Observations officielles du CEPD concernant:

- **la communication conjointe de la Commission européenne et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide»** (ci-après la «communication conjointe»)[i];

- **la proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)[ii];**

- **la recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs** (ci-après la «recommandation»)[iii];

- **la communication de la Commission au Parlement européen et au Conseil «Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union»** (ci-après la «communication SRI»**)[iv]**.

La Commission a adopté ces mesures le 13 septembre 2017 dans le cadre d'une mesure commune, appelée le «paquet cybersécurité» de 2017[v].

Le paquet inclut également une **proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces**[vi], que le CEPD peut considérer comme s'inscrivant dans un contexte différent.

Le 18 octobre, la Commission a adopté un paquet de mesures relatives à la sécurité de l'Union, qui s'étend sur certaines initiatives annoncées dans le paquet cybersécurité. Le cas échéant, le CEPD aborde ces éléments complémentaires dans les présentes observations officielles. Ces éléments concernent en particulier les initiatives politiques annoncées concernant le chiffrement.

I. Introduction et contexte

Le 13 septembre 2017, la Commission européenne et la haute représentante ont proposé une série de mesures visant à permettre à l'Europe de devenir «*plus résiliente face aux cyberattaques et [d']adopter des mesures efficaces, en matière de cyberdissuasion et de répression par le droit pénal, pour mieux protéger les citoyens, les entreprises et les institutions*

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
Adresse électronique: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél: 02-283 19 00 - Télécopie: 02-283 19 50

publiques européens», appelée «paquet cybersécurité». Les instruments susmentionnés en font partie.
Le 18 octobre 2017, la Commission a publié son rapport sur une union de la sécurité[vii], qui exposait plus en détail certains éléments de la communication conjointe. En particulier, elle a présenté plusieurs initiatives relatives au chiffrement.

Le CEPD suit depuis le début l'évolution de la stratégie de l'UE visant à renforcer sa capacité en matière de cybersécurité. Parmi d'autres avis officiels et informels, nous tenons à rappeler les avis suivants émis par le CEPD:

- l'avis de décembre 2010 sur la proposition de règlement concernant l'ENISA[viii];
- observations officielles du CEPD d'octobre 2012 sur la consultation publique de la Commission concernant l'amélioration de la sécurité des réseaux et de l'information (SRI) dans l'UE[ix];
- avis de juin 2013 sur la communication conjointe de la Commission et de la haute représentante sur la stratégie de cybersécurité de l'UE et sur la proposition de directive SRI[x];
- avis de décembre 2015 sur la diffusion et l'utilisation des technologies de surveillance intrusive[xi];
- lignes directrices de mars 2016 sur les mesures de sécurité relatives au traitement des données à caractère personnel[xii].

Le CEPD observe que de nombreux éléments du paquet actuel sont pertinents dans le contexte de la protection des données et de la vie privée. Nous observons que la Commission n'a pas respecté son engagement à consulter le CEPD avant l'adoption de ces propositions.

II. Portée des observations du CEPD

Le droit applicable en matière de protection des données, dont le règlement général sur la protection des données[xiii], considère la sécurité des informations comme facilitant la protection des personnes physiques par la protection de leurs données à caractère personnel. La sécurité des informations fait partie des «principes» de protection des données établis par la législation [article 5, paragraphe 1, point f)]. L'article 32 impose à tous les acteurs («responsables du traitement»[xiv] et «sous-traitants»[xv]) traitant des données à caractère personnel de mettre «*[...] en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque [...]*». Les articles 33 et 34 imposent l'obligation, dans certaines conditions, de notifier les violations de données à caractère personnel[xvi] susceptibles d'engendrer des risques pour les personnes à l'autorité de contrôle compétente dans les 72 heures et de notifier dans les meilleurs délais aux personnes concernées ces violations susceptibles d'engendrer un risque élevé pour elles.

Des dispositions analogues figurent dans l'actuel règlement (CE) nº 45/2001 relatif au traitement des données à caractère personnel par les institutions et organes de l'UE[xvii] ainsi que dans la proposition de nouveau règlement relatif à la protection des données à caractère personnel pour ces entités de l'UE.

En ce qui concerne plus particulièrement la protection de la vie privée dans le secteur des communications électroniques, l'article 4 de la directive 2002/58/CE contient des dispositions relatives à la cybersécurité. Certaines de ces obligations sont maintenues à l'article 17 de la

proposition de règlement «vie privée et communications électroniques»[xviii], qui établit l'obligation d'informer les utilisateurs finaux lorsqu'il existe un risque particulier susceptible de compromettre la sécurité des réseaux et des services de communications électroniques.

Si ces instruments soulignent l'importance des mesures de cybersécurité pour une protection efficace des données, la mise en œuvre de mesures de sécurité peut impliquer le traitement de données à caractère personnel. Ce traitement doit être conforme à la loi et tous les principes de protection des données, notamment la limitation de la finalité et la minimisation des données, s'appliquent.
Les présentes observations officielles analysent les instruments susmentionnés à la lumière du cadre juridique applicable et des considérations qui précèdent.

