La cybersécurité, un enjeu à la croisée des stratégies européennes

Cruquenaire, Alexandre

Published in:
L'influence du droit européen en droit économique

Publication date:
2022

Document Version
le PDF de l'éditeur

La cybersécurité, un enjeu à la croisée des stratégies européennes

Alexandre CRUQUENAIRE

Avocat
Chargé de cours invité à l'Université de Namur (CRIDS)

1. La démarche de droit comparé et l'élaboration de règles harmonisées au niveau international, et en particulier au sein de l'Union européenne, ont inspiré de nombreux travaux du professeur Denis Philippe. Le sujet de la cybersécurité nous semblait donc tout indiqué pour notre modeste contribution au présent ouvrage. En effet, ce thème illustre parfaitement le rôle crucial que (doit) joue(r) le droit européen afin de nous permettre de relever les grands défis socio-économiques qui se posent au sein de l'Union européenne.

2. L'importance croissante de la problématique de la cybersécurité s'est traduite par une intervention plus large et plus intense du législateur européen dans ce domaine. Dans le cadre de la présente contribution, nous soulignerons principalement deux aspects clés du développement de la législation européenne sur la cybersécurité[1] :

– la double nature de cette législation, à la fois transversale et spécialisée (I.),

– la portée des obligations spécifiques imposées aux acteurs de la chaîne de la cybersécurité (II).

3. La stratégie de cybersécurité définie par la Commission européenne en 2013 identifiait déjà la nécessité d'une approche collaborative entre le secteur public et le secteur privé – compte tenu du fait que de nombreux services critiques pour la vie socio-économique sont contrôlés par des acteurs privés – et entre les États membres par ailleurs– les menaces sur la

1 La présente contribution a été rédigée en août 2021. Elle n'a aucune prétention à l'exhaustivité. L'analyse livrée est uniquement basée sur les réflexions personnelles inspirées à l'auteur par l'analyse et la mise en œuvre pratiques des textes réglementaires relatifs à la cybersécurité dans le cadre de ses activités de conseil. Toute réflexion critique du lecteur sera appréciée et peut être échangée par email : a.cruquenaire@lexing.be.

cybersécurité se propageant au travers des réseaux de communication[2]. La démarche d'analyse et de gestion des risques y était déjà centrale.

4. La mise en œuvre de cette stratégie s'est concrétisée par l'adoption de plusieurs textes posant les bases de la réglementation sur la cybersécurité, et en particulier :

– la directive 2013/40 relative aux attaques contre les systèmes d'information[3] ;

– le Règlement 2014/910 sur les services de confiance (eIDAS)[4] ;

– la directive 2015/2366 relative aux services de paiement[5] ;

– la directive 2016/1148 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 (NIS)[6] ;

– le Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (règlement général sur la protection des données – RGPD)[7] ;

– la directive 2018/1972 établissant le code des communications électroniques[8] ;

---

2 Commission européenne et Haute Représentante de l'Union pour les Affaires étrangères et la sécurité, Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des Régions, *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, JOIN (2013) 1 Final, 7 février 2013, disponible sur le site officiel de l'Union européenne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013JC0001&from=HU, p. 6.

3 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *JOUE*, L218, 14 août 2013, p. 8.

4 Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE*, L257, 28 août 2014, p. 73.

5 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) 1093/2010, et abrogeant la directive 2007/64/CE, *JOUE*, L337, 23 décembre 2015, p. 35.

6 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, *JOUE*, L194, 19 juillet 2016, p. 1.

7 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), *JOUE*, L119, 4 mai 2016, p. 1.

8 Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen, *JOUE*, L321, 17 décembre 2018, p. 36.

5. Afin d'améliorer la résilience des systèmes d'information, le niveau de sécurité et de renforcer la confiance des citoyens par rapport aux outils numériques, l'Union européenne s'est ensuite dotée d'un Règlement sur la cybersécurité (*Cybersecurity Act*)[9], avec un double objectif : d'une part, renforcer l'Agence européenne pour la cybersécurité (ENISA), et, d'autre part, définir un cadre pour la mise en place de schémas européens de certification de cybersécurité des produits et services disponibles sur le marché de l'Union[10].

6. Plus récemment, la Commission européenne et le Haut Représentant de l'Union pour les Affaires étrangères et la Sécurité ont annoncé une nouvelle stratégie de cybersécurité visant à affirmer le rôle de fer de lance de l'Union dans le développement de services et outils numériques sûrs et dans la capacité à prévenir et lutter contre les cyberattaques[11]. Une proposition de Directive NIS 2 remplaçant la Directive NIS est ainsi en cours d'adoption.

