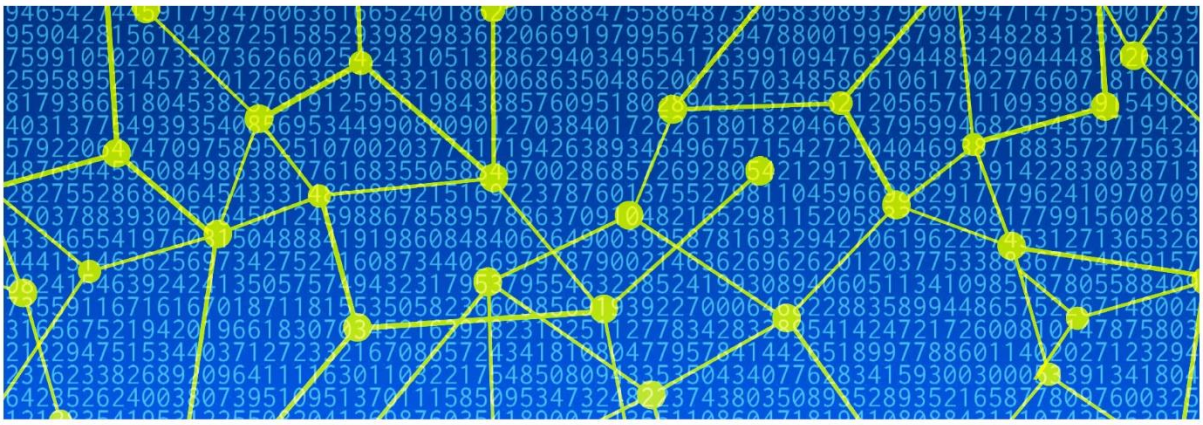

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 5/2021

sur la stratégie en matière de cybersécurité et la directive SRI 2.0

EDPS

11 mars 2021

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

En vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le présent avis est rendu par le CEPD dans le délai de huit semaines à compter de la réception de la demande de consultation prévue à l'article 42, paragraphe 3, du règlement (UE) 2018/1725, compte tenu de l'incidence sur la protection des droits et des libertés des personnes à l'égard du traitement des données à caractère personnel de la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148.

Synthèse

Le 16 décembre 2020, la Commission européenne a adopté une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (ci-après la «proposition»). Parallèlement, la Commission européenne et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont publié une communication conjointe au Parlement européen et au Conseil, intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique» (ci-après la «stratégie»).

Le CEPD soutient pleinement l'objectif général de la stratégie visant à garantir un internet ouvert et mondial doté de solides garde-fous pour faire face aux risques pour la sécurité et les droits fondamentaux, tout en reconnaissant la valeur stratégique de l'internet et de sa gouvernance et en renforçant l'action de l'Union en la matière grâce à un modèle multipartite.

Par conséquent, le CEPD se félicite également de l'objectif de la proposition consistant à apporter des modifications systémiques et structurelles à l'actuelle directive SRI, afin de couvrir un ensemble plus large d'entités dans l'Union, avec des mesures de sécurité renforcées, notamment l'obligation de gestion des risques, la création de normes minimales et la mise en place de dispositions pertinentes en matière de surveillance et d'exécution. À cet égard, le CEPD estime **qu'il est nécessaire d'intégrer pleinement les institutions, organes et organismes de l'Union dans le cadre général de cybersécurité à l'échelle de l'UE,** afin de garantir un niveau de protection uniforme, **en incluant explicitement les institutions, organes et organismes de l'Union dans le champ d'application de la proposition**.

Le CEPD souligne en outre l'importance d'**intégrer la dimension de la protection de la vie privée et des données dans les mesures de cybersécurité** découlant de la proposition ou des autres initiatives de la stratégie en matière de cybersécurité, de façon à garantir une approche holistique et à permettre des synergies dans la gestion de la cybersécurité et la protection des informations personnelles traitées par les institutions européennes. De même, il est important que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel suscitée par ces mesures respecte les critères énoncés à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, et, en particulier, qu'elle soit mise en œuvre par le biais d'une mesure législative et qu'elle soit à la fois nécessaire et proportionnée.

Le CEPD s'attend à ce que **la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel**, y compris les missions et les pouvoirs des autorités de contrôle indépendantes chargées de contrôler le respect de ces instruments. En d'autres termes, tous les systèmes et services de cybersécurité intervenant dans la prévention, la détection et la réaction aux cybermenaces devraient être conformes au cadre actuel de protection de la vie privée et des données. À cet égard, le CEPD estime qu'il est important et nécessaire d'établir une définition claire et univoque du terme «cybersécurité» aux fins de la proposition.

Le CEPD formule des recommandations spécifiques pour s'assurer que la proposition **complète** de manière correcte et efficace **la législation existante de l'Union en matière de protection des données à caractère personnel**, en particulier le RGPD et la directive «vie privée et communications électroniques», en faisant appel également au CEPD et au comité européen de protection des données lorsque cela est nécessaire, et en établissant des mécanismes clairs pour la collaboration entre les autorités compétentes des différents domaines réglementaires.

En outre, les dispositions relatives à la gestion des **registres des domaines de premier niveau de l'internet** devraient définir clairement le champ d'application et les conditions pertinentes dans la loi. Le concept de scannage proactif des réseaux et des systèmes d'information par les CSIRT nécessite également des clarifications supplémentaires en ce qui concerne le champ d'application et les types de données à caractère personnel traitées. L'attention est attirée sur les risques d'éventuels transferts de données non-conformes liés à la sous-traitance de services de cybersécurité ou à l'acquisition de produits de cybersécurité ainsi qu'à leur chaîne d'approvisionnement.

Le CEPD **se félicite de l'appel visant à promouvoir l'utilisation du chiffrement**, et en particulier du chiffrement de bout en bout, et réitère sa position sur la question du cryptage, qu'il considère comme une technologie critique et irremplaçable pour assurer une protection efficace des données et de la vie privée, et dont le contournement priverait le mécanisme de toute capacité de protection en raison du risque d'utilisation illicite et de la perte de confiance dans les contrôles de sécurité. À cet effet, il convient de préciser **que rien dans la proposition ne devrait être interprété comme un avis favorable à l'affaiblissement du chiffrement de bout en bout** par le biais de «portes dérobées» ou de solutions similaires.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne (la «charte»), et notamment ses articles 7 et 8,

vu le 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)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données[2], et notamment son article 42, paragraphe 1, son article 57, paragraphe 1, point g), et son article 58, paragraphe 3, point c),

vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[3],

A ADOPTÉ LE PRÉSENT AVIS:

1. INTRODUCTION

1. Le 16 décembre 2020, la Commission européenne a adopté une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148[4] (ci-après la «proposition»).

2. À la même date, la Commission européenne et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont publié une communication conjointe au Parlement européen et au Conseil, intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique» (ci-après la «stratégie»).[5]

3. La stratégie vise à renforcer l'autonomie stratégique de l'Union dans les domaines de la cybersécurité et à améliorer sa résilience et sa réponse collective, ainsi qu'à construire un internet mondial et ouvert doté de solides garde-fous pour faire face aux risques pour la sécurité et les libertés et droits fondamentaux des citoyens en Europe[6].

