Cybersécurité, vie privée, imputabilité, journalisation et log files

Dumortier, Franck

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

Publication date:
2019

Document Version
le PDF de l'éditeur

CYBERSÉCURITÉ, VIE PRIVÉE, IMPUTABILITÉ, JOURNALISATION ET LOG FILES

Franck Dumortier[906]

A. Introduction

Dans le contexte actuel de l'Internet des Objets, du Cloud Computing, du Big Data[907], et plus généralement de l'interconnexion ascendante des systèmes, l'ampleur, la fréquence et l'impact des incidents de cybersécurité ne cessent de croître[908]. La sécurité des données informatiques – en ce compris celle des données à caractère personnel au sens large[909] – est ainsi devenue un enjeu majeur, non seulement pour garantir le respect du droit fondamental à la vie privée mais également afin de préserver la confiance des consommateurs et des citoyens dans les réseaux, systèmes et produits ICT dont la fiabilité est essentielle à leur vie économique et sociétale. Qu'il y ait ou non traitement de données à caractère personnel, on enseigne que la sécurité de l'information[910] a pour objectifs principaux d'assurer la confidentialité, l'intégrité et la disponibilité des données[911]. Pour rappel, la confidentialité est la propriété d'une information de ne pouvoir être accédée que par des personnes, entités ou processus autorisés et de ne pouvoir être divulguée qu'à ceux-ci. L'intégrité consiste en sa garantie de ne pouvoir être altérée ou détruite de manière non autorisée, volontairement ou accidentellement. La disponibilité renvoie, quant à elle, à la

---

906. 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.

907. A propos du Big Data et de l'importance de la journalisation dans ce contexte, lire F. DUMORTIER et B. DESCAMPS, « Interconnexions et cybersécurité », in *Revue du Droit des Technologies de l'information*, n°70, 2018, pp. 31-52.

908. Pour un aperçu récent du phénomène, *voy.* ENISA, « Threat Landscape Report 2018 – Final version », janvier 2019, p.64 et *s.*

909. Voyez la définition large de « données à caractère personnel » prônée par le Groupe 29 dans son « Avis 4/2007 sur le concept de données à caractère personnel », *WP136*, 20 juin 2007. Lire également K. ROSIER, « La notion de 'donnée à caractère personnel' a-t-elle encore un sens dans la protection des données de communications électroniques ? », in *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde – Liber Amicorum Yves Poullet*, Larcier, 2018, pp.699-714.

910. Selon 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* » *in* EDPS, *Security Measures for Personal Data Processing – Guidance on Security Measures for Personal Data Processing – Art. 22 of Regulation 45/2001*, 21 mars 2016, p. 5.

911. S. GHERNAOUTI, *Sécurité informatique et réseaux*, Dunod, 2013, p. 1

propriété des informations, systèmes et processus d'être accessibles et utilisables à la demande d'une entité autorisée[912].

Les trois propriétés de cybersécurité susmentionnées doivent néanmoins être comprises comme étant « des finalités de base auxquelles s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification) et, d'autre part, l'existence d'une action (notion de non-répudiation d'une transaction, voire d'imputabilité) »[913]. En effet, vu le nombre d'intervenants, d'équipements et de processus impliqués dans les environnements numériques, des mesures permettant d'imputer adéquatement les responsabilités en cas d'incident s'avèrent extrêmement utiles afin d'en identifier l'origine ainsi que pour permettre aux personnes lésées d'exercer leurs droits en cas de dommage. Pour ces raisons, les principaux standards internationaux en matière de sécurité informationnelle – dont la suite ISO 27xxx[914] – considèrent qu'outre les trois critères de sécurité classiques[915] s'ajoutent d'autres propriétés, parmi lesquelles l'imputabilité « qui permet de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité) »[916].

De manière pragmatique, c'est l'activité de journalisation qui concrétise cette propriété d'imputabilité. Celle-ci consiste 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, etc.), à la manière d'un journal de bord, dans des fichiers appelés *log files*[917]. Un *log file* ou encore « fichier journal » est un fichier enregistrant une ligne de code par évènement ayant lieu dans un système d'information ou un réseau. Les données composant une entrée de *log file* incluent notamment le type d'évènement, la date et le moment exact de sa réalisation ainsi que des données permettant d'en identifier l'auteur. Ces *log files* peuvent être générés par de multiples applications, comme, par exemple, un système d'exploitation, un antivirus, un *firewall*, un système de détection d'intrusion ou de prévention, et, de manière plus générale, par n'importe quel programme installé sur un serveur, un ordinateur ou un équipement de réseautique[918].

Récemment, les trois propriétés classiques de sécurité informationnelle ont été légalement renforcées, notamment suite à l'adoption du Règlement général sur la protection des données[919] (ci-après « RGPD »), de la directive sur la sécurité des réseaux et des systèmes d'information[920] (ci-après « directive NIS ») et du *Cybersecurity Act*[921]. Dans cette contribution, après avoir rappelé qu'au contraire du RGPD [Point B.], les deux autres instruments cités prévoient explicitement la mise en œuvre de mesures de journalisation [Point C.], nous verrons néanmoins que, selon le risque identifié « pour les droits et libertés des personnes concernées »[922], une telle mesure de sécurité est fortement recommandée non seulement afin de rendre effective la protection des données à caractère personnel mais également afin de satisfaire à l'exigence d'*accountability*[923] [Point D.]. Enfin, les données de journalisation étant elles-mêmes qualifiables de données à caractère personnel, nous examinerons les conditions de leur traitement (stockage, accès, transmission, etc.) à l'aune des préceptes du RGPD, notamment en termes de licéité, de transparence, de finalité, de minimisation, de limitation de la conservation des données, de sécurité et de droit d'accès des personnes concernées [Point E.].

912. Ces définitions sont fournies par l'Autorité de protection des données (APD) dans sa « Note relative à la sécurité des données à caractère personnel », p. 2, disponible à l'adresse suivante : https ://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/note_securite_des_donnees_a_caractere_personnel.pdf. Dans sa note, l'APD s'inspire explicitement de la norme ISO/IEC 13335-1 :2004, depuis lors remplacée par la suite ISO 27xxx.

913. S. GHERNAOUTI, *op. cit.*, p. 1.

914. Les normes ISO sont établies par l'organisation internationale de normalisation. La famille de normes ISO 27xxx (ISO/IEC 27000 :2018 Information technology — Security techniques — Information security management systems – Overview and vocabulary) en matière de gestion de la sécurité de l'information (ISO/IEC 27001 :2013 Information technology — Security techniques — Information security management systems — Requirements (second edition) et de diverses implémentations (ISO 27002 – ISO 27017 – ISO 27018…) est considérée comme une véritable référence dans le domaine.

915. L'ISO 27000 insiste particulièrement sur le triptyque « Disponibilité – Intégrité – Confidentialité » mais mentionne également *« in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved »*.

916. APD, « Note relative à la sécurité des données à caractère personnel », *op. cit.*, p. 2.

917. S. GHERNAOUTI, *op. cit*, p. 6.

918. National Institute of Standards and Technology (NIST), « Guide to Computer Security Log Management », Septembre 2006, p. 9.

919. 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 »).

920. Directive (UE) 2016/1148 du Parlement Européen et du conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

921. 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).

922. RGPD, art. 32.1.

923. 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.

B. La journalisation non expressément prévue par le RGPD

Ainsi que nous l'avons rappelé dans notre première contribution[924], une innovation remarquable du RGPD est qu'il érige les principes « d'intégrité et de confidentialité »[925] 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). En cette matière, les articles 32 et suivants du RGPD s'appliquent tant aux entreprises privées qu'aux administrations publiques lorsqu'elles agissent comme « responsables du traitement » ou « sous-traitants »[926], tous deux considérés comme débiteurs de l'obligation de sécurité sous l'empire du RGPD[927]. Par conséquent, ceux-ci doivent évaluer le risque de leurs traitements pour les droits et libertés des personnes physiques afin de mettre en œuvre des mesures de sécurité appropriées[928]. Lors de l'évaluation du niveau de sécurité approprié, ces débiteurs doivent tenir compte « en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite »[929]. Au regard des risques identifiés, des

924. Voy. la contribution de F. DUMORTIER dans cet ouvrage, « Les obligations de sécurité et de notification des violations des traitements de données à caractère personnel » (Chap. 1).