Section 1. La double nature des règles relatives à la cybersécurité

7. La réglementation relative à la cybersécurité se compose de textes de portée horizontale, dédiés à la problématique de la sécurité, et de dispositions particulières intégrées dans des textes relatifs à d'autres sujets, mais soumis à des risques de cybersécurité.

8. La croissance ininterrompue de l'usage des technologies de l'information dans les nouveaux produits et services mis sur le marché ne permet plus de concevoir la réglementation en matière de cybersécurité exclusivement sur la base d'outils transversaux.

La stratégie européenne repose donc logiquement sur une combinaison de règles horizontales et de règles spécifiques à certains secteurs. Sans

9 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) 526/2013 (règlement sur la cybersécurité), *JOUE*, L151, 7 juin 2019, p. 15.

10 Pour un commentaire de ce Règlement, voy. M. KNOCKAERT, « La sécurité dans le marché unique numérique européen : le Règlement 2019/881 (*Cybersecurity Act*) », in *Les obligations légales de cybersécurité et de notifications d'incidents*, Bruxelles, Politeia, 2019, pp. 163 et s.

11 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

entrer dans des discussions théoriques sur la nature (plus ou moins) transversale de certains textes[12], nous considérons comme tels les textes dont la cybersécurité est l'objet principal et les textes non dédiés à ce thème, mais ayant quant à eux une portée générale[13].

La nature transversale d'un texte est d'ailleurs souvent relative. Ainsi, concernant les objets connectés, la Commission pourrait envisager de nouvelles règles horizontales visant à imposer une sécurité accrue de ces objets et des services liés[14]. Toutefois, des règles spécifiques pourront être ajoutées par rapport à certaines technologies, en fonction des risques spécifiques[15]. Cet exemple illustre parfaitement la nécessité d'une double approche combinée, à la fois générique à certains égards et spécialisée lorsque des risques particuliers sont identifiés.

9. Outre des textes de portée transversale, comme le RGPD et la directive NIS, le législateur européen intègre donc la dimension sécurité dans des textes dédiés à certains secteurs ou services.

La directive 2015/2366 relative aux services de paiement intègre ainsi une dimension de cybersécurité, compte tenu de son importance pour la confiance des utilisateurs de ce type de services.

Le Règlement eIDAS sur les services de confiance intègre également des exigences en termes de sécurité[16].

---

12 La nature horizontale de la Directive NIS pourrait ainsi être discutée, dans la mesure où elle cible certains secteurs et certains types de services. Nous l'avons toutefois classée dans cette catégorie, car la sécurité est son objet principal, même si le champ d'application de l'instrument n'est pas totalement transversal. À propos de la définition du champ d'application de la Directive NIS et de l'articulation entre la Directive NIS et le RGPD, voy. M. Fierens, S. Royer et P. Valcke, « Cyberbeveiliging : een blik op het amalgaam van Europese en Belgische regels », *RW*, 2020-2021/9, pp. 332-333, n° 29.

13 Ne ciblant pas certains types de services.

14 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, p. 9.

15 Tel est le cas pour les outils reposant sur l'intelligence artificielle ou les outils de communication. Voy. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, p. 5 (sur l'IA) et p. 8 (à propos des nouveaux réseaux 5G).

16 Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE*, L257, 28 août 2014, p. 73, article 19 (« *Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques*

La proposition de règlement sur l'intelligence artificielle[17] traduit parfaitement l'importance de la cybersécurité dans le développement de nouveaux services. Ici encore, la nécessaire confiance des consommateurs est invoquée pour justifier des obligations imposées aux fournisseurs et utilisateurs de ce type de services[18].

Section 2. Quelques réflexions sur la portée des obligations en matière de cybersécurité

10. La sécurité des produits et services numériques constituant un enjeu vital pour assurer la confiance des utilisateurs, il était nécessaire de définir des obligations claires en la matière.

La démarche du législateur reposant sur une logique de gestion des risques, il convient d'imposer aux opérateurs économiques proposant des produits ou services numériques des obligations de sécurité. Sans surprise, la stratégie de cybersécurité publiée en décembre 2020 suggère notamment d'imposer des obligations de sécurité aux éditeurs de logiciels relatifs aux objets connectés, comportant notamment le devoir de développer des patches de sécurité[19].