4. La stratégie contient des propositions d'initiatives réglementaires, d'investissement et de politique dans trois domaines d'action de l'Union: (1) la résilience, la souveraineté technologique et le leadership, (2) le renforcement des capacités opérationnelles de prévention, de dissuasion et de réaction, et (3) la promotion d'un cyberespace mondial et ouvert.

5. La proposition constitue l'une des initiatives réglementaires de la stratégie, en particulier dans les domaines de la résilience, de la souveraineté technologique et du leadership.

6. Selon l'exposé des motifs, l'objectif de la proposition est de moderniser le cadre juridique existant, à savoir la directive (UE) 2016/1148 (ci-après la «directive SRI»)[7]. La proposition vise à capitaliser sur l'actuelle directive SRI, qu'elle abroge, et qui était le premier acte législatif adopté à l'échelle de l'Union européenne dans le domaine de la cybersécurité et prévoyait des mesures juridiques pour renforcer le niveau général de cybersécurité dans l'Union. La proposition tient compte de l'utilisation croissante de supports et formats numériques dans le marché intérieur ces dernières années et de l'évolution du paysage des menaces qui pèsent sur la cybersécurité, qui se sont encore amplifiées depuis le début de la pandémie de COVID-19. La proposition vise à combler plusieurs lacunes identifiées dans la directive SRI et à accroître le niveau de cyber-résilience de tous les secteurs, publics et privés, qui remplissent une fonction importante pour l'économie et la société.

7. Les principaux éléments de la proposition sont les suivants:

   (i) étendre le champ d'application de l'actuelle directive SRI par l'ajout de nouveaux secteurs en fonction de leur niveau de criticité pour l'économie et la société;
   (ii) renforcer les exigences en matière de sécurité pour les entreprises et les entités couvertes, en imposant une approche de gestion des risques prévoyant une liste minimale d'éléments de sécurité de base qui doivent être appliqués obligatoirement;
   (iii) aborder la question de la sécurité des chaînes d'approvisionnement et des relations avec les fournisseurs en exigeant des entreprises individuelles qu'elles répondent aux risques de cybersécurité liés aux chaînes d'approvisionnement et aux relations avec les fournisseurs;
   (iv) accroître la coopération entre les autorités des États membres et avec les institutions, organes et organismes de l'Union pour traiter les activités liées à la cybersécurité, y compris la gestion des crises cyber.

8. Le 14 janvier 2021, le CEPD a reçu une demande de consultation formelle de la Commission européenne sur la «proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148».

2. OBSERVATIONS GÉNÉRALES

2.1. Concernant la stratégie de cybersécurité

9. Le CEPD se réjouit de la stratégie de cybersécurité et soutient pleinement l'objectif visant à garantir un internet ouvert et mondial doté de solides garde-fous pour faire face aux risques pour la sécurité et les droits fondamentaux, tout en reconnaissant la valeur stratégique de l'internet et de sa gouvernance et en renforçant l'action de l'Union en la matière grâce à un modèle multipartite.

10. L'article 5, paragraphe 1, point f), du règlement (UE) 2016/679 (RGPD)[8] a posé la sécurité comme l'un des grands principes relatifs au traitement des données à caractère personnel. L'article 32 du RGPD définit plus précisément l'obligation – applicable tant aux responsables du traitement qu'aux sous-traitants – de garantir un niveau de sécurité approprié. Ces deux dispositions indiquent clairement que la sécurité est essentielle au respect de la législation européenne en matière de protection des données. C'est pourquoi le CEPD convient que l'amélioration de la cybersécurité est essentielle à la sauvegarde des

droits et libertés fondamentaux, y compris du droit au respect de la vie privée et à la protection des données à caractère personnel, et soutient fermement la proposition d'un ensemble complet de mesures techniques et organisationnelles appropriées et efficaces.

11. Dans le même temps, le CEPD rappelle que la poursuite des objectifs de cybersécurité peut donner lieu au déploiement de mesures qui constituent une ingérence dans les droits à la protection des données et au respect de la vie privée des personnes. Il convient donc de veiller à ce que toute limitation potentielle du droit à la protection de la vie privée et des données à caractère personnel réponde aux exigences de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, et en particulier qu'elle soit mise en œuvre par le biais d'une mesure législative, qu'elle soit à la fois nécessaire et proportionnée[9] et qu'elle respecte le contenu essentiel du droit.

12. Les règles de sécurité, les politiques de sécurité et les normes de sécurité constituent l'épine dorsale d'une bonne gestion de la cybersécurité et de la sécurité de l'information. Aussi le CEPD se félicite-t-il tout particulièrement de l'objectif de la stratégie de créer:
    - des règles de sécurité pour la cybersécurité ainsi que la sécurité de l'information des institutions, organes et organismes de l'Union;
    - des règles de sécurité pour la cybersécurité de tous les produits connectés (IdO) et des services associés;
    - des normes de sécurité sur la sécurité de la 5G et des réseaux mobiles de future génération, avec un accent particulier sur la sécurité de la chaîne d'approvisionnement.

13. Le CEPD soutient pleinement les initiatives de la stratégie en matière de «souveraineté et de leadership technologiques». Dans sa stratégie pour 2020-2024[10], le CEPD a exprimé son soutien fort aux initiatives politiques visant à promouvoir la «souveraineté numérique» pour faire en sorte que les données générées en Europe se transforment en valeur pour les entreprises et les citoyens européens et soient traitées dans le respect des valeurs européennes. Le CEPD se félicite donc en particulier des initiatives suivantes:
    - la mise en place d'un réseau européen de centres des opérations de sécurité dans toute l'UE;
    - l'initiative visant à déployer une infrastructure de communication quantique (QCI) sûre exploitant les technologies européennes;
    - la mise au point d'un service public de résolution de noms de domaine de l'UE; et
    - la création du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et du Réseau de centres nationaux de coordination (CCCN), qui contribueront au développement de la souveraineté technologique de l'Union ainsi qu'à la réduction de la dépendance vis-à-vis d'autres parties du monde pour les technologies les plus cruciales.

14. Le CEPD est conscient du potentiel de l'intelligence artificielle dans le développement de capacités de cybersécurité de pointe pour la **détection, l'analyse, la maîtrise et la réponse en temps réel** aux cybermenaces dans un paysage numérique en constante expansion. Cependant, ces technologies nécessitent généralement le traitement de grandes quantités de données à caractère personnel (comme les données des journaux d'utilisateurs) et comportent leurs propres risques (comme le manque de transparence ou les biais dans les données), qu'il convient d'identifier et d'atténuer. L'utilisation de technologies pour améliorer la cybersécurité ne devrait pas constituer une ingérence indue dans les droits et libertés des personnes. La première étape pour éviter ou atténuer ces risques consiste à

appliquer les **exigences de protection des données dès la conception et par défaut visées à l'article 25 du RGPD**, ce qui permettra d'intégrer les garanties appropriées, telles que la pseudonymisation, le chiffrement, l'exactitude des données et la minimisation des données, dans la conception et l'utilisation de ces technologies et systèmes.