925. Bien que l'intitulé de l'article 5.1, f), du RGPD n'érige expressément au rang de principe que l'intégrité et la confidentialité des données à caractère personnel, le Groupe 29 considère que la disponibilité de celles-ci fait partie « des trois critères de sécurité classiques » que leur traitement doit respecter. A ce propos, lire F. DUMORTIER, « La sécurité des traitements de données, les analyses d'impact et les violations de données » in *Le règlement général sur la protection des données (RGPD/GDPR) : analyse approfondie,* sous la coordination de K. ROSIER et C. DE TERWANGNE, Larcier, pp. 152 et s.

926. Lire Groupe 29, « Avis 1/2010 sur les notions de 'responsable du traitement' et de 'sous-traitant' », *WP169*, adopté le 16 février 2010. Lire également 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

927. Des dispositions spécifiques sont prévues pour les activités de traitement effectuées par les « autorités compétentes » dans le domaine de la prévention et la détection des infractions pénales, à savoir les articles 29 et suivants de la directive 2016/680/UE (ci-après « directive Police & Justice ») tels que transposés dans le titre II de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi du 30 juillet 2018, *M.B.*, 5 septembre 2018, p. 68616). Dans la même logique, dans l'exercice de leurs missions, les services de renseignement et de sécurité sont soumis à un régime dérogatoire inscrit au titre III de la loi du 30 juillet 2018.

928. RGPD, art. 32.1.

929. *Ibid.*, art. 32.2. En ce qui concerne le vocabulaire utilisé, la notion de « traitements non-autorisés » semble couvrir les circonstances dans lesquelles des données sont traitées « sans droit » par des tiers, des destinataires externes ou par des personnes placées sous l'autorité directe du responsable du traitement ou du sous-traitant. Les termes « de manière accidentelle ou illicite » renverraient, quant à eux, aux traitements « non autorisés » réalisés respectivement de manière purement accidentelle ou de manière intentionnelle.

mesures – telles que le chiffrement, des antivirus, des *firewalls* ou encore des systèmes de détection et de prévention d'intrusion – doivent donc être prises.

En ce qui concerne la nature des mesures de sécurité devant être mises en œuvre, le RGPD en distingue deux types : d'une part, les mesures techniques, d'autre part, les mesures organisationnelles. En guise d'illustrations, l'article 32 du RGPD énumère, de manière non exhaustive, des mesures qui peuvent être envisagées « y compris entre autres, selon les besoins »[930], à savoir : « [...] des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; et, une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ». Si, entre les lignes, on peut entrevoir que la journalisation puisse être envisagée, celle-ci n'est pas expressément mentionnée par le Règlement[931], bien que l'autorité de protection des données fédérale (ci-après « APD ») la considère comme un exemple de mesure technique[932] qui semble être recommandée pour tout traitement de données à caractère personnel[933].

Outre le catalogue indicatif de mesures contenues en son article 32, le RGPD prévoit une marge de manœuvre pour les États Membres qui « peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement

930. RGPD, art. 32.1.

931. Bien que la propriété d'imputabilité ne soit pas expressément consacrée par le RGPD, la journalisation est imposée par d'autres instruments législatifs en matière de protection des données à caractère personnel ; parfois en raison de la sensibilité du contexte qu'ils régulent, parfois de manière plus horizontale. Il en va ainsi, par exemple, dans le cadre de la directive Police & Justice dont l'article 25 impose aux États membres de prévoir « que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel ». Ces journaux ne peuvent être utilisés qu'à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales. Par ailleurs ceux-ci doivent être mis à la disposition de l'autorité de contrôle lorsqu'elle les demande. Quasi mot pour mot, la même exigence de journalisation est introduite par l'article 88 du Règlement 2018/1725 régissant l'utilisation des données à caractère personnel par les institutions et organes de l'UE, à la différence près que ce texte précise sa durée de conservation : *« ces journaux sont effacés au bout de trois ans, sauf s'ils demeurent nécessaires à un contrôle en cours »*.

932. APD, Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données, n° 01/2018, 28 février 2018, p. 24.

933. APD, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 4,

des données génétiques, des données biométriques ou des données concernant la santé »[934] ainsi que prévoir « des garanties appropriées pour les droits et libertés des personnes concernées » lors du traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions[935]. Le législateur belge a fait usage de ces prérogatives dans les articles 9 et 10 de la loi du 30 juillet 2018 en imposant au responsable du traitement ou, le cas échéant, au sous-traitant, « de désigner les catégories de personnes ayant accès aux données à caractère personnel [...] avec une description précise de leur fonction par rapport au traitement des données visées »[936], de tenir à disposition de l'APD « la liste des catégories des personnes ainsi désignées »[937], et de veiller « à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées ».[938] Ces exigences supplémentaires de sécurité informationnelle requises lors du traitement de données « sensibles » ou « judiciaires » s'apparentent à des mesures de « sécurisation logique des accès » consistant, selon l'APD, à « 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 »[939]. Afin de protéger les consommateurs de services prestés, par exemple, par des professionnels de la santé ou par des avocats, une liste actualisée des différentes personnes habilitées à accéder et traiter leurs données sensibles et de leurs pouvoirs respectifs (création, consultation, modification, destruction) doit donc être tenue à jour[940]. Relevons néanmoins que la mesure de contrôle d'accès logique n'équivaut pas *stricto sensu* à celle de la journalisation puisque la première n'impose pas l'enregistrement d'évènements afin de « de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci »[941]. D'autres législateurs européens ont pourtant explicitement prévu la journalisation dans leurs lois d'implémentation nationales en exerçant les mêmes prérogatives laissées à leur appréciation. Il y va par exemple, dans la loi allemande[942] et dans la loi irlandaise[943]. Quoi qu'il en soit, rappelons toutefois que, compte tenu de leur nature, lorsque des données relatives à la santé sont traitées, la journalisation est fortement

934. RGPD, art. 9.4.
935. *Ibid.*, art. 10.
936. Loi du 30 juillet 2018, Titre 1er, art. 9 et 10.
937. *Ibid.*
938. *Ibid.*
939. APD, « Mesures de référence applicables à tout traitement de données à caractère personnel – version 1.0 », p. 4, disponible à l'adresse https ://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf.
940. *Ibid.*
941. *Ibid.*
942. Section 22(2), 12) of Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 of 30 June 2017 (DSAnpUG-EU).
943. Data Protection Act 2018, art. 36(1), (e), (i).

recommandée tant par le Conseil de l'Europe[944] que par le Groupe 29[945]. À cet égard, la Cour européenne des droits de l'homme a également eu l'occasion de mettre en exergue que la législation interne doit « ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention »[946].

C. La journalisation prévue par la directive NIS et le Cybersecurity Act

Qu'il y ait ou non traitement de données à caractère personnel, la directive NIS – dont la loi de transposition a été adoptée le 7 avril 2019[947] – a pour objectif d'affermir la résilience des réseaux et des systèmes d'information d'entités fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques. Son but est d'accroître la confiance de la population dans les réseaux et systèmes d'intérêt général pour la sécurité publique dans les secteurs de l'énergie, des transports, des finances, des soins de santé, de la distribution d'eau potable et de l'infrastructure numérique ainsi que dans l'utilisation de places de marché en ligne, de moteurs de recherche ou encore de services d'informatique en nuage. Par conséquent, les articles 14 et 16 de cette directive imposent aux opérateurs de services essentiels[948] (ci-après « OSE ») et aux fournisseurs de services numériques[949] (ci-après « FSN ») des obligations de cybersécurité pour éviter les inci-

944. Conseil de l'Europe, Recommandation n° R (97) 5 du Comité des ministres aux États membres relative à la protection des données médicales, adoptée le 13 février 1997 contient en son point 9 une imposante énumération des mesures qui devraient être prises pour assurer un niveau de sécurité approprié compte tenu, d'une part, de l'état de la technique et, d'autre part, de la nature sensible des données médicales et de l'évaluation des risques potentiels : contrôle à l'entrée des installations, contrôle des supports de données, contrôle de mémoire, contrôle de l'utilisation, contrôle d'accès, contrôle du transport, contrôle de disponibilité mais également des mesures appropriées devraient être prises visant « à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication) » et « à garantir qu'il puisse être vérifié et constaté a posteriori qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction) ».
945. Dans son document de travail sur les dossiers médicaux électroniques, le Groupe 29 indique que le cadre juridique concernant les mesures de sécurité devrait prévoir, en particulier, la *nécessité* « d'un système fiable et efficace d'identification et d'authentification électroniques ainsi que de registres constamment mis à jour pour vérifier si les personnes qui ont ou demandent l'accès au système de DME disposent de l'autorisation nécessaire » et de « de l'enregistrement et de la documentation exhaustifs de toutes les étapes de traitement qui ont eu lieu dans le système, en particulier les demandes d'accès pour lecture ou écriture, assortis de contrôles internes réguliers et du contrôle de l'authenticité de l'autorisation » (Groupe 29, « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) », *WP 131*, 15 février 2007, p. 22).
946. Cour eur. D.H., 17 juillet 2008, *I. v. Finlande*, req. n° 20511/03, § 95.
947. Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019.
948. Voy. Chap. 2, D.1, Notion d'OSE.
949. Voy. Chap. 2, E., Réseaux et systèmes d'information des fournisseurs de service numérique.