III. Observations du CEPD

1. Considérations générales sur le paquet cybersécurité, notamment la communication conjointe

- *La mise en œuvre d'une cybersécurité efficace dans l'UE ne peut être reportée*

Notre société repose de plus en plus sur l'échange d'informations via des réseaux de communication, la plupart du temps liés à l'internet mondial, pour rationaliser la fourniture et l'utilisation de services essentiels tels que la production et la distribution d'énergie et de biens, et les transports. Le traitement des informations et des données, notamment des données à caractère personnel, est considéré comme le fondement de l'économie numérique. La récente déclaration de Tallinn sur l'administration en ligne, qui vise à garantir aux citoyens et aux entreprises de l'UE des services publics numériques de haute qualité centrés sur l'utilisateur, constitue un excellent exemple du rôle que l'internet et les services en ligne sont appelés à jouer. Elle considère les mesures liées à la fiabilité et à la sécurité comme essentielles pour garantir que « *... les besoins en matière de sécurité de l'information et de protection de la vie privée sont pris en compte lors de la conception de services publics et de solutions d'administration publique fondées sur les technologies de l'information et de la communication (TIC), suivant une approche fondée sur le risque et utilisant des solutions de pointe...* ».

Dans de nombreux contextes, l'accès à l'internet est devenu indispensable pour participer pleinement aux activités économiques et sociales.

La cybersécurité n'est plus exclusivement une préoccupation des experts, mais la grande majorité des citoyens de l'UE reconnaît son importance, comme le montre une récente enquête Eurobaromètre[xix]: 87 % des répondants considèrent que la cybercriminalité constitue un défi important pour la sécurité intérieure de l'UE et que l'utilisation abusive des données à caractère personnel reste la principale préoccupation des internautes.

Nous saluons dès lors l'effort visant à «*...accroître la sécurité de l'internet et des réseaux et systèmes informatiques privés sur lesquels reposent les services dont dépend le fonctionnement de notre société et de nos économies...* », qui constitue le fondement du paquet de mesures, et nous le considérons comme essentiel et urgent.

Nous constatons que la communication conjointe met l'accent sur plusieurs mesures qui visent à améliorer la réaction après des cyberincidents. Nous reconnaissons qu'une réaction bien préparée, qui repose sur une bonne planification, la formation du personnel et la mise en place à l'avance de processus et de procédures appropriés, peut réduire considérablement les

dommages causés par un incident et contribuer à éviter une nouvelle propagation des dommages.

Nous rappelons toutefois que des mesures adéquates de prévention des incidents, par exemple une maintenance appropriée des systèmes informatiques, peuvent être encore plus efficaces car elles permettent d'arrêter les attaques avant que des dommages ne se produisent. Dans ce contexte, il convient d'observer que les attaques Wannacry de mai 2017 n'ont pas eu d'effets sur les systèmes qui avaient soit désactivé la fonctionnalité vulnérable (qui n'était pas utilisée dans de nombreux systèmes) soit installé une mise à jour disponible environ un mois avant les attaques et supprimé la vulnérabilité utilisée par l'attaquant[xx]. Nous soulignons donc l'importance de mettre en place des systèmes de pointe de gestion des risques en matière de sécurité de l'information, d'élaborer et d'appliquer des politiques appropriées pour tous les systèmes et d'attribuer les responsabilités dans toutes les organisations. Ces mesures correspondent à l'approche en matière de sécurité prévue par la législation pertinente sur la protection des données et d'autres instruments relatifs à la sécurité de l'information.
Wannacry et d'autres cyberincidents récents montrent que les objectifs de la stratégie de 2013 en matière de cybersécurité, à savoir améliorer la résilience et le niveau de préparation dans les secteurs public et privé, sont toujours valables et continuent de nécessiter des efforts considérables. L'investissement dans l'éducation et l'adoption de mesures préventives appropriées devraient jeter les bases d'une réaction efficace et rapide aux incidents en cours en vue de limiter les dommages causés. La stratégie en matière de cybersécurité doit suivre les deux axes et pourrait tirer parti d'une analyse approfondie des incidents passés afin de déterminer les facteurs qui ont conduit à l'absence de mesures de préparation et de prévention appropriées dans les organisations les plus touchées. Nous soutenons sans réserve les mesures visant à améliorer les compétences en matière de cybersécurité et à promouvoir une hygiène et une sensibilisation à la cybersécurité.

L'élimination ou la réduction des failles inhérentes aux produits et services peut être particulièrement efficace pour prévenir les cyberincidents. La communication conjointe fait référence à plusieurs approches qui peuvent contribuer à remédier aux failles inhérentes au marché actuel des produits et services:

- l'utilisation de l'approche reposant sur la «sécurité dès la conception»,
- l'établissement d'un principe de «devoir de vigilance»,
- l'attribution de la responsabilité des défaillances en matière de sécurité aux acteurs du marché.

