Les obligations de sécurité et de notification des violations des traitements de données à caractère personnel

Dumortier, Franck

Published in:
Les obligations légales de cybersécurité et de notifications d'incidents

Publication date:
2019

Document Version
le PDF de l'éditeur

LES OBLIGATIONS DE SÉCURITÉ ET DE NOTIFICATION DES VIOLATIONS DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Franck Dumortier[1]

A. Introduction

À l'ère numérique, 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[2]. Ce lien de dépendance a notamment été illustré par la Cour européenne des droits de l'Homme dans l'affaire *I. c. Finlande*[3] ; celle-ci estimant que le défaut de garanties relatives à la sécurisation des données contre des usages non autorisés constitue 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 »). Cette perception des choses est importante pour éclairer et interpréter l'obligation de sécurisation de données concernant des personnes physiques qui peuvent être identifiées directement ou indirectement[4].

---

1. Franck DUMORTIER est chercheur et maître de conférences au CRIDS. Il est chargé de cours en aspects légaux de la sécurité informatique dans le cadre du Master en cybersécurité à l'Université de Namur.
2. Les articles 8 de la CEDH et 22 de la Constitution belge consacrent le droit au respect de la vie privée. Avec l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Charte des droits fondamentaux de l'Union européenne a acquis force juridique obligatoire et le droit à la protection des données à caractère personnel a été érigé au rang de droit fondamental autonome en son article 8 (en plus du droit à la vie privée consacré en son article 7).
3. 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.
4. Cour eur. D.H., 4 décembre 2008, *Marper c. Royaume-Uni*, req. n° 30562/04 et 30566/04, § 103. Selon la Cour, « La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. [...] Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs (voir notamment l'article 7 de la Convention [n°108] sur la protection des données) ».

Sous l'empire de la loi du 8 décembre 1992[5] (ci-après « LVP »), l'obligation de sécurité n'était pas sanctionnée et les brèches de sécurité ne devaient pas explicitement être divulguées[6]. De ce point de vue, la sécurité des données était en quelque sorte le parent pauvre du régime de leur protection légale. Néanmoins, en janvier 2013, suite à d'importantes fuites d'informations personnelles[7], la Commission de la protection de la vie privée (ci-après « CPVP ») a vivement rappelé dans l'une de ses recommandations[8] que le manque de garanties de sécurité impliquait très potentiellement la violation d'autres principes essentiels de protection des données faisant, eux, l'objet de sanctions pénales : notamment les principes de finalité[9] et d'information[10]. En effet, sous ce régime antérieur, on considérait déjà la sécurité des données à caractère personnel comme une condition *sine qua non* de leur traitement[11]. Ainsi, Y. Poullet s'interrogeait en ces mots : « Sans elle, comment convaincre la personne concernée qui se prévaut de son droit d'accès, que les informations communiquées en conséquence de l'exercice de ce droit soient les seules détenues. Comment affirmer qu'aucune personne non autorisée n'aura jamais accès à des données détenues par le responsable pour des finalités illégitimes ? Comment enfin, garantir la personne concernée contre la non déformation des données voire l'ajout de certaines données non pertinentes ? »[12].

Par conséquent, la CPVP a haussé le ton et exhorté qu'elle soit informée des causes et des dommages de ce type d'incidents et qu'une campagne d'information subséquente au public soit réalisée ; menaçant également d'effectivement dénoncer au procureur du Roi

5. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993 (ci-après « LVP »).
6. A l'exception du secteur « télécom » dans lequel la directive 2002/58/CE sur la protection de la vie privée dans les communications électroniques fut été amendée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 en vue notamment d'y introduire une disposition spécifique aux « violation de données à caractère personnel ».
7. Il s'agissait de la publication en ligne via Google de la liste de clients de SNCB Europe concernant 1.500.000 personnes le 22 décembre 2012, de la publication d'une liste de 500 collaborateurs de la Défense le 3 janvier 2013 et d'une publication similaire le 8 janvier 2013 des données salariales de 15.000 personnes récoltées sur la base d'une enquête sur les salaires réalisée par Jobat.
8. Ancienne Commission de la protection de la vie privée (ci-après « CPVP »), Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données n° 01/2013 du 21 janvier 2013.
9. L'article 4, § 1, 2°, de la LVP ne permettait pas que des données dont dispose un responsable du traitement soient réutilisées pour une finalité incompatible avec la finalité pour laquelle il a initialement obtenu ces données. Il va de soi que la publication en ligne de données qui n'étaient pas destinées au départ à être publiées constitue un traitement de données impliquant une infraction à ce prescrit, laquelle était en outre pénalement sanctionnée par l'article 39, 1°, de la LVP.
10. L'article 9 de la LVP imposait au responsable du traitement l'obligation d'informer les personnes concernées des finalités pour lesquelles les données seront utilisées. S'il apparaissait ultérieurement que le responsable du traitement a utilisé les données pour une finalité incompatible avec la finalité initiale et à propos de laquelle il n'a fourni aucune information aux personnes concernées, il aurait commis une infraction punissable sur la base de l'article 39, 4° de la LVP.
11. Y. POULLET, « La sécurité informatique, entre technique et droit », *Cahiers du CRID*, n° 14, 1998, p. 17.
12. *Ibid.*

les infractions dont elle avait connaissance.[13] Dans la foulée, en 2014, le Groupe 29[14] rappela que l'obligation de sécurité imposée par l'article 17 de la Directive 95/46/CE[15] (ci-après « la Directive ») imposait une gestion proactive des risques dans laquelle l'utilisation de mécanismes d'inintelligibilité (par exemple le chiffrement) des données est particulièrement recommandée afin de minimiser l'impact de fuites de données, lesquelles devraient, le cas échéant, être communiquées aux personnes concernées[16]. La même année, le Groupe 29 réaffirma que *l'approche fondée sur le risque* (« *risk-based approach* ») était au cœur du cadre légal régissant la protection des données[17], sans remettre pour autant en question les principes de protection des données ou les droits des personnes concernées.
C'est donc tout naturellement que le Règlement général sur la protection des données[18] (ci-après « RGPD ») innove par rapport à la Directive en consacrant le principe « d'intégrité et de confidentialité » comme l'une des pierres angulaires de leur protection. L'élévation de l'obligation de sécurité au rang de principe de base n'est pas que théorique puisqu'elle soutenue dans le texte du Règlement par l'impératif documentaire découlant du devoir d'*accountability*[19] ayant pour outils principaux l'établissement d'un registre des activités de traitements (ci-après « Registre »)[20] et, dans certains cas, la conduite d'une analyse d'impact (ci-après « AIPD »)[21]. La culture de la sécurité des données se voit également promue par l'introduction de mesures concrètes telle la protection des données dès la conception et par défaut[22] ainsi que par la possibilité de recourir à des codes de

13. Conformément à l'article 32, § 2, de la LVP.
14. Le Groupe de travail « Article 29 » (Groupe 29) était le groupe de travail consultatif européen qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018. Depuis l'entrée en application du RGPD, il a été remplacé par le Comité Européen de la Protection des Données.
15. 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, *J.O.C.E.*, 23 novembre 1995, n° L 281/31 (ci-après « directive 95/46 »).
16. Groupe 29, « Avis 03/2014 sur la notification des violations de données à caractère personnel », *WP213*, 25 mars 2014, p. 3.
17. Groupe 29, « Statement on the role of a risk-based approach in data protection legal frameworks », *WP218*, 30 mai 2014, p. 2.
18. 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) (ci-après « RGPD »).
19. RGPD, art. 5, § 2 et 24. 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. Dans la plupart des autres langues européennes, du fait, essentiellement, de la diversité des systèmes juridiques, il est difficile de traduire le terme '*accountability*' » : Groupe 29, « Avis n° 3/2010 sur le principe de la responsabilité », *WP173*, 13 juillet 2010, p. 8.
20. RGPD, art. 30.
21. *Ibid.*, art. 35.
22. *Ibid.*, art. 25.

conduite ou des mécanismes de certification pour « faciliter » la démonstration du respect des exigences légales. De plus, dans la plupart des cas, les violations de données doivent maintenant être notifiées à l'Autorité de protection des données[23] (ci-après « APD ») et parfois même être communiquées aux personnes concernées[24]. Enfin, les manquements à l'obligation de sécurité sont dorénavant potentiellement punissables d'amendes administratives[25].

B. Les notions de base

1. La définition large de donnée à caractère personnel

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 ».

Dans un avis datant de 2007, le Groupe 29 insistait déjà sur le fait que « comme dans la Convention 108[26], une définition large est adoptée afin de couvrir toutes les informations qui peuvent être reliées à une personne »[27]. Dans son document, le Groupe analyse les quatre grands éléments constitutifs de la définition, à savoir 1) « toute information », 2) « concernant », 3) « une personne physique », 4) « identifiée ou identifiable ».

1) 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. 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. Du point de vue du contenu des informations, la notion englobe 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.)[28]. 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[29].

2) Afin de considérer que les données « concernent » une personne physique, la présence d'un élément de « contenu », de « finalité » ou de « résultat » est indispensable. Ces trois éléments (contenu, finalité, résultat) sont à considérer comme des conditions alternatives et non cumulatives. L'élément de « contenu » est présent lorsque des informations *ont trait* à une personne. À titre exemplatif, 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 »[30]. 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. À 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 ces données. À titre indicatif, le considérant 26 du GDPR considère ainsi 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 »[31].

23. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
24. RGPD, art. 34.
25. *Ibid.*, art. 83, § 4, a) et 83, § 5, a).
26. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Référence, *STE n°108*, 28 janvier 1981.
27. Groupe 29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP136*, 20 juin 2007, p. 4.
28. 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 (..) ».
29. Groupe 29, *WP136, op. cit.*, pp. 6 à 9.
30. Voy. dans le même sens la position prise par la Federal Trade Commission des États-Unis dans son document « Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers » : « *The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.* » (FTC Report, March 2012, p. 22).
31. EDRI, « Key aspects of the proposed General Data Protection Regulation explained », disponible à l'adresse suivante : https ://edri.org/files/GDPR-key-issues-explained.pdf. Voy. aussi Y. POULLET, « Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications », Conseil de l'Europe, Comité consultatif T-PD, *T-PD (2004) 04 final*, p. 28.

3) 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 »). Le considérant 26 du RGPD accorde une attention particulière au terme « identifiable », en énonçant que « pour déterminer si une personne physique est identifiable, il convient 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 [...]. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération 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 ». Le critère de « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne » doit notamment prendre en compte tous les facteurs en jeu. Les coûts engendrés par l'identification constituent un facteur, mais pas le seul. La finalité visée, la manière dont le traitement est structuré, l'intérêt escompté par le responsable du traitement, les intérêts en jeu pour les personnes, les risques de dysfonctionnements organisationnels (par exemple violations du devoir de confidentialité) et les défaillances techniques sont autant d'aspects qu'il convient de prendre en considération. De manière plus pédagogique, on peut affirmer que toute donnée qui, seule ou combinée à d'autres, pourrait permettre l'identification d'une personne physique par la police, les autorités judiciaires ou les services de renseignements doit être considérée comme étant à caractère personnel, même si une procédure doit être respectée pour que cette donnée soit légalement accessible par ces services[32]. Par ailleurs, il convient de tenir compte de l'état d'avancement technologique au moment du traitement et de changements éventuels pendant la période pour laquelle les données seront traitées. En effet, il se peut que l'identification ne soit pas possible aujourd'hui avec l'ensemble des moyens existants auxquels l'on peut raisonnablement recourir, mais qu'elle le soit pendant une phase future de la durée de traitement.

4) La protection conférée par le Règlement s'applique aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence[33] mais ne couvre pas le traitement des données à caractère personnel qui concerne les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de celles-ci[34]. Le règlement protège donc uniquement les personnes de chair et de sang dotés d'une « personnalité juridique » telle qu'évoquée à l'article 6 de la Déclaration universelle des droits de l'homme[35]. En Belgique, cette personnalité juridique est reconnue à tous les individus nés vivants et viables. En principe les données personnelles sont dès lors des données concernant des personnes vivantes identifiées ou identifiables. *A contrario*, le considérant 27 du RGPD indique qu'il « ne s'applique pas aux données à caractère personnel des personnes décédées ». Les Érats membres peuvent néanmoins prévoir des règles relatives au traitement des données à caractère personnel de celles-ci[36]. De plus, la législation nationale sur le droit au respect de l'image et de l'honneur peut également prévoir une protection de la mémoire de la personne décédée.

Étant donnée l'interprétation extrêmement large de la notion de « donnée à caractère personnel », nous recommandons aux lecteurs qu'à moins d'être en mesure de déterminer avec une certitude absolue que les données traitées ne correspondent pas à des personnes identifiables, de considérer celles-ci comme étant à caractère personnel.

2. Les traitements régis par le RGPD

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 ».

Trois éléments caractérisent la notion de traitement. Celle-ci se définit comme une « opération » ou un « ensemble d'opérations » auxquelles sont soumises des données à caractère personnel pour la réalisation d'une même finalité ou de finalités proches.[37] La notion de traitement se veut intentionnellement vague et générique en visant non les techniques utilisées mais, plus directement, les manipulations qu'elles permettent de réaliser. Pour qu'il y ait traitement, des « données à caractère personnel », dont on a souligné l'interprétation large à suffisance, doivent donc être soumises à des manipulations réalisées en vue d'atteindre un but commun.

32. Cour eur. D. H., 24 avril 2018, *Benedik c. Slovénie,* req. n° 62357/14. L'affaire porte sur le fait que la police slovène ne s'est pas procuré de décision de justice aux fins de la consultation de données sur un abonné associées à une adresse IP dynamique enregistrée par les autorités de police suisses lors de la surveillance des utilisateurs d'un réseau de partage de fichiers. L'accès à ces données permit d'identifier le requérant qui sur ce réseau avait partagé des fichiers, notamment des images pédopornographiques.

33. Le considérant 2 du RGPD stipule : « Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. »

34. RGPD, consid. 14.

35. L'article 6 de la Déclaration universelle des droits de l'homme se lit comme suit : « Chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique. ».

36. Ce n'est pas le cas en Belgique. Sous le régime de la directive 95/46, certains pays, tel que l'Italie, avait prévu des règles spécifiques applicables aux traitements de données à caractère personnel des personnes décédées.

37. « Le traitement est [...] constitué de l'ensemble des opérations matérielles effectuées en vue de la réalisation de la finalité recherchée », M.-H. BOULANGER, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 122. Voy. aussi Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 379.

Le RGPD s'applique dès que les opérations effectuées sur des données personnelles se réalisent, ne fût-ce qu'en partie, par des moyens automatisés. Le concept de « procédés automatisés » appelle l'interprétation la plus large qui soit. Ils englobent toutes les technologies de l'information : informatique, télématique, réseaux de télécommunication (Internet). 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, etc. Le RGPD s'applique aussi dès qu'une seule opération fait intervenir des moyens automatisés. Ainsi, l'agence de placement qui conserve les *curriculums vitae* des candidats sur papier mais qui les envoie par fax aux offreurs d'emploi devra respecter les prescrits du règlement pour tout ce qu'elle fait avec les *curriculums vitae* reçus (les conserver, les classer, les transmettre)[38]. Simplement chercher de l'information concernant une personne physique sur Internet (à l'aide d'un moteur de recherche) est déjà considéré comme un traitement.

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. »[39] 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 »[40]. *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[41]. En guise d'exemple, les e-mails qui se trouvent dans un programme de messagerie (par exemple Outlook) constituent un stockage structuré de données car de nombreux programmes de messagerie permettent une fonction de recherche sur une caractéristique unique qui peut être couplée à une personne physique. Un recueil de mails imprimés qui n'ont pas été collectés ou rangés selon un classement déterminé ne relève toutefois pas du champ d'application du RGPD.

La règle générale est donc que le Règlement s'applique à la plupart des situations. À notre époque moderne actuelle, 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 (fichiers manuels qui sont conservés sans le moindre archivage structuré, comme

38. CPVP, *La protection des données à caractère personnel en Belgique*, disponible à l'adresse suivante : https ://www.privacycommission.be/sites/privacycommission/files/documents/protection-donnees-a-caractere-personnel-en-belgique.pdf.
39. RGPD, consid. 15.
40. *Ibid.*, art. 4, 6).
41. *Ibid.*, consid. 15. Voy. également D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, p. 67 : « Pour un fichier, il est exigé que les données à caractère personnel soient structurées suivant des critères relatifs aux personnes et qui rendent accessibles facilement les données. Par conséquent un dossier, dans lequel des pièces sont classés suivant un ordre chronologique, n'est pas classé suivant des critères spécifiques relatifs aux personnes [...] ».

un recueil non classé d'articles de presse dans des archives). Dès qu'il y a un traitement automatisé (comme à l'aide de moyens ICT), une certaine structure sera présente dans le traitement de données à caractère personnel et le règlement sera dès lors d'application.

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[42]. 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 conditions de travail et à leurs passe-temps, a été considéré par la Cour de justice de l'Union européenne (« CJUE ») comme étant régie par le régime du RGPD[43].

C. L'avènement d'un « nouveau » principe de base d'intégrité et de confidentialité

Une innovation remarquable du RGPD est qu'il érige le principe « d'intégrité et de confidentialité » des données à caractère personnel au même rang que les traditionnels principes de qualité des données (licéité, loyauté, transparence, finalité, minimisation, exactitude et limitation de la conservation des données). Selon ce « nouveau » principe, les données à caractère personnel 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 »[44].

42. RGPD, consid. 18. 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).
43. C.J.C.E., arrêt du 6 novembre 2003, Bodil Lindqvist, aff. C-101/01.
44. RGPD, art. 5, § 1er, f). Les termes « y compris » ne sont pas anodins puisqu'ils ne sont pas inscrits dans l'article 17, § 1er, de la directive 95/46.

Le principe de sécurité énoncé à l'article 5, § 1er, f), du RGPD semble toutefois avoir un objet plus restreint que celui de la doctrine classique selon laquelle la sécurité de l'information a pour trois objectifs principaux d'assurer la *confidentialité, l'intégrité* et la *disponibilité* des données[45]. Cette limitation du principe de sécurité à l'intégrité et à la confidentialité des données contraste également avec l'affirmation de l'ENISA[46] selon laquelle « *one of the core obligations for data controllers and processors in GDPR is that of the security of personal data. In particular, according to GDPR security equally covers confidentiality, integrity and availability* »[47].

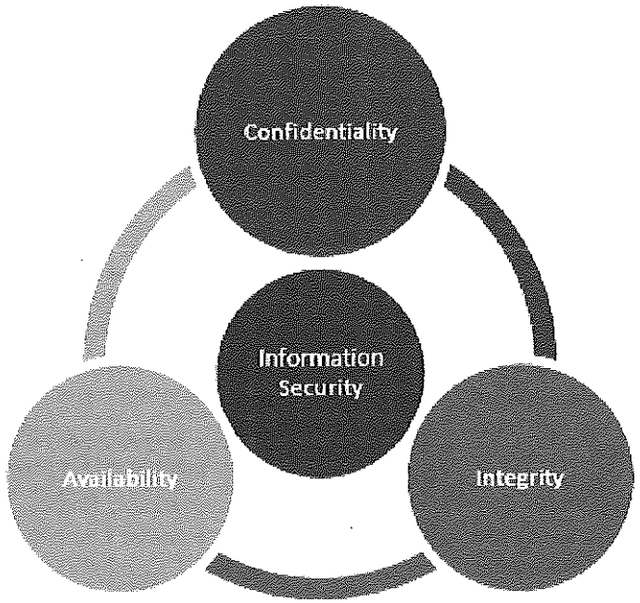

Figure 1- La triade intégrité-confidentialité-disponibilité selon l'ENISA[48]

Malgré un certain silence du RGPD sur la définition de la notion d'intégrité des données, 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

45. S. GHERNAOUTI, *Sécurité informatique et réseaux*, Dunod, 2013, p. 1.
46. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est une agence européenne créée pour servir le fonctionnement du marché intérieur. L'ENISA est un centre d'excellence en matière de sécurité des réseaux et de l'information pour les États membres et les institutions de l'Union européenne. Elle prodigue conseils et recommandations et agit comme une centrale d'informations en matière de bonnes pratiques. En outre, elle facilite les contacts entre les institutions européennes, les États membres, les entreprises privées et les acteurs de l'industrie.
47. ENISA, « Guidelines for SMEs on the security of personal data processing », décembre 2016, p. 7.
48. *Ibid.*, p.10.

ces systèmes reste inaltéré »[49]. Dans la même ligne, la CPVP, devenue l'Autorité de protection des données[50], 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 »[51].

Quant à la notion de confidentialité, le considérant 39 du RGPD suggère qu'elle consiste à « prévenir l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement ». L'APD va dans le même sens en définissant 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 »[52].