dents[950] et réduire au minimum l'impact de ceux-ci sur la continuité de leurs services[951]. De plus, les OSE et les FSN doivent notifier les incidents ayant un impact significatif sur la continuité de leurs services aux autorités compétentes[952]. Bien que la directive NIS n'impose pas explicitement la journalisation aux entités concernées[953], son règlement d'exécution[954] contraint les FSN « au contrôle de l'accès aux réseaux et systèmes d'information, c'est-à-dire la disponibilité d'une série de mesures visant à garantir que l'accès physique et logique aux réseaux et aux systèmes d'information, y compris la sécurité administrative de ceux-ci, est autorisé et limité en fonction d'exigences commerciales et de sécurité »[955] et à mettre en œuvre des « des processus et procédures de détection maintenus et contrôlés afin d'assurer en temps voulu la bonne connaissance des évènements anormaux »[956]. Dans la même perspective, dans son document de référence sur les mesures de sécurité pour les OSE[957], le Groupe de Coopération NIS recommande à ces derniers de configurer un système de journalisation *« in order to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the CIS and which covers application servers that support critical activities ; system infrastructure servers ; network infrastructure servers ; security equipments ; engineering and maintenance stations of industrial systems ; network equipments ; administrative workstations. The operator records through the logging system events with time and date-stamping using synchronised time sources and centralises archives for at least half-a-year »*[958]. Le Centre pour la Cybersécurité Belgique recommande comme

950. Dans le contexte de la directive NIS, un « incident » est défini comme étant « *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information* », même en l'absence de traitements de données à caractère personnel.

951. Les exigences en matière de sécurité et de notification prévues par la directive NIS ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 13*bis* et 13*ter* de la Directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, transposée en droit belge par les articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques. Il en va de même pour les prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement européen (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

952. Voy. l'article 8 de la directive NIS.

953. On peut noter que le considérant 46 de la directive NIS précise que « parmi les mesures de gestion des risques figurent celles permettant d'identifier tous les risques d'incidents, de prévenir, de repérer et de gérer les incidents et d'en atténuer l'impact. La sécurité des réseaux et des systèmes d'information inclut la sécurité des données stockées, transmises et traitées ».

954. Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

955. Règlement d'exécution (UE) 2018/151, art. 2.1, d).

956. *Ibid.*, art. 2.2, a).

957. NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, Publication 01/2018 (February 2018), https ://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

958. *Ibid*, p. 22.

mesures minimales à mettre en place la mise en œuvre de mesures « pour le contrôle des opérations : accès, stockage destruction, accès à distance, et *logging* »[959].

Quant à la loi NIS, elle précise que, sauf preuve contraire, l'OSE bénéficie d'une présomption de conformité du contenu de sa politique de sécurité de ses systèmes et réseaux d'information (PSI), « lorsque les mesures de sécurité qu'elle comporte répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi, par arrêté délibéré en Conseil des ministres »[960]. Or, comme nous le verrons plus loin, la journalisation fait partie intégrante des préceptes édictés par la suite ISO 27xxx.

Le *Cybersecurity Act* a pour vocation de compléter les exigences de sécurité du RGPD et de la directive NIS qui ne s'adressent pas explicitement aux fabricants de matériel ni aux développeurs de logiciels[961]. Ainsi, ce règlement – qui renforce le mandat de l'ENISA[962] – établit un cadre européen de certificats de cybersécurité pour les produits, les processus et les services ICT qui seront valables dans toute l'UE. L'objectif de la certification est de promouvoir la confiance des consommateurs en l'Internet des Objets en renforçant par défaut (« *security by default* »[963]) la sécurité des appareils connectés dès les premières phases de leur conception (« *security by design* »[964]). Tout comme le système d'étiquetage des produits alimentaires de l'UE permet aux consommateurs d'en savoir davantage sur la qualité de ce qui est dans leur assiette, les nouveaux certificats européens de cybersécurité ont pour but de garantir une certaine transparence quant à la fiabilité de milliards de dispositifs qui pilotent dorénavant les infrastructures critiques, tels que les réseaux d'énergie et de transport, mais

959. Centre pour la Cybersécurité Belgique, *Baseline Information Security Guidelines (BSG) Édition 2018*, Bruxelles, CCB, 2018, 4.2. Organisation de la sécurité, p. 15, https ://www.ccb.belgium.be/sites/default/files/Baseline%20Information%20Security%20Guidelines%20FR.pdf

960. Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *op. cit.*, art. 22.

961. Néanmoins, le considérant 78 du RGPD stipule que « lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics ». Dans le même sens, le considérant 50 de la directive NIS mentionne « Alors que les fabricants de matériel et les développeurs de logiciels ne sont pas des opérateurs de services essentiels ou des fournisseurs de service numérique, leurs produits renforcent la sécurité des réseaux et des systèmes d'information. Dès lors, ils jouent un rôle important en permettant aux opérateurs de services essentiels et aux fournisseurs de service numérique de sécuriser leurs réseaux et systèmes d'information. Ce matériel et ces logiciels font déjà l'objet de règles existantes sur la responsabilité du fait des produits ».

962. Pour rappel, l'ENISA est l'Agence Européenne chargée de la sécurité des réseaux et de l'information, telle que régie par le Règlement (UE) no 526/2013.

963. *Cybersecurity Act,* consid. 13 et art. 51(i).

964. *Ibid.*, consid. 12 et art. 51(i).

aussi de nouveaux équipements grand public, tels que les voitures, montres ou frigos connectés. En principe, la certification est réalisée sur une base volontaire, sauf disposition contraire du droit de l'Union ou du droit des États membres[965]. Il existe trois niveaux d'assurance différents : élémentaire, substantiel ou élevé[966]. Au niveau élémentaire, les fabricants ou les fournisseurs de services peuvent effectuer eux-mêmes l'évaluation de conformité[967]. Dans les autres cas, l'intervention d'organismes accrédités – et parfois même celle d'une autorité nationale de certification en cybersécurité – est requise[968]. Parmi les objectifs de sécurité du système européen de certification, le *Cybersecurity Act* prévoit ceux de « garder une trace des données, fonctions ou services qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui »[969] et d'être en mesure « faire en sorte qu'il soit possible de vérifier quel(le)s données, services ou fonctions ont été consultés, utilisés ou traités de toute autre façon, à quel moment et par qui »[970]. Étant donné qu'à l'ère de l'Internet des Objets, ces fonctions de journalisation devront être implémentées dans un nombre grandissant de produits, il va sans dire que la quantité des *log files* risque de s'accroître exponentiellement. Un consommateur pourrait, par exemple, y voir une opportunité pour identifier les personnes ayant accédé illégitimement aux données qu'il a communiquées à son enceinte intelligente afin d'entamer un recours en responsabilité.