Nous encourageons la Commission à élaborer et à mettre en œuvre des politiques et à proposer des mesures juridiques pour promouvoir ces objectifs. Ces mesures refléteraient et compléteraient des approches similaires déjà intégrées dans le droit de l'Union pour la protection des données à caractère personnel, telles que l'obligation de respecter le principe de la protection des données dès la conception et par défaut et les sanctions et responsabilités correspondantes.

Des chercheurs indépendants spécialisés en sécurité peuvent jouer un rôle important dans la détection, l'évaluation et l'atténuation des failles dans la cybersécurité. Cette recherche ne devrait pas être confrontée à des restrictions dues à une législation mal conçue, qui crée des risques de poursuites judiciaires pour des activités légitimes. Nous nous félicitons de la reconnaissance de cette nécessité dans la communication conjointe.

- *Concernant le projet de réseau de compétences en cybersécurité et de centre européen de recherche et de compétences en cybersécurité*

Nous prenons également note du plan visant à créer «*un réseau de centres de compétences en cybersécurité, au cœur duquel figurerait un centre européen de recherche et de compétences*». Ce réseau et ce centre «*stimuleraient le développement et le déploiement de technologies dans le domaine de la cybersécurité et compléteraient les efforts de renforcement des capacités dans ce domaine au niveau national et de l'Union*». Nous prenons note également que la Commission lancera une analyse d'impact en 2018.

Nous évaluerons cette proposition à un stade ultérieur, lorsque des instruments politiques pertinents, y compris juridiques, seront élaborés, et nous restons à la disposition de la Commission pour toute coopération éventuelle dans le cadre de notre rôle consultatif.

Nous saisissons cette occasion pour saluer l'accent placé sur la nécessité de développer et d'évaluer les capacités de chiffrement des produits et services en tant que caractéristiques essentielles pour protéger l'information et les droits fondamentaux des personnes en protégeant leurs données à caractère personnel.

- *Concernant la création d'une cyberdissuasion efficace*

Si nous partageons l'avis qu'une réponse policière percutante, axée sur la détection, la traçabilité et la poursuite des cybercriminels est nécessaire, nous insistons sur la nécessité d'exécuter cette réponse dans le respect total de la Charte des droits fondamentaux de l'UE, notamment du droit au respect de la vie privée et du droit à la protection des données. Nous en profitons pour rappeler notre avis contenu dans le «Necessity Toolkit» du CEPD d'évaluer l'incidence des nouvelles dispositions et mesures sur les droits fondamentaux des particuliers lors du traitement de leurs données à caractère personnel, de recenser les cas dans lesquels la limitation de ce droit est réellement nécessaire et de mettre en place des garanties adéquates pour contrebalancer le degré d'intrusion des mesures prévues.

La communication conjointe annonce des mesures relatives aux preuves électroniques. Nous rendrons un avis séparé concernant l'instrument législatif sur l'accès transfrontalier aux preuves électroniques, que la Commission a l'intention d'adopter en janvier 2018.

Le «Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective» aborde le sujet du problème de l'utilisation du chiffrement par les criminels, rencontré par les services répressifs et les autorités judiciaires dans le cadre des enquêtes pénales. Nous observons que la Commission prévoit de proposer des «*mesures juridiques visant à faciliter l'accès à des éléments de preuve chiffres*» et des «*mesures techniques visant à renforcer les capacités de déchiffrement*». Ces plans incluent le renforcement des capacités de déchiffrement d'Europol et une attention spécifique à la recherche et au développement financés par l'UE dans les technologies concernées. Nous observons également que la Commission propose également la mise en place d'un «*réseau de points d'expertise*» sur le sujet afin de partager les capacités et l'expertise au niveau national. Dans la proposition de la Commission, ce réseau devrait mettre au point et échanger un «*arsenal de techniques d'enquête alternatives*», dont le registre devrait être tenu par le Centre européen de lutte contre la cybercriminalité au sein d'Europol. Parmi d'autres mesures, la Commission reconnaît qu'«*il est nécessaire de procéder à une évaluation continue des aspects techniques et juridiques du rôle du chiffrement dans les enquêtes pénales, compte tenu de l'évolution constante des techniques de chiffrement, de leur utilisation accrue par les criminels et de l'incidence sur les enquêtes pénales*». La Commission soutiendra «*la mise en place d'une fonction d'observatoire*

en collaboration avec le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, le réseau judiciaire européen en matière de cybercriminalité (EJCN) et Eurojust».