Calquée sur la démarche de gestion des risques, la législation impose des obligations phasées, c'est-à-dire des obligations tenant à l'analyse préalable des risques et au choix de mesures appropriées (A.), et, ensuite, des obligations liées à la gestion des incidents si les mesures adoptées n'ont pas permis d'empêcher une réalisation du risque (B.).

Cette définition des obligations est basée sur une approche chronologique de la vie des produits/services, de la conception à la commercialisation, puis l'usage. Elle ne signifie toutefois nullement que les aspects

---

les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents »).

17 Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM(2021) 206 final, 21 avril 2021, disponible à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=FR.

18 Voy. not. considérants 45 et 81.

19 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, p. 9.

de sécurité liés à des phases ultérieures puissent être négligés dans les phases initiales de développement d'un produit/service. En effet, à l'instar de l'exigence du « *privacy-by-design* » promue par le RGPD[20], l'existence de risques de sécurité doit être prise en compte dès la conception (approche *security-by-design*)[21]. Le récent Règlement établissant un centre de compétences européen en matière de cybersécurité définit d'ailleurs la promotion de cette approche « *security-by-design* » comme un objectif fondamental[22].

§ 1. Les obligations de nature préventive

11. Les obligations préventives et d'analyse préalable des risques sont le plus souvent définies par une référence explicite au niveau de risques et à une exigence de proportionnalité des mesures adoptées afin d'y répondre.

20 Article 25.

21 En ce sens à propos de l'intelligence artificielle, voy. Y. POULLET, *Le RGPD face aux défis de l'intelligence artificielle*, Bruxelles, Larcier, 2020, pp. 84-90. La récente proposition de règlement sur l'intelligence artificielle consacre d'ailleurs l'obligation de *security-by-design*. Voy. Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM(2021) 206 final, 21 avril 2021, disponible à l'adresse https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=FR, article 15 : « *High-risk AI systems shall be* ***designed and developed*** *in such a way that they achieve, in the light of their intended purpose, an* ***appropriate level of*** *accuracy, robustness and* ***cybersecurity****, and perform consistently in those respects throughout their lifecycle* » (nous soulignons).

22 Règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination ; *JOUE*, L202, 8 juin 2021, p. 1, considérant 37 : « *Afin de créer un environnement de cybersécurité viable, il importe que la sécurité dès la conception soit mise en œuvre en tant que principe dans le processus de développement, de maintenance, d'exploitation et de mise à jour des infrastructures, des produits et des services, notamment en soutenant des méthodes de développement sûres de pointe, des essais de sécurité et des audits de sécurité appropriés, en mettant à disposition, sans tarder, des mises à jour remédiant aux vulnérabilités ou menaces connues et en permettant aux tiers, lorsque c'est possible, de créer et de fournir des mises à jour au-delà de la durée de vie respective de chaque produit. La sécurité dès la conception devrait être assurée sur l'ensemble du cycle de vie des produits, services ou processus TIC, ainsi que grâce à des processus de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante* ». Voy. aussi l'article 4, qui énonce parmi les objectifs du Centre de compétences « […] *promouvoir la résilience en matière de cybersécurité, l'adoption de bonnes pratiques en matière de cybersécurité,* ***le principe de la sécurité dès le stade de la conception*** *et la certification de la sécurité des produits et services numériques, d'une façon qui complète les efforts déployés par d'autres entités publiques* » (nous soulignons).

On relèvera ainsi l'obligation du prestataire de services de paiement de mettre en œuvre des mesures de sécurité « *proportionnées aux risques de sécurité concernés* »[23]. Cette proportionnalité entre le risque et les mesures conduit à ce que cette obligation autorise des assouplissements pour les paiements sans contact de faible valeur (considérant 96).

De même, la loi belge de transposition de la directive NIS prévoit que les opérateurs de services essentiels prennent les « *mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques* »[24].

Mieux encore, l'obligation de sécurité du responsable du traitement et du sous-traitant en matière de données à caractère personnel illustre à la perfection l'approche législative commentée : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :*

a) *la pseudonymisation et le chiffrement des données à caractère personnel ;*
b) *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
c) *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 ;*
d) *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* »[25].

La construction de la règle est remarquable. Après avoir lié la portée de l'obligation à l'état de l'art, le texte renvoie à une analyse préalable du

23 Directive 2015/2366, considérant 91 et article 95.

24 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, *MB*, 3 mai 2019, p. 42857, article 20.

