WP213, *op.cit.*, p.9.

mots de passe robustes. En outre, les récentes décisions des autorités de contrôles confirment la *ratio legis* du RGPD selon laquelle sécurité des données et *accountability* vont de pair : une obligation de moyens n'a de réelle puissance que lorsqu'elle est accompagnée de mesures permettant de vérifier si ses débiteurs ont été suffisamment prudents et diligents dans sa mise en œuvre.