Nous nous réjouissons du fait que la Commission envisage de proposer une série de mesures destinées à soutenir les autorités nationales dans la lutte contre le chiffrement dans les enquêtes pénales, «*sans interdire, limiter ni affaiblir le chiffrement*». **Nous saluons et soutenons l'affirmation de la Commission selon laquelle les «*mesures susceptibles d'affaiblir le chiffrement ou d'avoir une incidence sur un nombre élevé, voire inconsidéré, de personnes ne seraient pas prises en considération*».** Nous estimons que les mesures envisagées par la Commission peuvent être mises en œuvre dans le plein respect des droits fondamentaux, en observant les principes de nécessité et de proportionnalité.

Nous profitons de l'occasion pour réaffirmer que, selon nous, l'affaiblissement du chiffrement pour lutter contre la cybercriminalité n'est pas une option viable et que des mesures alternatives doivent être explorées[xxi]. Nous soulignons que ce point de vue est également le fondement des propositions de la Commission et est largement soutenu par les experts[xxii]. Nous nous félicitons des nouvelles recherches et sommes prêts à exercer notre rôle consultatif et à évaluer les propositions pertinentes. **En particulier, nous considérons que le projet d'«observatoire» peut jouer un rôle important dans la protection des droits fondamentaux des citoyens et nous espérons être consultés lors de sa préparation.** En outre, en notre qualité de contrôleur d'Europol pour le traitement des données à caractère personnel, nous veillerons à ce que les mesures, une fois appliquées dans la pratique, respectent les droits fondamentaux des personnes.

La communication conjointe propose que le futur centre européen de recherche et de compétences en cybersécurité et son réseau, en plus de soutenir la sécurité «*des produits et des services utilisés par les citoyens, les entreprises et les administrations au sein du marché unique numérique*», soutienne également la dimension «cyberdéfense» de l'UE. Nous recommandons d'envisager que les réalisations du Centre, destinées à la défense des citoyens de l'UE, puissent être utilisées contre eux si elles tombent entre de mauvaises mains ou sont mal utilisées.

Dans notre avis relatif aux technologies de surveillance intrusive[xxiii], nous avons déjà attiré l'attention sur les politiques de l'UE relatives aux produits et services potentiellement préjudiciables, notamment dans le domaine de la cybersécurité, et nous avons affirmé que la technologie de cybersurveillance doit être couverte de manière adéquate par des considérations telles que celles appliquées aux produits à «double usage». Nous avons mis en garde contre les risques associés au développement, à l'utilisation et à la commercialisation d'outils de piratage, qui sont très intrusifs dans la vie des personnes et qui représentent un risque élevé pour les libertés et les droits fondamentaux individuels. Nous avons indiqué que «*l'utilisation d'outils de surveillance devrait être couverte par une législation spécifique qui encadrerait les limites acceptables en matière de diffusion et d'utilisation de ces technologies et qui prévoirait les garanties nécessaires concernant cette utilisation*». Nous avons également ajouté que «*[d]ans le cadre du double usage, il conviendrait d'établir des normes permettant d'apprécier l'utilisation qui pourrait être faite des TIC ou des informations en cause et l'incidence que cette utilisation pourrait avoir sur les droits fondamentaux au sein de l'UE*». Nous prenons acte du fait que le Parlement européen examine actuellement un rapport sur la proposition de refonte de la Commission concernant le contrôle des exportations de biens à double usage[xxiv], qui inclurait certaines catégories d'outils de cybersurveillance dans le régime[xxv].

Outre la dimension extérieure, les outils avancés d'exploitation des failles ou des vulnérabilités en matière de sécurité peuvent également créer des risques pour ceux qui les produisent. Des rapports récents[xxvi] sur des outils de piratage préparés par une agence de sécurité de l'État qui

ont été divulgués et utilisés pour soutenir des cyberattaques malveillantes qui ont touché des dizaines de milliers d'ordinateurs et d'infrastructures critiques, entravant le fonctionnement des hôpitaux et bloquant les installations de l'administration en ligne, démontrent très clairement les risques.

La communication conjointe n'explique pas clairement comment seront gérés les risques liés à l'aide que l'UE prévoit d'offrir aux États membres pour «*développer des capacités à double usage dans le domaine de la cybersécurité*». Nous recommandons vivement de procéder à une évaluation approfondie des risques d'une telle stratégie et nous invitons la Commission à effectuer une analyse d'impact approfondie avant de lancer toute mesure.

- *En ce qui concerne l'application des obligations en matière de sécurité et de notification et la relation avec les notifications relatives aux violations de la sécurité et des données dans le RGPD*

Les organisations qui sont soumises aux obligations en matière de sécurité et d'information prévues par la directive SRI doivent simultanément veiller au respect des dispositions relatives à la sécurité des données à caractère personnel et à la notification des violations des données à caractère personnel. Si les deux instruments poursuivent des objectifs différents et que leur mise en œuvre nécessite la prise en considération de risques différents, les organisations qui sont soumises aux deux instruments devront mettre en œuvre des mesures appropriées pour répondre à toutes les exigences. Les entreprises et les autorités publiques qui traitent des données à caractère personnel doivent adopter une approche intégrée dans la prise en considération des exigences de sécurité et de protection des données à caractère personnel dans la prévention et le traitement des incidents de sécurité qui touchent les réseaux et les informations.
Nous recommandons à la Commission et aux États membres de tenir compte de la nécessité de cette synergie opérationnelle lorsqu'ils élaboreront des mesures pour la mise en œuvre efficace des dispositions relatives à la cybersécurité, telles que les mécanismes de notification et la coopération entre les autorités de contrôle de la protection des données et les autorités compétentes des États membres, telles qu'elles sont identifiées dans la directive SRI.