15. Si la sécurité des informations traitées par les organisations et les infrastructures critiques et importantes, telles que recensées dans la proposition, est de la plus haute importance pour l'économie et la société de l'Union, la protection de la vie privée et des données à caractère personnel est également largement soutenue par les petites et moyennes entreprises (PME) fournissant des services numériques, et, à cet égard, il est nécessaire de promouvoir la sensibilisation et le développement des compétences des personnes en matière de cybersécurité. **C'est pourquoi le CEPD salue le projet d'adoption généralisée des technologies de cybersécurité grâce à un soutien spécifique aux PME dans le cadre des pôles d'innovation numérique et d'autres instruments**, ainsi que les projets de renforcement de la sensibilisation à la cybersécurité parmi les personnes, en particulier les enfants et les jeunes, et les organisations, en particulier les PME, grâce à la version révisée du plan d'action en matière d'éducation numérique.

16. Le CEPD estime que le législateur, ainsi que les États membres et les institutions de l'UE, devraient prendre en compte le rôle de la cybersécurité dans la protection de la vie privée et des données à caractère personnel en intégrant cette «dimension» dans toutes les actions politiques susmentionnées, et en particulier la nécessité de protéger les personnes et leurs droits fondamentaux et de les considérer comme des actifs à protéger, au même titre que les autres types d'actifs dont ils ont la responsabilité. **L'intégration de la dimension de la protection de la vie privée et des données dans la gestion traditionnelle de la cybersécurité sera garante de l'adoption d'une approche holistique, et permettra aux organisations publiques et privées de bénéficier de synergies dans la gestion de la cybersécurité et dans la protection des informations qu'elles traitent sans multiplier inutilement les efforts.**

17. **Le CEPD se félicite du fait que la stratégie considère les institutions, organes et organismes de l'Union (les «institutions européennes») comme des organisations à défendre, au même titre que les entités et acteurs des États membres, dans le cadre d'une approche coordonnée de la cybersécurité à l'échelle de l'Union.** C'est notamment le cas en ce qui concerne le projet de création d'une unité conjointe de cybersécurité (JCU), qui vise non seulement à améliorer et accélérer la coordination entre tous les acteurs, mais aussi à permettre à l'UE de faire face aux incidents et crises de cybersécurité majeurs et d'y réagir. La stratégie souligne que «*dans le cadre de leur contribution à l'unité conjointe de cybersécurité, les acteurs de l'UE (Commission et agences et organes de l'UE) seront donc prêts à accroître sensiblement leurs ressources et capacités, de manière à renforcer leur état de préparation et leur résilience*». **Le CEPD recommande que les colégislateurs envisagent et prévoient l'utilisation de ces ressources par les institutions européennes** en vue de renforcer les capacités de ces dernières en matière de cybersécurité, et ce d'une manière qui respecte pleinement les valeurs de l'UE.

18. Comme mentionné ci-dessus dans le contexte plus général de la stratégie, le CEPD recommande que les actions et l'augmentation correspondante des ressources prennent en compte les dimensions de la cybersécurité liées à la protection de la vie privée et des données, en investissant dans des politiques, des pratiques et des instruments qui permettent d'intégrer la dimension de la protection de la vie privée et des données dans la gestion

traditionnelle de la cybersécurité, et de mettre en place des garanties de protection des données efficaces dans le traitement de données à caractère personnel effectué dans le cadre d'activités de cybersécurité.

2.2. Concernant la proposition

19. Le CEPD se félicite de l'objectif de la proposition consistant à apporter des modifications systémiques et structurelles à l'actuelle directive SRI afin de couvrir un ensemble plus large d'entités dans l'Union, à l'aide de mesures de sécurité renforcées, notamment en créant des normes minimales et des dispositions appropriées en matière de surveillance et d'exécution, mais aussi en favorisant la collaboration et le partage des responsabilités et la reddition de compte.

20. Le CEPD s'attend à ce que les modifications proposées aient un impact positif sur la sécurité des données à caractère personnel et des communications électroniques, en améliorant à la fois les pratiques de cybersécurité des entités qui sont directement couvertes par la proposition, mais aussi, de manière plus générale, la sécurité de l'internet.

21. Le CEPD se réjouit des nombreuses références à la protection des droits fondamentaux, et en particulier au droit à la protection des données et de la vie privée qui est mentionné dans plusieurs parties du texte de la proposition.

2.3. Concernant le champ d'application de la stratégie et de la proposition aux institutions, organes et organismes de l'Union

22. La stratégie propose des actions spécifiques visant à renforcer et à harmoniser la position des différentes institutions européennes en matière de sécurité de l'information. Parmi ces actions figurent notamment:

    a) deux propositions législatives de règles communes contraignantes en matière de sécurité de l'information et en matière de cybersécurité pour l'ensemble des institutions européennes en 2021;

    b) l'accroissement des investissements pour atteindre un niveau élevé de cybermaturité;

    c) le renforcement de CERT-UE grâce à un mécanisme de financement amélioré.

23. Le CEPD partage la conclusion formulée par la Commission dans la stratégie, selon laquelle le niveau de cyber-résilience et la capacité à détecter les actes de cybermalveillance et à y réagir varient considérablement entre les institutions européennes, en fonction de leur maturité. Le CEPD prend également note de l'engagement des institutions européennes, dont l'ENISA et la Commission, à assurer un niveau élevé de cybersécurité dans les États membres.

24. Le CEPD constate cependant que les dispositions des propositions ne visent que les États membres de l'Union. Compte tenu de la nécessité reconnue d'améliorer le niveau global de cybersécurité grâce à la mise en place de **règles cohérentes et homogènes**, le CEPD **recommande que les colégislateurs prennent en compte les besoins et le rôle des institutions européennes, afin que celles-ci puissent être intégrées dans le cadre global de cybersécurité à l'échelle de l'UE**, et qu'elles bénéficient du même niveau élevé de protection que les entités des États membres.

25. À cet effet, **le CEPD préconise d'inclure explicitement les institutions, organes et organismes de l'Union dans le champ d'application de la proposition**. À défaut, le CEPD recommande aux colégislateurs d'ajouter, dans le texte de la proposition, l'obligation explicite pour la Commission de présenter des propositions législatives distinctes pour les institutions européennes d'ici la fin de l'année 2021, dans le but de créer un lien concret entre la proposition elle-même et la future action législative au niveau des institutions de l'UE, afin d'établir des règles cohérentes et homogènes pour les États membres et les institutions de l'Union.

3. RECOMMANDATIONS SPÉCIFIQUES

26. Le reste du présent avis comporte des recommandations spécifiques visant à garantir que la proposition complète efficacement la législation existante de l'Union en matière de protection des données à caractère personnel, en particulier le RGPD et la directive «vie privée et communications électroniques»[11], et renforce la protection des droits et libertés fondamentaux des personnes concernées.

3.1. Relation avec la législation existante de l'Union en matière de protection des données à caractère personnel

27. Le CEPD observe que la proposition précise, dans différentes parties du texte[12], qu'elle est «sans préjudice» du RGPD et de la directive «vie privée et communications électroniques», mais seulement en lien avec des contextes précis, et parfois seul l'un des deux instruments est mentionné.

28. Le CEPD relève que, pour se conformer à la proposition, les entités couvertes par celle-ci devront déployer des contrôles de cybersécurité spécifiques qui donneront très probablement lieu au traitement de données à caractère personnel et de données de communications électroniques, notamment des données relatives au trafic.