25 Règlement 2016/679, article 32.

risque par rapport à la nature du traitement, afin d'imposer une obligation d'adopter les mesures nécessaires permettant d'assurer un niveau de sécurité adapté à ce risque, avec une liste exemplative de mesures à considérer dans le cadre de cette analyse.

Toujours dans cette logique de gestion des risques, le RGPD ajoute une obligation d'*accountability*[26], qui impose au responsable du traitement de démontrer qu'il s'est conformé aux obligations du RGPD. Cela exige une documentation de toute action de mise en conformité. Par conséquent, toute l'analyse de risques requise par la mise en œuvre de l'obligation de sécurité contenue dans le RGPD se doit d'être documentée d'une manière adéquate. À défaut, en cas d'incident, l'autorité de contrôle pourrait considérer que le responsable a failli à ses obligations par une analyse inappropriée des risques ayant conduit à un choix de mesures de sécurité insuffisantes[27].

La sécurité ne peut être assurée que moyennant une démarche intégrant toute la chaîne d'approvisionnement[28]. C'est pour cela que les obligations de sécurité ne se cantonnent pas au prestataire principal, mais s'étendent au-delà[29].

12. Si la démarche d'évaluation préalable des risques s'apparente le plus souvent à un exercice d'analyse technique et opérationnelle, le législateur va parfois plus loin.

En effet, la Cour de justice de l'Union européenne a donné une interprétation très rigoureuse des exigences du RGPD, qui tend à imposer au responsable du traitement une analyse juridique quant aux risques spécifiques posés par le transfert de données à caractère personnel vers certains États hors de l'Union européenne. En effet, dans son arrêt *Schrems II*, la Cour impose au responsable du traitement d'opérer une analyse du risque juridique lié au droit et aux pratiques administratives de l'État de destination des données lorsque cet État n'a pas fait l'objet d'une décision

26 Article 5.2. S'il est fait référence au terme « responsabilité » dans la version française du RGPD, la portée de l'obligation nous semble mieux décrite par le terme « *accountability* » de la version anglaise.

27 Analyse menée en amont de sa décision quant au choix des mesures de sécurité déployées.

28 Insistant sur l'importance de la sécurité de la chaîne d'approvisionnement, voy. A. Mantelero, G. Vaciago, M. Samatha Esposito et N. Monte, « The common EU approach to personal data and cybersecurity regulation », *International Journal of Law and Information Technology*, 2020/28, p. 327.

29 Voy. l'article 28 RGPD (sous-traitants). Voy. aussi le considérant 60 de la proposition de directive sur l'intelligence artificielle.

d'adéquation au sens de l'article 45 du RGPD[30]. Les recommandations publiées par l'EDPB[31] ont confirmé cette approche sans toutefois fournir de solution facilement exploitable[32].

Imposer une telle analyse juridique revient à reporter sur le responsable du traitement un poids excessivement lourd. Il est en effet peu réaliste d'exiger d'un opérateur individuel – privé de surcroît – de porter un jugement sur le caractère approprié des dispositifs de sauvegarde contenus dans un droit étranger, et, pire, d'évaluer si les pratiques du gouvernement de ce même État sont acceptables au regard du RGPD et des droits fondamentaux protégés au sein de l'Union européenne. Sur quelles bases un opérateur individuel peut-il effectuer d'une manière fiable une telle analyse, que ni la Commission européenne, ni l'EDPB, ni les autorités nationales de contrôle ne semblent pouvoir (vouloir ?) effectuer ? La portée des obligations contenues dans le RGPD devrait ici trouver ses limites, à défaut pour le législateur européen et les autorités de contrôle de donner des indications pratiques raisonnables quant à la portée de l'obligation des responsables de traitements[33]. Les conséquences de cette jurisprudence semblent claires. Par contre, la mise en œuvre pratique par les responsables du traitement fera sans doute couler beaucoup d'encre, car

30 CJUE, 16 juillet 2020, *Schrems II*, C-311/18, disponible sur le site web de la Cour, à l'adresse https://curia.europa.eu/juris/document/document.jsf;jsessionid=2D00F54CAD11920FB869F437734443DA?text=&docid=228677&page Index=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=4559398.

31 EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, version 2.0, 18 juin 2021, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

32 « *You must first assess, where appropriate in collaboration with the importer, if there is anything in the law and/or practices in force41 in the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer. This implies determining whether your transfer falls within the scope of legislation and/or practices which may impinge on the effectiveness of your Article 46 GDPR transfer tool. The assessment required must be based first and foremost on legislation publicly available* » (*Ibid.*, pt 30).