Plus en détail, nous estimons que **la relation entre la directive SRI et le RGPD en ce qui concerne la sécurité de l'information et les notifications des violations des données à caractère personnel devrait être clarifiée**[xxvii]**.** En vertu de l'article 1er, paragraphe 7, de la directive SRI, les dispositions relatives aux exigences en matière de sécurité et/ou de notification pour les fournisseurs de service numérique ou les opérateurs de services essentiels au titre de la directive ne sont pas applicables si une législation sectorielle de l'UE prévoit une exigence en matière de sécurité et/ou de notification, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues dans la directive SRI. Ce principe est rappelé dans la communication de la Commission, qui indique qu'une «*lex specialis*» prévaudrait sur les exigences en matière de sécurité et de notification prévues par la directive SRI[xxviii].

Toutefois, la directive SRI ou un acte juridique sectoriel n'a aucune incidence sur les obligations découlant du RGPD. La communication SRI reconnaît que les obligations de notification de la directive SRI sont «*sans préjudice de la notification à l'autorité de contrôle d'une violation de données à caractère personnel, visée à l'article 33 du règlement général sur la protection des données*».

Nous estimons que ce libellé est équivoque et nous tenons à clarifier la manière dont nous évaluons la relation entre les deux instruments juridiques sur ces obligations.

Selon nous, le RGPD ne peut pas être considéré comme un acte juridique sectoriel au sens de l'article 1er, paragraphe 7, de la directive SRI. Comme son titre l'indique, le RGPD a une portée générale et s'applique à toute entité traitant des données à caractère personnel, et ne comporte pas les limitations du champ d'application de la directive SRI et de certaines de ses dispositions spécifiques[xxix].

En conséquence, toutes les obligations du RGPD, notamment celles relatives à la sécurité des données à caractère personnel et aux atteintes aux données à caractère personnel, s'appliquent en plus de toutes les obligations éventuelles prévues par la directive SRI.
En outre, l'application parallèle du RGPD et de la directive SRI peut entraîner des difficultés pratiques pour les organisations soumises aux deux actes juridiques:

- L'article 32 du RGPD fait référence aux conditions dans lesquelles les responsables du traitement et les sous-traitants sont tenus de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques pour les personnes dont les données sont traitées. La directive SRI[xxx] adopte une approche basée sur les risques en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services ou d'en limiter l'impact. Bien que les résultats des deux évaluations différentes puissent, dans une certaine mesure, se chevaucher, les deux types d'actifs à protéger sont différents (droits fondamentaux des personnes physiques pour le RGPD, continuité de service pour la directive SRI) et l'organisation doit tenir compte de cette différence lorsqu'elle procède à l'évaluation des risques pour la sécurité.

- Les obligations de notification des incidents prévues par la directive SRI et les obligations de notification des violations des données à caractère personnel prévues par le RGPD[xxxi] sont déclenchées par des circonstances différentes, leurs finalités se recoupent partiellement, mais sont différentes et le destinataire de la notification est une autorité différente[xxxii].

  Alors que le RGPD impose la notification à l'autorité de protection des données compétente lorsqu'il existe un risque pour les données à caractère personnel, la directive SRI exige des opérateurs de services essentiels et des fournisseurs de service numérique qu'ils notifient aux autorités compétentes, en vertu de la directive, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent ou sur la fourniture du service offert par le fournisseur de service numérique. Les critères d'évaluation des différentes obligations de notification sont également différents. La directive SRI met l'accent sur la sécurité des systèmes d'information et le rétablissement des services, tandis que le RGPD se concentre sur la protection des personnes et de leurs données à caractère personnel. En outre, le RGPD exige également de notifier les personnes susceptibles d'être touchées, dans des circonstances et conditions spécifiques[xxxiii].

En tout état de cause, nous conseillons d'apporter davantage de clarté aux organisations visées (opérateurs de services essentiels et fournisseurs de services numériques) et aux États membres sur le fait que les exigences en matière de sécurité et de notification prévues par la directive SRI n'annulent pas ou ne remplacent pas celles prévues par le RGPD, mais plutôt que les deux textes juridiques s'appliquent et nécessitent une mise en œuvre intégrée efficace.
Dans ce contexte, nous nous associons à la Commission pour inviter le groupe de coopération prévu par la directive SRI à aider les États membres à suivre une approche cohérente dans le processus d'identification des opérateurs de services essentiels, lorsqu'ils agissent conformément à l'article 5, paragraphe 6, de la directive SRI.