Les concepts d'intégrité et de confidentialité des données étant relativement clairs, le vocabulaire utilisé par le Règlement pose néanmoins fondamentalement la question du sort réservé à la garantie de la *disponibilité des données*, non explicitement prévue par l'article 5, § 1er, f), de celui-ci. Ce questionnement est loin d'être théorique puisque dans le domaine de la sécurité de l'information[53] – lequel couvre un contexte sensiblement plus large que celui de la sécurité des données à caractère personnel –, les normes

49. Groupe 29, « Avis 05/2012 sur l'informatique en nuage », *WP196*, p. 18.
50. Depuis le 25 mai 2018, l'Autorité de protection des données (« APD ») est le successeur de la Commission de la protection de la vie privée (CPVP) (qui était mieux connue sous la dénomination « Commission vie privée »). L'APD a été créée par la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.
51. CPVP, « Note relative à la sécurité des données à caractère personnel », p. 1, disponible à l'adresse suivante : http ://www.privacycommission.be/sites/privacycommission/files/documents/note_securite_des_donnees_a_caractere_personnel.pdf.
52. *Ibid.*
53. La « sécurité de l'information » est définie comme « l'ensemble de mesures de gestion qui veillent à ce que la confidentialité, l'intégrité et la disponibilité *de toutes les formes d'information* – tant sous la forme électronique (numérique) que papier – soient maintenues, dans le but d'assurer la continuité des informations et de l'information et de limiter à un niveau acceptable prédéfini les éventuelles conséquences d'incidents en matière de sécurité de l'information », *in* CPVP, « Lignes directrices pour la sécurité de l'information de données à caractère personnel-Version 2.0 », décembre 2014, p. 4. Voy. aussi, la définition donnée par le Contrôleur européen à la protection des données (EDPS) : « *Information Security applies irrespective of the nature of the information ; its key concepts apply whether or not personal data is processed* », EDPS, Security Measures for Personal Data Processing – Guidance on Security Measures for Personal Data Processing – Article 22 of Regulation 45/2001, 21 mars 2016, p. 5.

internationales[54] considèrent que la sécurité a non seulement pour objectif d'assurer l'intégrité et la confidentialité des données, mais également leur disponibilité entendue comme « la propriété des informations, systèmes et processus d'être accessibles et utilisables sur demande d'une entité autorisée »[55]. La notion de disponibilité des données serait ainsi intimement liée à celle de « résilience » des réseaux et des systèmes d'information. Il est donc légitime de s'interroger, d'une part, sur l'importance accordée par le RGPD à la *disponibilité* des données à caractère personnel, et, d'autre part, sur la signification donnée par le Règlement à cette propriété de sécurité considérée par le Groupe 29 comme faisant partie « des trois critères de sécurité classiques »[56].

En ce qui concerne la prise en considération de la disponibilité des données par le RGPD, un premier constat s'impose : pour la toute première fois dans le domaine de la protection des données à caractère personnel, un instrument législatif européen fait expressément référence aux *propriétés de disponibilité et de résilience* au sein de son corpus normatif. Ainsi, l'article 32, § 1er, du RGPD – lequel énumère de manière non exhaustive des moyens devant être mis en place *« selon les besoins »* – cite « des moyens permettant de garantir la confidentialité, l'intégrité, la *disponibilité* et la *résilience* constantes des systèmes et des services de traitement » ainsi que « 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 ». Clairement, cette innovation témoigne du fait que le législateur considère la *continuité de certains traitements* comme étant nécessaire à la protection de la vie privée des personnes concernées.

Pour mieux cerner la manière dont la propriété de disponibilité doit être prise en compte, il nous semble utile d'évoquer deux exemples qui, pour le Groupe 29, illustrent une certaine *granularité des exigences de disponibilité* selon *« les besoins »*[57]. Le Groupe évoque l'hypothèse d'un hôpital dans lequel des données médicales critiques relatives à des patients sont temporairement indisponibles pouvant potentiellement conduire à l'annulation d'opérations cliniques et mettre la vie desdits patients en danger. Il imagine ensuite le cas d'une société dans le secteur des médias empêchée de communiquer des *newsletters* à

54. La famille de norme ISO27xxx (ISO27000 – ISO/IEC 27000 :2016 Information technology — Security techniques — Information security management systems – Overview and vocabulary) d'un système de gestion de la sécurité (ISO27001 – 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. Un guide élaboré en janvier 2017 par la commission de normalisation AFNOR (« Protection des données personnelles : l'apport des normes volontaires ») recense les normes ISO incontournables en matière de protection des données personnelles.

55. CPVP, « Note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 1.

56. Groupe 29, *WP213*, *op. cit.*, p. 5. Le Groupe s'inspire clairement de l'ISO/CEI 27001 qui insiste particulièrement sur le triptyque « Disponibilité – Intégrité – Confidentialité ». L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013, son titre est « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences ». Elle fait partie de la suite ISO/CEI 27000 et permet de certifier des organisations.

57. Groupe 29, *WP250*, *op. cit.*, p. 9.

ses abonnés suite à une attaque par déni de service[58] (ci-après « DDoS ») ou à cause d'une simple coupure de courant. Dans la première situation, « des moyens permettant de garantir la confidentialité, l'intégrité, la *disponibilité* et la *résilience* constantes des systèmes et des services de traitement » sont fortement recommandables au vu de la susceptibilité d'un risque élevé pour les personnes concernées en cas de discontinuité – même « temporaire » – du service ; dans la seconde, « 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 » seront très vraisemblablement considérés comme suffisants. Malheureusement, l'EDPB (European Data Protection Board) s'est pour l'instant abstenu d'illustrer des cas de figure d'indisponibilité temporaires se situant dans l'échelle de gravité sans pour autant atteindre les antipodes mentionnés. Pensons, par exemple, à la vague de DDoS revendiqués par « Down-Sec Belgium » en 2015 et 2016 ayant perturbé les sites Internet du Premier ministre, du Sénat, du Comité P, de la N-VA, du cdH, de BNP Paribas Fortis, de l'Office national de l'Emploi, de la Fédération Wallonie-Bruxelles, de l'Agence Fédérale de Contrôle Nucléaire ou encore de Belgocontrol, parmi de nombreux autres dont Tax-on-Web. Certes, ces incidents n'eurent pas pour conséquence de porter atteinte à l'intégrité et à la confidentialité des données traitées, mais il semble néanmoins raisonnable, par exemple, de considérer que l'atteinte à la continuité d'un service permettant aux personnes physiques d'introduire leur déclaration fiscale en ligne est susceptible d'entraîner pour celles-ci un risque pour leurs droits et libertés pouvant potentiellement avoir pour répercussions dommageables des pertes financières ou du moins un léger préjudice sous la forme d'une perte de temps et de désagrément.

Le précédent exemple soulève la question de l'étendue des violations de disponibilité des données qui doivent être notifiées à l'APD conformément à l'article 33 du Règlement et communiquées aux personnes concernées dans les circonstances visées à l'article 34. Dans un premier avis datant de 2014, le Groupe 29 estimait que la notion de « violation de la disponibilité » renvoyait à « la destruction ou à la perte, accidentelles ou illicites, de données à caractère personnel »[59]. Ce premier avis avait pour mérite d'avoir consciencieusement aligné les contours de la propriété de disponibilité des données sur les éléments de la définition des « violations de données à caractère personnel »[60] qui doivent lui être notifiées dans les cas prévus à l'article 33 du RGPD. Néanmoins, un certain flou régnait tou-

58. Une attaque par déni de service est une tentative concertée de rendre un ordinateur ou un élément de réseau indisponibles à leurs utilisateurs autorisés, que ce soit temporairement ou indéfiniment (par exemple, en utilisant de nombreux systèmes d'intrusion, qui paralysent leur cible en lançant de multiples demandes de communication externe).

59. A titre illustratif, le Groupe 29 évoquait l'hypothèse de quatre ordinateurs portables volés dans un établissement de soins contenant des données relatives à la santé de 2050 enfants. Selon le Groupe, une telle violation de la disponibilité des données pourrait avoir les conséquences et effets néfastes potentiels suivants : « Elle peut troubler la continuité du traitement des enfants, entraînant l'aggravation de la maladie ou une rechute ; elle peut entraîner un empoisonnement accidentel en raison d'une allergie à un médicament ou de médicaments incompatibles, ce qui peut causer plusieurs problèmes de santé, voire le décès ; elle peut entraîner un retard excessif dans les remboursements ou l'assistance financière accordés aux personnes concernées, ce qui aurait des retombées financières pour les familles concernées » (Groupe 29, *WP213*, *op. cit.*, p. 6).

60. RGPD, art. 4, 12).

jours quant à savoir si devaient ou non être communiquées aux personnes concernées des incidents ayants des effets disruptifs susceptibles d'entraîner des risques élevés pour celles-ci dans les cas où ces incidents n'entraînent pas de destruction ou de perte définitives de données à caractère personnel[61]. Cette interrogation ne manqua pas d'être relevée par le Groupe 29 dans les termes suivants : « Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data. The question may be asked whether a *temporary loss of availability* of personal data should be considered as a breach and, if so, one which needs to be notified »[62].

Pour cette raison, dans un avis plus récent de février 2018, le Groupe 29 révisa quelque peu le contour de la notion de « violation de la disponibilité » en la définissant comme englobant, 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[63]. Le Groupe justifia cette adaptation en considérant que « *it is well established that 'access' is fundamentally part of 'availability'* » en se basant sur une définition établie par le National Institute of Standards and Technology[64] selon laquelle la propriété de disponibilité garantit également « *timely and reliable access to and use of information* »[65]. Le Groupe s'aligne ainsi sur la définition qu'il avait utilisée dans son avis de 2012 relatif au *Cloud computing* dans lequel « assurer la disponibilité, c'est garantir un accès fiable et en temps opportun aux données à caractère personnel »[66]. Évidemment, une indisponibilité temporaire de données résultant d'une opération de maintenance programmée ne relève pas de la définition de violation de sécurité au sens de l'article 4, 12), du Règlement. Par contre, un incident illicite ou accidentel ayant pour conséquence une indisponibilité temporaire de données à caractère personnel devrait *toujours être considéré comme étant un type de violation* de sécurité dès lors qu'il est susceptible d'avoir une incidence sur les droits et libertés des personnes concernées. Par conséquent, à l'instar des autres types de violations de sécurité, une violation temporaire de disponibilité doit être documentée par le responsable du traitement, lequel doit indiquer les faits concernant l'indisponibilité temporaire des données à caractère personnel, ses effets et les mesures prises pour y remédier[67].

61. La question se posait également pour la notification de tels incidents à l'APD dans les cas précisés en application de l'article 33, § 1er, du RGPD.
62. Groupe 29, « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 », *WP250*, adoptées le 6 février 2018, p. 8.
63. *Ibid*, p. 7.
64. Le National Institute of Standards and Technology, ou NIST (qu'on pourrait traduire par « Institut national des normes et de la technologie ») est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.
65. Le Groupe 29 cite NIST SP800-53rev4 dans son *WP250, op. cit.*, p. 7.
66. Groupe 29, *WP196, op. cit.*, p. 17.
67. RGPD, art. 33, § 5.

D. Les débiteurs de l'obligation de sécurité

Sous l'empire du RGPD, l'obligation de sécurité s'applique tant aux entreprises privées qu'aux administrations publiques lorsqu'elles agissent comme « responsables du traitement » ou « sous-traitants »[68]. 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 [...] ». Quant au sous-traitant, il est « 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 ».[69]

Toutefois, pour ce qui est du respect du principe d'intégrité et de confidentialité prescrit à l'article 5, § 1er, f), du Règlement, les articles 5, § 2 et 24 prévoient que le responsable du traitement en endosse la responsabilité, tant pour tout traitement de données à caractère personnel qu'il effectue lui-même que pour ceux qui sont réalisés pour son compte[70]. Il ne peut d'ailleurs faire appel qu'à des sous-traitants qui « présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées »[71]. Qui plus est, afin de satisfaire à l'exigence d'*accountability*, le responsable du traitement doit être en mesure de démontrer que ledit principe de sécurité est respecté, en ce compris l'efficacité des mesures[72], lesquelles doivent être réexaminées et actualisées si nécessaire[73]. À ce titre, c'est également le responsable du traitement qui assume la responsabilité d'effectuer une AIPD lorsqu'une telle démarche doit être entreprise[74]. Néanmoins, « si nécessaire et sur demande », le sous-traitant doit aider le responsable du traitement, à assurer le respect des obligations découlant de la réalisation de ces AIPD[75]. A cet effet, l'article 28, § 3, f), du RGPD impose que le contrat de sous-traitance mentionne obligatoirement cette collaboration « compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ».

68. Voy. Groupe 29, « Avis 1/2010 sur les notions de 'responsable du traitement' et de 'sous-traitant' », *WP169*, adopté le 16 février 2010 ; APD, « Le point sur les notions de responsable de traitement / sous-traitant au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats », disponible à l'adresse suivante : https ://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Notions_RT_ST.pdf
69. RGPD, art. 4, 8).
70. *Ibid.*, consid.74.
71. *Ibid.*, consid. 81 et art. 28, § 1er.
72. *Ibid.*, consid. 74 et art. 24.
73. *Ibid.*, art. 24.
74. *Ibid.*, consid. 84.
75. *Ibid.*, consid. 95.

Le sous-traitant est d'autant plus impliqué puisque contrairement à l'article 17, § 1er, de la Directive 95/46/CE qui ne visait expressément que le seul responsable du traitement[76], l'article 32 du RGPD considère non seulement le responsable du traitement mais également le sous-traitant comme débiteurs de l'obligation de sécurité. Par conséquent, en cas de manquement, leur responsabilité solidaire 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[77]. Sur le plan civil, la personne lésée pourra, au choix, demander réparation du préjudice subi à l'un ou à l'autre[78], lequel pourra ensuite se retourner contre le partenaire contractuel en ce qui concerne sa part de responsabilité dans le dommage[79].

Autant dire qu'en cas de sous-traitance, des dispositions conventionnelles détaillées en matière de sécurité sont d'une importance cruciale pour assurer à l'un ou l'autre acteur la possibilité de prouver que le fait qui a provoqué le dommage lui est partiellement ou nullement imputable et ainsi être exonéré de responsabilité, en tout ou en partie. A cet égard, le contrat de sous-traitance doit notamment obligatoirement prévoir que :

- le sous-traitant aide le responsable du traitement à garantir le respect de l'obligation de sécurité de ce dernier compte tenu de la nature du traitement et des informations à la disposition du sous-traitant[80] ;
- le sous-traitant mette à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de son obligation de sécurité, 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 contribuer à ces audits[81].

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.

76. Néanmoins, relevons que l'article 17, § 2, de la directive 95/46 imposait aux Etats Membres de prévoir que le responsable du traitement « doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures ». De plus, l'article 17, § 3 exige que « la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que [...] les obligations visées au paragraphe 1, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci ». Même sous le régime de la directive 95/46, le devoir principal du responsable du traitement étant de veiller à ce que les données traitées ne le soient pas ultérieurement de manière incompatible avec les finalités déterminées initialement, il va de soi qu'en cas d'incident de sécurité impliquant une fuite de données engendrant un détournement de finalité, un sous-traitant négligeant pourrait voir sa qualification juridique réformée en responsable du traitement.

77. RGPD, art. 83, § 2, d).

78. *Ibid.*, art. 82, § 1er.

79. *Ibid.*, art. 82, § 5.

80. *Ibid.*, art. 28 § 3, f).

81. *Ibid.*, art. 28, § 3, f) et h).

E. Nature de l'obligation de sécurité

Le RGPD prévoit que responsables de traitements et sous-traitants 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 »[82] 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[83]. Ainsi que le résume C. De Terwangne, « l'exigence de sécurité est donc 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 »[84]. Par conséquent, l'obligation légale de sécurisation doit être interprétée comme étant une obligation de moyens[85] ne mettant en jeu la responsabilité de ses débiteurs que s'il est prouvé 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[86], et, d'autre part, parce que le RGPD laisse à ses débiteurs le soin d'évaluer les risques « inhérents »[87] à leurs traitements afin de choisir les mesures qu'ils considèrent 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

82. *Ibid.*, art. 32, § 1er. En ce qui concerne les 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 ». 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 », *WP248*, adoptées le 4 avril 2017, p. 7.

83. 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 ». Voy. APD, Recommandation d'initiative n° 01/2018 concernant l'analyse d'impact relative à la protection des données, 28 février 2018, p. 17.

84. 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.

85. « 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 », in 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. A l'inverse, l'obligation de notification et, le cas échéant, de communication en cas de violations de données prévues les articles 33 et 34 du RGPD doivent être analysées comme étant des obligations de résultat engageant automatiquement la responsabilité de leurs débiteurs en cas de non-respect.

86. CPVP, « Note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 8.

87. 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 probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent) ». APD, Recommandation n° 01/2018, *op. cit.*, p. 20.

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 fortement nuancée parce que l'exigence d'*accountability*[88] 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 de ses mesures de sécurité et de leur efficacité sur demande de l'autorité de contrôle[89].

La discipline d'*accountability* à laquelle sont tenus les débiteurs de l'obligation de sécurité prend corps, d'une part, avec la tenue d'un registre[90] – devant contenir, dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles – et, d'autre part, avec l'obligation du responsable du traitement d'effectuer une AIPD lorsque ses traitements sont « susceptibles d'engendrer un risque élevé »[91]. Lorsqu'une AIPD est requise, les principes de *privacy by design*[92] et de *privacy by default*[93] imposent au responsable du traitement de la réaliser avant le traitement[94], le cas échéant, avec l'aide du ou des sous-traitant(s) ayant l'obligation de lui fournir toutes les informations nécessaires[95]. Cette analyse doit notamment contenir une évaluation des risques pour les droits et libertés des personnes concernées et les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées[96]. Ces documents sont une source non négligeable d'informations utiles afin de jauger la prudence et la diligence dont doivent faire preuve les débiteurs de l'obligation de sécurité dans leur choix d'opter ou non pour l'une ou l'autre mesure de sécurité.

Cependant, il convient de rappeler si que le Registre doit être mis à disposition de l'autorité de contrôle sur demande, il n'est par contre pas destiné aux personnes concernées ni au public en général. De même, il n'y a pas d'obligation légale de publier une AIPD. C'est le responsable du traitement qui décide lui-même de la publier ou non, quand bien même

88. RGPD, art. 5, § 2, et 24.
89. *Ibid.*, art. 58, § 1, a).
90. *Ibid.*, art. 30. Cependant, il convient de rappeler que si le registre doit être mis à disposition de l'autorité de contrôle sur demande, il n'est par contre pas destiné aux personnes concernées ni au public en général.
91. RGPD, art. 35.
92. *Ibid.*, art. 25, § 1er.
93. *Ibid.*, art. 25, § 2.
94. 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, *WP248*, *op. cit.*, p. 17.
95. A cet effet, l'article 28, § 3, f), du RGPD impose que le contrat de sous-traitance mentionne obligatoirement cette collaboration « compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ».
96. RGPD, art. 35, § 7.

cette publication est encouragée par le Groupe 29[97]. Du point de vue des personnes concernées, l'obligation de sécurité de leurs débiteurs reste donc essentiellement une obligation de moyens même si les exigences documentaires susmentionnées contribueront solidement à l'évaluation des éventuels manquements par les autorités de contrôle, voire judiciaires[98].

En revanche, dans les relations entre le responsable du traitement et le sous-traitant, 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 matière de contrôle des accès physiques et logiques, de journalisation, de techniques cryptographiques spécifiques, d'interdiction du BYOD[99], etc.). Dans cette éventualité, ces obligations de résultat permettront au responsable du traitement de mettre en jeu la responsabilité du sous-traitant par la simple constatation que le résultat n'a pas été atteint, sans avoir à prouver une quelconque faute. Le sous-traitant ne pourra alors se dégager de sa responsabilité que s'il parvient à prouver l'existence d'une cause étrangère comme la survenance d'un cas de force majeure, la faute du responsable du traitement ou le fait d'un tiers.

97. « La publication peut accroître la confiance dans les opérations de traitement du responsable du traitement et donner des gages de transparence. Il est notamment de bonne pratique de publier une AIPD lorsque des citoyens sont affectés par l'opération de traitement. Tel peut en particulier être le cas lorsqu'une autorité publique réalise une AIPD. L'AIPD publiée n'a pas besoin d'inclure l'intégralité de l'analyse, notamment lorsque celle-ci pourrait donner des informations spécifiques relatives à des risques en matière de sécurité concernant le responsable du traitement ou divulguer des secrets d'affaires ou des informations commercialement sensibles. Dans pareille situation, la version publiée peut consister simplement en un résumé des principales constatations de l'AIPD, ou même uniquement en une déclaration selon laquelle une AIPD a été effectuée », 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 », *WP248*, 4 avril 2017, p. 22.
98. RGPD, art. 77.
99. 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*, adoptées le 8 juin 2017, p. 16).

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

Ainsi que le souligne le Groupe 29, l'approche fondée sur les risques (« *risk-based approach* ») n'est pas un concept nouveau[100], puisqu'il était déjà bien connu sous l'empire de la Directive[101].

Cependant, le RGPD prête davantage d'attention à cette approche puisqu'elle n'est plus seulement explicitement le pivot de l'obligation de sécurité, mais également au centre de l'exigence d'*accountability*. En effet, les deux types de contraintes – étroitement liées entre elles pour les raisons précédemment invoquées – imposent à leurs débiteurs *de pouvoir démontrer* leur prise en compte des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques[102]. Selon le Groupe 29, l'approche du RGPD fondée sur les risques a donc pour but de promouvoir une « approche évolutive et proportionnelle »[103] sans toutefois dispenser du respect des principes fondamentaux. 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[104]. Toutefois, l'obligation de sécurité étant essentiellement une obligation de moyens, cette approche implique que les débiteurs de l'obligation de sécurité doivent prendre davantage de mesures pour des traitements présentant un « risque élevé » que pour des traitements à risque faible[105].