33 Si une liste noire est sans doute politiquement trop délicate, une liste grise mettant en regard les États présentant des risques jugés excessifs avec les mesures supplémentaires recommandées permettrait d'assurer une cohérence et une clarté dans la mise en œuvre des conséquences de cet arrêt de la Cour de justice. En l'absence de tels outils, la grande majorité des responsables de traitement ne pourra (ou ne voudra) se livrer à une telle analyse et procédera à une analyse de pure forme visant à simplement documenter le respect d'une exigence légale dont les contours sont par trop imprécis. L'arrêt *Schrems II* aura alors été un coup dans l'eau.

les difficultés sont réelles et la validation des autorités de contrôle très aléatoire à défaut de lignes directrices précises[34].

13. Au-delà des obligations directes de sécurité, d'autres obligations peuvent contribuer à une bonne gestion du risque de cybersécurité. Ainsi, lorsque le RGPD impose le principe de minimisation des données[35] et le principe de limitation de durée de conservation[36], la sécurité du traitement est en filigrane de ces obligations. En effet, une stratégie de minimisation des données permet de limiter les risques en cas d'incident de sécurité ou de fuite de données[37]. À l'inverse, cette même exigence de minimisation peut imposer des limites à l'usage d'outils techniques de sécurité[38].

14. Un autre moyen indirect de promouvoir un renforcement de la sécurité des services numériques consiste à favoriser les services présentant un niveau de sécurité supérieur. Le Règlement eIDAS[39], bien que contenant un principe de non-discrimination, confère ainsi une valeur juridique renforcée aux dispositifs reposant sur un niveau de sécurité plus élevé[40]. Le Règlement définit de la sorte une hiérarchie entre les dispositifs simples, avancés et qualifiés, avec un régime juridique incitant les utilisateurs à préférer les solutions intégrant davantage de sécurité.

---

34 Un arrêt *Schrems III* semble probable, avec persistance de l'insécurité juridique dans l'intervalle… On ne peut que le regretter.

35 Article 5.1, c) du RGPD, énonçant 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]* ».

36 Article 5.1, d) du RGPD se référant à l'exigence que les données à caractère personnel soient « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées […]* ».

37 A. Mantelero, G. Vaciago, M. Samatha Esposito et N. Monte, « The common EU approach to personal data and cybersecurity regulation », *International Journal of Law and Information Technology*, 2020/28, p. 301.

38 À propos de l'usage des *log files*, voy. l'analyse approfondie de F. Dumortier, « Cybersécurité, vie privée imputabilité, journalisation et *log files* », *DCCR*, 2019/122-123, pp. 220-228.

39 Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE*, L257, 28 août 2014, p. 73.

40 Voy. le considérant 48 qui expose la nécessité de tolérer des services moins sûrs dans certains cas, mais soumettant la reconnaissance mutuelle à une exigence de sécurité supérieure.

§ 2. Les obligations postérieures à un incident de sécurité

15. Sans entrer dans une étude exhaustive, l'on peut relever principalement quatre types d'obligations relatives au suivi d'un incident de sécurité :

– l'obligation de mettre en place des procédures de gestion et suivi des incidents[41] ;

– l'obligation d'analyse post-incident et d'adoption de mesures d'atténuation ;

– l'obligation de réparer les conséquences dommageables de l'incident ;

– l'obligation de notifier l'incident à une autorité de contrôle et/ou aux personnes potentiellement affectées par les conséquences de l'incident.

16. La mise en place de procédures de gestion coordonnée des incidents de sécurité avait été identifiée comme un objectif majeur dès la Communication de 2013 sur la stratégie de sécurité européenne de cybersécurité[42]. L'actualisation de cette stratégie en 2020 prévoit un renforcement du réseau des centres de sécurité nationaux, notamment afin de promouvoir les bonnes pratiques au sein des PME, et une révision de la directive NIS[43]. Il s'agit donc d'un axe important de la réglementation relative à la cybersécurité.

Dans les textes actuellement en vigueur, l'on soulignera que la loi belge de transposition de la directive NIS prévoit que l'opérateur de services essentiels « *notifie, sans retard, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité*

41 D'un point de vue théorique, l'on pourrait discuter de la nature préventive ou curative de ces mesures, puisqu'elles ne sont mises en œuvre qu'après un incident. Par analogie, un airbag est considéré comme relevant de la sécurité passive d'une automobile car il ne permet pas de limiter les risques qu'un accident se produise. Il semble donc logique de classer ces mesures en tant que mesures d'atténuation des effets d'un incident.