Nous constatons que la Commission a également lancé une consultation sur un règlement d'exécution visant à fournir des spécifications supplémentaires sur les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques posés à la sécurité des réseaux et des systèmes d'information, ainsi que les paramètres permettant de déterminer si un incident a une incidence substantielle[xxxiv]. Nous invitons la Commission à veiller à ce que le futur règlement d'exécution soutienne une approche qui est non seulement compatible, mais qui bénéficie et complète efficacement les dispositions juridiques relatives aux obligations en matière de violation des données, ainsi que les orientations pratiques fournies à ce sujet par les autorités chargées de la protection des données au sein du groupe de travail de l'article 29 et du futur comité européen de la protection des données (CEPD).

Afin de parvenir à une approche cohérente dans la mise en œuvre de la directive SRI et du RGPD, nous recommandons une coopération renforcée entre les autorités de contrôle de la protection des données et les autorités nationales chargées de la mise en œuvre de la directive SRI, l'ENISA et les centres de réponse aux incidents de sécurité informatique afin de remédier à la fragmentation des différents cadres en ce qui concerne les obligations en matière de sécurité et de notification des organisations et de les soutenir dans l'élaboration de méthodologies et d'outils pour une approche intégrée du risque pour la sécurité de l'information et de la gestion des violations de données qui pourraient être efficaces pour satisfaire aux exigences de la directive SRI, du RGPD et de tout autre acte législatif applicable.

IV. Concernant la proposition de règlement sur la cybersécurité (*ci-après la «proposition»*).

1. Concernant la réforme de l'ENISA

Nous nous réjouissons du mandat permanent et des nouvelles responsabilités et ressources attribuées à l'ENISA. Nous notons que son rôle accru d'assistance et de conseil en matière de développement et de révision de la politique et du droit de l'Union dans le domaine de la cybersécurité peut être la clé d'une protection plus efficace des actifs numériques de l'UE et des politiques qu'ils soutiennent. Nous estimons qu'un mandat fort dans l'élaboration des politiques requiert un modèle de gouvernance approprié pour l'Agence, qui garantit la coordination avec d'autres organisations ayant des tâches dans des domaines connexes, ainsi que le contrôle total par les institutions de l'Union, en particulier en ce qui concerne la préparation et la mise en œuvre de la législation.

Outre une fonction politique élargie, la proposition de règlement attribuerait à l'ENISA un rôle opérationnel de centre de connaissances pour les incidents conformément à la directive SRI, au règlement eIDAS et à la directive établissant le code des communications électroniques européen (article 5, paragraphe 5, de la proposition).

Nous nous félicitons de ce que l'article 7 confirme que l'ENISA sera chargée de la coopération opérationnelle avec, entre autres, les institutions, organes, offices et agences de l'Union et les autorités de contrôle responsables de la protection de la vie privée et des données à caractère personnel, en vue de traiter les questions d'intérêt commun.

L'article 20 confirme l'existence et le rôle d'un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, notamment les représentants des autorités chargées de la protection des données. Même si le groupe permanent des parties prenantes n'a qu'une fonction consultative, nous estimons qu'une représentation plus importante des autorités de contrôle en matière de protection des données serait très bénéfique pour le groupe et contribuerait à améliorer la qualité de ses avis.

Nous constatons certains changements, dans la proposition, dans les références aux compétences de l'ENISA en matière de protection de la vie privée et des données à caractère personnel.

Bien qu'aucun véritable changement n'ait été apporté aux dispositions de fond dans les tâches de l'ENISA en matière de protection de la vie privée et des données à caractère personnel [voir l'article 3, point e), du règlement (UE) nº 526/2013 et l'article 7, paragraphe 2, de la proposition], de nombreux considérants du règlement (UE) nº 526/2013 se référaient directement à ces tâches (considérants 13 et 16). Ces considérants ne figurent plus dans la proposition et l'article 10 relatif aux tâches de l'ENISA en matière de recherche et d'innovation ne mentionne plus la protection de la vie privée et des données.

Nous déplorons que la disparition de cette tâche dans le domaine de la recherche et du conseil risque d'entraîner l'arrêt des travaux de l'ENISA sur les technologies renforçant la protection de la vie privée et des données (PET)[xxxv] et, plus généralement, sur la protection des données dès la conception et par défaut[xxxvi], car nous sommes fermement convaincus qu'il est nécessaire de stimuler ces activités de recherche et de conseil, notamment en ce qui concerne les obligations en matière de protection des données dès la conception et par défaut créées par le RGPD. Il n'existe actuellement aucun organe de l'UE qui pourrait combler cette lacune.