Le RGPD, la directive NIS et le *Cybersecurity Act* s'appliquent de manière cumulative lorsque leurs champs d'application matériels se rencontrent. Ainsi, un opérateur de *cloud* considéré comme sous-traitant au sens du RGPD sera aussi qualifié de fournisseur de services numériques et devra, par conséquent, également respecter les prescrits de la directive NIS, à moins qu'il ne s'agisse d'une microentreprise ou d'une petite entreprise telle que définie dans la recommandation 2003/361/CE de la Commission[971]. Cet exemple illustre d'ailleurs une certaine aberration, l'importance d'un incident n'étant pas forcément liée au chiffre d'affaires ou au nombre de personnes occupées par une société[972]. Heureusement, l'opérateur du cloud en question ne pourra toutefois pas écarter sa responsabilité découlant de l'application du RGPD en arguant du simple fait qu'il n'a pas connaissance du traitement des données à caractère personnel qu'il héberge[973]. Par conséquent, il sera tenu de notifier au responsable du traitement toute violation de données à caractère personnel « dans les meilleurs délais après en avoir pris connaissance »[974]. Dans

965. *Ibid.*, art. 56. A cet égard, la Commission européenne peut identifier si des régimes particuliers doivent être rendus obligatoires par la législation de l'Union, en particulier dans les secteurs visés par l'Annexe II de la directive NIS.
966. *Cybersecurity Act*, art. 56.
967. *Ibid.*, art. 53.
968. *Ibid.*, art. 56.
969. *Ibid.*, art. 51(e).
970. *Ibid.*, art. 51(f).
971. Directive NIS, art. 16.11.
972. Notons néanmoins que l'article 20 de la directive NIS prévoit la possibilité de notifications volontaires.
973. La simple conservation de données est expressément listée par l'article 4(2) du RGPD comme exemple de traitement.
974. RGPD, art. 33.2.

le cas d'espèce, une clause contractuelle précisant un délai plus précis de notification au responsable du traitement est donc fortement recommandée au risque pour ce dernier de ne pouvoir se conformer au délai « maximum » de 72 heures[975] en ce qui concerne sa propre notification à l'autorité de protection des données. Pour le surplus, l'opérateur concerné pourrait également tomber sous le champ matériel du *Cybersecurity Act* si celui-ci souhaite certifier son application mobile permettant aux consommateurs de gérer leurs données dans le cloud. Afin de déterminer sa potentielle obligation de journalisation ainsi que les conditions du traitement de ses *log files*, l'opérateur de notre exemple pourrait donc devoir tenir compte des trois cadres légaux susmentionnés.

D. La journalisation, une mesure appropriée de sécurisation des données à caractère personnel

1. La journalisation recommandée par la doctrine et la jurisprudence

Lorsque l'obligation de journalisation n'est pas légalement prévue, se pose la question de savoir si sous l'empire du RGPD, compte tenu des risques identifiés[976], les responsables de traitements et les sous-traitants peuvent – ou même doivent – envisager cette mesure pour garantir un niveau de sécurité approprié. À cet égard, le considérant 39 du RGPD énonce que les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, « y compris pour 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 ». À s'en tenir à la lettre du considérant en question, le RGPD ne prévoirait que l'obligation de prendre des mesures de sécurité préventives afin de garantir la protection des données contre les traitements non autorisés, que ceux-ci soient accidentels ou illicites. Ceci signifierait que les débiteurs de l'obligation de sécurité ne seraient pas obligés « de prendre des mesures de sécurité a posteriori, comme, par exemple, des mesures de contrôle. Pour le dire autrement, la prévention des usages (traitements) non autorisés de données à caractère personnel n'imposerait que la mise en place de polices d'accès, mais pas de log files, ces derniers répondant en ce sens à

975. Selon le Groupe 29, « le contrat entre le responsable du traitement et le sous-traitant devrait inclure des dispositions précisant la façon de satisfaire aux exigences définies à l'article 33, paragraphe 2, parallèlement à d'autres dispositions du RGPD. Ces dispositions pourraient inclure des exigences de notification rapide par le sous-traitant, ce qui aiderait le responsable du traitement à respecter l'obligation d'informer l'autorité de contrôle dans les 72 heures ». Groupe 29, « Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 », *WP250rev.01*, adoptées le 6 février 2018, p. 14.
976. Pour rappel, contrairement à la directive NIS dont la notion de risque est axée autour de l'impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information essentiels au maintien d'activités sociétales ou économiques critiques, le RGPD se place sous l'angle du risque « pour les droits et libertés des personnes concernées ».

une mesure de contrôle, c'est-à-dire à une mesure de sécurité a posteriori »[977]. Néanmoins, ainsi que le souligne à raison J. Herveg, « cette interprétation, même si elle peut se prévaloir d'arguments tirés d'une lecture (trop) littérale des textes, ne nous paraît pas devoir être retenue. En effet, il ne peut être sérieusement contesté que les log files représentent une mesure de sécurité majeure dans les traitements de données à caractère personnel, fut-ce par leur effet dissuasif à l'encontre des contrevenants potentiels, et qui ne se conçoit que liée à un système performant d'identification des personnes et de leurs actions »[978]. D'autant plus que le considérant 87 du RGPD souligne l'importance d'être en mesure d'identifier une violation[979] et que le Groupe 29 considère, par conséquent, que « le responsable du traitement devrait disposer de procédures internes afin d'être en mesure de détecter une violation et d'y remédier. Par exemple, afin de détecter certaines irrégularités dans le traitement des données, un responsable du traitement ou un sous-traitant peut avoir recours à certaines mesures techniques telles que des analyseurs de flux de données et de journaux, qui permettront de définir des incidents et des alertes en établissant des corrélations entre des données journal »[980].

Dans *I. c. Finlande*[981], la Cour européenne des droits de l'homme fut saisie du cas d'une infirmière qui avait vu son contrat de travail non renouvelé après que des rumeurs aient circulé sur son état de santé. Celle-ci avait échoué à obtenir la réparation de son préjudice devant les juridictions nationales qui considéraient qu'elle ne rapportait pas la preuve d'un accès non autorisé à son dossier médical tenu dans l'hôpital où elle travaillait. Considérant qu'au regard du droit finlandais, le responsable du traitement devait garantir que les données à caractère personnel étaient protégées de manière adéquate contre les accès non autorisés afin que seul le personnel en charge du patient puisse accéder à son dossier[982], la Cour a rappelé que le besoin de garanties suffisantes était particulièrement important lors du traitement de données hautement intimes et sensibles comme en l'espèce, où, de plus, la personne concernée travaillait dans l'hôpital où elle était soignée[983]. Or, le système de dossiers médicaux contesté était tel qu'il n'était pas possible de clarifier rétroactivement l'utilisation des dossiers des patients, car il ne conservait en mémoire que les traces des cinq dernières consultations, lesquelles, de surcroît, étaient effacées une fois le dossier versé aux archives[984]. La Cour en déduisit que le système de dossiers en place à l'hôpital

977. J. Herveg, « L'accès du patient aux log files de son dossier informatisé », *D.C.C.R.*, 2011, liv. 90, p. 44.
978. *Ibid.*
979. Le considérant 87 du RGPD stipule 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 ».
980. Groupe 29, *WP250rev.01*, *op. cit.*, p. 13.
981. Cour eur. D.H., 17 juillet 2008, *I. c. Finlande*, req. n° 20511/03.
982. *Ibid.*, § 39.
983. *Ibid.*, § 40.
984. *Ibid.*, § 41.

n'était manifestement pas conforme aux exigences légales finlandaises de l'époque. Dans la mesure où la requérante avait perdu son action civile parce qu'elle était dans l'incapacité de rapporter la preuve de la relation causale entre les déficiences dans les règles relatives à la sécurité de l'accès et la divulgation des informations relatives à sa condition médicale, la Cour a considéré que placer cette preuve à sa charge négligeait le fait que les déficiences dans la conservation du dossier par l'hôpital étaient reconnues[985]. À cet égard, la Cour relève que le simple fait que la législation nationale ait permis à la requérante de demander réparation pour le préjudice causé par une prétendue divulgation illicite de données à caractère personnel n'était pas suffisant pour protéger sa vie privée. Ce qui était requis en premier lieu est une *protection réelle et effective* qui exclut toute possibilité d'accès non autorisé afin d'obtenir une indemnisation pour le dommage causé par une divulgation non autorisée de données à caractère personnel[986].

2. L'importance de la journalisation au regard de l'obligation d'accountability

Ainsi que le souligne J. Herveg, « le fait que les log files fassent partie de l'éventail des mesures techniques et organisationnelles susceptibles d'assurer la sécurité d'un traitement de données n'implique pas que tout système ou logiciel informatique qui tombe sous le coup [du RGPD] doit en être pourvu, contrairement à ce que semble affirmer la Commission de la protection de la vie privée dans sa note sur les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel »[987]. En effet, rappelons que 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* »[988] tout en prenant en compte l'état des connaissances[989], les coûts de mise en

985. *Ibid.*, § 44.
986. *Ibid.*, § 47.
987. J. Herveg, *op. cit.*, p. 44.
988. RGPD, art. 32.1. 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*, 4 avril 2017, p. 7.
989. La prise en compte de l'état des connaissances doit se lire 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 » (Y. Poullet, « La sécurité informatique, entre technique et droit », *Cahiers du CRID*, n° 14, 1998, p. 43). Le Conseil de l'Europe précise, quant à lui, 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 » (Conseil de l'Europe, « Rapport explicatif de Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », 2018, p. 12.