42 Commission européenne et Haute Représentante de l'Union pour les Affaires étrangères et la sécurité, Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des Régions, *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, JOIN (2013) 1 Final, 7 février 2013, disponible sur le site officiel de l'Union européenne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013JC0001&from=HU, p. 6.

43 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, pp. 5-7.

des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit »[44].

Bien que la loi belge ne prévoie pas explicitement une obligation de mise en place d'une procédure de gestion des incidents, l'existence d'une telle obligation ne peut faire aucun doute. En effet, l'article 28 de la même loi prévoit que la gestion des incidents est de la responsabilité des opérateurs de services essentiels, alors que la définition de la notion de « *gestion d'incident* » se réfère à « *toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident* »[45]. En outre, le respect de l'exigence de notification « *sans retard* » de tous les incidents ayant un impact significatif sur les systèmes d'information qu'ils utilisent[46] impose indirectement aux opérateurs de services essentiels la mise en place de procédures de gestion des incidents.

La directive NIS n'est pas davantage explicite sur ce point, sauf pour les fournisseurs de services numériques[47]. Précisons toutefois que la proposition de directive NIS 2 impose cette fois explicitement l'adoption de mesures techniques et organisationnelles assurant un niveau de sécurité approprié, ces mesures devant « à tout le moins inclure : […] b) la gestion des incidents (prévention, détection et réponse aux incidents) […] »[48].

---

44 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, *MB*, 3 mai 2019, p. 42857, article 24.

45 Article 6, 14°.

46 Article 24 précité.

47 Directive 2016/1145, article 16 : « Les États membres veillent à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III, et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants : a) la sécurité des systèmes et des installations ; b) la gestion des incidents ; c) la gestion de la continuité des activités ; d) le suivi, l'audit et le contrôle ; e) le respect des normes internationales » (nous soulignons).

48 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16 décembre 2020, disponible sur le site de la Commission européenne : https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (article 18.2, traduction libre).

La directive relative aux services de paiements prévoit quant à elle expressément la mise en place de procédures de gestion des incidents de sécurité à charge des prestataires de services[49].

Dans le cadre du RGPD, l'obligation de mise en place d'une procédure de gestion des incidents n'est pas explicite, mais découle nécessairement de la combinaison des obligations à charge du responsable du traitement[50]. En effet, l'article 33 du RGPD énonce que :

> « 1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
>
> […]
>
> 3. La notification visée au paragraphe 1 doit, à tout le moins : a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ; b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; c) décrire les conséquences probables de la violation de données à caractère personnel ; d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
>
> […]
>
> 5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour

49 Directive 2015/2366, article 95 : « Les États membres veillent à ce que les prestataires de services de paiement établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité, liés aux services de paiement qu'ils fournissent. Ce cadre prévoit que les prestataires de services de paiement établissent et maintiennent des procédures efficaces de gestion des incidents, y compris pour la détection et la classification des incidents opérationnels et de sécurité majeurs ».

50 Dans le même sens, voy. F. Dumortier, « Les obligations de sécurité et de notification des violations de traitements de données à caractère personnel », in *Les obligations légales de cybersécurité et de notifications d'incidents*, Bruxelles, Politeia, 2019, pp. 90-91 (soulignant la nécessité pratique de disposer d'une procédure de gestion d'incidents afin de pouvoir se conformer à ces obligations).

y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article ».

Le principe d'*accountability* énoncé à l'article 5 requiert donc que le responsable du traitement soit en mesure de justifier toute action dans le suivi d'un incident (le suivi imposant de procéder à l'analyse des effets sur les droits des personnes concernées et à la documentation de celle-ci pour pouvoir justifier les mesures prises et la décision de notifier ou pas l'incident à l'autorité de contrôle et, le cas échéant, aux personnes concernées)[51].

17. L'obligation d'analyse des incidents et d'adoption de mesures d'atténuation constitue le corollaire de l'obligation préventive d'adopter des mesures de sécurité appropriées aux risques. En effet, la sécurité totale étant une vue de l'esprit, il convient d'anticiper la possible survenance d'un incident de sécurité, afin que ses effets puissent être contenus et sa propagation évitée.