1. La notion de risque sous le RGPD

Le considérant 4 du RGPD rappelle que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité »[106]. 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 »[107]. 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

100. Groupe 29, « Avis 5/2009 sur les réseaux sociaux en ligne », *WP163*, 12 juin 2009, p. 2.
101. « The so-called 'risk-based approach' is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Art. 17) and the DPA prior checking obligations (Art. 20). The legal regime applicable to the processing of special categories of data (Art. 8) can also be considered as the application of a risk-based approach : strengthened obligations result from processing which is considered risky for the persons concerned.», Groupe 29, *WP218*, *op.cit*, p. 2.
102. RGPD, art. 24, § 1er, et 32, § 1er.
103. En anglais : « a scalable and proportionate approach to compliance », Groupe 29, *WP218*, *op. cit*, p. 2.
104. *Ibid.*
105. APD, Recommandation n° 01/2018, *op. cit.*, p. 6.
106. RGPD, consid. 4.
107. *Ibid.*, consid. 75.

l'angle du risque pour les droits et libertés des personnes concernées afin de déterminer le niveau de sécurité approprié. Quant à 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 »[108]. 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[109].

2. Les sources des risques pour les personnes physiques

L'article 5, § 1er, f), du Règlement exige que les données soit protégées *y compris* contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle. A cet égard, le Règlement élargit quelque peu l'objet de la protection requise par l'article 17, § 1er, de la Directive, notamment par l'ajout de la locution prépositive « y compris ». Cette précaution de non-exhaustivité semble suggérer que la protection requise astreint à prévenir tout traitement effectué en violation du Règlement[110]. De manière similaire, dans le cadre de l'évaluation des risques pour la sécurité des données, « il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, *tel 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 [...] »[111]. Ainsi que nous l'avons mentionné plus haut, « selon les besoins », il peut donc être également souhaitable de prendre en compte les risques résultant d'une indisponibilité temporaire non voulue du traitement, que celle-ci soit accidentelle (par exemple, une coupure de courant) ou illicite (par exemple, suite à un DDoS).

En ce qui concerne le vocabulaire utilisé, la notion de « traitements non autorisés » couvre les circonstances dans lesquelles des données sont traitées « sans droit » par des tiers, des destinataires ou par des personnes placées sous l'autorité directe du responsable du traitement ou du sous-traitant. Les termes « de manière accidentelle ou illicite » renvoient, quant à eux, aux traitements « non autorisés » réalisés respectivement de manière purement accidentelle ou de manière intentionnelle.

La problématique des traitements non autorisés des données informatiques n'est pas neuve. En février 1990, les tribunaux belges eurent déjà à traiter du cas d'un bourgmestre ayant permis l'accès au registre national à des personnes n'appartenant pas au personnel

108. Groupe 29, *WP248*, *op. cit.*, p. 7.
109. *Ibid.*
110. RGPD, consid. 83.
111. *Ibid.*, art. 32, § 2, et consid. 83.

communal autorisé[112]. La même année, deux personnes piratèrent le serveur informatique du premier ministre de l'époque, Wilfried Martens, à l'aide d'un mot de passe détourné[113], ce qui n'avait pas manqué de mettre « la criminalité informatique dans tous ses états »[114]. Plus récemment, partout à travers le monde, des entreprises ont fait l'objet d'attaques dirigées vers les données : Myspace, Ebay, LinkedIn, Dropbox mais également, Ashley Madison, ou encore Yahoo à qui 500 millions de profils d'utilisateurs ont été volés. Criminalité et sécurité informatique sont ainsi les deux versants de la même médaille. Comme l'indique le Groupe 29, « l'intégration de la protection des données dans les cultures des organisations aidera les autorités chargées de la protection des données à mener à bien leurs missions de contrôle et de lutte contre la criminalité [...], ce qui aura pour effet d'accroître l'efficacité des mesures de protection de la vie privée »[115].

Conscient de l'enjeu, dès 2001, le Conseil de l'Europe adopta la Convention de Budapest laquelle prohibe notamment l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système, les abus de dispositifs, la falsification informatique et la fraude informatique. Chaque Partie doit adopter dans son droit interne les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales ces actes commis intentionnellement et sans droit. En Belgique, le Code pénal réprime ainsi notamment le faux informatique[116], la fraude informatique[117], le *hacking* – tant externe[118] qu'interne[119] –, le sabotage[120] ainsi que les actes non autorisés de prise de

112. Corr. Charleroi, 10e ch., 1er février 1990, *J.L.M.B.*, 1990, p. 1147.
113. Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p.11 et Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340.
114. T. VERBIEST, I. DERVAUX, « La criminalité informatique dans tous ses états », *R.D.C.*, 2002, liv. 8, p. 607-613.
115. 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. 21.
116. Code pénal, art. 210*bis*. Le faux informatique requiert une altération de la vérité par l'introduction, la modification ou l'effacement de données qui sont stockées, traitées ou transmises par un système informatique ou par la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique avec une *intention frauduleuse ou le dessein de nuire*. Comme pour le faux en écritures de droit commun, il est requis que les données manipulées aient une portée juridique. A ce sujet, voy. O. LEROUX, « Criminalité informatique », *in Les infractions contre les biens*, Bruxelles, Larcier, 2008, p. 388. Pour une étude approfondie de cette incrimination, voy. O. LEROUX, « Le faux informatique », *J.T.*, 2004, pp. 509 et s.
117. L'article 504*quater* du Code pénal incrimine celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique.
118. L'article 550*bis*, § 1er du Code pénal sanctionne celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient.
119. L'article 550*bis*, § 2 du Code pénal vise celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique.
120. L'article 550*ter* du Code pénal réprime celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique.

connaissance des communications électroniques[121] Selon l'infraction envisagée, l'élément moral requis est un dol général ou spécial[122].

Cela étant dit, tout détournement de finalité résultant d'un traitement « non autorisé » ne sera pas forcément qualifié d'infraction de criminalité informatique. Ainsi, dans un arrêt de janvier 2017, la Cour de cassation a considéré qu'une employée d'une ville belge qui disposait d'un accès illimité à l'ensemble du système informatique à des fins d'assistance technique, de maintenance et de dépannage ne commettait pas un hacking interne en accédant à certaines données à des fins totalement différentes et étrangères à ses missions, dans la mesure où la personne disposait d'un pouvoir d'accès aux données[123]. Un tel agissement doit, par contre, être considéré comme une violation du principe édicté à l'article 29 du RGPD selon lequel « le sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre ».

3. Un risque à géométrie variable

Pour ce qui est de l'évaluation des risques pour les droits et libertés des personnes physiques, 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 évènement et ses effets, estimés en termes de gravité et de probabilité »[124] 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[125].

a) La probabilité du risque

En ce qui concerne l'analyse de la première variable, il faut admettre que le texte du RGPD n'est pas des plus clairs. En effet, évaluer la probabilité d'un risque revient à l'idée de statistiquement analyser la récurrence potentielle d'un évènement possible qui n'est peut-être encore jamais intervenu. Néanmoins, dans son « *Handbook on Security of Personal Data Processing* »[126], rédigé en collaboration avec les APD hellénique et italienne,

121. Voy., notamment, les articles 314*bis* et 259*bis* du Code pénal.
122. Pour une analyse de ces infractions, lire O. LEROUX, « Section 1. – Criminalité informatique spécifique », in *Les infractions – Volume 1*, Bruxelles, Larcier, 2016, pp. 448-508.
123. Cass., 24 janvier 2017, P.16.0048.N, *T. Strafr.*, 2017/3, pp. 206-207.
124. Groupe 29, *WP248*, *op. cit*, p.7
125. 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 »).
126. ENISA, « Handbook on Security of Personal Data Processing », décembre 2017, disponible à l'adresse suivante : https ://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport.

l'ENISA 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.

b) La gravité du risque

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 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 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 évènements 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 »[127].

Le risque étant par nature un évènement dont la survenance n'est pas certaine mais qui peut potentiellement entraîner des « dommages physiques, matériels ou un préjudice moral »[128] 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.[129] 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. »[130]. Ainsi que le souligne Y. Poullet, les trois types de dommages cités ci-dessus 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

127. APD, Recommandation n° 01/2018, *op. cit.*, p. 21.
128. RGPD, consid. 75.
129. Y. POULLET, *op. cit.*, p. 20.
130. C.T. Mons (10e ch.), 16 décembre 2015, RG n°2015/AM/313 (inédit).

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 »[131].

G. L'analyse du risque

1. Objet

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 probabilité qu'un impact négatif se produise, malgré les mesures qui sont prises pour influencer (limiter) le risque (inhérent) »[132].

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 »[133]. 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) »[134].

Ainsi qu'illustrées dans les précédentes sections, la gravité et/ou la probabilité d'un risque peuvent fortement varier en fonction de la nature, de la portée, du contexte, des finalités du traitement[135] ainsi que des sources du risque. Par conséquent, le RGPD impose tant

131. Y. POULLET, *op. cit.*, p. 20.
132. APD, Recommandation n° 01/2018, *op. cit.*, p. 20.
133. 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.
134. APD, Recommandation n° 01/2018, *op. cit.*, p. 19.
135. 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 ». APD, Recommandation n° 01/2018, *op. cit.*, p. 17.

au responsable du traitement qu'au sous-traitant d'évaluer les risques inhérents afin de pouvoir déterminer le caractère « approprié » des mesures techniques et organisationnelles mises en place pour atténuer ces risques inhérents et de parvenir à un risque résiduel acceptable ou tolérable.

Méthodologiquement, l'importance de l'évaluation du risque dépendra du niveau du risque identifié. En effet, tous les traitements de données à caractère personnel ne donnent pas lieu aux mêmes risques inhérents : certains risques inhérents pouvant être qualifiés d'élevés et d'autres non.

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 AIPD pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque[136]. 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[137].

Par conséquent, quel que soit le niveau du risque identifié, lors de l'évaluation de celui-ci, l'APD estime que le responsable du traitement doit se poser les questions suivantes : quelle est l'ampleur de l'impact potentiel sur les personnes concernées et quelle est la probabilité que cet impact se produise[138] ?

Il n'est pas toujours possible de répondre de manière bien tranchée à ces questions, il s'agira souvent en pratique d'une pondération qui permettra de déterminer le niveau de risque. Cela implique en particulier d'établir, pour chaque risque, au moins les éléments suivants : les sources des risques ; les impacts potentiels sur les droits et libertés des personnes concernées, en particulier en cas d'évènements tels qu'un accès illicite aux données, une modification non désirée ou leur disparition ; les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition et la probabilité et la gravité du risque[139].

2. Méthodologie de l'évaluation des risques

Qu'une AIPD soit effectuée ou non, l'article 32 du RGPD impose aux débiteurs de l'obligation de sécurité d'évaluer les risques inhérents au traitement afin de mettre en œuvre des mesures adéquates pour les atténuer. 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[140]. Néanmoins, dans le but d'éviter qu'une situation d'insécurité juridique ne survienne, l'APD a formulé plusieurs caractéristiques minimales d'une bonne gestion des risques[141].

Outre le fait que la gestion des risques doit, entres autres, être étayée méthodologiquement[142], être adaptée sur mesure au contexte et au profil du débiteur de l'obligation de sécurité, être lisible et accessible à un public aussi large que possible, elle doit également être structurée de manière à contenir notamment :

- la définition du contexte pertinent (incluant 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) ;
- l'identification, analyse et évaluation des risques (y compris l'identification des vulnérabilités, des menaces et l'attribution d'une valeur de risque) ; et
- l'identification de mesures d'atténuation des risques appropriées (c'est-à-dire les mesures techniques, organisationnelles et juridiques qui sont nécessaires pour ramener le risque à un niveau acceptable).

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 correcte. Une description claire des critères utilisés pour évaluer le risque est quoi qu'il en soit indispensable »[143].

Selon l'APD il y a également lieu d'impliquer ceux qui sont les mieux placés pour contribuer au processus d'identification, d'analyse, d'évaluation et de gestion des risques : « [...] ce groupe comprend non seulement le délégué à la protection des données et/ou le conseiller en sécurité mais également les concepteurs de nouvelles applications, ceux qui prennent des décisions stratégiques en matière de développement de projets et les membres du personnel (ou leurs représentants) qui utiliseront les données à caractère personnel en question dans le cadre de l'exercice de leurs missions »[144].

Enfin, des mesures de gestion et de contrôle devraient être prévues : « un rapport daté et écrit des appréciations du risque effectuées doit être rédigé. Un organe interne mandaté

136. RGPD, consid. 84.
137. APD, Recommandation n° 01/2018, *op. cit.*, p. 11.
138. *Ibid.*, p. 22.
139. *Ibid.*

140. *Ibid.*, p. 23.
141. *Ibid.*, « Annexe 1 : Caractéristiques minimales d'une bonne gestion des risques », pp. 39 à 41.
142. 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.
143. APD, Recommandation n° 01/2018, *op. cit*, p. 41.
144. *Ibid.*

qui prend des décisions (par exemple : le comité de direction, le comité stratégique ou le comité de sécurité, mandaté par le conseil de direction) doit être informé périodiquement du résultat (ou du statut) du processus d'appréciation du risque. Cet organe mandaté doit approuver formellement l'évaluation des risques ainsi que les mesures visant à atténuer les risques. Le processus d'appréciation du risque ne peut toutefois pas être réduit à un simple processus bureaucratique. Le responsable du traitement doit prendre des mesures adéquates afin de veiller à ce que la bonne gestion des risques fasse partie de la « culture d'entreprise » du responsable du traitement.

Une appréciation du risque qui a été effectuée doit être contrôlée périodiquement et au moins en cas de circonstances changeantes pouvant avoir une influence essentielle sur une appréciation qui a été réalisée dans le passé. La fréquence de la vérification périodique doit être déterminée en fonction du risque présenté par l'opération de traitement. En outre, l'APD recommande également que le résultat du contrôle soit officiellement soumis à l'approbation de la plus haute autorité au sein de l'organisation du responsable du traitement[145].

3. L'obligation d'effectuer une AIPD en cas de risque élevé

Sous le régime du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une AIPD doit être effectuée « *avant le traitement* »[146]. Cette exigence est cohérente avec les principes de protection des données dès la conception et de protection des données par défaut[147].

Le paragraphe 3 de l'article 35 précise qu'une AIPD est, *en particulier,* requise dans les cas suivants :

- 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[148] ;
- le traitement à grande échelle de catégories particulières de données visées à l'article 9, § 1er ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ou

145. *Ibid.*

146. RGPD, art. 35, §§ 1 et 10 et consid. 90 et 93. À moins qu'il s'agisse d'un traitement déjà existant ayant préalablement fait l'objet d'un examen par l'autorité de contrôle, auquel cas l'AIPD sera effectuée avant toute mise en œuvre de modifications significatives.

147. RGPD, art. 25 et consid. 78.

148. L'article 35, § 3, a), du RGPD évoque des « décisions » produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Il est important de faire remarquer qu'il n'est pas requis qu'il s'agisse d'une prise de décision « entièrement automatisée » au sens de l'article 22 du RGPD. Dès lors, l'article 35, § 3, a), du RGPD s'applique aussi lorsque la prise de décision en question ne se base pas exclusivement sur un traitement automatisé

- la surveillance systématique[149] à grande échelle d'une zone accessible au public[150].

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 néanmoins présenter un risque inhérent aussi élevé[151].

4. La notion de risque élevé

La notion de « risque élevé » bourgeonnait déjà dans la Directive. En effet, l'article 20, § 1er de celle-ci prévoyait que les États membres devaient préciser les traitements susceptibles de présenter des « risques particuliers » au regard des droits et libertés des personnes concernées et veiller à ce que ces traitements soient examinés *avant* leur mise en œuvre. Le considérant 53 précisait que ces « risques particuliers » pouvaient découler « du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle ». Pour de tels traitements à « risque particulier », les États membres devaient prévoir un examen préalable à leur mise en œuvre[152].

La notion de « risque élevé » n'est pas définie en détail dans le RGPD[153]. Consciente du fait que des organisations différentes utilisent des échelles et des méthodes différentes lorsqu'elles procèdent à une évaluation des risques, l'APD estime « qu'il est dès lors possible que l'interprétation de ces valeurs diffère selon l'échelle de risque et la méthode utilisées »[154]. Toutefois, 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,

149. Le RGPD ne définit pas ce que l'on entend par la notion de « systématique ». D'après le Groupe 29, cette notion doit être interprétée selon une ou plusieurs des manières qui suivent : une chose qui se déroule selon un système ; qui est préparée, organisée ou méthodique ; qui se déroule dans le cadre d'un plan général de collecte de données ; qui est réalisée dans le cadre d'une stratégie.

150. Une « zone accessible au public » est un lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple (CPVP, Recommandation n° 01/2018, *op. cit.*, p. 13).

151. Groupe 29, *WP 248*, *op. cit.*, p. 10.

152. Directive 95/46, consid. 54.

153. La notion de « risque élevé » au sens du RGPD ne correspond toutefois pas nécessairement à la notion de « risque élevé » telle qu'on la retrouve dans d'autres modèles de gestion des risques puisque le RGPD vise à protéger les risques pour les droits et libertés des personnes physiques.

154. APD, Recommandation n° 01/2018, *op. cit.*, p. 8

la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux »[155].

Sous le régime du RGPD, afin de déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque élevé, les lignes directrices élaborées par le Groupe 29 sont particulièrement importantes[156]. 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. Avant la publication de cette liste, chaque Autorité est tenue de communiquer celle-ci au Comité européen de la protection des données (ci-après « EDPB » pour *European Data Protection Board*) afin qu'il puisse rendre un avis. En Belgique, dans l'attente de la mise en place de l'APD, la CPVP a adopté une Recommandation relative aux AIPD à laquelle était notamment annexé un projet de liste des opérations de traitements impliquant obligatoirement la réalisation d'une AIPD[157]. L'APD a ensuite tenu compte de l'avis de l'EDPB[158] impliquant des modifications au projet de liste adoptée par la CPVP et ensuite ratifié par l'APD[159].

Ainsi, sont considérés comme susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques et donc nécessitant la conduite d'une AIPD, les catégories de traitements suivants :

1) lorsque le traitement utilise des données biométriques[160] en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public ;

2) lorsque des données à caractère personnel sont collectées auprès de tiers afin d'être prises ensuite en considération dans le cadre de la décision de refuser ou de cesser un contrat de service déterminé avec une personne physique ;

155. *Ibid.*
156. Groupe 29, *WP248*, *op. cit.*
157. APD, Recommandation n° 01/2018, *op. cit.*
158. EDPB, « *Opinion 2/2018 on the draft list of the competent supervisory authority of Belgium regarding the processing operations subject to the requirement of a data protection impact assessment* (GDPR, art. 35.4) », adoptées le 25 septembre 2018.
159. 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) », adoptée le 16 janvier 2019.
160. L'article 4, 14), du RGPD définit les « données biométriques » comme étant les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

3) lorsque des données de santé d'une personne concernée sont collectées par voie automatisée à l'aide d'un dispositif médical implantable actif[161] ;

4) lorsque des données sont collectées à grande échelle auprès de tiers afin d'analyser ou de prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

5) lorsque des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD[162] ou des données de nature très personnelle (comme des données sur la pauvreté, le chômage, l'implication de l'aide à la jeunesse ou le travail social, des données sur les activités domestiques et privées, des données de localisation) sont échangées systématiquement entre plusieurs responsables du traitement ;

6) lorsqu'il est question d'un traitement à grande échelle de données générées au moyen d'appareils dotés de capteurs qui envoient des données via Internet ou via un autre moyen (applications de « l'Internet des objets », comme les télévisions intelligentes, les appareils ménagers intelligents, les jouets connectés, les « smart cities », les compteurs d'énergie intelligents, etc.) et que ce traitement sert à analyser ou prédire la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements de personnes physiques ;

7) lorsqu'il est question d'un traitement à grande échelle et/ou systématique de données de téléphonie, d'Internet ou d'autres données de communication, de métadonnées ou de données de localisation de personnes physiques ou permettant de mener à des personnes physiques (par exemple le wifi-tracking ou le traitement de données de localisation de voyageurs dans les transports publics) lorsque le traitement n'est pas strictement nécessaire pour un service demandé par la personne concernée ;

8) lorsqu'il est question de traitements de données à caractère personnel à grande échelle où le comportement[163] de personnes physiques est observé, collecté, établi ou influencé, y compris à des fins publicitaires, et ce de manière systématique via un traitement automatisé.

Attirons l'attention sur le fait que cette liste est évolutive et peut être adaptée s'il s'avère qu'elle n'atteint pas son objectif. En effet, l'article 10 du Règlement d'ordre intérieur de l'APD prévoit que « cette liste est actualisée tous les six mois, en fonction notamment de

161. Il s'agit de tout dispositif médical actif qui est conçu pour être implanté en totalité ou en partie dans le corps humain ou, dans un orifice naturel et qui est destiné à rester après l'intervention.
162. Les catégories particulières de données incluent en particulier, conformément à l'article 9 du RGPD, les donnée à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuse ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle d'une personne physique.
163. Par exemple : le comportement de visionnage, d'écoute, de navigation, de clic, physique ou d'achat.

l'évolution des nouvelles technologies ». De plus, l'APD souligne que l'existence d'une liste des opérations de traitement pour lesquelles une AIPD est requise ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques. En outre, la liste susmentionnée n'est absolument pas exhaustive : une AIPD est toujours requise dès lors que les conditions d'application définies à l'article 35, § 1er, du RGPD sont remplies.

Dans ce contexte, il est également recommandé aux responsables du traitement de se référer aux critères énumérés dans les lignes directrices du Groupe 29[164], chaque liste nationale venant compléter et les préciser davantage. Dans la plupart des cas, le responsable du traitement pourrait considérer qu'un traitement satisfaisant à deux des neuf critères identifiés par le Groupe 29 nécessite une AIPD[165]. D'une manière générale, le Groupe estime que plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD. Néanmoins, dans certains cas, le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD. À l'inverse, une opération de traitement peut correspondre à l'un des critères et être néanmoins considérée par le responsable du traitement comme non « susceptible d'engendrer un risque élevé ». Dans pareil cas, il convient que le responsable du traitement explique et documente les motifs de sa décision de ne pas procéder à une AIPD en incluant/rapportant par ailleurs l'opinion à cet égard du délégué à la protection des données. Dans ses lignes directrices, le Groupe 29 cite des exemples qui illustrent la façon dont il convient d'utiliser les critères pour déterminer si une opération de traitement considérée nécessite une AIPD[166].