œuvre[990] ainsi que la nature, la portée, le contexte et les finalités du traitement[991]. 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 »*[992]. Par conséquent, l'obligation légale de sécurisation doit être interprétée comme étant une obligation de moyens[993] 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[994], et, d'autre part, parce que le RGPD laisse à ses débiteurs le soin d'évaluer les risques « inhérents »[995] 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 débiteur n'a pas été suffisamment prudent ou diligent dans la mise en œuvre des moyens qui auraient été nécessaires pour l'éviter. Une affirmation qui mérite néanmoins d'être fortement nuancée, non seulement eu égard à la jurisprudence *I c. Finlande* susmentionnée, mais également parce que l'exigence d'*accountability*[996] 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[997].

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[998] – 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 analyse d'impact relative à la protection des données[999] (ci-après « AIPD ») lorsque ses traitements sont « susceptibles d'engendrer un risque élevé »[1000]. Lorsqu'une AIPD est requise, les principes de *privacy by design*[1001] et de *privacy by default*[1002] imposent au responsable du traitement de la réaliser avant le traitement[1003], le cas échéant, avec l'aide du ou des sous-traitant(s) ayant l'obligation de lui fournir toutes les informations néces-

990. 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 » (Y. POULLET, *op. cit.*, p. 43). L'APD va dans le même sens en estimant que « le coût des mesures envisagées ne peut pas en soi constituer une raison de réaliser un traitement sans garanties suffisantes. Si le responsable du traitement n'est pas en mesure de prévoir des garanties suffisantes et de ramener le risque à un niveau acceptable, au vu de la technologie disponible et des frais d'exécution, il doit le cas échéant soit renoncer au traitement, soit réaliser une consultation préalable de l'autorité de contrôle » (APD, Recommandation n° 01/2018, *op. cit.*, p. 25).

991. 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 n° 01/2018, *op. cit.*, p. 17.

992. 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.

993. « On se situe d'ailleurs pour l'essentiel dans le cadre d'obligations de moyens et ne seront nécessaires que les mesures dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent ». Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.*, Ch. repr., Sess. ord. 1990- 1991, doc. 1610/1, 6 mai 1991, p. 21. 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.

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

995. 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.

996. RGPD, art. 5.2 et 24.

997. *Ibid.*, art. 58.1, a).

998. *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.

999. *Ibid.*, art. 35. Relevons qu'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 cette publication est encouragée par le Groupe 29 : « 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, *WP248*, *op. cit.*, p. 21).

1000. Selon l'APD, « 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. Une 'conséquence négative sensible' signifie que, dans le cas où le risque inhérent se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux ». APD, Recommandation n° 01/2018, *op. cit.*, p. 8. Pour déterminer s'il est ou non probable qu'un traitement envisagé puisse donner lieu à un risque inhérent élevé, les lignes directrices élaborées par le Groupe 29 sont particulièrement importantes puisqu'elles identifient neuf critères qui doivent être pris en considération (Voy. Groupe 29, *WP248*, *op. cit.*, pp.10-13). De plus, l'article 35.4 du RGPD oblige chaque autorité de contrôle à établir une liste des types d'opérations de traitement pour lesquelles une AIPD est requise et à communiquer ensuite cette liste au Comité européen de la protection des données (CEPD). L'APD belge a soumis son projet de liste au CEPD et l'a ensuite adapté afin de suivre les recommandations du CEPD (Voy. APD, « Liste des types d'opérations de traitement pour lesquelles une AIPD est requise », disponible à l'adresse suivante : https ://www.autoriteprotectiondonnees.be/sites/privacy-commission/files/documents/Liste_des_traitements_AIPD.pdf).

1001. RGPD, art. 25.1.

1002. *Ibid.*, art. 25.2.

1003. 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).

saires[1004]. Cette analyse doit notamment contenir 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 ; une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ; 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[1005]. 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 la journalisation en tant que mesure appropriée.

Tout récemment, le Comité européen à la protection des données (ci-après « CEPD ») a eu l'occasion de se prononcer sur l'importance qu'il accordait à la journalisation en tant que mesure de sécurité appropriée selon les risques identifiés dans le contexte des annuaires WHOIS[1006] de l'ICANN[1007]. Ces annuaires contiennent notamment le nom, l'adresse postale, le numéro de téléphone ainsi que l'e-mail des personnes ou entités ayant enregistré un nom de domaine. Cette base de données accessible au public ne posait pas de souci dans les années 1980 à l'époque où seuls quelques chercheurs possédaient un nom de domaine, mais elle expose actuellement des millions de personnes au harcèlement et au spam[1008]. C'est dans ces circonstances que le CEPD a récemment considéré que « *unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log any access to non-public personal data in the context of WHOIS. In this context, such logging is considered as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2)* »[1009].

1004. 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 ».
1005. RGPD, art. 35.7.
1006. Le service WHOIS de l'ICANN est un outil de recherche public qui sert à interroger les bases de données des registres et des bureaux d'enregistrement afin de trouver les informations de contact des titulaires des noms de domaine.
1007. L'ICANN (Internet Corporation for Assigned Names and Numbers) est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, telles que l'adressage IP et les noms de domaines de premier niveau, et de coordonner les acteurs techniques
1008. Au sujet des considérations relatives à la vie privée posées par le WHOIS, lire International Working Group on Data Protection in Telecommunications, « Working Paper on Privacy and Data Protection Issues with Regard to Registrant data and the WHOIS Directory at ICANN », 62nd meeting, 27-28 November 2017.
1009. C.E.P.D., « Letter to ICANN », 5 juillet 2018, p. 5.

3. L'importance de la journalisation en cas de sous-traitance

Nous avons déjà souligné que, sous le régime du RGPD, le responsable du traitement et le sous-traitant sont tous deux 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 RGPD. Sur le plan administratif, la répartition des éventuelles amendes[1010] 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[1011]. Sur le plan civil, la personne lésée pourra, au choix, demander réparation du préjudice subi à l'un ou à l'autre[1012], lequel pourra ensuite se retourner contre le partenaire contractuel en ce qui concerne sa part de responsabilité dans le dommage[1013]. À 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[1014]et qu'il mette à la disposition du responsable du traitement toutes les informations nécessaires pour en démontrer le respect, ainsi que pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et qu'il contribue à ces audits[1015]. Non seulement plusieurs parties peuvent intervenir en tant que sous-traitants mais il est également habituel que des sous-traitants confient des activités à des sous-traitants de second rang. Dans ce cas, le RGPD prévoit que le sous-traitant ne peut pas recruter un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement[1016]. De plus, le contrat régissant les relations entre le sous-traitant et le sous-traitant de second rang doit contenir les mêmes obligations en matière de protection de données que celles fixées dans le contrat entre le responsable du traitement et le sous-traitant, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées[1017]. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant principal demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations[1018].

1010. En Belgique, l'article 221, § 2, de la loi du 30 juillet 2018 précitée prévoit, en principe, l'absence d'amendes administratives pour les autorités publiques. Il se lit comme suit : « L'article 83 du Règlement ne s'applique pas aux 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 ».
1011. RGPD, art. 83.2, d).
1012. *Ibid.*, art. 82.1.
1013. *Ibid.*, art. 82.5.
1014. *Ibid.*, art. 28.3, f).
1015. *Ibid.*, art. 28.3, f) et h).
1016. *Ibid.*, art. 28.2. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.
1017. *Ibid.*, art. 28.4.
1018. *Ibid.*

Autant dire qu'en cas de sous-traitance ou de sous-traitance de second rang, 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[1019]. En effet, « la responsabilité informatique est particulièrement importante pour enquêter sur les violations de données à caractère personnel, lorsque les clients, les fournisseurs et les sous-traitants ultérieurs peuvent tous assumer une part de responsabilité opérationnelle »[1020]. À cet égard, le principe de convention-loi ne s'oppose pas à ce que les contrats de sous-traitance contiennent des obligations additionnelles *de résultat* en matière de sécurité informationnelle, par exemple en matière de journalisation. C'est pourquoi le Groupe 29 considère que « dans la mesure où un scénario type d'informatique en nuage peut facilement impliquer un grand nombre de sous-traitants, le risque de traiter des données à caractère personnel pour d'autres finalités qui seraient incompatibles doit donc être considéré comme assez élevé. Pour réduire ce risque au minimum, le contrat entre le fournisseur d'informatique en nuage et son client devrait prévoir des mesures techniques et organisationnelles, de manière à garantir la journalisation et l'audit des opérations de traitement des données à caractère personnel effectuées par les employés du fournisseur d'informatique en nuage ou par les sous-traitants »[1021].