Ici encore, l'approche consiste à se référer à une obligation non spécifique permettant d'assurer un niveau de sécurité adapté au risque concerné[52]. La nécessaire collaboration avec les fournisseurs constitue un point crucial dans la gestion des incidents, car les failles de sécurité peuvent trouver leur origine dans des vulnérabilités des produits ou services des fournisseurs[53]. Il est donc logique que les obligations aient une portée qui englobe ces relations avec les fournisseurs et sous-traitants[54]. La proposition de directive NIS 2 vise d'ailleurs à imposer que les mesures appropriées englobent la sécurité tout au long de la chaîne

51 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 – Analyse approfondie*, Collection du CRIDS, n° 44, Bruxelles, Larcier, 2018, p. 177 (soulignant que le principe d'accountability renforce considérablement la nature de l'obligation de sécurité).

52 Voy. par exemple, la disposition précitée de la proposition de directive NIS 2 ou encore l'article 95 de la directive 2015/2366.

53 En ce sens, voy. 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 – Analyse approfondie*, Collection du CRIDS, n° 44, Bruxelles, Larcier, 2018, p. 176.

54 Voy. ainsi l'article 32 du RGPD, qui vise explicitement le responsable du traitement et le sous-traitant, en imposant à ce dernier une obligation légale de sécurité distincte de celle du responsable du traitement. L'article 28 du RGPD ajoute que le choix du sous-traitant doit être guidé par les garanties que celui-ci offre quant à la conformité aux exigences légales (notamment de sécurité) et impose une formalisation des garanties dans un contrat ou un autre acte juridique qui doit prévoir l'engagement du sous-traitant d'adopter toutes les mesures requises au titre de l'article 32 du RGPD.

d'approvisionnement en précisant les relations entre les différentes entités selon leurs rôles respectifs[55].

18. L'obligation de réparer les conséquences dommageables vise quant à elle un double objectif : renforcer la confiance des utilisateurs et inciter les prestataires de services à ne pas négliger leurs obligations préventives en matière de sécurité.

Ainsi, le RGPD envisage la réparation d'une manière large, en prévoyant une responsabilité solidaire (ou *in solidum*) entre le responsable et le sous-traitant, afin de renforcer la protection de toute personne subissant un préjudice du fait de la violation des obligations légales (dont celle de sécurité)[56].

19. L'obligation de notification des incidents s'impose compte tenu des risques de propagation des incidents de sécurité. Il est donc logique que le législateur en ait fait un élément clé des dispositifs sur la cybersécurité.

L'obligation de notification constitue ainsi un rouage central des règles sur la sécurité dans le RGPD[57]. Pareillement, la directive sur les services de paiement et le règlement eIDAS imposent une double notification des incidents, en fonction de l'éventuel risque pour les utilisateurs des services concernés[58]. La notification est donc, à juste titre, perçue comme un instrument visant à promouvoir la résilience des systèmes, en évitant une extension des incidents à d'autres services que ceux initialement affectés, et la confiance des utilisateurs, en prévoyant une information spécifique à leur égard visant à leur permettre de prendre toute mesure utile d'atténuation du préjudice potentiel.

La directive *e-privacy*[59] comporte une obligation de notification à charge du fournisseur d'un service de communications électroniques accessible

55 Voy. l'article 18.2, d), qui vise « supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services ».

56 Sur la portée de ce régime et ses limites, voy. K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD », in *Le Règlement général sur la protection des données – Analyse approfondie*, Collection du CRIDS, n° 44, Bruxelles, Larcier, 2018, pp. 679-681.

57 L'article 33 du RGPD consacre une obligation de notification étendue, visant à permettre une analyse des risques ultérieurs tant par les autorités de contrôle que par les personnes concernées.

58 Voy. Directive 2015/2366, article 96 et Règlement eIDAS, article 19.

59 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *JOUE*, L201, 31 juillet 2002, p. 37.

au public[60], dont la portée couvre non seulement les incidents avérés, mais également les risques de violation de la sécurité du réseau[61].

La portée de ces obligations devrait logiquement s'étendre dans les prochains textes, la stratégie de l'Union européenne[62] soulignant que le partage d'informations et de bonnes pratiques[63] sont essentiels afin d'améliorer le niveau général de sécurité et de résilience des systèmes d'information et services numériques. La récente proposition de directive NIS 2 comporte d'ailleurs un élargissement des obligations d'information, avec notamment : une obligation de notification dans les 24 heures en cas d'incident (article 20), la création d'une base de données sur les vulnérabilités des produits et services (article 6), l'obligation de *reporting* non seulement des incidents, mais également des menaces identifiées (article 20)[64].