Nous recommandons que le législateur réfléchisse à la meilleure manière de poursuivre et d'améliorer cette tâche politique, soit en confirmant explicitement le rôle de l'ENISA à cet égard par des dispositions de fond dans la proposition, soit en transférant les compétences en matière de protection des données à caractère personnel à un autre organe de l'UE. La protection des données à caractère personnel couvre la sécurité, mais ne s'y limite pas et un mandat sur cet aspect de la politique devrait être défini dans un contexte spécialisé et soutenu par des ressources adéquates.

Le CEPD qui, conformément à l'article 46, point e), du règlement (CE) nº 45/2001, «*surveille les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications*», est prêt à poursuivre et à renforcer sa contribution, soit en collaboration plus étroite avec l'ENISA, soit de toute autre manière prévue par le législateur, pour autant que des ressources adéquates soient mises à disposition.

Une possibilité de renforcer la recherche et le conseil sur les technologies renforçant la protection des données consisterait à confier un mandat plus fort au CEPD, si possible reflété dans la réforme en cours du règlement (CE) nº 45/2001 et, en se fondant sur les tâches déjà existantes, à surveiller et à promouvoir le développement de technologies renforçant la protection de la vie privée et des données et de méthodes de protection des données dès la conception et par défaut. Cette tâche pourrait être accomplie en coordination avec des recherches nationales pertinentes menées par des universités, l'industrie et les autorités publiques, y compris les autorités chargées de la protection des données, à condition que les ressources nécessaires soient allouées par les autorités budgétaires.

2. Cadre concernant la certification européenne en matière de cybersécurité

L'amélioration de la transparence de l'*assurance* de la cybersécurité, qui est l'un des objectifs moteur de la nouvelle proposition, augmente la capacité des utilisateurs à faire confiance aux fournisseurs de services numériques traitant des données à caractère personnel et contribue à la

capacité des responsables du traitement à choisir des sous-traitants garantissant le respect de l'obligation de sécurité imposée par la législation en matière de protection des données.

Conformément à son article 43, la proposition de règlement sur la cybersécurité a pour objectif d'établir un cadre de certification de cybersécurité visant à émettre des certificats qui attestent «*que les produits et services TIC qui ont été certifiés (...) satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné*», à des actions visant à compromettre la sécurité. La certification vise les produits et les services, les objectifs sont liés à la résilience face aux actions qui visent à compromettre l'objectif de sécurité centrale et la certification concerne trois niveaux d'assurance différents. Les autorités nationales de contrôle de la certification seront notamment compétentes pour traiter les plaintes déposées par des personnes physiques ou morales concernant les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire et pourront imposer des sanctions conformément au droit national[xxxvii].

Ce cadre diffère considérablement de l'approche utilisée par le RGPD. La certification d'une opération de traitement ou plus au titre de l'article 42 du RGPD peut contribuer, dans certaines circonstances, à démontrer le respect du RGPD lui-même, en application du principe comptable. Le groupe de travail de l'article 29 élabore actuellement des orientations sur les critères de certification et d'accréditation dans le RGPD. Entre autres éléments, les systèmes de certification reconnus dans le cadre du RGPD peuvent couvrir les obligations prévues à l'article 32 du RGPD sur la sécurité des opérations de traitement. L'objet de la certification au titre du RGPD est les opérations de traitement des données à caractère personnel, la sécurité n'est qu'un des domaines couverts et le concept de niveaux d'assurance n'est pas applicable.

Étant donné que les mêmes organisations peuvent chercher à obtenir des certifications au titre des deux instruments, il est de la plus haute importance que des synergies techniques et de gouvernance soient créées afin que les certifications au titre du cadre européen de certification de cybersécurité et du RGPD ne soient pas perçues comme contradictoires ou sans lien entre elles par les organisations qui s'efforcent de se conformer aux instruments pertinents. Bien que le champ d'application différent des systèmes de certification empêche leur intégration harmonieuse, les organismes de l'UE impliqués dans leur mise en œuvre doivent veiller à ce qu'ils se complètent et se renforcent mutuellement. La Commission et l'ENISA sont invitées à prendre contact avec le groupe de travail de l'article 29 et le futur CEPD en vue d'une éventuelle coopération. Avant d'envisager l'adoption d'un acte d'exécution relatif à un système de certification au titre de l'article 44 du projet de règlement sur la cybersécurité, le Commission peut consulter le CEPD et tenir compte de son avis.

La coopération avec les autorités nationales de contrôle de la protection des données, le cas échéant, permettrait une surveillance plus efficace pour les deux types d'autorités compétentes. La règlement sur la cybersécurité devrait explicitement inclure les autorités de contrôle de la protection des données parmi les autorités avec lesquelles coopérer [article 50, paragraphe 6, point d)].

Bruxelles, le 15 décembre 2017

Wojciech Rafał WIEWIÓROWSKI

Notes

[i] Communication conjointe de la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, JOIN/2017/0450 final, 13.9.2017, http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=JOIN%3A2017%3A450%3AFIN

[ii] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité), COM/2017/0477 final, 13.9.2017, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017PC0477R(01)

[iii] Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs, JO L 239 du 19.9.2017, p. 36.