29. Partant, le CEPD considère que l'extension du champ d'application de la proposition à un ensemble plus large d'activités entraînera une augmentation du traitement de données à caractère personnel à des fins de cybersécurité. En outre, le CEPD constate que, conformément à l'article 2, paragraphe 2, la proposition s'applique également aux «réseaux de communications électroniques publics ou aux services de communications électroniques accessibles au public», lesquels sont également couverts par la directive «vie privée et communications électroniques». Par conséquent, il conviendra de prendre en compte les dispositions du RGPD et celles de la directive «vie privée et communications électroniques».

30. Le CEPD relève que les organisations agissant en tant que responsables du traitement et sous-traitants n'ont pas toujours conscience du fait que les données traitées dans des systèmes et des services de cybersécurité peuvent constituer des données à caractère personnel (comme, par exemple, les adresses IP, les identifiants des appareils, les fichiers journaux du réseau, les fichiers journaux de contrôle des accès, etc.). Cette situation donne lieu à un non-respect du RGPD (notamment en ce qui concerne des principes tels que la limitation de la finalité, la limitation de la conservation ou la protection des données dès la conception et par défaut) et des exigences relatives à la conformité des transferts de

données. Le CEPD considère qu'il doit être clairement précisé que tous les systèmes et services de cybersécurité intervenant dans la prévention, la détection et la réaction aux cybermenaces devraient être conformes au cadre actuel de protection des données et devraient prendre des mesures techniques et organisationnelles appropriées pour garantir cette conformité de manière responsable.

31. Le CEPD juge donc nécessaire de préciser, à l'article 2 de la proposition, que la **législation de l'Union en matière de protection des données à caractère personnel**, en particulier le RGPD et la directive «vie privée et communications électroniques», **s'applique à tout traitement de données à caractère personnel entrant dans le champ d'application de la proposition** (et pas seulement dans des contextes spécifiques). De même, il devrait être précisé dans le considérant correspondant que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments.

3.2. La définition de «cybersécurité»

32. Le CEPD constate que le principal terme de la proposition est «cybersécurité» (terme qui apparaît également dans le titre de la proposition), alors que, dans l'actuelle directive SRI, le principal terme est «sécurité des réseaux et des systèmes d'information». Cependant, le terme «sécurité des réseaux et des systèmes d'information» continue d'être utilisé dans la proposition aux côtés du terme «cybersécurité». De surcroît, ces termes ne sont pas utilisés de manière cohérente dans le texte.

33. L'article 4, paragraphe 3 de la proposition, qui renvoie à l'article 2, paragraphe 1, du règlement (UE) 2019/881[13], définit la «cybersécurité» en ces termes: «*les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenace*s». Le terme «cybermenace», tel que défini à l'article 2, paragraphe 8, du règlement (UE) 2019/881, désigne quant à lui «*toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes*».

34. Conformément à l'article 4, paragraphe 2, de la proposition[14], le terme «sécurité des réseaux et des systèmes d'information» est défini comme suit: «*la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles*».

35. Le CEPD estime que le terme «cybersécurité», tel qu'il est défini dans le règlement (UE) 2019/881 et utilisé dans la proposition, prend également en compte les incidences négatives sur «*...les utilisateurs de tels systèmes et d'autres personnes*». Cette définition, qui permet de tenir compte de la gestion des risques pour les droits et libertés fondamentaux des personnes lorsque les données à caractère personnel les concernant sont traitées par le biais de réseaux et de systèmes d'information, implique une approche intégrée.

36. Dans le même temps, nous constatons que le terme «sécurité des réseaux et des systèmes d'information» n'inclut pas cette dimension, puisqu'*il ne fait pas explicitement référence*

à la protection des personnes. Cela n'est pas un problème dans la mesure où l'emploi de ce terme ne sert qu'à souligner l'accent mis sur les infrastructures de réseaux et de systèmes d'information proprement dits et sur la nécessité impérieuse de protéger ces actifs, qui est elle-même fonction de la protection d'autres actifs, dont les personnes. Néanmoins, le CEPD observe que ces deux termes sont utilisés de manière presque interchangeable dans la proposition [15], ce qui pourrait avoir des conséquences opérationnelles non désirées s'agissant de la nécessité de prendre en compte la protection des personnes.

37. Le CEPD invite donc les colégislateurs à clarifier ce point. Le CEPD estime que, compte tenu de son champ d'application plus large, le terme «cybersécurité» devrait être utilisé de manière générale, tandis que le terme «sécurité des réseaux et des systèmes d'information» ne devrait être utilisé que lorsque le contexte le permet (par exemple dans un contexte purement technique, sans tenir compte des incidences sur les utilisateurs des systèmes et d'autres personnes).

3.3. Noms de domaine et données d'enregistrement (les «données WHOIS»)

38. Le CEPD se félicite du considérant 59 de la proposition, qui dispose que lorsque le traitement de «données WHOIS» comprend des données à caractère personnel, ce traitement doit s'effectuer conformément au droit de l'Union en matière de protection des données. En outre, le considérant 60 confirme également que l'accès à ces données par les autorités compétentes doit être conforme au droit de l'Union en matière de protection des données dans la mesure où il concerne des données à caractère personnel. Comme indiqué ci-dessus (voir section 3.1), le CEPD recommande vivement de remplacer les exemples donnés à l'article 2 par une règle matérielle générale sur l'application du droit de l'Union en matière de protection des données.

39. L'article 23, paragraphe 2, de la proposition fait référence aux *«informations pertinentes pour identifier et contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau»*. Le CEPD préconise de **définir clairement en quoi consistent les «informations pertinentes»** aux fins de cette disposition, en incluant les données à caractère personnel, compte tenu des principes de nécessité et de proportionnalité. Cette précision permettrait d'accroître la sécurité juridique et de garantir une approche cohérente dans l'ensemble des 27 États membres de l'UE.

40. L'article 23, paragraphe 4, de la proposition dispose en outre que les États membres veillent à ce que les registres et les entités fournissant des services d'enregistrement de noms de domaines publient, dans les meilleurs délais, des données d'enregistrement de domaine qui ne sont pas des données personnelles. Le CEPD recommande également de préciser de manière plus détaillée **quelles catégories de données d'enregistrement de noms de domaines** (lesquelles ne constituent pas des données à caractère personnel) **devraient faire l'objet d'une publication**.

41. Le considérant 14 du RGPD dispose que le règlement «*ne couvre pas le traitement de données concernant des personnes morales, en particulier les entreprises établies en tant que personnes morales (y compris le nom et la forme de la personne morale ainsi que ses coordonnées)*». Le CEPD rappelle que si les coordonnées d'une personne morale n'entrent pas dans le champ d'application du RGPD pour autant qu'elles n'identifient pas une

personne physique, les coordonnées des personnes physiques entrent, elles, dans le champ d'application du règlement[16].

42. En outre, l'article 4, paragraphe 1, du RGPD définit les données à caractère personnel comme «toute information se rapportant à une personne physique identifiée ou identifiable». Une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Dès lors, comme l'a précisé la CJUE, même les données concernant des personnes morales peuvent, dans certains cas, être considérées comme des données à caractère personnel[17]. Dans ces cas, le facteur déterminant est de savoir si les informations «se rapportent» à une personne physique «identifiable».