H. Les traitements non soumis à l'obligation d'AIPD

Avant tout, rappelons qu'une analyse des risques inhérents doit être réalisée qu'il y ait ou non une obligation (ou une forte recommandation) 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. Cela étant dit, l'article 35, § 5, du RGPD prévoit que l'autorité de contrôle peut établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle doit communiquer cette liste à l'EDPB.

164. Groupe 29, *WP248*, *op. cit.*
165. *Ibid.*, p. 13.
166. *Ibid.*, pp. 13 à 14.

1. Les critères énumérés par le Groupe 29

Dans ses lignes directrices, le Groupe 29 considère qu'une AIPD n'est pas nécessaire :

- lorsque le traitement n'est pas « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[167] ;
- lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'une AIPD. Dans un tel cas, les résultats de l'AIPD réalisée pour le traitement similaire peuvent être utilisés[168] ;
- lorsque le traitement a fait l'objet d'un examen mené par une autorité de contrôle avant mai 2018 dans des conditions spécifiques qui n'ont pas changé[169] ;
- lorsque le traitement a pour fondement de licéité le respect d'une obligation légale[170] ou l'exécution d'une mission d'intérêt public[171] et qu'il a une base juridique dans le droit de l'Union ou dans le droit de l'État membre, que ce droit réglemente l'opération de traitement spécifique et qu'une AIPD a déjà été réalisée dans le cadre de l'établissement de la base juridique en question[172], à moins qu'un État membre n'estime qu'il est nécessaire de procéder à une telle analyse avant les activités de traitement. À cet égard, en Belgique, l'article 23 de la loi du 30 juillet 2018[173] précise que dans le secteur public, « une analyse d'impact spécifique de protection des données est effec-

167. RGPD, art. 35, § 1er.
168. Article 35, § 1er, du RGPD selon lequel « une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».
169. Aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, selon le considérant 171, « Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées ». À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en œuvre (portée, finalités, données à caractère personnel collectées, identité des responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'examen préalable effectué par l'autorité de contrôle ou le détaché à la protection des données et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD.
170. RGPD, art. 6, § 1er, c).
171. *Ibid.*, art. 6, § 1er, e).
172. *Ibid.*, art. 35, § 10. Dans le cas d'une AIPD réalisée au stade de l'élaboration d'une législation conférant une base juridique à un traitement, un réexamen pourrait malgré tout être nécessaire avant le lancement des opérations. En effet, la législation adoptée est susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il est possible que les détails techniques disponibles en ce qui concerne le traitement effectif soient insuffisants au moment de l'adoption de la législation, même si une AIPD a été effectuée. Dans de tels cas, il pourrait s'avérer nécessaire d'effectuer une AIPD spécifique avant d'exécuter les activités de traitement proprement dites.
173. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

tuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale » ;

– lorsque le traitement figure dans la liste facultative (établie par l'autorité de contrôle) des opérations de traitement qui ne requièrent pas d'AIPD[174]. Cette liste peut recenser les activités de traitement conformes aux conditions fixées par l'autorité en question, en particulier par l'intermédiaire de lignes directrices, de décisions ou autorisations spécifiques, de règles de conformité, etc. Dans pareil cas et sous réserve d'une réévaluation par l'autorité de contrôle compétente, il n'est pas nécessaire d'effectuer une AIPD, à la condition exclusive, toutefois, que le traitement relève strictement du champ d'application de la procédure pertinente indiquée dans la liste et continue de satisfaire pleinement à toutes les exigences applicables du RGPD.

2. Projet de liste de l'APD de traitements non soumis à l'AIPD

Ainsi que nous l'avons mentionné, l'article 35, § 5, du RGPD autorise l'autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD n'est pas requise[175]. Par conséquent, dans l'annexe 3 de ses recommandations[176], l'APD estime que pour les types de traitement suivants, une AIPD n'est pas nécessaire :

1) les traitements réalisés par des entités privées qui sont nécessaires pour répondre à une obligation légale qui leur incombe, moyennant une définition par la loi des finalités du traitement, des catégories de données à caractère personnel traitées et des garanties destinées à prévenir les abus ou l'accès ou le transfert illicite ;

2) les traitements de données à caractère personnel qui concernent uniquement des données qui sont nécessaires à l'administration des salaires de personnes en service ou actives pour le compte du responsable du traitement lorsque les données sont exclusivement utilisées pour cette administration des salaires, sont uniquement communiquées aux destinataires qui sont autorisés à cet effet et ne sont pas conservées plus longtemps que le temps nécessaire aux finalités du traitement ;

3) les traitements de données à caractère personnel qui concernent exclusivement l'administration du personnel en service ou actif pour le compte du responsable du traitement, dans la mesure où ce traitement ne porte pas sur des données relatives à la santé de la personne concernée, ni sur des catégories particulières de données au sens de l'article 9 du RGPD, ni sur des condamnations pénales et des infractions au sens de l'article 10 du RGPD ou sur des données ayant pour but une évaluation de la personne concernée et où les données à caractère personnel traitées ne sont pas conservées plus longtemps que le temps nécessaire à l'administration du personnel et uniquement dans le cadre de l'application d'une disposition légale ou réglementaire ou sont communiquées si nécessaire à des tiers pour la réalisation des finalités du traitement ;

4) les traitements de données à caractère personnel qui concernent exclusivement la comptabilité du responsable du traitement lorsque les données sont exclusivement utilisées pour cette comptabilité, lorsque le traitement concerne uniquement les personnes dont les données sont nécessaires pour la comptabilité et lorsque les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire à la réalisation des finalités du traitement et que les données à caractère personnel traitées sont uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ou lorsque la communication est nécessaire pour la comptabilité ;

5) les traitements de données à caractère personnel qui concernent exclusivement l'administration des actionnaires et associés lorsque le traitement porte uniquement sur des données nécessaires à cette administration, lorsque ces données concernent uniquement des personnes dont les données sont nécessaires à cette administration, lorsque les données sont communiquées à des tiers uniquement dans le cadre de l'application d'une disposition légale ou réglementaire et que les données à caractère personnel ne sont pas conservées plus longtemps que le temps nécessaire à la réalisation des finalités du traitement ;

6) les traitements de données à caractère personnel effectués par une fondation, association ou toute autre institution sans but lucratif dans le cadre de ses activités habituelles, pour autant que le traitement porte uniquement sur des données à caractère personnel relatives à ses propres membres, relatives aux personnes avec lesquelles le responsable du traitement entretient des contacts réguliers et relatives aux bénéficiaires de la fondation, association ou institution et qu'aucune personne ne soit enregistrée sur la base de données obtenue de tiers et que les données à caractère personnel traitées ne soient pas conservées plus longtemps que le temps nécessaire à l'administration des membres, des personnes de contact et des bénéficiaires et soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire ;

7) les traitements de données à caractère personnel qui concernent exclusivement l'enregistrement de visiteurs dans le cadre d'un contrôle d'accès lorsque les données traitées restent limitées au nom et à l'adresse professionnelle du visiteur, à l'identification de son employeur, à l'identification du véhicule du visiteur, au nom, à la section et à la fonction de la personne visitée et au moment de la visite et où les données à caractère

174. RGPD, art. 35, § 5.

175. L'APD souligne que la liste susmentionnée ne porte en rien préjudice à l'obligation générale du responsable du traitement de procéder à une bonne appréciation du risque et à une bonne gestion des risques, conformément à l'article 24, § 1er, du RGPD. Cette obligation générale d'appréciation du risque et de gestion des risques s'applique sans préjudice de l'existence d'une liste de traitements spéciaux pour lesquels une AIPD n'est pas requise en tant que telle. Enfin, l'APD attire encore l'attention sur le fait que ces listes sont évolutives et peuvent être adaptées s'il s'avère qu'elles n'atteignent pas leur objectif.

176. APD, Recommandation 01/2018, *op. cit*, annexe 3.

personnel traitées peuvent exclusivement être utilisées pour le contrôle d'accès et ne pas être conservées plus longtemps que le temps nécessaire à cette finalité ;

8) les traitements de données à caractère personnel effectués par des établissements d'enseignement en vue de la gestion de leurs relations avec leurs élèves ou étudiants dans le cadre de leurs missions d'enseignement, dans la mesure où le traitement ne porte que sur des données à caractère personnel relatives à des élèves ou étudiants potentiels, actuels et anciens de l'établissement d'enseignement en question et qu'aucune personne ne soit enregistrée sur la base de données obtenue de tiers et que ces données soient uniquement communiquées à des tiers dans le cadre de l'application d'une disposition légale ou réglementaire et ne soient pas conservées plus longtemps que le temps nécessaire à la gestion de la relation avec l'élève ou l'étudiant ;

9) les traitements de données à caractère personnel qui concernent exclusivement la gestion de la clientèle ou des fournisseurs du responsable du traitement, pour autant que le traitement concerne uniquement des clients ou fournisseurs existants et anciens du responsable du traitement et que le traitement ne concerne pas des catégories particulières de données au sens de l'article 9 du RGPD, ni des condamnations pénales et des infractions visées à l'article 10 du RGPD et qu'en ce qui concerne l'administration de la clientèle, aucune donnée provenant de tiers ne soit enregistrée et que les données à caractère personnel traitées ne soient pas conservées pour une durée excédant celle nécessaire à la gestion normale de l'entreprise du responsable du traitement et ces données ne peuvent être transmises à des tiers que dans le cadre de l'application d'une disposition légale ou réglementaire ou pour la gestion normale de l'entreprise.

I. L'analyse d'impact relative à la protection des données

1. Objet

Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe d'*accountability*, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au Règlement. Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve[177].

177. Notre section relative à l'analyse d'impact est fortement basée sur le document du Groupe 29 (*WP248*, *op. cit.*) et sur la Recommandation de l'APD (Recommandation n° 01/2018, *op. cit.*).

L'AIPD doit être lancée le plus tôt possible dans le cycle de conception du traitement, même si certaines opérations de traitement sont encore inconnues. La mise à jour de l'AIPD tout au long du projet assurera la prise en compte des questions liées à la protection des données et de la vie privée et encouragera la création de solutions favorisant la conformité. Il peut également être nécessaire de répéter les différentes étapes de l'évaluation au fur et à mesure de l'avancée du processus de développement étant donné que le choix de certaines mesures techniques ou organisationnelles peut modifier la gravité ou la probabilité des risques associés au traitement[178]. Le fait que l'AIPD puisse devoir être actualisée après le lancement effectif du traitement n'est pas une raison valable pour la différer ou pour ne pas l'effectuer. Une telle analyse est un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements[179]. De plus, l'obligation d'effectuer une AIPD s'applique aux opérations de traitement *existantes* susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement[180].

En outre, le simple fait que les conditions déclenchant l'obligation d'effectuer une AIPD – décrites plus haut – ne soient pas remplies ne restreint toutefois pas l'exigence générale faite aux débiteurs de l'obligation de sécurité d'évaluer les risques afin de mettre en œuvre des mesures appropriées. Enfin, cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[181]. En cas de doute quant à la nécessité d'effectuer une AIPD, dans la mesure où les AIPD sont un outil important pour les responsables du traitement aux fins du respect de la législation sur la protection des données, le Groupe 29 recommande d'en effectuer une malgré tout[182].

2. Étendue de l'AIPD

Une AIPD peut concerner une opération de traitement de données unique. Cependant, l'article 35, § 1er dispose qu'« une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ». Le considérant 92 ajoute qu'« il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un

178. Groupe 29, *WP248*, *op. cit.*, p. 17.
179. *Ibid.*
180. *Ibid.*, p. 16.
181. *Ibid.*, p. 7.
182. *Ibid.*, p. 9.

environnement de traitement commun à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée ».

Une seule et même AIPD peut donc être utilisée pour évaluer plusieurs opérations de traitement similaires en termes de nature, de portée, de contexte, de finalités et de risques. En effet, « les AIPD visent à assurer l'étude systématique des nouvelles situations susceptibles d'entraîner des risques élevés pour les droits et libertés des personnes physiques, et il n'est pas nécessaire de procéder à une AIPD dans les cas (à savoir des opérations de traitement effectuées dans un contexte spécifique et à des fins spécifiques) qui ont déjà été étudiés. Tel peut être le cas lorsque des technologies similaires sont utilisées pour collecter le même type de données pour les mêmes finalités. Par exemple, un groupe d'autorités municipales mettant chacune en place un système similaire de surveillance par CCTV pourrait se contenter d'une AIPD unique couvrant le traitement envisagé par chacun de ces responsables distincts ; un opérateur ferroviaire (un seul responsable du traitement) pourrait quant à lui couvrir la vidéosurveillance de l'ensemble de ses gares au moyen d'une seule et même AIPD. Ceci peut également valoir pour des opérations de traitement similaires mises en œuvre par différents responsables du traitement. Dans pareils cas, il y a lieu qu'une AIPD de référence soit partagée ou rendue publiquement accessible, les mesures décrites dans l'AIPD doivent être mises en œuvre et une justification de la réalisation d'une AIPD unique doit être fournie. Lorsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives. Il convient que leur AIPD détermine quelle partie est responsable des différentes mesures destinées à faire face aux risques et à protéger les droits et libertés des personnes concernées, et que chaque responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par ex.) et à ne pas divulguer de vulnérabilités publiquement »[183].

Une AIPD peut également être utile « pour évaluer l'impact sur la protection des données d'un produit technologique, par exemple un matériel ou un logiciel, lorsque celui-ci est susceptible d'être utilisé par divers responsables du traitement pour réaliser différentes opérations de traitement. Bien entendu, le responsable du traitement déployant le produit reste tenu d'effectuer sa propre AIPD pour ce qui concerne sa mise en œuvre spécifique, mais il peut s'appuyer pour cela sur une AIPD élaborée par le fournisseur du produit, le cas échéant. Prenons l'exemple de la relation entre fabricants de compteurs intelligents et entreprises de services publics. Il conviendrait que chaque fournisseur ou sous-traitant partage les informations utiles en s'assurant de ne compromettre aucun secret ni de menacer la sécurité en divulguant des vulnérabilités »[184].

183. *Ibid.*
184. *Ibid.*

3. Rôles des différents acteurs lors de l'exécution de l'AIPD

a) Le responsable du traitement

L'obligation de procéder à une AIPD incombe en premier lieu au responsable du traitement. Il est celui qui en endosse la responsabilité finale et doit rendre compte si l'AIPD n'est pas (ou pas correctement) réalisée lorsque celle-ci est bel et bien obligatoire en vertu de l'article 35 du RGPD. L'AIPD peut être réalisée par quelqu'un d'autre, à l'intérieur ou à l'extérieur de l'organisation, mais le responsable du traitement reste responsable en dernier ressort de cette tâche[185].

L'APD estime indispensable que le responsable du traitement veille à ce que les bonnes personnes au sein de l'entreprise soient impliquées dans le processus d'évaluation des risques[186]. Il est recommandé de documenter expressément la tâche et le rôle de chacune de ces personnes lors de la réalisation (de parties) d'une AIPD[187] en tenant compte de la politique, des processus et des règles internes[188].

b) Le sous-traitant

Le sous-traitant doit, en fonction de la nature du traitement, assister le responsable du traitement dans l'exécution d'une AIPD. Dans les précédentes versions du projet du RGPD, il était même explicitement prévu que l'obligation de procéder à une AIPD en tant que telle reposerait également directement sur le sous-traitant. Dans la version finale du RGPD, il est toutefois précisé que le contrat entre le responsable du traitement et le sous-traitant doit établir que le sous-traitant « aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant »[189]. Le considérant 95 du RGPD confirme que le sous-traitant doit aider le responsable du traitement, « si néces-

185. *Ibid.*, p. 18.
186. Selon l'APD, « Afin d'éviter que le processus d'évaluation des risques soit ramené à un pur exercice écrit, ceux qui sont les mieux placés pour contribuer à une évaluation des risques de qualité doivent être impliqués en temps opportun dans le processus d'identification, d'évaluation et de gestion des risques. La Commission pense ici en premier lieu non seulement au délégué à la protection des données et/ou au conseiller en sécurité, mais aussi aux concepteurs de nouvelles applications (par exemple des architectes ICT), aux analystes, aux juristes d'entreprises, aux personnes qui prennent des décisions stratégiques en matière de développement de projets, aux responsables de la sous-traitance, aux responsables de la gestion du personnel, aux membres du personnel (ou à leurs représentants) qui utiliseront les données à caractère personnel en question dans l'exercice de leurs tâches, etc. ». APD, Recommandation 01/2018, *op. cit*, pp. 27 et 28.
187. Pour un exemple de présentation de cette répartition, l'APD (Recommandation 01/2018, *op. cit*, p. 28) renvoie au document « Privacy Impact Assessment (PIA) – Methodology (how to carry out a PIA) » de 2015 (et plus spécifiquement à sa p. 9) de la Commission Nationale de l'Informatique et des Libertés française (la CNIL).
188. L'APD illustre une telle division des rôles aux pages 28 et 29 de sa Recommandation 01/2018, *op. cit.*
189. RGPD, art. 28, § 3, f).

saire et sur demande », à assurer le respect des obligations découlant de la réalisation d'une AIPD[190].

c) Le délégué à la protection des données

Lorsqu'un délégué à la protection des données (ci-après « DPD ») a été désigné, celui-ci a pour mission de conseiller le responsable du traitement dans l'exécution d'une AIPD[191]. Toutefois, le but n'est pas que le DPD rédige seul l'intégralité d'une AIPD[192]. Son rôle purement consultatif –et non décisionnel[193]– devrait porter sur les aspects suivants :

- faut-il effectuer ou non une AIPD ?
- quelle méthodologie faut-il suivre lors de la réalisation d'une AIPD ?
- l'AIPD doit-elle être effectuée en interne ou être externalisée ?
- quelles garanties (dont les mesures techniques et organisationnelles) doivent être appliquées afin d'atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ?
- la question de savoir si l'AIPD a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD[194].

Si le responsable du traitement n'est pas d'accord avec l'avis rendu par le délégué à la protection des données, il doit motiver spécifiquement et par écrit dans la documentation de l'AIPD les raisons pour lesquelles il n'a pas été tenu compte de cet avis[195].

d) Les personnes concernées ou leurs représentants

L'article 35, § 9 du RGPD dispose que « *le cas échéant*, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement

190. Selon l'APD, « Compte tenu des dispositions précitées, l'ampleur de l'obligation d'assistance du sous-traitant doit être déterminée à la lumière (1) de la nature du traitement ; (2) des informations mises à disposition du sous-traitant ; (3) de l'opportunité de l'aide du sous-traitant afin de parvenir à une analyse et à une gestion des risques correctes et de qualité ». APD, Recommandation 01/2018, *op. cit.*, p. 29.
191. RGPD, art. 35, § 2.
192. C'est ce qui ressort notamment de l'article 39, § 1er, c), du RGPD qui dispose que le délégué à la protection des données dispense des conseils, sur demande, en ce qui concerne l'AIPD et vérifie son exécution.
193. Toute autre interprétation pourrait en outre donner lieu à un conflit d'intérêts. « Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel », Groupe 29, « Lignes directrices concernant les délégués à la protection des données », *WP243*, 5 avril 2017, p. 20.
194. *Ibid.*
195. *Ibid.* Le Groupe 29 conseille par ailleurs que le responsable du traitement fixe clairement, par exemple dans le contrat du délégué à la protection des données, mais aussi dans les informations fournies aux travailleurs, au management (et à d'autres personnes concernées, au besoin), les tâches précises du délégué à la protection des données et leur ampleur, notamment en ce qui concerne la réalisation d'une analyse d'impact relative à la protection des données.

prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement »[196].

Par conséquent, l'APD belge « estime que l'idée derrière la formulation choisie est univoque, plus précisément que la décision de procéder ou non à la consultation des personnes concernées (ou de leurs représentants) revient en premier lieu au responsable du traitement. Il n'est toutefois pas entièrement facultatif pour le responsable du traitement de consulter ou non les personnes concernées ou leurs représentants. Là où il existe suffisamment de motifs importants de procéder à une telle consultation, compte tenu de la nature, du contexte, de la portée et de la finalité du traitement, ainsi que de l'impact potentiel sur les personnes concernées, il est nécessaire qu'une telle consultation ait effectivement lieu. Une consultation des personnes concernées est en particulier recommandée lorsqu'elles disposent d'informations essentielles ou qu'elles peuvent formuler des remarques importantes qui sont pertinentes pour la réalisation de l'AIPD. Si le responsable du traitement juge qu'il n'est pas approprié de demander l'avis des personnes concernées, par exemple parce que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable, il doit documenter sa motivation de ne pas s'enquérir de l'avis des personnes concernées »[197].

Selon l'APD, la consultation de personnes concernées ou de leurs représentants peut présenter une plus-value importante, tant lors de l'identification et de l'évaluation des risques du traitement que lors de la finalisation d'une AIPD, afin de vérifier si tous les risques ont été suffisamment cernés. L'ampleur de la consultation (quelles personnes ainsi que leur nombre) sera déterminée de préférence en fonction du risque et de l'ampleur du traitement. Si un traitement envisagé n'entraîne des risques que pour un nombre limité de personnes concernées (par exemple les travailleurs d'une petite organisation), la consultation peut se limiter à un nombre restreint de ces travailleurs et/ou de leurs représentants. Si le traitement envisagé implique des risques pour un grand nombre de personnes concernées (par exemple tous les habitants), il convient alors d'organiser une consultation plus large[198].