E. Le traitement de log files au regard des principes du RGPD

1. Les log files contiennent des données à caractère personnel

L'ISO 27002[1022] recommande que les *log files* contiennent, tant que possible, « a) les identifiants des utilisateurs ; b) les activités du système ; c) les dates, heures, et détails des évènements clés, par exemple l'ouverture d'une session et la déconnexion ; d) l'identité ou l'emplacement du dispositif, si possible, ainsi que l'identifiant du système ; e) les enregistrements des tentatives d'accès au système réussies et rejetées ; f) les enregistrements des tentatives d'accès aux données et autres ressources réussies et rejetées ; g) les modifications de la configuration du système ; h) l'utilisation des privilèges ; i) l'utilisation des utilitaires et des applications du système ; j) les fichiers consultés et type d'accès ; k) les adresses et protocoles réseau ; l) les alarmes déclenchées par le système de contrôle d'accès ; m) l'activation et la désactivation de systèmes de protection, tels les antivirus et les systèmes de

1019. *Ibid.*, art. 82.3.
1020. Groupe 29, « Avis 05/2012 sur l'informatique en nuage », *WP196*, 1er juillet 2012, p. 20.
1021. *Ibid.*, p. 14.
1022. L'ISO/IEC 27002 :2013 donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.

détection d'intrusion ; et n) les enregistrements des transactions exécutées par les utilisateurs dans les applications »[1023].

Étant données les catégories d'informations appelées à être contenues dans les *log files*, l'Autorité de protection des données fédérale considère que les données de journalisation sont « elles-mêmes des données à caractère personnel »[1024]. Cette qualification semble aller de soi : « prétendre que les personnes physiques ne sont pas identifiables alors que la finalité du traitement est précisément de les identifier serait une contradiction absolue *in terminis*. Il est dès lors essentiel de considérer ces informations comme concernant des personnes physiques identifiables et d'appliquer les règles de protection des données à leur traitement »[1025].

2. Finalité, minimisation et base de licéité des log files

Le RGPD commande que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)[1026]. Appliqué aux *log files*, ce principe implique, selon l'APD que « l'enregistrement de ces informations de contrôle peut concerner, suivant les cas, l'accès physique, l'accès logique ou les deux. La granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte. Des mécanismes supplémentaires de détection d'intrusion pourraient être requis »[1027]. La CNIL française[1028] estime, quant à elle, que « la journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ; dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné »[1029].

1023. ISO/IEC 27002 :2013, section 12.4, p.44. Ledit ISO en déduit que les *log files* peuvent contenir des données sensibles et des informations personnelles ayant pour conséquence que des mesures appropriées de la protection de la vie privée devraient être prises.
1024. APD, « Mesures de référence applicables à tout traitement de données à caractère personnel – version 1.0 », p. 4.
1025. Groupe 29, « Avis 4/2007 sur le concept de données à caractère personnel », 20 juin 2007, p. 17-18. Le groupe a encore eu l'occasion de rappeler que « les données journal facilitant la vérifiabilité par exemple du stockage, des modifications ou de l'effacement des données peuvent aussi être qualifiées de données à caractère personnel concernant la personne qui a lancé les opérations de traitement respectives » dans son *WP250.rev01, op. cit.*, p. 13.
1026. RGPD, art. 5.1, c).
1027. APD, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 4.
1028. La CNIL est l'autorité de protection des données française.
1029. CNIL, « La sécurité des données personnelles », in *Les guides de la CNIL*, édition 2017, p. 10.

Le RGPD impose que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes, et que celles-ci ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités[1030]. Selon l'ISO 27002, l'objectif de la journalisation est « d'enregistrer les évènements et de générer des preuves »[1031]. La CNIL précise que l'enregistrement de certaines des actions effectuées sur les systèmes informatiques a pour but « de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident »[1032]. Assurément, il s'agit d'être en mesure de démontrer que le traitement est effectué conformément aux principes du RGPD[1033] et de prévenir des violations de données à caractère personnel en rassemblant des preuves signalant des accès non autorisés à celles-ci. En effet, selon le Groupe 29, « le responsable du traitement devrait disposer de procédures internes afin d'être en mesure de détecter une violation et d'y remédier »[1034]. Les *log files* permettent ainsi d'établir l'existence d'une violation et d'évaluer son risque afin de déterminer si celle-ci doit être notifiée au sens de l'article 33 du RGPD, voire communiquée au sens de l'article 34 du même texte[1035]. De plus, l'enregistrement de *log files* peut aider le responsable du traitement à satisfaire à son obligation de documenter toutes les violations, que celles-ci doivent être notifiées ou non[1036], en conservant systématiquement « les causes, les faits et les données à caractère personnel concernées »[1037]. Bien entendu, il s'agit de ne pas confondre les finalités susmentionnées avec celle de la surveillance des communications électroniques des employés[1038] qui pose la délicate question de « l'équilibre entre l'intérêt légitime de l'employeur à protéger ses activités et les attentes raisonnables des personnes

1030. RGPD, art. 5.1, b).
1031. ISO/IEC 27002 :2013, *op. cit.*, p. 43.
1032. CNIL, « La sécurité des données personnelles », in *Les guides de la CNIL*, édition 2017, p. 10.
1033. Art. 5.2 et 24.
1034. Groupe 29, *WP250 rev.0*, *op. cit.*, p.13.
1035. Pour rappel, la notification d'une violation à l'APD est obligatoire à moins que cette violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus, tandis que la communication d'une violation aux personnes concernées ne devient nécessaire que lorsque ladite violation est susceptible d'engendrer un risque *élevé* pour leurs droits et libertés.
1036. RGPD, art. 33.5. « Cette obligation de documentation est liée au principe de responsabilité du RGPD figurant à l'article 5, paragraphe 2. Cette exigence de tenir des registres des violations, qu'elles soient sujettes à notification ou non, est également liée aux obligations du responsable du traitement au titre de l'article 24, et l'autorité de contrôle peut demander à voir lesdits registres. Les responsables du traitement sont donc encouragés à établir un registre interne des violations, qu'ils soient tenus de les notifier ou non » (Groupe 29, *WP250 rev.01*, *op. cit.*, p.30).
1037. *Ibid.*
1038. Dans le cadre de cette contribution, nous n'analysons pas la problématique de la protection des données à caractère personnel des employés dans le contexte du travail. A ce propos lire, K. ROSIER, S. GILSON & F. LAMBINET, *Le droit au respect de la vie privée du travailleur : état des lieux*, Anthemis, 2012. Voy. également APD, Recommandation n° 08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, 2 mai 2012.

concernées, à savoir les employés, en matière de respect de la vie privée »[1039] réglée, en Belgique, par le biais la Convention collective de travail n° 81[1040].

Outre les cas dans lesquels la journalisation est légalement requise, se pose la question de leur fondement de licéité. À cet égard, le consentement des personnes concernées n'est pas nécessaire[1041], l'intérêt légitime du responsable du traitement ou d'un tiers autorisé à traiter les données étant suffisant. En effet, le considérant 49 du RGPD stipule explicitement que « le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations [...] constitue un intérêt légitime du responsable du traitement concerné »[1042]. Selon le RGPD, il « pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par « déni de service » et des dommages touchant les systèmes de communications informatiques et électroniques »[1043]. Ainsi, la Cour de justice de l'Union européenne a estimé que « des services de médias en ligne pourraient également avoir un intérêt légitime à garantir, au-delà de chaque utilisation concrète de leurs sites Internet accessibles au public, la continuité du fonctionnement desdits sites »[1044], jugeant par conséquent que « l'objectif visant à garantir la capacité générale de fonctionnement des mêmes services puisse justifier l'utilisation des [log files] après une session de consultation de ceux-ci »[1045].