43. L'article 23, paragraphe 5, de la proposition exige des États membres qu'ils veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau donnent accès aux données spécifiques d'enregistrement de noms de domaines sur demande légitime et dûment justifiée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. La proposition ne définit ni ce qu'il faut entendre par «demande légitime et dûment justifiée», ni ce que signifie le terme «demandeurs d'accès légitimes», pas plus qu'elle ne précise les finalités d'un tel accès. La proposition ne fixe pas non plus de critère objectif permettant de déterminer les limites de l'accès des «demandeurs d'accès légitimes» aux données et de l'utilisation ultérieure de celles-ci.

44. L'article 23, paragraphe 5, de la proposition oblige les États membres à s'ingérer dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'il prévoit un traitement des données à caractère personnel[18].

45. Conformément à l'article 52, paragraphe 1, de la Charte, la CJUE a précisé à plusieurs reprises que la base juridique permettant l'ingérence doit elle-même définir la portée de la limitation de l'exercice du droit concerné[19]. En conformité avec le principe de proportionnalité, les dérogations et limitations à la protection des données à caractère personnel ne doivent s'opérer que dans les limites du strict nécessaire[20]. Pour satisfaire à cette exigence, la législation concernée qui donne lieu à l'ingérence **doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales,** de telle sorte que les personnes dont les données ont fait l'objet d'un accès disposent de garanties suffisantes permettant de protéger efficacement leurs données personnelles contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé[21].

46. Au vu de ces exigences, **le CEPD souligne que le texte de la proposition doit donc préciser davantage quelles entités (publiques ou privées) peuvent constituer des *«demandeurs d'accès légitimes»***. Par exemple, il convient de préciser si l'accès est limité aux entités répertoriées au considérant 60 de la proposition, ou si d'autres catégories de destinataires peuvent également se voir accorder un accès. Le CEPD soutient que, dans la pratique, les entités situées en dehors de l'EEE pourraient également demander l'accès à des données spécifiques d'enregistrement de noms de domaines. Aussi le CEPD invite-t-il les législateurs à préciser dans cette proposition si, oui ou non, les données à caractère personnel détenues par les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient également être accessibles aux entités situées en dehors de l'EEE. Si tel était le cas, la proposition devrait clairement définir les conditions, les limitations et les procédures applicables à un tel accès, en tenant compte également, le cas échéant, des exigences de l'article 49, paragraphe 2, du RGPD.

47. Dans le même ordre d'idées, le CEPD recommande également d'introduire des précisions supplémentaires sur **ce qui constitue une demande *«légitime et dûment justifiée»***, grâce à laquelle l'accès est accordé, et sous quelles conditions.

3.4. «Scannage proactif du réseau et des systèmes d'information» par les CSIRT

48. Le CEPD constate que l'article 10, paragraphe 2, point e), de la proposition confie aux CSIRT la réalisation, à la demande d'une entité (essentielle ou importante), d'un «*scannage proactif du réseau et des systèmes d'information utilisés pour la fourniture de leurs services*». Pour le CEPD, cette tâche se rapporte non seulement au scannage du réseau mais aussi à l'analyse des systèmes d'information en général (applications, serveurs et bases de données).

49. Le considérant 25 indique que «*[e]n ce qui concerne les données à caractère personnel, les CSIRT devraient être en mesure de réaliser, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil relatif aux données à caractère personnel, au nom et sur demande d'une entité en vertu de la présente directive, une analyse des réseaux et des systèmes d'information utilisés pour la fourniture de leurs services*».

50. Le CEPD relève que le considérant 69 clarifie davantage les activités des CSIRT en précisant, en des termes généraux, leur objectif («garantir la sécurité du réseau et des informations par des entités»), leur champ d'application («des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration») et les types de données à caractère personnel susceptibles d'être concernées [«adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et adresses électroniques»).

51. Le CEPD considère que la proposition ne délimite pas suffisamment la nature du traitement des données à caractère personnel concernées par le scannage proactif. Le CEPD déduit du libellé du considérant 69 («peuvent nécessiter») que l'objectif de l'article 10, paragraphe 2, point e), n'est pas de permettre la collecte et l'analyse systématiques, par les CSIRT, de

données à caractère personnel et/ou de données de communications électroniques. Dans l'intérêt de la sécurité juridique, le CEPD recommande que les colégislateurs **délimitent plus clairement les types d'analyse proactive que les CSIRT peuvent être invités à mener** et **identifient**, dans le texte de la proposition, **les principales catégories de données à caractère personnel concernées**.

3.5. Sous-traitance et chaîne d'approvisionnement

52. Les considérants 42 et 44 de la proposition laissent entendre que les entités essentielles et importantes ont la possibilité de sous-traiter tout ou partie de leurs activités de cybersécurité à des prestataires de services externes, tels que les «fournisseurs de services gérés de sécurité».

53. Le CEPD rappelle que la sous-traitance de ces activités par le responsable du traitement doit se faire en totale conformité avec le RGPD. En particulier, conformément à l'article 28 du RGPD, le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique relevant du droit de l'Union ou des États membres. En outre, le CEPD rappelle que les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales doivent respecter le chapitre V et la jurisprudence pertinente de la Cour de justice[22].

54. Le CEPD se félicite des mesures visant à atténuer, grâce à des évaluations coordonnées (sectorielles) des risques liés aux chaînes d'approvisionnement, les risques dus à des facteurs techniques, et, le cas échéant, non techniques, de la chaîne d'approvisionnement[23]. Le CEPD se félicite également du fait que, parmi les critères permettant d'identifier les chaînes d'approvisionnement qui devraient faire l'objet d'une évaluation coordonnée des risques, la proposition mette l'accent sur l'importance de services, systèmes ou produits TIC critiques spécifiques traitant, entre autres, des données à caractère personnel.

55. Le CEPD souligne que, parmi les facteurs spécifiques à prendre en compte pour l'évaluation de chaînes d'approvisionnement en technologies et de systèmes traitant des données à caractère personnel, une **attention particulière devrait être accordée aux caractéristiques garantissant la mise en œuvre effective du principe de protection des données dès la conception et par défaut**. La prise en compte de ces facteurs permettrait de favoriser le respect de l'article 25 du RGPD et de contribuer à la protection effective des communications et des équipements terminaux au sens de la directive «vie privée et communications électroniques».

56. En outre, le CEPD considère que, dans l'évaluation des risques liés aux chaînes d'approvisionnement, l'accent devrait être mis sur les **services, systèmes ou produits TIC soumis à des exigences spécifiques dans le pays d'origine, qui pourraient représenter un obstacle au respect de la législation européenne en matière de protection de la vie privée et des données**.

57. Le CEPD recommande également que le **comité européen de la protection des données instauré par l'article 68 du RGPD (le «comité») soit consulté** lors de la définition de ces critères et, si nécessaire, lors de l'évaluation coordonnée sectorielle des risques mentionnée au considérant 46.

58. Le CEPD tient également à recommander qu'il soit mentionné dans un considérant que les **produits de cybersécurité libres** (logiciels et matériel), y compris les systèmes de cryptage à source ouverte, peuvent offrir la transparence nécessaire pour atténuer les risques inhérents aux chaînes d'approvisionnement.

3.6. Chiffrement

59. Le CEPD se félicite de l'inclusion, à l'article 18 de la proposition, du chiffrement et de la cryptographie dans la liste des garanties minimales en matière de cybersécurité. En outre, le CEPD salue également les références au chiffrement faites dans la stratégie[24].

60. Le CEPD soutient pleinement la déclaration, au considérant 54 de la proposition, consistant à encourager l'utilisation du chiffrement de bout en bout, voire à l'imposer, pour les fournisseurs de services de communications électroniques.