Le responsable du traitement décide en principe librement de la manière dont les personnes concernées ou leurs représentants sont consultés. Leur avis peut, selon le contexte, être recueilli de différentes manières (par exemple : une étude générique relative aux finalités et aux moyens du traitement, une question adressée aux représentants du personnel ou des enquêtes habituelles qui sont envoyées aux futurs clients du responsable du traitement)[199].

196. L'APD fait remarquer que la lecture séparée des versions anglaise, française et néerlandaise de l'article 35, § 9, du RGPD pourrait donner lieu à des interprétations divergentes : « Là où la version néerlandaise indique que la consultation des personnes concernées ou de leurs représentants doit se faire 'in voorkomend geval', le texte anglais indique qu'une telle consultation doit se faire 'where appropriate'. Le texte français indique quant à lui 'le cas échéant' ». APD, Recommandation 01/2018, *op. cit*, p. 31.
197. *Ibid.* Voy. également Groupe 29, *WP248*, *op.cit*, pp. 18 et 19.
198. APD, Recommandation 01/2018, *op .cit*, p. 32.
199. *Ibid.* Voy. également Groupe 29, *WP248*, *op. cit.*, p. 18.

Si la décision finale du responsable du traitement diffère de l'avis des personnes concernées, il y a lieu qu'il documente les raisons de sa décision de persévérer ou non[200].

4. Éléments essentiels d'une AIPD

a) Aperçu

L'article 35, § 7, du RGPD prévoit qu'une AIPD doit au moins contenir les éléments suivants :

1) *une description systématique des opérations de traitement envisagées et des finalités du traitement*, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
2) une *évaluation de la nécessité et de la proportionnalité* des opérations de traitement au regard des finalités ;
3) une *évaluation des risques* pour les droits et libertés des personnes concernées et
4) *les mesures envisagées pour faire face aux risques*, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

b) Description des opérations de traitement envisagées

L'article 35, § 7, du RGPD exige en premier lieu que l'AIPD contienne une description systématique des opérations de traitement envisagées et des finalités du traitement. Il est important que l'on tienne compte à cet égard de la nature, de la portée, du contexte, des finalités du traitement ainsi que des sources des risques[201]. Par conséquent, le Groupe 29 considère que la description des traitements doit comporter au moins les éléments suivants :

- une description claire du traitement, y compris d'éventuels processus d'entreprise et exigences du système ;
- les données à caractère personnel, les destinataires et la durée pendant laquelle les données à caractère personnel seront enregistrées ;
- les actifs sur lesquels reposent les données à caractère personnel (par exemple matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier)[202].

c) Contrôle de la nécessité et de la proportionnalité

Une AIPD doit comporter une évaluation de la *nécessité et de la proportionnalité* des opérations de traitement au regard des finalités. Le responsable du traitement doit dès lors justifier explicitement, d'une part, pour quelle(s) raison(s) le traitement de données à caractère personnel est nécessaire et, d'autre part, pour quelle(s) raison(s) chacun des traitements visés est nécessaire pour atteindre la (les) finalité(s) poursuivie(s).

Lors de l'évaluation de la nécessité, si plusieurs traitements ou moyens de traitement sont utilisés pour atteindre la (les) finalité(s), le responsable du traitement doit en principe choisir les moyens de traitement qui sont les moins intrusifs. Le responsable du traitement a alors intérêt à bien documenter la (les) raison(s) pour laquelle (lesquelles) les moyens de traitement choisis sont moins intrusifs que les alternatives[203].

Lors de l'évaluation de la proportionnalité, le responsable du traitement doit également examiner la *pertinence* du traitement envisagé. En somme il s'agit de répondre à la question « peut-on raisonnablement espérer que le traitement envisagé atteindra sa finalité (légitime) » ? Enfin, le responsable du traitement doit aussi veiller à maintenir un équilibre adéquat entre les intérêts pertinents[204].

Par conséquent, lors de l'évaluation de la nécessité et de la proportionnalité du traitement envisagé, il faut tenir compte au moins des éléments suivants :

- la (les) finalité(s) spécifiée(s), explicite(s) et légitime(s) du traitement envisagé ;
- le fondement juridique sur lequel se base le traitement de données[205] ;
- une justification du fait que les données à caractère personnel traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire[206] ;
- une justification du délai de conservation envisagé des données à caractère personnel, qui ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[207] ;
- une justification du fait que les intérêts de la personne concernée ne prévalent pas sur les intérêts légitimes du responsable du traitement ou d'éventuels tiers.

En outre, il est également recommandé que le responsable du traitement propose un relevé de toutes les mesures techniques et organisationnelles prises pour remplir les obligations de sécurité. En effet, au moment de l'exécution de l'AIPD, le responsable du traitement qui la réalise aura peut-être déjà pris plusieurs mesures pour respecter ses obligations. Ces mesures existantes peuvent avoir une influence sur l'évaluation des

200. RGPD, art. 35, § 2. Voy. également Groupe 29, *WP248*, *op. cit.*, p. 17.
201. Voir également le considérant 90 du RGPD.
202. Groupe 29, *WP 248*, *op. cit.*, p. 28.
203. APD, Recommandation 01/2018, *op. cit*, p. 17.
204. L'évaluation de l'équilibre d'intérêts à ce stade de l'AIPD ne sera généralement que provisoire, étant donné qu'elle ne tient pas encore compte des mesures de protection visées (Groupe 29, *WP248*, *op. cit*, p. 28).
205. RGPD, art. 6. En principe, une opération de traitement qui ne poursuit qu'une seule finalité ne peut être justifiée qu'à l'aide d'un seul des fondements juridiques repris à l'article 6 du RGPD. « Il est toutefois possible qu'un même traitement poursuive plusieurs finalités. Dans ce cas, il est possible que plus d'un fondement juridique entre en considération pour justifier le traitement de données envisagé » (Groupe 29, « Guidelines for consent under 2016/679 », *WP259*, 28 novembre 2017, p. 22).
206. RGPD, art. 5, § 1er, c).
207. *Ibid.*, art. 5, § 1er, e).

risques pour les droits et libertés des personnes physiques. Il est dès lors important que celles-ci soient documentées, afin qu'elles puissent aussi être prises en compte lors de l'évaluation et de la détermination des risques résiduels finaux[208]. Enfin, l'APD s'attend à ce que l'AIPD fournisse également un aperçu des mesures qui contribuent aux droits des personnes concernées[209], de la manière dont les relations avec les sous-traitants sont régies[210] ainsi que, le cas échéant, des garanties concernant le (les) transfert(s) international (internationaux) qui seront prévues[211].

d) L'évaluation des risques dans le cadre d'une AIPD

En ce qui concerne l'évaluation des risques dans le cadre d'une AIPD, les considérants 84 et 90 du RGPD précisent que celle-ci vise en premier lieu les risques « élevés ». Si, par exemple, lors d'un traitement déterminé, il y a un risque élevé d'atteinte à la réputation mais qu'il n'y a qu'un très faible risque de discrimination, ce dernier risque ne doit pas *nécessairement* être repris en tant que tel dans l'évaluation des risques d'une AIPD. Néanmoins, l'APD recommande, dans le cadre d'une AIPD, de cartographier expressément tous les risques qui ne sont pas négligeables et d'identifier des mesures de protection efficaces, étant donné que même des risques moyens peuvent constituer un facteur important lors de l'évaluation de *la nécessité et de la proportionnalité* du traitement de données envisagé. Quoi qu'il en soit, une AIPD doit comporter un relevé de toutes les mesures prises afin d'apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. Dans cette optique également, il est important que tous les risques pertinents soient pris en compte.

Dans l'annexe 2 de ses lignes directrices, le Groupe 29 énumère les critères qui peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD est considérée comme suffisamment complète aux fins du respect des exigences du RGPD[212]. Le Groupe rappelle également qu'un certain nombre de cadres développés par les autorités de contrôle de l'UE ainsi que de cadres sectoriels européens ont été publiés[213].

e) Consultation préalable de l'autorité de contrôle

L'article 36, § 1er du RGPD dispose que « le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un

208. Groupe 29, *WP248*, *op. cit.*, p. 7.
209. Dont l'information communiquée à la personne concernée (RGPD, art. 12 à 14) ; le droit d'accès et le droit à la portabilité des données (RGPD, art. 15 et 20) ; le droit de rectification et le droit à l'effacement de données (RGPD, art. 16, 17 et 19) ; le droit d'opposition et le droit à la limitation du traitement (RGPD, art. 18, 19 et 21).
210. RGPD, art. 28.
211. Groupe 29, *WP248*, *op. cit*, p. 28.
212. *Ibid.*, p. 26.
213. *Ibid.*, p. 24.

risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ». Il ressort de la formulation de cet article qu'une consultation préalable n'est obligatoire que lorsque le risque résiduel est élevé. Une consultation préalable n'est donc requise que lorsque l'AIPD démontre que le traitement va de pair avec un risque élevé que le responsable du traitement ne puisse l'atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre. Si le risque peut être limité efficacement à l'aide de mesures techniques et organisationnelles appropriées, aucune consultation préalable ne doit avoir lieu[214].

Selon le Groupe 29, un risque résiduel élevé inacceptable existe par exemple lorsqu'il est probable que les personnes concernées soient confrontées à des conséquences considérables ou irréversibles (par exemple : un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière). Il semble ainsi évident que le risque se concrétisera dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée[215].

Si l'autorité de contrôle estime que le traitement envisagé n'est pas conforme au RGPD ou que les risques ne sont pas suffisamment identifiés ou atténués, elle fournit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58 du RGPD, y compris le pouvoir d'imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement[216]. Ce délai de 8 semaines peut être prolongé de 6 semaines[217]. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation[218].

Lorsqu'une consultation préalable est obligatoire, le responsable du traitement doit fournir les informations suivantes[219] :

- le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;
- les finalités et les moyens du traitement envisagé ;
- les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du RGPD ;
- le cas échéant, les coordonnées du délégué à la protection des données ;

214. APD, Recommandation 01/2018, *op. cit*, p. 26.
215. Groupe 29, *WP248*, *op. cit.*, p. 22.
216. RGPD, art. 58, § 2, e).
217. Dans le cas d'une telle prolongation, l'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard notamment, dans un délai d'un mois à compter de la réception de la demande de consultation.
218. RGPD, art. 36, § 2.
219. *Ibid.*, art. 36, § 3.

- l'analyse d'impact relative à la protection des données prévue à l'article 35 du RGPD ;
- et, toute autre information demandée par l'autorité de contrôle.

Enfin, rappelons que l'autorité de contrôle doit en général être consultée lors de la préparation d'une mesure législative ou réglementaire qui concerne la protection des données à caractère personnel[220]. En effet, l'article 23 de la loi du 3 décembre 2017[221] prévoit que le centre de connaissances de l'APD « émet soit d'initiative, soit sur demande du gouvernement, des Chambres législatives, des Gouvernements de communauté ou de région, des Parlements de communauté ou de région, du Collège réuni ou de l'Assemblée réunie visés à l'article 60 de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises : 1° des avis sur toute question relative aux traitements de données à caractère personnel ; 2° des recommandations relatives aux développements sociaux, économiques et technologiques qui peuvent avoir une incidence sur les traitements de données à caractère personnel ». Dans ses avis et recommandations, le centre de connaissances tient compte des mesures de sécurité techniques et organisationnelles nécessaires.

J. Le caractère « approprié » des mesures de sécurité

1. La politique de la sécurité de l'information

Qu'une AIPD soit effectuée ou non, dans l'objectif d'être en mesure de démontrer que le traitement est conforme à l'obligation de sécurité, l'article 24, § 2 du RGPD astreint le responsable du traitement à mettre en œuvre, lorsque cela est proportionné, *des politiques appropriées* en matière de protection des données. Dans le même esprit, le Règlement considère que celui-ci « devrait adopter *des règles internes* et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut »[222]. De plus, ainsi que nous l'avons déjà mentionné, le responsable du traitement ne peut faire appel qu'à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

C'est à la lumière de ces prescrits que doit être lue la recommandation de l'APD selon laquelle « tout organisme traitant des données à caractère personnel doit rédiger un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser ces données »[223]. Celle-ci comprendra utilement :

- l'exposé de la démarche d'évaluation des risques relatifs aux données à caractère personnel ;
- les priorités retenues et les mécanismes mis ou à mettre en place consécutivement à cette analyse des risques ;
- le planning de mise en œuvre ;
- la description des différentes responsabilités et des règles organisationnelles mises en place ;
- la description du processus de gestion des incidents de sécurité ;
- la description du processus de sensibilisation de l'organisme à cette politique ;
- les dispositions retenues afin de maintenir à jour le système de sécurisation une fois installé.

Enfin, cette politique de sécurité de l'information devrait être « approuvée par le plus haut niveau de la hiérarchie ainsi que par les divers responsables et suffisamment diffusée au sein de l'organisme afin d'être connue de tous »[224].

2. L'état des connaissances et les coûts de mise en œuvre

Outre la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, l'article 32, § 1er du RGPD énumère deux facteurs supplémentaires qui doivent être pris en compte pour assurer la mise en œuvre de mesures de sécurité appropriées, à savoir « l'état des connaissances et les coûts de mise en œuvre »[225]. 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.

a) Les coûts de mise en œuvre

En ce qui concerne la référence légale aux coûts, Y. POULLET insiste sur le fait que celle-ci « 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 »[226]. L'APD va dans le même sens en estimant que « le coût de la mise en place des mesures de sécurité doit évidemment être évalué en comparaison des conséquences

220. *Ibid.*, art. 36, § 4 et 57, § 1er, c). De plus, conformément à l'article 36, § 5, du RGPD, « [...] le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique. »
221. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
222. RGPD, consid. 78.
223. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 2.
224. *Ibid.*
225. RGPD, art. 32, § 1er.
226. Y. POULLET, *op. cit.*, p. 43.

que pourrait avoir un incident de sécurité dû à une absence de protection »[227]. Toutefois, « 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 »[228].

b) L'état des connaissances

Quant à la prise en compte de l'état des connaissances, celle-ci doit se lire, selon Y. POULLET comme une obligation de « s'informer des diverses techniques de sécurité présentes sur le marché et à les évaluer à l'aune des risques décelés »[229]. 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 »[230].

Récemment, 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[231]. 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 ». 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 »[232], réalisation de l'approche minimale

227. CPVP, « Note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 9.
228. APD, Recommandation n° 01/2018, *op. cit.*, p. 25.
229. Y. POULLET, *op. cit.*, p. 43. L'auteur 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.
230. 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.
231. ENISA et TeleTrusT, « IT Security Act (Germany) and EU General Data Protection Regulation – Guideline 'State of the art' – Technical and organizational measures », juin 2019.
232. 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.

(y compris le « hardening »[233]), 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.

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[234]. 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.

3. Codes de conduite, certifications, labels et marques

Selon l'article 32, § 3 du RGPD, « l'application d'un code de conduite approuvé [...] ou d'un mécanisme de certification approuvé [...] peut servir d'élément pour démontrer le respect des exigences [de sécurité] »[235]. De plus, le Règlement considère que « des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du [RGPD], notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données »[236].

a) Codes de conduite

L'article 40, § 2 du RGPD prévoit que « les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement, telles que : [...] d) la pseudonymisation des données à carac-

233. En informatique, le durcissement est le processus destiné à sécuriser un système. La démarche 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.
234. ENISA, « Recommendations on shaping technology according to GDPR provisions – Exploring the notion of data protection by default », 28 janvier 2019.
235. Dans le même esprit, l'article 24, § 3, du RGPD dispose que « L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement. ».
236. RGPD, consid. 77.

tère personnel ; [...] h) les mesures et les procédures visées aux articles 24 [obligation *d'accountability*] et 25 [*privacy by design* et *privacy by default*] et les mesures visant à assurer la sécurité du traitement visées à l'article 32 [obligation de sécurité] ; i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées [...] ».

Les codes de conduite permettent de prendre en compte la spécificité de certains secteurs, notamment dans l'application des aspects de sécurité informatique susmentionnés. Cet outil peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement et/ou aux sous-traitants.

Les associations et autres organismes qui ont l'intention d'élaborer un code de conduite ou de le modifier ou de le proroger doivent soumettre le projet de code, la modification ou la prorogation à l'autorité de contrôle compétente. Celle-ci doit alors rendre un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le RGPD et approuve ce projet de code, cette modification ou cette prorogation si elle estime qu'il offre des garanties appropriées suffisantes[237]. En Belgique, la loi du 3 décembre 2017prévoit que le secrétariat général de l'APD a pour mission d'approuver les codes de conduite[238]. Si le code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'approbation finale pourra être accordée par la Commission européenne après avis de l'EDPB qui vérifiera s'ils présentent des garanties appropriées en vue du respect du règlement[239].

Les codes de conduite proposés doivent comprendre les mécanismes permettant à un organisme agréé par l'autorité de contrôle compétente pour contrôler le respect d'un code de conduite[240]. A cet égard, l'article 20, § 1er de la loi du 3 décembre 2017[241] précise que l'APD a pour tâches d'établir et de faire connaître les critères pour l'agrément d'un organe de contrôle des codes de conduite ainsi que de veiller à l'agrément d'un organe de contrôle des codes de conduite.

En cas de violation de l'une des dispositions du RGPD, l'application d'un code de conduite approuvé pourrait donner à l'autorité de contrôle une indication de la nécessité réelle d'intervenir sous la forme d'une amende administrative efficace, proportionnée et dissuasive ou sous la forme d'autres mesures correctives. Lorsque le responsable du traitement ou le sous-traitant applique un code de conduite approuvé, l'autorité de contrôle peut se contenter du fait que la communauté chargée d'administrer le code prend elle-même les mesures appropriées à l'encontre de son membre, par exemple au travers des programmes de contrôle et d'application des règles prévus par le code de conduite lui-même. Par conséquent, l'autorité de

237. *Ibid.*, art. 40, § 5.
238. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 20, § 1er, al. 4.
239. RGPD, art. 41, §§ 7 à 10.
240. *Ibid.*, art. 40, § 4 et 41.
241. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *op. cit.*

contrôle peut considérer que de telles mesures sont suffisamment efficaces, proportionnées ou dissuasives dans ce cas particulier et qu'il n'est pas nécessaire qu'elle impose elle-même des mesures supplémentaires. Certaines formes de sanctions de comportements non conformes peuvent passer par le programme de contrôle[242], et comprendre la suspension ou l'exclusion du responsable du traitement ou du sous-traitant concerné de la communauté appliquant le code en question. Néanmoins, les pouvoirs de l'organisme de contrôle sont « sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente »[243], ce qui signifie que l'autorité de contrôle n'est pas tenue de prendre en considération les sanctions déjà imposées dans le cadre du programme d'autorégulation. Le non-respect de mesures d'autorégulation pourrait également être révélateur de la négligence du responsable du traitement ou du sous-traitant ou de son intention délibérée de ne pas s'y conformer[244].

Selon l'APD, les codes de conduite applicables aux traitements de données à caractère personnel ne sont pour l'instant que peu développés. Cela a pour conséquence que l'expérience à ce niveau en termes de processus est limitée. Néanmoins, l'autorité nationale estime d'ores et déjà que les principes généraux suivants sont fondamentaux et doivent impérativement guider l'élaboration de tout code de conduite :

- être conforme au RGPD et à ses transpositions en droit national, si applicable. Les codes de conduites ne peuvent en aucun cas contenir des dispositions qui font exception au règlement ;
- avoir pour objet de spécifier et préciser l'application du RGPD ;
- apporter une valeur ajoutée par rapport aux dispositions du RGPD permettant de régler les problématiques et questions spécifiques rencontrées par les organisations auxquelles le code apporte des réponses claires et opérationnelles ;
- disposer d'un exposé des motifs qui explique la problématique à laquelle le secteur concerné est confronté nécessitant la mise en place d'un code de conduite ainsi que la plus-value de chaque disposition en lien avec le secteur concerné par le code ;
- avoir un objet clairement défini. Le projet de code doit déterminer avec précision et clarté les traitements (ou caractéristiques de traitements) de données à caractère personnel couverts ainsi que les catégories de responsables de traitements et/ou sous-traitants concernés ;
- désigner l'organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code dans le but de permettre le contrôle obligatoire du respect de ses dispositions par les responsables de traitement ou les sous-traitants qui s'engagent à l'appliquer.

Pour le surplus, l'EDPB a émis des lignes directrices sur les codes de conduites afin d'apporter clarté, transparence et harmonisation sur la procédure ainsi que sur le contenu de ceux-ci[245].

242. Conformément à l'article 41, § 2, point c), et à l'article 42, § 4, du RGPD.
243. RGPD, art. 40, § 4.
244. EDPB, « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 », *WP253*, adoptées le 3 octobre 2017, pp. 16 et 17.
245. EDPB, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 – version adopted after public consultation », adoptées le 4 juin 2019.

b) Certifications, labels et marques

L'article 42, § 1er, du RGPD prévoit que « les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération ».

En matière de sécurité informationnelle, des mécanismes de certification approuvés au sens du RGPD peuvent être utilisés comme élément de démonstration du respect des obligations des responsables du traitement et des sous-traitants dans les contextes suivants :

- la mise en œuvre et la démonstration de mesures techniques et organisationnelles appropriées en matière d'accountability[246], de *privacy by design* & *by default*[247] et de sécurité[248] ;
- les garanties suffisantes de sous-traitant à responsable du traitement[249] et de sous-traitant de second rang à sous-traitant[250].