20. L'importance de la cybersécurité se traduit également par la protection des lanceurs d'alerte lorsqu'ils révèlent des violations de la directive sur la sécurité des réseaux et systèmes d'information (directive NIS). L'intérêt général[65] exige de protéger les personnes qui contribuent à la révélation d'incidents de sécurité[66].

---

60 Art. 4.2 de la directive *e-privacy* et art. 114/1 de la loi du 13 juin 2005 relative aux communications électroniques.

61 Pour une comparaison avec les obligations du RGPD, voy. F. Coton et J.-F. Henrotte, « Données à caractère personnel et sécurité des systèmes d'information : quand faut-il siffler la fin de la récréation ? », in *Time to Re-shape the Digital Society*, Actes de la conférence célébrant les 40 ans du CRIDS, à paraître.

62 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN(2020) 18 Final, 16 décembre 2020, disponible sur https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, spéc. pp. 3, 6-7, 13-14.

63 Par exemple, en termes de mesures d'atténuation prises rapidement après la découverte d'un incident.

64 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16 décembre 2020, disponible sur le site de la Commission européenne : https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union. La directive e-privacy.

65 Faisant le lien entre la protection des lanceurs d'alerte et l'intérêt général, voy. not. Rapport sur la proposition de directive du Parlement européen et du Conseil sur la protection des personnes dénonçant les infractions au droit de l'Union, Commission des affaires juridiques, A8-0398/2018, COM(2018)0218 – C8-0159/2018 – 2018/0106(CNS), 26 novembre 2018, p. 145. Sur la notion d'intérêt général au sens de la directive 2019/1937, voy. A. Lachapelle, « L'encadrement juridique du lancement d'alerte au sein de l'Union européenne. Commentaire de la directive sur les lanceurs d'alerte », *RDTI*, 2020/1-2, pp. 30-33.

66 Directive 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union, *JOUE*, L305, 26 novembre 2019, p. 17, considérant 14 et article 2.

Section 3. Conclusion

21. En raison de son caractère par essence global, la cybersécurité ne peut être efficacement régulée sans une approche internationalement coordonnée. Comme souvent, le niveau européen constitue un laboratoire en vue de promouvoir une évolution des règles en la matière.

L'analyse panoramique livrée dans la présente fait apparaître plusieurs éléments clés.

22. Tout d'abord, un socle commun de règles (plus ou moins largement) transversales semble nécessaire, mais avec des règles spécifiques en complément lorsque des risques particuliers sont identifiés. Pas d'approche monolithique, donc.

23. Ensuite, la notion de gestion des risques apparaît comme la pierre angulaire de toute réglementation sur la sécurité.

Le développement du cadre européen l'illustre parfaitement. L'intégration des analyses de risques à tous les stades de mise en application des obligations légales constitue une évolution marquante dans la réglementation. La souplesse que cette approche permet a pour corollaire la nécessaire documentation des décisions prises par les destinataires des règles légales. En effet, lorsque l'application de la règle repose sur une analyse de risques tout au long du cycle de mise en œuvre, comment établir le respect des obligations concernées sans documentation ?

24. La détermination du caractère approprié des mesures de sécurité est donc guidée par une analyse de risques laissée aux mains du destinataire de l'obligation, et non plus une analyse faite en amont de l'adoption d'une loi qui prescrirait les mesures à prendre. La cybersécurité imposait sans doute une telle approche, afin d'éviter l'adoption de textes immédiatement obsolètes.

L'orientation pose toutefois question par rapport à la capacité des acteurs économiques à procéder à ce type d'analyses, parfois très complexes. À cet égard, les actions menées par l'Union européenne afin de promouvoir une culture de la sécurité et de faciliter les échanges d'informations sont cruciales afin de rendre la cybersécurité accessible à toutes les PME qui constituent la majorité du tissu économique de l'Union européenne.

Le choix d'une réglementation basée sur une analyse de risques par les destinataires de la norme impose de repenser le rôle du législateur, avec une responsabilité accrue dans l'accompagnement et le soutien aux destinataires dans le but de faciliter une bonne mise en œuvre.

25. Ces brèves réflexions nous mènent naturellement à rendre hommage à Denis Philippe. En effet, dans sa pratique du droit, Denis fait

volontiers « confiance à l'équipe » pour évaluer les risques d'une stratégie juridique, mais sans jamais négliger pour autant son rôle de support et de guide. Le tout, dans une atmosphère marquée par une cordialité sans failles. Une approche très en ligne avec celle du législateur européen[67], donc.

67 La cordialité en plus.