61. Toutefois, le considérant 54 dispose également qu'il convient de «concilier» l'utilisation du chiffrement de bout en bout avec les pouvoirs dont disposent les États membres pour garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et pour permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Il est notamment indiqué que «*[l]es solutions pour un accès légal aux informations contenues dans les communications chiffrées de bout en bout devraient préserver l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité*».

62. Le CEPD souhaite réaffirmer que, conformément à la déclaration du Groupe de travail Article 29[25], le chiffrement est une technologie critique et irremplaçable pour assurer une protection efficace des données et de la vie privée. **Il est impératif de pouvoir utiliser un chiffrement renforcé pour atténuer les risques élevés pour les droits et libertés des personnes.** À titre d'exemple de la nécessité d'utiliser un chiffrement renforcé, le CEPD rappelle les récentes recommandations 01/2020 du comité sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE[26], recommandations qui énumèrent certains cas dans lesquels le chiffrement renforcé peut être utilisé pour atténuer les risques liés aux transferts de données non conformes.

63. Tout affaiblissement ou contournement du chiffrement (par exemple, par le biais de portes dérobées obligatoires, d'autorités de séquestre obligatoires ou de canaux de communication cachés) priverait le mécanisme de toute capacité de protection efficace des données en raison du risque d'utilisation illégale et de la perte de confiance dans les contrôles de sécurité. En raison des risques importants pour l'économie et la société en général, cela compromettrait inévitablement la protection des droits fondamentaux à la protection de la vie privée et des données personnelles. Même lorsque le chiffrement renforcé n'est pas utilisé alors qu'il est encore disponible, **le décryptage non autorisé, la rétro-ingénierie du code de cryptage, ou la surveillance des communications électroniques en dehors d'un mandat légal clair, devraient être interdits.**

64. Si le CEPD reconnaît que les forces de l'ordre ont besoin de moyens pour lutter contre la criminalité sur internet, toute mesure constituant une ingérence dans la confidentialité des communications doit respecter les exigences de légalité, de nécessité et de proportionnalité,

en fonction d'éléments de preuve concrets. Bien que le chiffrement rende difficile la collecte de données en masse et la surveillance de masse, il ne constitue pas un facteur limitant pour l'adoption de mesures plus ciblées et spécifiques. **Le CEPD recommande donc de clarifier au considérant 54 que rien dans la proposition ne devrait être interprété comme un avis favorable à l'affaiblissement du chiffrement de bout en bout par le biais de «portes dérobées» ou d'autres solutions.**

3.7. Mesures de gestion des risques en matière de cybersécurité

65. Le CEPD accueille favorablement l'article 18, qui exige des États membres qu'ils veillent à ce que les entités essentielles et importantes prennent les mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information, ainsi que l'ensemble des mesures minimales prévues à l'article 18, paragraphe 2.

66. Le CEPD rappelle que la gestion des risques pour les droits et libertés des personnes, dans le cadre du traitement des données à caractère personnel les concernant, est une obligation pour tous les responsables du traitement (et pas seulement pour les entités essentielles et importantes) en vertu de l'article 32 du RGPD. Alors que les mesures de gestion des risques en matière de cybersécurité prévues à l'article 18 de la proposition visent à protéger les réseaux et les systèmes d'information de l'organisation (ainsi que les données qu'ils contiennent), l'article 32 du RGPD vise, quant à lui, à protéger les personnes (qui n'appartiennent pas nécessairement à la même organisation) et leurs droits en protégeant leurs données. Les actifs à protéger dans le cadre de ces deux activités sont différents, ce qui pourrait aboutir, dans certaines circonstances, à des conclusions différentes. Dans le même temps, le processus de gestion des risques de cybersécurité peut contribuer à l'analyse de l'impact sur la protection des données des faiblesses dans la sécurité des données à caractère personnel. Comme indiqué ci-dessus concernant la mesure plus générale de la stratégie, le CEPD recommande d'**intégrer les considérations relatives à la protection de la vie privée et des données dans la gestion des risques de cybersécurité**, afin d'assurer une approche holistique et de permettre aux organisations publiques et privées de bénéficier de synergies dans la gestion de la cybersécurité et la protection des informations qu'elles traitent, sans multiplier inutilement les efforts.

67. **Le CEPD suggère d'ajouter ces considérations dans les considérants et dans la partie consacrée au fond de la proposition**, de telle manière que les éventuels futurs actes d'exécution de la Commission, les orientations de l'ENISA sur la cybersécurité au niveau de l'UE et ses travaux sur les schémas européens de certification en matière de cybersécurité (voir l'article 21 de la proposition), et les travaux des organismes de normalisation de l'UE (voir article 22), puissent prendre en compte cette dimension et, ainsi, intégrer la gestion des risques pour les personnes et leurs droits fondamentaux liés aux menaces de cybersécurité.

68. Compte tenu des liens étroits qui existent entre la gestion de la cybersécurité et la protection des données à caractère personnel, le CEPD suggère également d'**ajouter l'obligation pour l'ENISA de consulter le comité** lors de l'élaboration des avis pertinents. Ces actes et orientations peuvent également être utiles aux organisations qui, bien que ne relevant pas du champ d'application de la directive, pourraient néanmoins offrir des avantages similaires et favoriser le respect des obligations du RGPD en matière de sécurité des données à caractère personnel.

3.8. Violations de données à caractère personnel

69. Conformément à l'article 20, paragraphe 2, de la proposition, les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT toute cybermenace importante que ces entités décèlent et qui aurait pu entraîner un incident significatif. L'article 20, paragraphe 3, définit les conditions dans lesquelles un incident doit être considéré comme «significatif». Une des options envisagées est que l'incident a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des pertes matérielles ou non matérielles considérables.

70. Le CEPD se félicite de l'article 20, paragraphe 3, point b), de la proposition, qui considère les incidences sur l'organisation, mais aussi sur les personnes physiques qui peuvent être affectées. Par ailleurs, le CEPD note que la définition visée à l'article 20, paragraphe 3, point b), engloberait certaines «violations de données à caractère personnel», telles que définies à l'article 4, paragraphe 12, du RGPD. Il semblerait également que les obligations de notification correspondantes puissent recouper, dans certains cas, la notification de violations de données à caractère personnel aux autorités compétentes prévue à l'article 33 du RGPD. Néanmoins, la définition des conditions donnant lieu à l'obligation, les délais maximaux fixés et les autorités compétentes auxquelles signaler/notifier les violations diffèrent. Des obligations analogues de notification aux autorités compétentes sont prévues dans la directive «vie privée et communications électroniques», qui est actuellement en cours de révision.

71. Le CEPD se félicite de l'article 28, paragraphe 2, qui dispose que, pour traiter des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes en vertu de la proposition coopèrent étroitement avec les autorités chargées de la protection des données, d'où la création de synergies entre les instruments juridiques. Le CEPD se réjouit également de l'obligation faite par l'article 32, paragraphe 1, aux autorités compétentes d'informer les autorités compétentes en matière de protection des données lorsqu'elles disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 18 et 20 donne lieu à une violation de données à caractère personnel devant être notifiée en vertu de l'article 33 du RGPD.