Le RGPD ne définit pas la « certification », mais prévoit néanmoins qu'elle « est volontaire et accessible via un processus transparent »[251]. En outre, le règlement précise que son objectif est de permettre « aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question »[252]. Il énonce également qu'une certification ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du RGPD[253]. Néanmoins, tout comme en matière de codes de conduites, le respect des mécanismes de certification approuvés est un facteur que les autorités de protection des données doivent prendre en compte comme circonstance aggravante ou atténuante au moment de décider du montant de l'amende potentielle en cas de violation de données[254].

Le RGPD utilise les termes « certification », « labels » et « marques » de manière indifférenciée. Dans la pratique, on considère cependant qu'un certificat est une attestation de conformité ; un label ou une marque ont, quant à eux, pour objet d'afficher la réussite d'une procédure de certification. En effet, un label ou une marque font généralement référence à un logo ou à un symbole dont la présence (en plus d'un certificat) indique que

246. RGPD, art. 24, §§ 1er et 3.
247. *Ibid.*, art. 25.
248. *Ibid.*, art. 32, §§ 1er et 3.
249. *Ibid.*, art. 28, § 1er.
250. *Ibid.*, art. 28, § 4.
251. *Ibid.*, art. 42, § 3.
252. *Ibid.*, consid. 100.
253. *Ibid.*, art. 42, § 4.
254. *Ibid.*, art. 83, § 2, point j).

l'objet de la certification a été évalué de manière indépendante dans une procédure de certification et qu'il est conforme aux exigences de celle-ci. Quant aux tiers qualifiés pour octroyer un certificat, un label ou une marque, le Règlement précise qu'ils ne peuvent être délivrés que par les organismes de certification agréés ou par l'autorité de contrôle compétente[255]. À cet égard, l'article 18 de la loi du 30 juillet 2018[256] prévoit que les organismes de certification doivent être accrédités conformément à la norme EN-ISO/IEC 17065[257] et aux exigences supplémentaires établies par l'APD par l'organisme national d'accréditation désigné conformément au Règlement (CE) n° 765/2008[258]. En Belgique, l'unique organisme d'accréditation est BELAC[259]. L'article 20 de la loi du 3 décembre 2017[260] donne pour tâche au secrétariat général de l'APD d'établir et faire connaître les critères pour l'agrément d'un organe de certification. L'organisme de certification ainsi agréé ne peut délivrer de certification que sur la base des critères qu'il développe mais qui doivent être approuvés par l'autorité de contrôle compétente[261]. Dans le cas d'une certification européenne commune – appelée le « le label européen de protection des données » –, ces critères doivent être approuvés par l'EDPB[262].

Un organisme de certification ne peut délivrer une certification dans un État membre donné qu'en se conformant aux critères approuvés par l'autorité de contrôle de cet État membre. En d'autres termes, selon l'EDPB, les critères de certification doivent être approuvés par l'autorité compétente où l'organisme de certification vise à offrir une certification et obtient l'accréditation[263]. Dans le cas du label européen de protection des données, l'accréditation doit en principe être obtenue dans l'État dans lequel l'organisme de certification demandeur a son établissement principal[264]. Quant à la demande d'approba-

255. *Ibid.*, art. 42, § 5.
256. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
257. L'ISO/IEC 17065 :2012 comporte des exigences portant sur les compétences, la cohérence des activités et l'impartialité des organismes de certification de produits, processus et services.
258. Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil.
259. Arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité.
260. Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
261. RGPD, art. 42, § 5 et Loi du 3 décembre 2017, art. 20, § 1er.
262. RGPD, art. 42, § 5 et 70, § 1er, o).
263. EDPB, « Guidelines 1/2018 on certification and identifying certification criteria in accordance with articles 42 and 43 of the Regulation », adoptées 4 juin 2019, p. 12.
264. « *Accreditation for the scope of a European Data Protection Seal will require accreditation in the Member State of the headquarters of the certification body intending to operate the scheme, i.e. responsible for issuing certifications and managing the certification activities of its entities and subsidiaries in other Member States. Where other establishments or offices manage and perform certifications autonomously, each of these establishments or offices will require separate accreditation in the Member State where they are based. In other words, accreditation is necessary only in the Member State of the headquarters of the certification body when only the headquarters issue the certificates. By contrast, when other establishments of the certification body also issue certificates, these establishments need to be accredited as well* », *ibid*, p. 14.

tion des critères de certification par l'EDPB, celle-ci doit passer par une autorité de contrôle compétente. Le choix du lieu où présenter une demande d'approbation de critères est fondé sur l'établissement principal du propriétaire du schéma de certification ou de l'organisme de certification[265]. Par conséquent, selon l'EDPB, « si un organisme de certification n'a pas été accrédité pour certifier sous le régime du label européen de protection des données, les critères approuvés par l'EDPB ne peuvent pas être utilisés et le label ne peut pas être octroyé »[266].

La coexistence de schémas de certification nationaux et européens au sens du RGPD soulèvera sans aucun doute des questions importantes d'ordre pratique. Au niveau juridique, cette possibilité de cohabitation géographique est également en contradiction flagrante avec l'un des objectifs principaux du récent *Cybersecurity Act*[267] selon lequel « le manque de solutions interopérables (normes techniques), de pratiques et de dispositifs de certification à l'échelle de l'Union constitue l'une des [...] lacunes affectant le marché unique dans le domaine de la cybersécurité »[268]. Pour cette raison, « le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC »[269]. C'est dans cette logique que le *Cybersecurity Act* prévoit que « les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur »[270]. Certes, l'objectif de la certification au sens du *Cybersecurity Act* diffère quelque peu de celui poursuivi par ce mécanisme sous le RGPD : là où le premier se concentre sur la préservation de la cybersécurité des produits, services et processus TIC contre les cybermenaces[271], le second vise à protéger les droits et libertés des personnes physiques. Pourtant, la frontière entre ces objectifs respectifs étant poreuse, les deux régimes susmentionnés risquent fort d'être amenés à se rencontrer régulièrement.

En effet, d'après l'organisation internationale de normalisation (ISO), la certification consisterait en « la fourniture par un organisme indépendant d'une assurance écrite (un certificat) que le produit, le service ou le système en question répond à des exigences

265. *Ibid.*, p. 13.
266. *Ibid.*, p. 14.
267. 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) (ci-après « *Cybersecurity Act* »).
268. *Cybersecurity Act,* consid. 66.
269. *Ibid.*, art. 46.
270. *Ibid.*, art. 57.
271. Au sujet du *Cybersecurity Act*, lire la contribution publiée dans le présent ouvrage de M. KNOCKAERT « La sécurité dans le marché unique numérique européen : le Règlement 2019/881 (« Cybersecurity Act ») » (Voy. Chap. 3).

spécifiques »[272]. Toutefois, selon l'EDPB, dans le cadre des articles 42 et 43 du RGPD, plutôt qu'un produit, un service ou un système, l'objet de la certification concernerait les opérations de traitement effectuées par les responsables de traitements et les sous-traitants[273]. Cela étant, la portée de ce qui peut être certifié mérite d'être nuancée puisque l'EDPB considère que le RGPD offre de larges possibilités, à condition que l'objectif soit d'aider à démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le Règlement[274]. Par conséquent, le Comité est d'avis que « a processing operation or a set of operations may result in a product or service in the terminology of ISO 17065 and such can be subject of [GDPR] certification. For instance, the processing of employee data for the purpose of salary payment or leave management is a set of operations within the meaning of the GDPR and can result in a product, process or a service in the terminology of ISO »[275].

Ce qui amène l'EDPB à cette conclusion est que, lors d'une évaluation d'une opération de traitement, les trois éléments principaux suivants doivent être pris en compte, le cas échéant :

1) les données à caractère personnel (champ d'application matériel du RGPD) ;
2) les systèmes techniques – l'infrastructure, telle que le matériel et les logiciels, utilisés pour traiter les données à caractère personnel et
3) les processus et procédures liés au(x) traitement(s)[276].

Ces trois éléments principaux sont pertinents pour la conception des procédures et des critères de certification. Néanmoins, selon l'objet de la certification, leur prise en compte peut varier, et, dans certains cas, certains éléments peuvent être ignorés s'ils ne sont pas jugés pertinents par rapport à l'objet de la certification. Chaque élément pertinent utilisé dans les opérations de traitement doit être soumis à une évaluation en fonction des critères approuvés par l'autorité compétente. Au moins quatre facteurs significatifs différents peuvent avoir une influence sur l'étendue de l'évaluation : 1) l'organisation et la structure juridique du responsable du traitement ou du sous-traitant ; 2) le service, l'environnement et les personnes impliquées dans les opérations de traitement ; 3) la description technique des éléments à évaluer et enfin 4) l'infrastructure informatique prenant en charge le traitement, y compris les systèmes d'exploitation, les systèmes virtuels, les bases de données, les systèmes d'authentification et d'autorisation, les routeurs et les pare-feu, les systèmes de stockage, l'infrastructure de communication ou l'accès à Internet et les mesures techniques associées.

272. Dans le document « ISO / IEC 17000 : 2004 – Évaluation de la conformité – Vocabulaire et principes généraux » (auxquels ISO17065 fait référence), la certification est définie dans les termes suivants : « Attestation de tierce partie... liée aux produits, processus et services ». L'attestation est une « délivrance d'une déclaration basée sur une décision à la suite d'un réexamen, que des exigences spécifiques ont été démontrées » (section 5.2, ISO 17000 : 2004).
273. EDPB, Guidelines 1/2018, *op. cit.*, p. 8.
274. *Ibid.*, p.15.
275. *Ibid.*, p16.
276. *Ibid.*

La portée du mécanisme de certification au sens du RGPD est à distinguer de l'objet – aussi appelée « target of evaluation » (ToE) – de celle-ci dans le cadre des projets individuels de certifications dans le contexte d'un mécanisme de certification[277]. Un mécanisme de certification peut définir son champ d'application de manière générale ou par rapport à un type spécifique d'opérations de traitement et peut donc déjà identifier les objets de certification du mécanisme de certification (par exemple, le stockage sécurisé de données dans un coffre-fort numérique). Dans tous les cas, une évaluation fiable et significative de conformité ne peut avoir lieu que si l'objet individuel d'un projet de certification est décrit précisément. Il s'agit donc de décrire clairement quels traitements sont inclus dans l'objet de certification mais également indiquer quels composants essentiels – c'est-à-dire les données, les processus et les infrastructures – seront évalués et lesquels ne le seront pas. Ce faisant, les interfaces avec d'autres processus doivent toujours être prises en compte et décrites. Clairement, ce qui n'est pas connu et décrit ne peut pas faire partie de l'évaluation et ne peut donc pas être certifié. Dans ses guidelines, l'EDPB fournit des exemples utiles pour déterminer avec précision le ToE d'un mécanisme de certification[278].

La certification au sens du RGPD est délivrée à un responsable du traitement ou à un sous-traitant pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions tant que les exigences applicables continuent d'être satisfaites. La certification est retirée, s'il y a lieu, par les organismes de certification ou par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus satisfaites[279]. Le Règlement impose aux organismes de certification d'informer leur autorité de contrôle avant de délivrer ou renouveler les certifications[280] pour permettre à l'autorité de contrôle compétente de pouvoir retirer une certification ou ordonner à l'organisme de certification de retirer une certification, ou encore ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites[281].

Dans le cadre de la présente contribution, nous n'analysons pas plus en détail l'importante thématique de la certification au sens du RGPD et de sa complexe relation avec le régime de certification prévu par le *Cybersecurity Act*. À titre purement indicatif, nous renvoyons le lecteur aux recommandations relatives à la certification en matière de protection des données publiées par l'ENISA en novembre 2017[282] dans lequel l'agence mentionne que « data protection certification mechanisms, seals or marks under GDPR have specificities that do not allow for a direct analogy with existing successful certification practises and approaches in other domains, such as ICT security. GDPR provisions require that a certification mechanism must concern an activity of data processing. Such activity may be (also an integral) part of a product, a system, or service, but the certification must be granted in relation to the processing activit(ies), and not to the product, system or service as such, which is not the case in the aforementioned example of ICT security certification. Nevertheless, the experience accumulated and the best practises already implemented in other domains could support European Commission, EDPB and national certification and supervisory authorities on further laying out and implementing certification mechanisms under GDPR. Such experience can pertain identification and analysis of relevant market needs and trends to better match demand and supply, mutual recognition procedures, identification of standardisation gaps and coordination of standardisation activities at EU level »[283]. Gageons que les divers acteurs compétents communiqueront de manière efficace.

277. *Ibid.*
278. *Ibid*, pp. 17 et 18.
279. RGPD, art. 42, § 7, et Loi du 3 décembre 2017, art. 100, § 1er.
280. RGPD, art. 43, § 1er.
281. *Ibid.*, art. 58, § 2, h).
282. ENISA, « Recommendations on European Data Protection Certification, version 1.0 », novembre 2017, disponible à l'adresse suivante : https ://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/at_download/fullReport.

K. De quelques mesures de sécurité

1. Objet

En ce qui concerne la nature des mesures de sécurité devant être mises en œuvre par les débiteurs de l'obligation de sécurité, le Règlement en distingue deux types : d'une part, les mesures techniques, et, d'autre part les mesures organisationnelles.

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 »[284].

L'APD opère, quant à elle, la distinction suivante entre mesures techniques, organisationnelles ou juridiques[285] :

- mesures organisationnelles : accroissement de la conscientisation, formation, mesures politiques, séparation des fonctions (ce qu'on appelle une « Muraille de Chine »), rapport, contrôles périodiques, possibilités supplémentaires de choix, de participation ou d'opposition pour les personnes concernées, etc. ;

283. *Ibid.*, p. 29.
284. 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.
285. APD, Recommandation n° 01/2018, *op. cit.*, p. 24.

- mesures techniques : limitations techniques à la collecte et/ou à la communication de données à caractère personnel (par exemple utilisation de techniques cryptographiques particulières pour faire de la minimalisation de données), l'anonymisation, la pseudonymisation et/ou le cryptage de données à caractère personnel après leur collecte, les limitations techniques à la réutilisation de données à caractère personnel (finalité), l'authentification multifacteurs, la journalisation et le monitoring, la scission de données, les sauvegardes supplémentaires, etc. ;
- mesures juridiques : garanties contractuelles, règles d'entreprise contraignantes, etc.

L'article 32, § 1er, du RGPD énumère, quant à lui, *de manière non exhaustive*, des mesures qui peuvent être envisagées « selon les besoins », à savoir :
- la pseudonymisation et le chiffrement ;
- 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 ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Aperçu de quelques mesures de sécurité techniques

a) L'anonymisation

À titre liminaire, rappelons que le RGPD ne s'applique pas au traitement de données anonymes, à savoir « les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable »[286]. 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[287]. Les principales techniques d'anonymisation, à savoir la *randomisation* et la généralisation ont été décrites par le Groupe 29[288].

À l'issue du processus d'anonymisation, afin de vérifier si les données permettent l'identification d'une personne physique et si ces informations peuvent être considérées comme anonymes ou pas, l'exposé des motifs de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui transposait la Directive (la « LVP ») disposait qu'« elles ne perdent leur caractère de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen

286. RGPD, consid. 26.
287. Groupe 29, « Avis 05/2014 sur les techniques d'anonymisation », *WP216*, adopté le 10 avril 2014, p. 3.
288. *Ibid.*

raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat »[289].

L'exposé des motifs de la Recommandation N° R (97)18[290] abonde dans le même sens concernant la question des moyens raisonnables permettant une réidentifcation : « (..) le risque de réidentification ne doit pas être strictement nul, on peut considérer qu'il est nul en pratique lorsque la réidentification demanderait des opérations excessivement compliquées, longues et coûteuses. Aucun coffre-fort n'est rigoureusement inviolable ; on doit exiger des précautions qui rendent la violation non pas strictement impossible, mais très improbable. Et cette exigence peut varier selon la nature des données, selon qu'elles sont plus ou moins sensibles ». En pratique, pour savoir si des données peuvent être considérées comme anonymes, il faut donc procéder à un examen au cas par cas pour tenir compte de toutes les circonstances. Cela s'avère particulièrement important dans le cas des informations statistiques où, en dépit du fait que lesdites informations peuvent se présenter sous forme agrégée, l'échantillon initial ne sera pas suffisamment important si d'autres éléments d'information peuvent permettre d'identifier les personnes physiques[291]. Par conséquent, à défaut d'être absolument certains d'avoir affaire à des données réellement anonymes, nous recommandons aux débiteurs de l'obligation de sécurité de les considérer comme restant « à caractère personnel ».

b) La pseudonymisation

La « pseudonymisation » est définie par le RGPD 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 »[292]. Concrètement, la pseudonymisation 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. La personne concernée reste donc, par conséquent, toujours susceptible d'être identifiée indirectement[293]. 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

289. Exposé des motifs de la loi du 11 décembre 1998, *Doc. Parl.*, Chambre, sess. ord. 1997-1998, n° 1566/1, p. 12.
290. Recommandation (97)18 du Conseil de l'Europe sur la protection des données à caractère personnel, collectées et traitées à des fins statistiques, adoptée par le Comité des Ministres le 30 septembre 1997.
291. Groupe 29, *WP136*, *op. cit.*, p. 23.
292. RGPD, art. 4, 5).
293. Groupe 29, *WP216*, *op. cit.*, p. 22.

hachage ou d'un système de chiffrement[294]. Certaines techniques de pseudonymisation ont été décrites et analysées par le Groupe 29 dans un avis de 2014[295].

Sous le régime de la LVP, les données pseudonymisées étaient 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 ».[296] L'exposé des motifs de la loi précisait que 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 clés nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne »[297]. De la même manière, sous l'empire du RGPD, les données pseudonymisées sont par définition des données relatives à un individu identifiable, 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[298]. Par ailleurs, le RGPD considère que « des mesures de pseudonymisation devraient être possibles chez un même responsable du traitement, tout en permettant une analyse générale, lorsque celui-ci a pris les mesures techniques et organisationnelles nécessaires afin de garantir, pour le traitement concerné, que le présent règlement est mis en œuvre, et que les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise soient conservées séparément »[299]. Dans ce cas, le responsable du traitement qui traite les données à caractère personnel devrait indiquer les personnes autorisées à cet effet.

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[300]. Notons toutefois que l'introduction explicite de la pseudonymisation dans le RGPD ne vise pas à exclure d'autres mesures de sécurité des données, par exemple le chiffrement[301].

294. *Ibid.*
295. *Ibid*, pp. 23 à 25.
296. Arrêté royal du 13 février portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, art. 1er, § 1er, 3°.
297. Exposé des motifs de la loi du 11 décembre 1998, *op. cit.*
298. 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. ».
299. RGPD, consid. 29.
300. L'usage de la pseudonymisation peut également être utile dans le cadre de l'application de l'article 11 du RGPD.
301. RGPD, consid. 28.

Récemment, l'ENISA a publié un rapport en la matière[302]. Celui-ci a notamment pour objectifs d'examiner la notion de pseudonymisation et ses objectifs de protection des données, de décrire différentes techniques pouvant être utilisées pour la pseudonymisation de données, et enfin, de discuter des meilleures pratiques possibles en matière de pseudonymisation, en particulier pour l'écosystème des applications mobiles.

c) Le chiffrement

Contrairement à la Directive qui ne mentionnait pas le chiffrement, le RGPD y fait explicitement référence 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 »[303]. 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 »[304].

Premièrement, 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' »[305]. 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) »[306]. Utilisé de cette manière, en plus de mettre en place une garantie appropriée de sécurité, l'intérêt pour le responsable du traitement de procéder au chiffrement de données, en les rendant incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, est d'être *dans certaines circonstances* dispensé de son obligation de communiquer une violation de telles données aux personnes concernées[307] et, par conséquent, d'être davantage à l'abri d'une perte de confiance de celles-ci.

302. ENISA, Recommendations on shaping technology according to GDPR provisions – An overview on data pseudonymization, novembre 2018.
303. Loi du 13 juin 2005 relative aux communications électroniques, art. 48. 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.
304. Loi du 13 juin 2005 relative aux communications électroniques, art. 2, 40°. 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.
305. Groupe 29, *WP196*, *op. cit.*, p. 18.
306. Groupe 29, *WP213*, *op. cit.*, p. 10.
307. RGPD, art. 34, § 3, a).

Un second avantage de l'utilisation du chiffrement, tant pour le responsable du traitement que pour les personnes concernées, est « de recourir à des mécanismes d'authentification cryptographiques tels que les codes ou signatures d'authentification des messages afin de détecter les modifications apportées aux données à caractère personnel ».[308] De telles pratiques peuvent s'avérer extrêmement utiles afin de compléter judicieusement des politiques d'accès logiques aux données[309]. À titre indicatif, mentionnons que des études relatives aux méthodes de chiffrement dans le contexte de la protection des données à caractère personnel ont été publiées par l'ENISA[310].

d) La sécurité des réseaux

L'évolution de la technologie et de l'interconnexion entre les systèmes d'informations, la dématérialisation desdits systèmes ainsi que de leurs supports ne font qu'accroître les risques de violations de données. Selon l'APD, « la disponibilité inadéquate de données à caractère personnel sur Internet constitue un problème majeur, et ce d'autant plus que ces données peuvent avoir une valeur marchande et que leur diffusion en devient incontrôlable à l'heure actuelle si des mesures de sécurité appropriées ne sont pas prises »[311]. L'APD considère que lorsque « le réseau interne de l'organisme est connecté à un réseau externe public, l'organisme doit prendre les mesures nécessaires afin de protéger le ou les réseaux impliqué(s) dans le traitement des données à caractère personnel contre tout accès non autorisé »[312], qu'il s'agisse de menaces (actions extérieures ou intérieures malveillantes) ou de vulnérabilités (risques propres aux systèmes et applications).