[iv] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, COM/2017/0476 final, 13.9.2017, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2017:476:FIN

[v] https://ec.europa.eu/digital-single-market/en/cyber-security

[vi] Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil, COM(2017)489, 13.9.2017, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017PC0489

[vii] Communication de la Commission au Parlement européen, au Conseil européen et au Conseil, Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017DC0608

[viii] Avis du CEPD du 10 décembre 2010 sur la proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), https://edps.europa.eu/sites/edp/files/publication/10-12-20_enisa_fr.pdf

[ix] Observations du CEPD du 12 octobre 2012 sur la consultation publique de la DG Connect concernant l'amélioration de la sécurité des réseaux et de l'information (SRI) dans l'UE: https://edps.europa.eu/sites/edp/files/publication/12-10-10_comments_nis_en.pdf

[x] Avis du CEPD de juin 2013 sur la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» et sur la proposition de directive de la Commission concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union: https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_fr.pdf

[xi] Avis du 15 décembre 2015 sur la diffusion et l'utilisation des technologies de surveillance intrusive: https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_fr.pdf

[xii] Lignes directrices du CEPD du 21 mars 2016 sur les mesures de sécurité concernant le traitement des données à caractère personnel - article 22 du règlement nº 45/2001: https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf

[xiii] 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 (le règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

[xiv] Voir la définition de «responsable du traitement» à l'article 4, paragraphe 7, du RGPD.

[xv] Voir la définition de «sous-traitant» à l'article 4, paragraphe 8, du RGPD.

[xvi] Voir la définition de «violation de données à caractère personnel» à l'article 4, paragraphe 12, du RGPD.

[xvii] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO L 8 du 12.1.2001, p. 1.

[xviii] Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM(2017) 010 final, 10.1.2017, http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52017PC0010

[xix] Eurobaromètre Spécial 464a, L'attitude des Européens à l'égard de la cybersécurité, publié en septembre 2017.

[xx] CERT-EU Security Advisory 2017-012 du 22 mai 2017, WannaCry Ransomware Campaign Exploiting SMB Vulnerability, https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf
[xxi] Discours de Giovanni Buttarelli, CEPD, «Chiffrement, Sécurité et Libertés» à l'Assemblée nationale française, Paris, France: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/encryption-protects-security-and-privacy_en
[xxii] Avis scientifique nº 2/2017 du 24 mars 2017 du groupe de conseillers scientifiques de haut niveau de la Commission sur la cybersécurité dans le marché unique numérique européen, section 4.1.3,https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pd
[xxiii] Voir la note de bas de page **Error! Bookmark not defined.**.
[xxiv] Proposition de règlement du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte), COM(2016) 616 final, 28.9.2016.
[xxv] 2016/0295(COD) Régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage Refonte,
[xxvi] Voir par exemple: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html
[xxvii] Voir la note de bas de page **Error! Bookmark not defined.**.
[xxviii] La communication et la directive SRI fournissent des exemples de législation sectorielle spécifique:

- Obligations au titre de la directive 2002/21/CE applicables aux réseaux et services de communications électroniques à la disposition du public.
- Obligations au titre du règlement nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques.
- Notifications au titre de la directive 2014/64/UE sur les marchés des instruments financiers.
- Obligations au titre du règlement (UE) nº 648/2012 du Parlement européen et du Conseil sur les contreparties centrales et les référentiels centraux.
- Obligations au titre de la directive 2 sur les services de paiement.

[xxix] Par exemple, l'article 16, paragraphe 11, de la directive SRI.
[xxx] Voir articles 14 et 16 de la directive SRI.
[xxxi] Le Groupe de l'article 29 a présenté un projet de lignes directrices sur la manière d'interpréter les dispositions du RGPD relatives aux violations des données à caractère personnel: http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 Une version finale sera produite dans les mois qui viennent.
[xxxii] Voir également ENISA, Incident notification for DSPs in the context of the NIS Directive - A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive (en anglais), février 2017, p. 20, disponible à l'adresse www.enisa.eu: «*Les fournisseurs de service numérique pourraient devoir signaler le même incident aux deux autorités responsables. En théorie, le RGPD couvre la confidentialité des données à caractère personnel et la directive SRI couvre la confidentialité du service offert et des données sous-jacentes (qui, dans la plupart des cas, sont des données à caractère personnel). Contrairement à la directive SRI, le RGPD ne prévoit pas d'approche allégée».*
[xxxiii] Voir l'article 34 du RGPD.
[xxxiv] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4460501_et
[xxxv] P.ex. Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies of March 2016 and subsequent measures on PETS; Privacy Enhancing Technologies: Evolution and State of the Art, mars 2017, https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art
[xxxvi] P.ex. Report on Privacy and Data Protection by Design, janvier 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
[xxxvii] Voir l'article 50, paragraphe 7, et l'article 54 de la proposition de règlement sur la cybersécurité.