72. Le CEPD relève que la notification par les autorités compétentes de la violation de données aux autorités compétentes en vertu du RGPD doit se faire «dans un délai raisonnable». Le CEPD observe que cette obligation est sans préjudice de l'obligation de notification imposée aux responsables du traitement, telle que définie à l'article 33 du RGPD, notification qui doit intervenir «dans les meilleurs délais» et «72 heures au plus tard» après avoir pris connaissance de la violation de données à caractère personnel. Afin de permettre aux autorités de protection des données d'accomplir efficacement leurs missions, **le CEPD suggère de remplacer la formulation de la proposition «dans un délai raisonnable» par «dans les meilleurs délais».**

3.9. Groupe de coopération

73. L'article 12 de la proposition crée un groupe de coopération afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres dans le domaine d'application de la proposition. Compte tenu de la mission de ce groupe et du lien

possible avec le cadre de protection des données, **le CEPD recommande de nommer un représentant du comité en tant que membre du groupe de coopération**.

3.10. Compétence et territorialité

Le CEPD constate que la notion d'«établissement principal» utilisée à l'article 24, paragraphe 2, de la proposition[27] n'est pas définie de la même manière qu'à l'article 4, paragraphe 16, du RGPD.

74. En ce qui concerne le RGPD, la notion d'«établissement principal» est particulièrement importante dans les cas de traitement transfrontalier de données à caractère personnel. L'article 56, paragraphe 1, du RGPD contient une règle supérieure et dispose que l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant[28]. Par conséquent, le CEPD recommande de **préciser** dans le texte juridique **que la proposition n'affecte pas les compétences des autorités de contrôle de la protection des données en vertu du RGPD** (voir ci-dessus, section 3.8).

75. Le CEPD réaffirme son soutien à l'article 28, paragraphe 2, de la proposition, qui prévoit que, pour traiter des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données (voir ci-dessus, paragraphe 67).

76. Dans le même temps, le CEPD souligne la nécessité de prévoir dans la proposition **une base juridique plus complète pour la coopération et l'échange d'informations pertinentes** entre les autorités compétentes en vertu de la proposition et les autres autorités de contrôle concernées, chacune agissant dans son domaine de compétence respectif. En particulier, le CEPD recommande de préciser que les autorités compétentes en vertu de la proposition devraient être en mesure de fournir aux autorités de contrôle compétentes en vertu du règlement (UE) 2016/679, sur demande ou de leur propre initiative, toute information obtenue dans le cadre d'audits et d'enquêtes ayant trait au traitement de données à caractère personnel et d'inclure une base juridique explicite à cet effet.

4. CONCLUSIONS

77. À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

Concernant la stratégie de cybersécurité

- tenir compte du fait que la première étape pour atténuer les risques liés à la protection des données et de la vie privée que présentent les nouvelles technologies visant à améliorer la cybersécurité, telles que l'IA, consiste à appliquer les exigences de protection des données dès la conception et par défaut visées à l'article 25 du RGPD, ce qui contribuera à intégrer les garanties appropriées, telles que la pseudonymisation, le chiffrement, l'exactitude des données ou la minimisation des données, dans la conception et l'utilisation de ces technologies et systèmes;

- tenir compte de l'importance d'intégrer la dimension de la protection de la vie privée et des données dans les politiques et normes liées à la cybersécurité et dans la gestion traditionnelle de la cybersécurité, afin de garantir une approche holistique et de permettre aux organisations publiques et privées de bénéficier de synergies dans la gestion de la cybersécurité et dans la protection des informations qu'elles traitent, sans multiplier inutilement les efforts;

- envisager et prévoir l'utilisation de ressources par les institutions européennes pour renforcer les capacités de ces dernières en matière de cybersécurité, et ce d'une manière qui respecte pleinement les valeurs de l'UE;

- prendre en compte les dimensions de la cybersécurité liées à la protection de la vie privée et des données en investissant dans des politiques, des pratiques et des instruments permettant d'intégrer la dimension de protection de la vie privée et des données dans la gestion traditionnelle de la cybersécurité et de mettre en place des garanties efficaces de protection des données dans le traitement de données à caractère personnel effectué dans le cadre d'activités de cybersécurité.

Concernant le champ d'application de la stratégie et de la proposition aux institutions, organes et organismes de l'Union:

- tenir compte des besoins et du rôle des institutions européennes afin que celles-ci soient intégrées dans le cadre global de cybersécurité à l'échelle de l'UE, et qu'elles bénéficient du même niveau élevé de protection que les entités des États membres; et

- inclure explicitement les institutions, organes et organismes de l'Union dans le champ d'application de la proposition.

Concernant la relation avec la législation existante de l'Union en matière de protection des données à caractère personnel:

- préciser, à l'article 2 de la proposition, que la législation de l'Union en matière de protection des données à caractère personnel, en particulier le RGPD et la directive «vie privée et communications électroniques», s'applique à tout traitement de données à caractère personnel entrant dans le champ d'application de la proposition (et pas seulement dans des contextes spécifiques); et

- préciser également dans un considérant pertinent que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour contrôler le respect de ces instruments.

Concernant la définition de la cybersécurité:

- clarifier l'utilisation différente des termes «cybersécurité» et «sécurité des réseaux et des systèmes d'information», et utiliser le terme «cybersécurité» en général et le terme «sécurité des réseaux et des systèmes d'information» uniquement lorsque le contexte le permet (par exemple, dans un contexte purement technique, sans tenir compte des incidences sur les utilisateurs des systèmes et d'autres personnes).

Concernant les noms de domaine et données d'enregistrement (les «données WHOIS»):

- définir clairement ce qui constitue des «informations pertinentes» afin d'identifier et de contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau;

- préciser de manière plus détaillée quelles catégories de données d'enregistrement de noms de domaines (qui ne constituent pas des données à caractère personnel) devraient faire l'objet d'une publication;

- préciser davantage quelles entités (publiques ou privées) pourraient constituer des *«demandeurs d'accès légitimes»;*

- préciser si les données à caractère personnel détenues par les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient également être accessibles aux entités situées en dehors de l'EEE et, si tel est le cas, définir clairement les conditions, les limitations et les procédures applicables à un tel accès, en tenant compte également, le cas échéant, des exigences de l'article 49, paragraphe 2, du RGPD; et

- introduire des précisions supplémentaires sur ce qui constitue une demande «*légitime et dûment justifiée*», grâce à laquelle l'accès est accordé, et sous quelles conditions.

Concernant le «scannage proactif du réseau et des systèmes d'information» par les CSIRT:

- délimiter clairement les types d'analyse proactive que les CSIRT peuvent être invités à mener, et identifier les principales catégories de données à caractère personnel concernées dans le texte de la proposition.

Concernant la sous-traitance et la chaîne d'approvisionnement:

- prendre en compte les caractéristiques garantissant la mise en œuvre effective du principe de protection des données dès la conception et par défaut, lors de l'évaluation des chaînes d'approvisionnement en technologies et des systèmes traitant des données à caractère personnel;

- prendre en compte les exigences spécifiques du pays d'origine qui pourraient représenter un obstacle au respect de la législation européenne en matière de protection de la vie privée et des données, lors de l'évaluation des risques liés à la chaîne d'approvisionnement de services, systèmes ou produits TIC;

- inclure dans le texte juridique l'obligation de consulter le comité lors de la définition des caractéristiques susmentionnées et, le cas échéant, lors de l'évaluation coordonnée sectorielle des risques mentionnée au considérant 46; et

- recommander de préciser dans un considérant que les **produits de cybersécurité libres** (logiciels et matériel), y compris les systèmes de cryptage à source ouverte, pourraient

offrir la transparence nécessaire pour atténuer les risques spécifiques aux chaînes d'approvisionnement.