À cet égard, l'autorité recommande une architecture informatique locale « basée sur le principe des couches de sécurité, en implémentant une segmentation logique et/ou physique des zones. L'accès direct aux systèmes applicatifs depuis Internet sera contrecarré par l'utilisation simultanée de divers moyens disponibles selon les cas, par exemple des serveurs relais tels 'Proxy/Reverse Proxy', par la translation des adresses IP, par un pare-feu (*firewall*) ou un routeur convenablement paramétrés »[313]. En fonction des ressources disponibles, la mise en place et le suivi d'un système de détection (et de prévention) d'intrusion (IDS/IPS) sont un plus permettant de repérer des activités anormales ou suspectes[314].

308. Groupe 29, *WP196*, *op. cit.*, p. 18.
309. Voir Section 8.6.3 de la présente contribution.
310. L'ENISA a publié, entre autres, le document « Recommended cryptographic measures – Securing personal data » le 20 septembre 2013 ; le document « Algorithms, Key Sizes and Parameters Report – 2013 » le 29 octobre 2013 ; le document « Study on cryptographic protocols » le 21 novembre 2014 et, enfin, le document « Updated Report on Algorithms, Key Sizes and Parameters » le 21 novembre 2014.
311. CPVP, Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données, *op. cit.* p. 2.
312. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 4.
313. CPVP, Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données, *op. cit.* p. 4.
314. *Ibid.*

3. Aperçu de quelques mesures de sécurité organisationnelles

a) L'organisation et les aspects humains de la sécurité de l'information

Il va de soi qu'une première mesure organisationnelle importante est la désignation d'un DPD dans les circonstances prévues par l'article 37 du RGPD. Un DPD doit exercer les fonctions précisées dans l'article 38 du Règlement et avoir pour missions celles énumérées à l'article 39 dont fait partie « le contrôle des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant »[315].

Qu'un DPD doive être désigné ou non, il est fortement recommandé que chaque débiteur de l'obligation de sécurité définisse clairement les responsabilités et processus de gestion en matière de sécurité des données à caractère personnel et les intègre adéquatement dans son organisation générale et son fonctionnement[316]. En effet, l'article 32, § 4, du RGPD impose explicitement tant au responsable du traitement qu'au sous-traitant de prendre des mesures afin de garantir que toute personne physique agissant sous leur autorité qui a accès à des données à caractère personnel, « *ne les traite pas, excepté sur instruction du responsable du traitement*, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre ». Dans le même esprit, l'article 28, § 3, b), du Règlement impose au sous-traitant de 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 ».

Par conséquent, la mise en place « de 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 » est fortement recommandée[317].

L'APD estime également que « la réussite de la sécurisation d'un système d'information dépendant fortement de l'information correcte des différents acteurs, l'organisme doit prendre les mesures nécessaires afin que toute personne (interne ou externe) intervenant dans le traitement des données personnelles soit constamment suffisamment informée de ses devoirs et responsabilités lors de ces traitements et suffisamment et correctement formée à l'exercice de sa fonction et de ses responsabilités de sécurité de l'information. D'éventuels suivis disciplinaires doivent être prévus en cas de non-respect des règles édictées et un engagement de confidentialité requis lorsque les risques le justifient »[318]. Enfin, il va de soi que lorsque l'organisme sous-traite tout ou partie de ses traitements, il veillera

315. RGPD, art. 39, § 1er, b).
316. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 3.
317. *Ibid.*
318. *Ibid.*

à répercuter, dans le contrat de sous-traitance, les obligations de sécurité qu'il estime opportunes[319].

b) La sécurité physique et de l'environnement

Afin de garantir la protection physique des données à caractère personnel, il est fortement recommandé de s'assurer que les supports des données à caractère personnel et les systèmes informatiques soient placés, conformément à leur classification, dans des locaux identifiés et protégés et dont l'accès est limité aux seules personnes autorisées et aux seules heures justifiées par leur fonction[320].

L'APD belge estime également que, dans les cas où une continuité des services s'avère nécessaire, « des dispositifs de prévention, de détection et de traitement de dangers physiques tels que les incendies ou les inondations doivent être installés et régulièrement contrôlés. L'organisme doit aussi prendre les mesures de sauvegarde (*backup*) nécessaires afin de pouvoir contrer la perte ou l'altération accidentelle de données à caractère personnel »[321]. Ainsi que nous l'avons déjà mentionné, des références aux mesures garantissant, selon les besoins, la disponibilité et la résilience des données sont explicitement mentionnées dans l'article 32, § 1er, du RGPD.

c) La sécurisation logique des accès

Une importante recommandation adressée aux débiteurs de l'obligation de sécurité est de « s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation »[322]. Selon le Groupe 29, « il 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 et de moindre privilège [...] ces personnes devraient uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues, pour une durée qui se limite à ce qui est strictement nécessaire. L'utilisation des comptes disposant d'un 'accès global' à la base de données devrait être limitée et des méthodes de traçage et de restriction de l'utilisation de ce type de comptes devraient être appliquées »[323]. À cet effet, il s'agit 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). Ces différentes autorisations « doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de communication, etc.) intervenant dans le traitement des données à caractère personnel »[324].

En Belgique, l'article 9 de la loi du 30 juillet 2018[325] impose explicitement au responsable du traitement de prendre les mesures suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

- les catégories de personnes ayant accès aux données à caractère personnel doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées ;
- la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de l'APD par le responsable du traitement ou, le cas échéant, par le sous-traitant ;
- les personnes désignées doivent être tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

L'article 10 de la même loi contient une disposition similaire en cas de traitement de données relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes.

De plus, selon l'APD, « si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification »[326]. La CNIL va dans le même sens en affirmant que « 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 »[327]. Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés selon qu'ils font intervenir :

- ce que l'on sait, par exemple un mot de passe ;
- ce que l'on a, par exemple une carte à puce ;
- une caractéristique qui nous est propre, par exemple une modalité biométrique[328].

La CNIL qualifie l'authentification d'un utilisateur comme étant forte lorsqu'elle a recours à une combinaison d'au moins deux de ces catégories[329]. En outre, dès que des moyens d'authentification sont compromis, il s'agira « d'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 »[330].

319. Voy. à ce sujet les sections 3.1 et 3.2 de la présente contribution.
320. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 3.
321. *Ibid*, p. 4.
322. *Ibid.*
323. Groupe 29, *WP213*, *op. cit.*, p. 10.
324. *Ibid.*
325. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
326. *Ibid.*
327. CNIL, *La sécurité des données personnelles*, *op. cit.*, p. 7.
328. Evidemment, une modalité biométrique étant considérée comme une donnée sensible au sens de l'article 9 du Règlement, il s'agit d'appliquer le RGPD en fonction.
329. CNIL, *La sécurité des données personnelles*, *op. cit.*, p. 7.
330. Groupe 29, *WP213*, *op. cit.*, p. 9.

Ces dispositions techniques devraient inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires de sauvegarde). À cet égard, il s'agit d'ailleurs « de réaliser une stricte séparation des environnements de développement, test, acceptation/intégration et production et de n'accorder des accès à l'environnement de production qu'aux gestionnaires systèmes dûment autorisés et identifiés »[331].

d) La journalisation

Une contribution de cet ouvrage s'intéresse particulièrement à l'enjeu de la journalisation. Nous renvoyons le lecteur à celle-ci[332]. Pour rappel, la journalisation concrétise la propriété d'imputabilité consistant « à enregistrer les informations pertinentes concernant des évènements du système au cours de son activité (accès à un système ou à un dossier, modification d'un fichier, transfert de données, envoi ou réception d'un message électronique, réalisation d'une transaction commerciale, etc.), à la manière d'un journal de bord, dans des fichiers appelés *log files* »[333]. Paradoxalement, afin de garantir la protection des données à caractère personnel, l'obligation de sécurité peut donc avoir pour conséquence, selon les besoins, d'imposer un traitement de données à caractère personnel additionnel ou accessoire ayant pour finalité l'imputabilité des actions réalisées sur les traitements initiaux[334].

Le Contrôleur européen de la protection des données[335] (ci-après « EDPS ») s'est également penché sur la question et a formulé quelques lignes directrices sur le sujet. Selon celui-ci, il s'agit tout d'abord de tenir compte du principe de minimisation pour définir le contenu des journaux de sécurité et leur durée de conservation en fonction des besoins du débiteur de l'obligation de sécurité[336]. Ensuite, conformément au principe de finalité, les données collectées à des fins de contrôle de la sécurité ne peuvent être utilisées qu'à cet effet[337]. Enfin le Groupe 29 indique que, si les fichiers de journalisation sécurisés sont fiables (c'est-à-dire s'ils ne sont pas compromis), ceux-ci peuvent être d'une grande utilité en cas de violation de données[338].

331. CPVP, Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données, *op. cit.* p.5.
332. Au sujet de la journalisation, lire la contribution publiée dans le présent ouvrage de F. DUMORTIER : « Cybersécurité, vie privée, imputabilité, journalisation et log files » (Voy. Chap. 4).
333. S. GHERNAOUTI, *op. cit.*, p. 6.
334. Dans le contexte de la lutte contre l'échange non autorisé de fichiers électroniques musicaux réalisé grâce à des logiciels « peer-to-peer », la CJUE a estimé que « [...] la collecte et l'identification des adresses IP des utilisateurs qui sont à l'origine de l'envoi des contenus illicites sur le réseau [sont] des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs » CJUE, 24 novembre 2011, *Scarlet Extended SA contre Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10).
335. Le Contrôleur européen de la protection des données (en anglais *European Data Protection Supervisor* – EDPS) est une autorité de contrôle indépendante qui a pour mission première d'assurer que les institutions et organes européens respectent le droit à la vie privée et à la protection des données lorsqu'ils traitent des données à caractère personnel et élaborent de nouvelles politiques.
336. EDPS, « Lignes directrices sur les données à caractère personnel et les communications électroniques au sein des institutions de l'Union », adoptées en décembre 2015, p. 8.
337. *Ibid*, p. 9.
338. Groupe 29, *WP213*, *op. cit.*, p. 9.

e) Les audits

L'article 32, § 1er, d), du Règlement stipule explicitement que, selon les besoins, doit être mise en place « une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ». Dans le même esprit, l'article 28, § 3, h) prévoit qu'en cas de sous-traitance, le contrat doit obligatoirement « permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ».

L'APD s'inscrit dans la même logique en recommandant que « l'organisme doit s'assurer que les mesures de sécurité techniques ou organisationnelles sont validées et font l'objet de révisions régulières. Les besoins de maintenance de la sécurité doivent pouvoir être détectés par une surveillance portant sur les traitements, l'évolution des ressources et l'analyse des journaux de traçage. Les systèmes d'information et les risques auxquels ils sont exposés étant en constante évolution, l'organisme s'assurera régulièrement (au moins une fois par an) que les objectifs initialement poursuivis et les mesures de sécurité mises en place consécutivement restent d'actualité afin d'y apporter les éventuels correctifs, si nécessaire »[339]. Les organismes s'assureront évidemment de soumettre l'auditeur désigné à une obligation de confidentialité. Par ailleurs, l'article 39, § 1er, b), du RGPD met à charge du DPD la mission de contrôler lesdits audits. Un aperçu des principales méthodes d'audit a été publié par l'ENISA en 2013[340].

L'importance des audits est également rappelée par le Groupe 29 selon lequel « un contrôle permanent des vulnérabilités potentielles des technologies utilisées, incluant au moins une analyse régulière des vulnérabilités du site Web et une mise à jour des logiciels (y compris des logiciels de sécurité), [peuvent permettre d'éviter une] violation soit de réduire son incidence. Même si les attaques jour zéro exploitant des vulnérabilités de sécurité sont difficiles à éviter, des stratégies adéquates et efficaces permettant d'empêcher de manière proactive l'exploitation des vulnérabilités de sécurité, notamment un examen du code, peuvent réduire la marge de risque à un niveau acceptable. En outre, une bonne politique de gestion des incidents de sécurité peut également réduire les conséquences d'une violation en limitant l'ampleur et la durée de ses effets négatifs »[341].

f) La gestion des incidents

Pour rappel, l'article 32, § 1er, c), du RGPD impose aux débiteurs de l'obligation de sécurité de mettre en œuvre, selon les besoins, « des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en

339. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 5.
340. ENISA, « Auditing Security Measures – An Overview of schemes for auditing security measures », septembre 2013.
341. Groupe 29, *WP213*, *op. cit.*, p. 8.

cas d'incident physique ou technique ». De telles mesures ne peuvent se concevoir sans plan de gestion des incidents de sécurité.

Ainsi, selon l'APD, « en cas d'incidents mettant en péril la confidentialité et l'intégrité des données à caractère personnel, la rapidité d'intervention est primordiale pour réduire les conséquences d'une telle situation. Pour ce faire, l'organisme doit avoir prévu les procédures spécifiant la marche à suivre en cas de détection d'incident de sécurité relatifs aux données à caractère personnel ainsi que les personnes responsables pour gérer l'incident et restaurer une situation saine. En outre, les conditions de l'incident doivent être analysées afin d'en déduire les mesures préventives ou correctrices destinées à éviter la reproduction de ce genre d'incident ou de permettre un retour plus rapide à une situation normale »[342]. De plus, selon l'APD, « les organismes, contraints d'assurer la continuité de leurs services, doivent prévoir les plans de recouvrement et de continuité permettant de couvrir les incidents de sécurité pouvant provoquer des interruptions de service dépassant les délais acceptables et veiller particulièrement à ce que la confidentialité et l'intégrité des données personnelles soient toujours assurées lors de l'exécution de ces divers plans »[343].

La mise en place d'un plan de gestion adéquat est capitale puisque le RGPD considère qu'il « convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs [...] »[344].

L. La notification et la communication des violations de données

1. Objet

Le concept de « violation de données à caractère personnel » est défini à l'article 4, 12) du RGPD comme étant « une 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 ». Ainsi que nous l'avons déjà mentionné, le Groupe 29 considère que ce concept couvre tant les violations d'intégrité, de confidentialité que celles de

342. CPVP, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 5.
343. *Ibid.*
344. RGPD, consid. 87.

disponibilité des données, même si ces dernières sont seulement temporaires. Évidemment, ces différents types de violations de données peuvent avoir lieu séparément ou de manière cumulative[345].

L'article 33, § 1er, du RGPD prévoit que le responsable du traitement est tenu de notifier de telles violations de données à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. 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. Toutefois, cette notification à l'APD n'est pas requise lorsque la violation en question *n'est pas susceptible d'engendrer un risque* pour les droits et libertés des personnes physiques. Enfin, 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 communiquer ladite violation de données à caractère personnel à la personne concernée dans les meilleurs délais[346].

2. Prise de connaissance et délais

a) Le délai de notification

En cas de violation de données, l'article 33, § 1er, du RGPD impose au responsable du traitement notifier celle-ci à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures[347] au plus tard « après en avoir pris connaissance »[348].

Quant au sous-traitant, le second paragraphe du même article 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. L'obligation faite au sous-traitant de notifier la violation au responsable du traitement permet à ce dernier d'y remédier et de déterminer s'il est nécessaire d'avertir l'autorité de contrôle conformément à l'article 33, § 1er, ainsi que les personnes concernées conformément à l'article 34, § 1er. Le sous-traitant doit simplement établir si une violation s'est produite puis la notifier au responsable du traitement. Le responsable du traitement pourrait également analyser lui-même la violation en question, dès lors 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 carac-

345. Groupe 29, *WP250*, *op. cit.*, p. 8.
346. RGPD, art. 34, § 1er.
347. Pour ce qui concerne les règles européennes en matière de calcul des délais, voyez le Règlement (CEE, Euratom) n° 1182/71 du Conseil du 3 juin 1971portant détermination des règles applicables aux délais, aux dates et aux termes.
348. RGPD, art. 33, § 1er.

tère 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[349].

Dans la même logique, « a processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller »[350].

b) Le point de départ des délais de notification

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[351]. Néanmoins, ainsi que nous l'avons déjà mentionné, le RGPD impose un plan de gestion des incidents adéquat « pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée »[352]. Cela étant dit, le moment concret de la prise de connaissance dépendra évidemment des circonstances : « in some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised »[353]. Le Groupe 29 donne pour exemples :

- le cas d'une clé USB perdue sur laquelle sont stockées des données non chiffrées. Dans cette hypothèse, c'est évidemment le moment de la perte de la clé qui doit être pris en compte ;
- les cas dans lesquels un tiers informe un débiteur de l'obligation de sécurité qu'il a accidentellement ou volontairement obtenu des données et lui en fournit la preuve. Dans ces hypothèses, c'est le moment où la preuve est fournie qui doit être pris en considération ;
- une intrusion potentielle est détectée dans un réseau et le gestionnaire vérifie si des données ont été compromises. Dans ce cas, la prise de connaissance a lieu au moment où l'intrusion est confirmée et qu'elle consiste en une « violation de données ».

349. Selon le Groupe 29, « *The contract between the controller and processor should specify how the requirements expressed in article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours* », Groupe 29, *WP250, op. cit.*, p. 14.
350. *Ibid.*
351. Groupe 29, *WP250, op. cit*, p. 11.
352. RGPD, consid. 87.
353. Groupe 29, *WP250, op. cit*, p. 11.

Selon le Groupe 29, dans certaines hypothèses, le moment où « un degré raisonnable de certitude » qu'un incident a eu lieu entraînera une courte période d'enquête pour déterminer s'il y a eu ou non « violation de données » au sens de l'article 4, 12), du RGPD. « During this period of investigation the controller may not be regarded as being 'aware'. However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place ; a more detailed investigation can then follow »[354].

3. Les critères de gravité d'une violation de données

Afin de déterminer si le responsable du traitement doit se conformer à l'exigence de notification à l'autorité de contrôle et/ou à celle de la communication aux personnes concernées, celui-ci doit respectivement procéder, d'une part, à une évaluation de l'existence de la susceptibilité d'un risque pour les personnes concernées, et, d'autre part de la gravité que ce risque pourrait engendrer pour celles-ci. En effet, la communication aux personnes concernées n'est requise que lorsque la violation de données est *susceptible d'engendrer un risque élevé pour celles-ci*. Le considérant 85 du RGPD énumère des exemples de risques pour les droits et libertés des personnes physiques en cas de violation de données.

Dans ce contexte, il s'agit à l'évidence de tenir compte des conséquences résultant de la matérialisation effective du risque suite à la violation de données. A cet égard, le Groupe 29 estime que « assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue ; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals »[355].

Par conséquent, afin d'évaluer le risque pour les personnes physiques résultant d'une violation de données, le responsable du traitement doit prendre en considération les circonstances particulières de ladite violation, en ce compris la gravité et la probabilité de l'impact potentiel pouvant concrètement en découler. Dans cet exercice, le Groupe 29 recommande aux responsables du traitement de tenir compte des facteurs suivants :

- le type de violation[356] ;

354. *Ibid.*
355. Groupe 29, *WP250, op. cit*, p .23.
356. Selon le Groupe 29, « *The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost and are no longer available* », Groupe 29, *WP250, op. cit.*, p. 24.

- la nature[357], la sensibilité[358] et le volume des données[359] ;
- la facilité d'identification des personnes concernées[360]. À cet égard le Groupe insiste particulièrement sur l'importance du chiffrement et/ou de la pseudonymisation[361] ;
- la gravité des conséquences pour les personnes concernées[362] ;
- les caractéristiques particulières des personnes concernées[363] ;
- les caractéristiques particulières du responsable du traitement[364] ;

357. Selon le Groupe 29, « *Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child […]. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals* ». Groupe 29, *WP250*, *op. cit.*, p. 24.

358. Selon le Groupe 29, « Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data ». Groupe 29 *WP250*, *op. cit.*, p. 24.

359. Selon le Groupe 29, « *Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals* ». Groupe 29, *WP250*, *op. cit.*, p. 24.

360. Selon le Groupe 29, « *An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches* ». Groupe 29, *WP250*, *op. cit.*, pp. 24 et 25.

361. Selon le Groupe 29, « *personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible* ». Groupe 29, *WP250*, *op. cit.*, p. 25.

362. Selon le Groupe 29, « *Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm […] Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term* ». Groupe 29, *WP250*, *op. cit*, p. 25.

363. Selon le Groupe 29, « *A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them* ». Groupe 29, *WP250*, *op. cit*, p. 25.

364. Selon le Groupe 29, « *The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper* ». Groupe 29, *WP250*, *op. cit*, pp. 25 et 26.

- le nombre de personnes affectées par la violation de données[365].

Enfin, le Groupe 29 rappelle que l'ENISA a publié des recommandations pour évaluer la gravité d'une violation de données[366] dont les responsables du traitement et les sous-traitants peuvent s'inspirer afin de rédiger leurs plans de gestion des incidents de sécurité[367].

4. Les violations de données ne devant pas être notifiées

Une violation de données doit être notifiée à l'autorité de contrôle que lorsqu'elle est *susceptible d'engendrer un risque* pour les droits et libertés des personnes physiques. Ainsi que le mentionne le Groupe 29, « this is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority »[368].