1039. Groupe 29, « Avis 2/2017 sur le traitement des données sur le lieu de travail », *WP249*, 8 juin 2017, p. 4. Voy. également Groupe 29, « Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel », *WP48*, 13 septembre 2001 et Groupe 29, « Document de travail concernant la surveillance des communications électroniques sur le lieu de travail », *WP55*, 29 mai 2002.
1040. Convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau et rendue obligatoire par l'arrêté royal du 12 juin 2002. Toutefois, ces deux types de préoccupations peuvent partiellement se rencontrer puisque parmi les quatre finalités pour lesquelles le contrôle de données de communication électroniques en réseau est autorisé au sens de l'article 5 la CCT n° 81, figurent non seulement celle de la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise mais également celle de la prévention de faits illicites, qui peuvent notamment consister « en des actes de piratage informatique, dont la prise de connaissance non autorisée de données de communication électroniques en réseau relatives à la gestion du personnel ou de fichiers médicaux confidentiels » ainsi que celle du respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise, en ce compris des clauses de confidentialité particulières relatives au traitement de données à caractère personnel que ces règles contiennent.
1041. Encore moins lorsqu'il s'agit de *log files* relatifs à l'activité des employés : « les employés sont rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé » (Groupe 29, *WP249*, *op.cit*, p. 4).
1042. La notion de « sécurité du réseau et des informations » y est par ailleurs définie comme étant « *la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises* ».
1043. RGPD, consid. 49.
1044. C.J.U.E.., 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, C-582/14, § 60.
1045. *Ibid.*, § 65.

Sont également considérés comme relevant de l'intérêt légitime, « la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications électroniques et des fournisseurs de technologies et services de sécurité »[1046]. C'est dans cette perspective que la directive NIS prévoit que « dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes [en matière de cybersécurité] et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents »[1047].

Dans le même esprit, le considérant 50 du RGPD stipule que « le fait, pour le responsable du traitement, de révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement. Néanmoins, cette transmission dans l'intérêt légitime du responsable du traitement ou le traitement ultérieur des données à caractère personnel devrait être interdite lorsque le traitement est incompatible avec une obligation de confidentialité légale, professionnelle ou toute autre obligation de confidentialité contraignante »[1048]. Rappelons que les autorités judiciaires peuvent également exiger que des responsables de traitements ou des sous-traitants leur transmettent des *log files*, notamment sur la base des articles 39*bis* et 88*quater* du Code d'instruction criminelle[1049].

1046. RGPD, consid. 49.
1047. Directive NIS, consid. 63.
1048. Dans la même perspective, le considérant 62 de la directive NIS indique qu'un incident « peut être le résultat d'activités criminelles, à propos desquelles la prévention, les enquêtes et les poursuites sont soutenues par la coordination et la coopération entre les opérateurs de services essentiels, les fournisseurs de service numérique, les autorités compétentes et les services répressifs. Lorsqu'il y a lieu de suspecter qu'un incident est lié à des activités criminelles graves au regard du droit de l'Union ou du droit national, les États membres devraient encourager les opérateurs de services essentiels et les fournisseurs de service numérique à signaler aux services répressifs compétents tout incident de ce type. Le cas échéant, il est souhaitable que la coordination entre les autorités compétentes et les services répressifs de différents États membres soit facilitée par le Centre européen de lutte contre la cybercriminalité (EC3) et l'ENISA ».
1049. A cet égard le considérant 31 du RGPD indique que « les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement ». Pour une analyse de ces méthodes d'enquête, lire C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ? », *R.D.T.I.*, n°66-67, 2017, pp.25-52.

3. Durée de conservation et droits d'accès aux log files

Dans son arrêt *Rijkeboer*[1050], la Cour de justice de l'Union européenne a apporté des éclaircissements concernant la durée de conservation[1051] des *log files* et le droit d'accès[1052] à ceux-ci. Dans le cas d'espèce, un citoyen néerlandais avait demandé au Collège de Rotterdam de l'informer de tous les cas où des informations le concernant provenant de l'administration communale avaient été communiquées à des personnes tierces, au cours des deux années précédant sa demande. Il désirait connaître l'identité de ces personnes et le contenu de l'information qui leur avait été transmise. M. Rijkeboer qui avait déménagé dans une autre commune souhaitait savoir en particulier à qui son ancienne adresse avait été communiquée. Le Collège n'avait accédé que partiellement à cette demande en ne lui communiquant que l'information relative à la période d'un an précédant sa demande d'accès, les données antérieures ayant été automatiquement effacées conformément à la loi nationale. C'est dans ces circonstances que la Cour de justice de l'Union européenne eut à déterminer si le droit d'accès d'une personne à l'information sur les destinataires ou les catégories de destinataires de données à caractère personnel la concernant ainsi que sur le contenu des données communiquées peut être limité à la période d'un an précédant sa demande d'accès[1053].

Dans un premier temps, la Cour distingue deux types de catégories de données. La première concerne les données à caractère personnel détenues par la commune sur une personne, comme son nom et son adresse, qui forment, en l'occurrence, des « données de base »[1054]. La seconde catégorie a trait à l'information sur les destinataires ou les catégories de destinataires auxquels ces données de base sont communiquées ainsi que sur le contenu de celles-ci[1055]. Concernant ces dernières, la Cour estime que *« le droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés »*[1056]. Outre ce but de contrôle, la Cour rappelle que le droit d'accès à ces données *« est également nécessaire pour permettre à la personne concernée d'exercer le droit d'opposition [...] ou le droit de recours en cas de dommage subi [...] »*[1057].

Dans un second temps, s'agissant du droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données de base ainsi que sur le contenu des données

1050. C.J.U.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M. E.E. Rijkeboer*, C-553/07. A propos de cette affaire, lire C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 22 décembre 2010, *R.D.T.I.*, n° 43, 2011, pp. 65-81. Voy. également J. HERVEG, *op. cit.* p. 49 et *s.*
1051. RGPD, art. 5, 1, e).
1052. *Ibid.*, art. 15.
1053. CJUE., aff. *Rijkeboer, op. cit, § 31.*
1054. *Ibid.*, § 42.
1055. *Ibid.*, § 43.
1056. *Ibid.*, § 49.
1057. *Ibid.*, § 52.

communiquées, la Cour constate que la directive 95/46/CE, depuis lors remplacée par le RGPD, ne précise pas si ce droit concerne le passé ni, le cas échéant, la période visée dans le passé[1058]. À cet égard, la Cour affirme que, pour assurer l'effet utile, « *ce droit doit nécessairement concerner le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi* »[1059]. Selon C. de TERWANGNE, « *cela implique l'obligation de conservation pendant une certaine durée des renseignements relatifs aux personnes destinataires des données ainsi qu'aux données précisément consultées ou transmises* »[1060]. Quant à l'étendue de ce droit dans le passé, la Cour estime que la durée de conservation des données de base peut constituer un paramètre utile sans toutefois être déterminant[1061]. La Cour propose encore comme paramètres le nombre des destinataires concernés et la fréquence des communications. En outre, il s'agirait de prendre en compte un « *juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des droits de rectification, d'effacement et de verrouillage des données, en cas de non-conformité du traitement [...], ainsi que des droits d'opposition et d'introduction d'un recours juridictionnel et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement* »[1062]. En l'occurrence, selon la Cour, une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne constitue pas un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement[1063].

De manière plus pragmatique, la CNIL recommande, quant à elle, que « *ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important)* »[1064]. Cette recommandation va dans le sens de l'approche transversale du RGPD fondée sur les risques. Néanmoins, « *even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk* »[1065]. Étant donné que l'effectivité du droit d'accès des personnes concernées est manifestement liée à la durée de conservation des *log files*, la plus grande prudence est donc requise lors de sa détermination lorsque celle-ci n'est pas fixée par la loi[1066].

1058. *Ibid.*, § 53.
1059. *Ibid.*, § 54.
1060. 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 », *op. cit.*, p. 113.
1061. C.J.U.E., aff. *Rijkeboer, op. cit, § 58.*
1062. *Ibid.*, § 64.
1063. *Ibid.*, § 66.
1064. CNIL, « La sécurité des données personnelles », *op. cit.*, p. 10.