Concernant le chiffrement:

- préciser, au considérant 54, que rien dans la proposition ne doit être interprété comme un avis favorable à l'affaiblissement du chiffrement de bout en bout par le biais de «portes dérobées» ou de solutions similaires.

Concernant les mesures de gestion des risques en matière de cybersécurité:

- inclure, dans les considérants et dans la partie consacrée au fond de la proposition, le concept selon lequel l'intégration de la dimension de la protection de la vie privée et des données dans la gestion traditionnelle des risques de cybersécurité garantira une approche holistique et permettra aux organisations publiques et privées de bénéficier de synergies dans la gestion de la cybersécurité et la protection des informations qu'elles traitent, sans multiplier inutilement les efforts;

- ajouter dans le texte juridique l'obligation pour l'ENISA de consulter le comité lors de l'élaboration des avis pertinents.

Concernant les violations de données à caractère personnel:

- remplacer le texte «dans un délai raisonnable» de l'article 32, paragraphe 1, par «dans les meilleurs délais».

Concernant le groupe de coopération:

- inclure dans le texte juridique la participation du comité au groupe de coopération, en tenant compte du lien entre la mission de ce groupe et le cadre de la protection des données.

Concernant la compétence et la territorialité:

- préciser dans le texte juridique que la proposition n'affecte pas les compétences des autorités de contrôle de la protection des données en vertu du RGPD;

- fournir une base juridique complète pour la coopération et l'échange d'informations entre les autorités compétentes et les autorités de contrôle, chacune agissant dans ses domaines de compétence respectifs; et

- préciser que les autorités compétentes en vertu de la proposition devraient être en mesure de fournir aux autorités de contrôle compétentes en vertu du règlement (UE) 2016/679, sur demande ou de leur propre initiative, toute information obtenue dans le cadre d'audits et d'enquêtes ayant trait au traitement de données à caractère personnel et d'inclure une base juridique explicite à cet effet.

Bruxelles, le 11 mars 2021

[signature électronique]
Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.

[4] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, COM (2020) 823 final.
[5] La stratégie de cybersécurité de l'UE pour la décennie numérique, JOIN (2020) 18 final.
[6] Voir chapitre I. INTRODUCTION, page 4 de la stratégie.
[7] 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, JO L 194 du 19.7.2016, p. 1-30.
[8] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1-88.
[9] Voir pour plus de détails: Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits

fondamentaux à la vie privée et à la protection des données à caractère personnel, 19/12/2019, (https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_fr), ainsi que le document du CEPD «Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel», 11/04/2017 (https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_fr).
[10] CEPD, Shaping a Safer Digital Future: a New Strategy for a New Decade [Façonner un avenir numérique plus sûr: une nouvelle stratégie pour une nouvelle décennie], 30/06/2020 (https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en, disponible en anglais uniquement).
[11] 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 (directive vie privée et communications électroniques), JO L 201 du 31.07.2002, p. 37-47.
[12] Le considérant 25 de la proposition fait uniquement référence au règlement (UE) 2016/679 concernant l'analyse proactive des réseaux et des systèmes d'information; le considérant 48 fait référence à la fois au règlement (UE) 2016/679 et à la directive 2002/58/CE concernant les obligations de notification; le considérant 56 fait référence à la fois au règlement (UE) 2016/679 et à la directive 2002/58/CE concernant les obligations de notification incluses dans différents instruments juridiques; le considérant 58 fait uniquement référence à la directive 2002/58/CE concernant la compromission de données à caractère personnel dans le cadre d'incidents de sécurité, alors qu'il devrait également citer le règlement (UE) 2016/679; l'article 26 fait référence au règlement (UE) 2016/679 concernant l'échange d'informations en matière de cybersécurité entre les États membres; et l'article 32 fait référence au règlement (UE) 2016/679 concernant les infractions donnant lieu à une violation de données à caractère personnel.
[13] 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), JO L 151 du 7.6.2019, p. 15-69.
[14] Cette même définition est reprise dans l'actuelle directive SRI.
[15] Par exemple, l'article 4, paragraphe 4, de la proposition dispose ce qui suit: *«"stratégie nationale en matière de cybersécurité", le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information dans cet État membre.»*
[16] https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf (p. 4)
[17] Voir Cour de justice de l'Union européenne, dans les affaires jointes C-92/09, Volker und Markus Schecke GbR contre Land Hessen, et C-93/09, Eifert contre Land Hessen et Bundesanstalt für Landwirtschaft und Ernährung, au point 53, où la CJUE a jugé que les personnes morales pouvaient invoquer la protection des articles 7 et 8 de la Charte dans la mesure où le titre officiel de la personne morale identifie une ou plusieurs personnes physiques.

[18] Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

[19] Voir, en ce sens, Cour de justice de l'Union européenne, arrêt du 17 décembre 2015, WebMindLicenses, C-419/14, EU:C:2015:832, point 81.

[20] Cour de justice de l'Union européenne, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56; du 8 avril 2014, Digital Rights Ireland et autres, C-293/12 et C-594/12, EU:C:2014:238, points 51 et 52; du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 92; et du 21 décembre 2016, Tele2 Sverige et Watson et autres, C-203/15 et C-698/15, EU:C:2016:970, points 96 et 103.

[21] Voir Cour de justice de l'Union européenne, avis 1/15 de la Cour du 26 juillet 2017, points 140 et 141.

[22] Voir arrêt C-311/18 (Schrems II) de la Cour de justice de l'Union européenne (CJUE) (http://curia.europa.eu/juris/liste.jsf?num=C-311/18#)

[23] Considérant 46 et article 19 de la proposition.

[24] Ces références sont les suivantes: i) l'inclusion du chiffrement dans l'ensemble des technologies importantes pour la stratégie, et dont la chaîne d'approvisionnement doit être contrôlée par l'UE (page 1), et dans les technologies que l'Union devrait continuer à développer (page 18); ii) l'affirmation, à la section 2.4 de la stratégie, selon laquelle le chiffrement est considéré comme l'une des trois technologies clés pour l'intégration de la cybersécurité; et l'intention de développer «de nouvelles formes de cryptage plus sûres offrant une protection contre les cyberattaques» dans le contexte du déploiement d'une infrastructure de communication quantique (ICQ) sûre pour l'Europe, qui offrira un niveau de confidentialité élevé.

[25] Déclaration du WP29 sur le chiffrement et son impact sur la protection des personnes à l'égard du traitement de leurs données à caractère personnel dans l'UE, Bruxelles, 11 avril 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229.

[26] Recommandations 01/2020 du comité sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_fr.

[27] Conformément à l'article 24, paragraphe 2, de la proposition, les entités visées au paragraphe 1 de la proposition sont réputées avoir leur établissement principal dans l'Union dans l'État membre où sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité.

[28] Voir l'avis 8/2019 du comité sur la compétence d'une autorité de contrôle en cas de changement de circonstances concernant l'établissement principal ou unique adopté le 12 juillet 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishment_fr.pdf.