Cette exception à l'obligation de notification est illustrée par le Groupe 29 à l'aide de deux exemples. Dans le premier cas, une clé USB contenant des informations chiffrées et ayant fait l'objet d'un backup est volée. Dans cette hypothèse, selon le Groupe, « as long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required »[369]. Dans le second cas d'espèce, un call-centre fait l'objet d'une coupure de courant entraînant une indisponibilité temporaire des données pendant quelques minutes. Dans cette éventualité, le Groupe considère que « this is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller »[370].

365. Selon le Groupe 29, « *A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected* ». Groupe 29, *WP250*, *op. cit*, p. 26.

366. ENISA, « *Recommendations for a methodology of the assessment of severity of personal data breaches* », décembre 2013. Soulignons que ces recommandations ont été écrites en collaboration avec des experts issus des APD hellénique et allemande.

367. Groupe 29, *WP250*, *op. cit.*, p. 26.

368. *Ibid.*, p. 18.

369. *Ibid.*, p. 31.

370. *Ibid.*

5. Les violations de données ne devant pas être communiquées

L'article 34, § 3, du RGPD prévoit que la communication aux personnes concernées n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

- 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 ;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;
- 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.

Conformément au principe d'*accountability*, les responsables des traitements doivent être en mesure de démontrer qu'une ou plusieurs des conditions susmentionnées est/sont rencontrée(s). Ceux-ci doivent également garder à l'esprit que, même si une communication n'est pas initialement requise, elle peut le devenir avec l'écoulement du temps si la susceptibilité d'un risque élevé apparaît. En outre, l'article 34, § 4 du Règlement prévoit que « si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie ». Dans la décision de communiquer ou non une violation de données aux personnes concernées, il s'agit d'être extrêmement attentif aux multiples potentielles conséquences concrètes que ladite violation peut engendrer. Par exemple, dans son avis de 2014, le Groupe 29 avait considéré qu'une « violation de la confidentialité de données à caractère personnel qui ont été cryptées à l'aide d'un algorithme de pointe constitue tout de même une violation de données à caractère personnel, et celle-ci doit être notifiée à l'autorité. Néanmoins, si la confidentialité de la clé de cryptage est intacte, les données sont en principe *incompréhensibles* à toute personne qui n'est pas autorisée à y avoir accès, et la violation n'est donc pas susceptible de porter atteinte à la personne concernée et ne nécessite dès lors pas de lui être communiquée »[371]. Néanmoins, même en cas de chiffrement, une perte ou une altération de données peut être susceptible d'engendrer des conséquences négatives pour les personnes concernées, par exemple dans le cas où aucun backup n'a été prévu. Par conséquent, dans son avis de 2017, le Groupe 29 estime que, dans le cas d'espèce susmentionné, non seulement une notification à l'APD est requise mais également une communication aux personnes concernées[372].

371. Groupe 29, *WP213*, *op. cit.*, p. 3.
372. Groupe 29, *WP250*, *op. cit*, p. 18.

Enfin, il est intéressant de relever le raisonnement du Groupe 29 en cas d'indisponibilité temporaire de données chiffrées faisant l'objet d'un backup : « *where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the 'the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'* »[373].

6. Contenu de la notification à l'autorité de contrôle

La notification à l'autorité de contrôle doit contenir, à tout le moins[374] :

- 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.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu[375]. Selon le Groupe 29, « *this means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more*

373. *Ibid.*, p. 19.
374. RGPD, art. 33, § 3.
375. *Ibid.*, art. 33, § 4.

details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority »[376].

7. Contenu et modalités de la communication aux personnes concernées

a) Contenu de la communication

Lorsque la communication aux personnes concernées est requise, celle-ci doit contenir et décrire « en des termes clairs et simples »[377] 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.

L'objectif principal de la communication est de permettre aux personnes concernées de « prendre les précautions qui s'imposent »[378]. Il s'agit donc de « formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels »[379]. 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 »[380].

376. Groupe 29, *WP250*, *op. cit.*, p. 15
377. RGPD, art. 34, § 2.
378. *Ibid.*, consid. 86.
379. *Ibid.*
380. Groupe 29, *WP213*, *op. cit.*, p. 9.

b) Modalités de la communication

Lorsque la communication aux personnes concernées est requise, celle-ci doit être réalisée directement envers les personnes concernées sauf si celle-ci exigerait des efforts disproportionnés[381]. 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[382].

Afin d'être transparente, la communication doit être envoyée séparément d'autres informations telles que des updates ou des newsletters[383]. Selon le Groupe 29, « *examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel* »[384].

En ce qui concerne l'élément temporel, la communication aux personnes concernées doit, en principe, être réalisée « dans les meilleurs délais »[385], c'est-à-dire « aussi rapidement qu'il est raisonnablement possible »[386]. Néanmoins, il s'agit d'agir « en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication »[387]. Dans le même sens, le considérant 88 du RGPD rappelle qu'il faut tenir compte « de l'intérêt légitime des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel ».

381. RGPD, art. 34, § 3, c).
382. *Ibid.*
383. Groupe 29, *WP250*, *op. cit.*, p. 21.
384. *Ibid.*
385. RGPD, art. 34, § 1er.
386. *Ibid.*, consid. 86.
387. *Ibid.*

8. Documentation

L'article 33, § 5, du RGPD impose au responsable du traitement de documenter toute violation de données à caractère personnel « en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier ».

S'il appartient au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, certaines informations clés devraient être incluses en toutes circonstances. Comme requis à l'article 33, § 5, le responsable du traitement doit reprendre des informations concernant la violation, y compris les causes, les faits et les données à caractère personnel concernées. Il devrait également inclure les effets et les conséquences de la violation ainsi que les mesures prises par le responsable du traitement pour y remédier.

Cette exigence de tenir des registres 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.

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 et au fondement juridique du traitement. 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.

Outre ces informations, le Groupe 29 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, la justification de cette décision devrait être documentée. Cette 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.

Lorsque le responsable du traitement ne notifie pas une violation à l'autorité de contrôle, mais que la notification est retardée, le responsable du traitement doit être en mesure de fournir les raisons d'un tel retard ; une documentation à cet égard pourrait contribuer à démontrer que le retard de notification est bien justifié et n'est pas excessif.

Lorsque le responsable du traitement communique une violation aux personnes concernées, il devrait être transparent en ce qui concerne la violation en question et communiquer de façon efficace et en temps utile. Conserver la trace d'une telle communication

aiderait le responsable du traitement à démontrer son respect du principe de responsabilité et du RGPD en général.

Dans le but de favoriser leur conformité avec les articles 33 et 34 du RGPD, il serait bénéfique à la fois pour les responsables du traitement et les sous-traitants de disposer d'une procédure de notification documentée définissant la procédure à suivre lorsqu'une violation est détectée, y compris concernant la façon d'endiguer, de gérer et de remédier à l'incident, d'évaluer le risque et de notifier la violation. À cet égard, toujours afin de prouver leur conformité avec le RGPD, il pourrait être utile de démontrer que les employés ont été informés de l'existence de tels mécanismes et procédures et qu'ils savent comment réagir en cas de violation.

Il convient de noter qu'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 du RGPD.

M. Conclusion

Le renforcement de l'obligation de sécurité des traitements de données à caractère personnel dans le cadre du RGPD s'inscrit dans un contexte plus large dans lequel la sécurité des données et des systèmes informatiques est devenu un enjeu majeur pour le législateur européen. En témoignent différentes initiatives telles que la directive NIS, déjà citée, mais également le *Cybersecurity Act*[388], le Règlement eIDAS[389] ou encore la Directive PSD2[390] qui

388. 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) (ci-après « *Cybersecurity Act* »).

389. Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. A ce sujet, lire D. GOBERT, « L'identification électronique et les services de confiance dans le règlement eIDAS », *J.D.E.*, 2016/7, n° 231, p. 250-258 ; H. JACQUEMIN, « Principes applicables à tous les services de confiance et au document électronique » publié dans *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Éditions Larcier, 2016, p. 101-137 ; J.-B. HUBIN, « Le cachet électronique des personnes morales » publié dans *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Bruxelles, Éditions Larcier, 2016, p. 175-202.

390. Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (Texte présentant de l'intérêt pour l'EEE). A ce sujet, lire D. PHILIPPE, « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche », *Actualités en droit commercial et bancaire*, Bruxelles, Éditions Larcier, 2017, p. 455-477.

dépassent le cadre de la présente contribution[391]. Selon le champ d'application de ces instruments[392], les débiteurs de l'obligation de sécurité de traitements de données à caractère personnel devront toutefois en tenir compte, tant en ce qui concerne les mesures techniques et organisationnelles à mettre en œuvre qu'en termes de notification en cas de violation de sécurité[393]. En guise d'exemples, le Groupe 29 indique qu'un « cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach »[394].

Ayant rappelé cette tendance, l'objectif de notre texte est avant tout de mettre l'accent sur l'avènement d'un « nouveau » principe de base étroitement lié à l'exigence d'*accountability*. Outre les obligations de notification et de communication en cas de fuite de données, en attestent le fait, d'une part, que tous les responsables de traitements et sous-traitants doivent tenir un Registre dès lors que leurs traitements ne sont pas occasionnels[395] mentionnant, dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles et, d'autre part, qu'une évaluation des risques inhérents doit être documentée qu'il y'ait ou non obligation de procéder (ou d'aider à la réalisation) d'une AIPD ; laquelle doit, du reste, être réalisée dans de nombreux cas.

Force est de constater que la volonté du législateur se matérialise en pratique puisque, depuis le 25 mai 2018, des autorités de protection des données nationales n'ont pas hésité à sanctionner des manquements à l'obligation de sécurité ; et ce tant dans le secteur public que dans le secteur privé.

Ainsi, en ce qui concerne le secteur public, le 18 février 2019, l'autorité de contrôle maltaise a prononcé une amende de 5.000 euros à l'encontre de l'autorité foncière nationale après avoir mené une enquête sur une fuite de données portée à son attention par le *Times of Malta*. Les conclusions de l'enquête ont établi que la plateforme de demande en ligne disponible sur le portail de l'autorité n'était pas assortie de mesures techniques et organisationnelles nécessaires pour assurer la sécurité du traitement. Le montant de l'amende a été fixé après que le commissaire ait tenu compte des circonstances énoncées à l'article 83, § 2

391. Sans oublier le « Règlement e-Privacy » en cours de négociations. Voy. Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE, 2017/0003 (COD).
392. Nous ne prétendons à aucune exhaustivité dans l'énumération des régimes légaux potentiellement applicables selon le contexte.
393. Groupe 29, *WP250*, *op. cit.*, pp. 28 et 29.
394. *Ibid.*
395. A cet égard, lire Groupe 29, « Position paper on the derogations from the obligation to maintain records of processing activities pursuant to article. 30(5) GDPR », adopté le 19 avril 2018.

du RGPD[396], y compris le fait que l'autorité foncière ait offert au commissaire toute sa collaboration, sans restriction, tout au long de l'enquête[397].

Dans une seconde affaire, le 4 mars 2019, l'autorité norvégienne de protection des données (la *Datatilsynet*) a infligé une amende administrative de 1,6 million de couronnes norvégiennes, soit l'équivalent de 170.000 euros, à la commune de Bergen. L'incident avait pour objet des noms d'utilisateurs et des mots de passe de plus de 35.000 comptes du système informatique de la municipalité concernant à fois les élèves des écoles primaires et les employés des mêmes écoles. En raison de l'insuffisance des mesures de sécurité, ces données n'étaient pas protégées et étaient donc librement accessibles. Le fait que la violation de sécurité concerne un grand nombre de personnes dont la majorité était des enfants a été considéré comme un facteur aggravant. La municipalité avait également été avertie à plusieurs reprises, à la fois par l'autorité et par un lanceur d'alerte interne, que la sécurité des données était insuffisante[398]. Relevons qu'en Belgique, l'article 221, § 2 de la loi du 30 juillet 2018[399] dispose que des amendes administratives ne peuvent être prononcées à l'égard des autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché[400]. Toutefois, en cas de manquement à l'obligation de sécurité par une autorité publique, l'APD dispose d'une large panoplie d'autres mesures correctrices[401] et des amendes pénales peuvent être prononcées à leur encontre par les juridictions[402].

Pour ce qui est du secteur privé, le 21 mars 2019, l'autorité de contrôle hongroise a infligé une amende administrative de 11 millions de HUF (environ 35.000 euros) à un parti hongrois, la Coalition Démocratique (DK). L'autorité hongroise avait été prévenue par un citoyen qu'une base de données contenant les données personnelles des membres et sympathisants du parti était accessible via un forum pirate. Les données impliquées contenaient les adresses électroniques des utilisateurs, leurs noms complets, leurs *logins* ainsi que leurs mots de passe faiblement protégés (MD5). Ces données avaient été rendues accessibles sur ce forum de pirates informatiques suite à une attaque rendue possible à

396. Voy. également Groupe 29, « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 », *WP253*, 3 octobre 2017.
397. Voir le communiqué de presse de l'IDPC du 18 novembre 2019, disponible à l'adresse suivante : https ://idpc.org.mt/en/Press/Pages/Lands-Authority-Personal-Data-Breach.aspx
398. « Le système en question contenait des informations sur le nom d'un utilisateur, son mot de passe, sa date de naissance, son adresse, son affiliation scolaire et son niveau scolaire. Lorsque les employés et les élèves se connectaient, ils avaient accès à divers systèmes, par exemple la plate-forme d'apprentissage numérique, qui contient le travail scolaire des élèves et les évaluations des enseignants sur les performances de chaque élève à l'école ». Voy. https ://edpb.europa.eu/news/national-news/2019/administrative-fine-eu170000-imposed-bergen-municipality_fr.
399. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.
400. Cette disposition fait l'objet d'un recours par la FEB devant la Cour constitutionnelle pour discrimination. Voy. https ://www.lecho.be/economie-politique/belgique/general/la-feb-attaque-le-rgpd-pour-discrimination/10106223.html.
401. RGPD, art. 58, § 2.
402. Loi du 30 juillet 2018, art. 222.

cause d'une vulnérabilité SQLi sur la page Web du parti. DK était au courant de la violation de données, puisque le pirate les en avait avertis, mais n'avait pas encore notifié ni communiqué celle-ci conformément aux articles 33 et 34 du RGPD. L'APD hongroise a considéré comme circonstance aggravante le fait que les données impliquées constituaient des catégories particulières de données révélant des opinions politiques et que DK utilisait une méthode de protection obsolète (MD5) pour les mots de passe. Ces deux circonstances engendraient un risque élevé pour les droits et libertés des personnes concernées, car la disponibilité publique de ces données pouvait entraîner d'autres violations de services en ligne utilisés par les utilisateurs[403].

Dans une seconde affaire, le 21 mai 2019, l'autorité de contrôle lituanienne a infligé une amende administrative de 61.500 euros à MisterTango UAB – une société de paiements électroniques – pour une violation de données à caractère personnel dans le système de paiement qui n'avait pas été signalée à l'autorité de contrôle. Après avoir mené l'enquête, l'autorité a déterminé que la société avait traité des données bancaires sur des copies d'écran non chiffrées rendues publiques pendant deux jours. Lors de la fixation de l'amende, le chiffre d'affaires mondial annuel total de la société a été pris en compte.

Dans un troisième cas, le 7 juin 2019, l'autorité de contrôle italienne a rendu une décision contre l'un des principaux fournisseurs de services de messagerie en Italie suite à une enquête ouverte après que la société eut notifié l'autorité d'une violation de données. Dans cette notification, la société avait déclaré que des mesures de détection d'incidents avaient permis de repérer, le 20 février, des accès frauduleux via un point d'accès WiFi. Ces accès frauduleux affectaient environ un million et demi de données d'authentification de courrier électronique appartenant à des utilisateurs ayant accédé au service de messagerie. Pour tenter de limiter les conséquences de la violation de données, la société avait « obligé » les utilisateurs à réinitialiser leurs mots de passe et mis en ligne une page Web contenant des informations sur la violation de données avant d'envoyer par courrier électronique une communication à tous les utilisateurs concernés. Cette communication s'est révélée être en deçà des exigences du RGPD car la société avait envoyé deux communications différentes selon que l'utilisateur en question avait changé de mot de passe ou non dans les 48 heures suivant la publication des informations sur la violation de données. Dans les deux cas, la communication faisait référence à des « activités inhabituelles dans nos systèmes informatiques » et les utilisateurs qui avaient changé leurs mots de passe n'avaient pas été invités à prendre des mesures supplémentaires, car il avait été déclaré que le mot de passe modifié avait rendu les anciens identifiants inutiles. À l'inverse, les utilisateurs qui n'avaient pas modifié leur mot de passe n'avaient été invités à le faire que pour « éliminer le risque d'accès non autorisé à votre compte de messagerie ». Le Garante (l'APD italienne) a estimé que ces informations étaient insuffisantes compte tenu des risques élevés auxquels les utilisateurs étaient exposés et a ordonné à la société de réitérer la communication de la violation de données aux utilisateurs concernés, en décrivant le type de violation et ses conséquences possibles et en fournissant aux utilisateurs des indications

403. Voy. https ://edpb.europa.eu/news/national-news/2019/hungarian-sa-investigation-regarding-data-breach-democratic-coalition-dk_fr.

précises sur les mesures à prendre pour éviter des risques supplémentaires, telles que ne pas utiliser les informations d'identification affectées et modifier les mots de passe pour accéder à tout autre service en ligne si ces mots de passe étaient identiques ou similaires à ceux qui avaient été violés[404].

Dans une quatrième affaire, le 26 juin 2019, l'APD roumaine a infligé une amende administrative de 613.912 lei, soit 130.000 euros, à Unicredit Bank S.A. suite à une violation de données contenant le numéro d'identification personnel et l'adresse du payeur de 337.042 personnes concernées. Ce qui a été reproché à la banque était l'absence de mise en œuvre des mesures techniques et organisationnelles appropriées, tant pour la détermination des moyens de traitement que pour les opérations de traitement elles-mêmes, conçues pour rendre efficaces les principes de protection des données[405]. Un mois plus tard, le 2 juillet 2019, suite à une notification d'une violation, l'APD roumaine achevait une enquête à l'égard de World Trade Center Bucharest S.A. et condamnait ce responsable à une amende administrative de 71.028 lei, soit l'équivalent de 15.000 euros. La violation consistait dans le fait qu'une liste imprimée utilisée pour contrôler les clients de l'hôtel participant au petit-déjeuner avait été photographiée par des personnes extérieures à la société et divulguée en ligne par la suite. Dans sa décision, l'autorité a estimé que le responsable n'avait pris aucune mesure visant à garantir que ses employés ayant accès aux données à caractère personnel ne traitent celles-ci que sur instructions dudit responsable[406]. Quelques jours plus tard, le 5 juillet 2019, la même APD roumaine a condamné Legal company & Tax hub SRL, à une amende de 14.173,50 lei, soit l'équivalent de 3.000 euros suite à une violation de données ayant conduit à la divulgation et à l'accès non autorisés des noms, prénoms, adresses postales, e-mails, téléphones, professions, détails des transactions effectuées par les personnes concernées sur le site Web avocatoo.ro.

Le lecteur se souviendra également de l'intention de l'autorité de contrôle britannique d'infliger des amendes administratives à British Airways[407] et Mariott International[408].

Enfin, dans une dernière affaire, le 20 septembre 2019, suite à une fuite de données concernant environ 2,2 millions de personnes, la DPA polonaise a infligé une amende de 2,8 millions de zlotys (environ 645.000 euros) à Morele.net, un site d'e-commerce, en considérant que les mesures techniques et organisationnelles prises par la société n'étaient pas adaptées au risque. Dans le cas d'environ 35.000 personnes, les données en question concernaient leur demande de prêt à tempérament et comprenaient leur numéro d'identification personnel, le numéro de la pièce d'identité, leurs études, l'adresse de facturation,

404. Voy. https ://edpb.europa.eu/news/national-news/2019/italian-sa-users-must-receive-specific-helpful-information-case-data-breach_fr.
405. Voy. https ://edpb.europa.eu/news/national-news/2019/first-fine-romanian-supervisory-authority_fr.
406. Voy. https ://edpb.europa.eu/news/national-news/2019/second-fine-romanian-supervisory-authority_fr.
407. Voy. https ://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.
408. Voy. https ://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

l'adresse de correspondance, la source de revenus, le montant du revenu net, le coût de la vie du ménage, le statut matrimonial ainsi que le montant des engagements de crédit ou des obligations alimentaires. Dans sa décision, l'autorité de contrôle a souligné que le risque d'effets néfastes sur les personnes concernées était particulièrement important, pouvant potentiellement conduire à des vols d'identité. L'enquête a révélé que l'infraction était due à une évaluation inadéquate des risques inhérents. Selon l'APD polonaise, des procédures de réponse appropriées pour faire face à l'émergence d'un trafic réseau inhabituel faisaient défaut et des mesures insuffisantes d'authentification d'accès avaient été mises en place. Pour déterminer le montant de l'amende, l'autorité de contrôle a toutefois tenu compte de circonstances atténuantes, telles que : les mesures prises par la société pour mettre fin à l'infraction, la bonne coopération avec le responsable du traitement et le fait que la société n'avait pas violé le RGPD auparavant[409].

Les exemples susmentionnés ne sont évidemment pas exhaustifs et notre APD nationale n'est d'ailleurs pas en reste[410]. Ces décisions confortent 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.

409. Voy. https ://edpb.europa.eu/news/national-news/2019/polish-dpa-imposes-eu645000-fine-insufficient-organisational-and-technical_fr.

410. Voy., par exemple, https ://www.autoriteprotectiondonnees.be/news/les-autorites-de-protection-des-donnees-belges-et-allemandes-collaborent-sur-le-dossier-Mastercard.