4. Information et sécurité des log files

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, l'article 13 du RGPD impose au responsable du traitement de lui fournir, au moment où les données en question sont obtenues, un certain nombre d'informations, parmi lesquelles les finalités du traitement auquel sont destinées les données à caractère personnel, la base juridique du traitement comme, par exemple, les intérêts légitimes poursuivis, ainsi que les destinataires ou les catégories de destinataires des données à caractère personnel[1067]. Afin de garantir un traitement équitable et transparent, il est également recommandé de préciser la durée de conservation ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ainsi que l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel. Cette règle de transparence vaut évidemment en ce qui concerne le traitement de *log files*. Enfin, « les données de traçage étant elles-mêmes des données à caractère personnel, tout traitement de celles-ci doit s'accompagner des mesures de sécurité adéquates »[1068]. À cet égard, la CNIL recommande de « protéger les équipements de journalisation et les informations journalisées contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée »[1069]. Dans le même sens, l'APD

1065. « Statement on the role of a risk-based approach in data protection legal frameworks », *WP218*, 30 mai 2014, p. 2.
1066. Pour le surplus, relevons que le droit d'accès des personnes concernées peut être limité par la loi conformément à l'article 23 du RGPD, lorsqu'une telle mesure est nécessaire et proportionnée dans une société démocratique pour garantir, entres autres, la sécurité publique ou la prévention et la détection d'infractions pénales.
1067. La notion de destinataire est définie à l'article 4, 9), du RGPD comme étant « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ». Sont donc visés, tant les destinataires internes (tels les employés habilités à accéder aux *log files*) qu'externes (tels d'éventuels sous-traitants). En ce qui concerne l'accès aux *log files*, une version préparatoire du RGPD prévoyait que le délégué à la protection des données devrait, au moins avoir, entre autres, les compétences suivantes « *[...] the ability to carry out inspections, consultation, documentation, and log file analysis [...]* ». Voy. le considérant 75a de la Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), *COM(2012)0011 — C7-0025/2012 — 2012/0011(COD).*
1068. APD, « Mesures de référence applicables à tout traitement de données à caractère personnel », *op. cit.*, p. 4.
1069. CNIL, « La sécurité des données personnelles », *op. cit.*, p. 10.

conseille « l'extraction, en temps réel ou dès que possible, des données de surveillance journaux, logs, traces) pour un stockage dans une zone sécurisée ('silo' : serveur spécifique, fichier chiffré…) dont les accès sont strictement limités et tracés spécifiquement »[1070]. Davantage de précisions peuvent être trouvées dans les recommandations de sécurité pour la mise en œuvre d'un système de journalisation[1071] de l'ANSSI[1072].

F. Conclusions

Étant donnée l'adoption de nouvelles réglementations européennes – telles la directive NIS et le *Cybersecurity Act*[1073] – dans le cadre desquelles la journalisation est explicitement prévue, la multiplication de *log files* ne fait aucun doute. D'autant plus que le relatif silence du RGPD sur la question est compensé par la jurisprudence européenne ainsi que par la convergence d'opinions entre le Groupe 29 et les autorités nationales de protection des données, de sorte que la propriété d'imputabilité reçoive toute l'attention qu'elle mérite.

Assurément, la personne concernée verra d'un bon œil le fait que la journalisation soit encouragée : la mise en œuvre de cette pratique lui permettra d'obtenir des éléments probants nécessaires à l'effectivité d'un recours en cas de dommage. Toutefois, en l'absence de disposition légale imposant la journalisation et précisant le délai de conservation des *log files*, bien malin celui qui prétend détenir des réponses génériques pour permettre aux responsables de traitements et aux sous-traitants de savoir avec certitude, si, selon l'importance des risques qu'ils ont identifiés pour les personnes physiques, le traitement de *log files* doit être envisagé et pendant combien de temps ces données doivent être conservées. Des recommandations peuvent néanmoins être formulées.

Force est de constater que le principe de *privacy by default* édicté par le RGPD requiert, en particulier, que des mesures soient prises afin de garantir que *« par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée »*[1074]. Une version préparatoire du RGPD complétait *« et que les personnes concernées ont la possibilité de contrôler la diffusion de leurs données à caractère personnel »*[1075]. De plus, l'article 32 du Règlement dispose clairement que le responsable du traitement et le sous-traitant doivent mettre en œuvre les

1070. APD, Recommandation n° 08/2012, *op. cit.*, p. 50.
1071. ANSSI, « Note technique – Recommandations de sécurité pour la mise en œuvre d'un système de journalisation », 2 décembre 2013.
1072. L'ANSSI est l'autorité nationale française en matière de sécurité et de défense des systèmes d'information.
1073. Nous ne prétendons à aucune exhaustivité. Nous avons fait le choix de nous limiter aux instruments susmentionnés.
1074. RGPD, art. 25.2.
1075. Résolution législative du Parlement européen du 12 mars 2014, *op. cit.*, art. 23.2.

mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté des données à caractère personnel : *« la capacité de détecter une violation, d'y remédier et de la communiquer dans les meilleurs délais devrait être considérée comme un élément essentiel de ces mesures »*[1076]. Il est donc fortement recommandé de mettre en place des processus permettant d'établir *« immédiatement si une violation des données à caractère personnel s'est produite »*[1077], d'évaluer les risques pour les personnes concernées et de déterminer ensuite s'il est nécessaire d'informer l'autorité de contrôle compétente et de communiquer, si nécessaire, la violation aux personnes concernées. Étant donné que, lors de l'évaluation du risque présenté par une violation, le responsable du traitement doit tenir compte des circonstances spécifiques à l'incident qui s'est déjà produit, l'accent doit être entièrement mis sur le risque *in concreto* présenté par ladite violation pour les personnes concernées.[1078] Il n'est pas donc pas aisé de déterminer son degré d'importance *a priori*[1079].

Pour cette raison, qu'une violation doive être notifiée à l'autorité de contrôle ou non, le responsable du traitement est tenu de documenter toutes les violations. Cette exigence de tenir des registres des violations est liée à l'obligation d'*accountability* du responsable du traitement et l'autorité de contrôle peut demander à voir lesdits registres[1080]. S'il appartient au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, il est évident que des *log files* lui seront utiles pour enquêter et rassembler des preuves concernant un accès non autorisé à des données à caractère personnel. Dans ce contexte, l'intérêt légitime du responsable du traitement peut être invoqué afin de procéder à ce traitement de données à caractère personnel additionnel ou accessoire qu'est la journalisation ayant pour finalité l'imputabilité des actions réalisées sur les traitements initiaux. En cas de sous-traitance, les *log files* permettront également d'assurer l'effectivité des « obligations et responsabilités découlant de la législation en matière de protection des données et d'éviter qu'elles ne soient dispersées tout au long de la chaîne de sous-traitance, afin de garantir le contrôle effectif des activités de traitement et de répartir précisément les responsabilités en la matière »[1081].

1076. Groupe 29, *WP250rev.01*, *op. cit.*, p. 6.
1077. RGPD, consid. 87.
1078. Le Groupe 29 recommande que l'évaluation du risque d'une violation tienne compte des critères suivants : le type de violation, la nature, le caractère sensible et le volume des données à caractère personnel, la facilité d'identification des personnes concernées, la gravité des conséquences pour les personnes concernées, les caractéristiques particulières des personnes concernées, les caractéristiques particulières du responsable du traitement et le nombre de personnes concernées (Groupe 29, *WP250rev.01*, *op. cit.*, pp. 26-29).
1079. A cet égard, « il est à noter que l'évaluation du risque présenté par une violation pour les droits et libertés des personnes concernées se fait selon une approche différente de celle adoptée dans le cadre d'une AIPD. L'AIPD envisage en effet autant les risques encourus si le traitement des données est effectué comme prévu que les risques en cas de violation. Dans le cadre de son appréciation d'une éventuelle violation, une telle analyse évalue de façon générale la probabilité d'une telle violation ainsi que les dommages qu'elle pourrait engendrer pour les personnes concernées ; il s'agit, en d'autres termes, de l'évaluation d'un incident hypothétique. En cas de violation réelle, l'incident s'est déjà produit et l'accent est donc entièrement mis sur le risque présenté par la violation pour les personnes concernées. » (*ibid*, p. 26).
1080. RGPD, art. 33.5.
1081. Groupe 29, *WP196*, *op. cit.*, p. 11.

Enfin, vis-à-vis des personnes concernées, la journalisation est la condition *sine qua non* pour rendre effectif leur droit d'accès pour le passé leur permettant de vérifier que leurs données ont été adressées à des destinataires autorisés, et, le cas échéant, d'obtenir les éléments nécessaires afin d'introduire efficacement un recours juridictionnel pour obtenir la réparation du préjudice subi. La détermination de la durée de conservation des *log files* n'est donc pas une question à prendre à la légère lors de l'élaboration d'une bonne politique de sécurité des données.