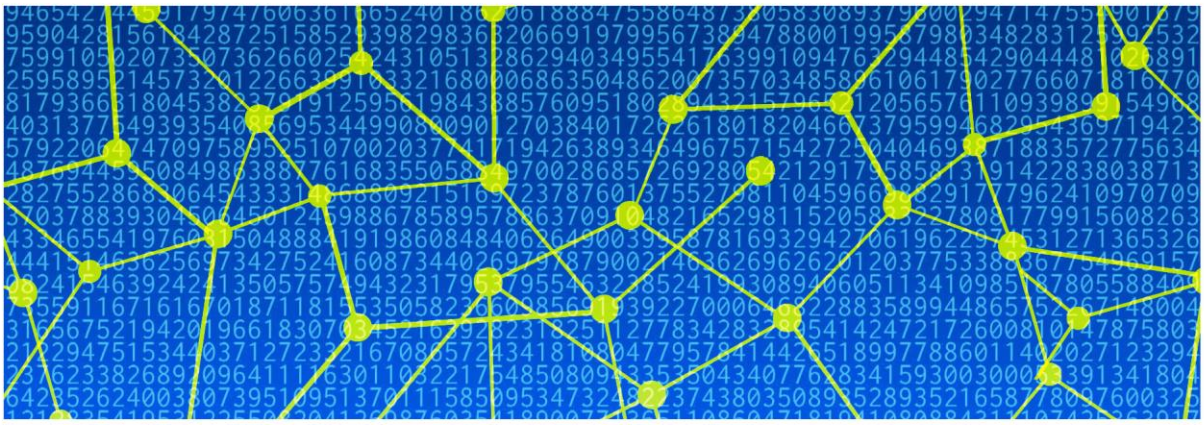

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 5/2018

Avis préliminaire sur le respect de la vie privée dès la conception

EDPS

31 mai 2018

Le contrôleur européen de la protection des données (CEPD) est une institution de l'Union européenne indépendante chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[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 leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, «lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel…», de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis vise à contribuer au succès de la nouvelle obligation de «protection des données dès la conception et [de] protection des données par défaut» prévue à l'article 25 du règlement général sur la protection des données (RGPD) en sensibilisant les parties concernées, en favorisant le débat et en proposant des axes d'action possibles.

Les principes de respect de la vie privée dès la conception et par défaut sont explorés dans leur évolution historique et dans leur traduction en méthodes d'ingénierie de la vie privée et en technologies renforçant la protection de la vie privée («privacy enhancing technologies», PET).

Cette analyse se situe dans le contexte de la nécessité croissante et généralisée de fonder le développement technologique sur les valeurs humaines et l'éthique. L'application effective du principe de respect de la vie privée dès la conception et par défaut peut constituer une étape importante sur la voie d'une conception technologique fondée sur les valeurs humaines.

Résumé

Les possibilités et les limites de la technologie jouent un rôle de plus en plus important dans nos vies personnelles et dans nos sociétés. La mesure dans laquelle les êtres humains jouissent de leurs droits fondamentaux dépend non seulement des cadres juridiques et des normes sociales, mais aussi des fonctionnalités de la technologie à leur disposition. Les récentes découvertes d'utilisation inappropriée de données à caractère personnel ont porté le débat public sur la protection des données à un niveau sans précédent. Il est nécessaire que le façonnage et l'utilisation de la technologie tiennent compte de la nécessité de respecter les droits des personnes, et ne soient pas exclusivement motivés par les intérêts économiques de quelques entreprises.

Avec la mise en application totale du règlement général sur la protection des données dans l'Union européenne à compter du 25 mai 2018, la protection des données dès la conception et par défaut devient une obligation juridique exécutoire. Nous devons maintenir la dynamique afin que cette nouvelle obligation puisse renforcer l'efficacité de la protection promise par le RGPD. Cela contribuera à cet objectif en sensibilisant les parties concernées, en favorisant la création de valeur publique et de bien-être sociétal et en appelant toutes les parties concernées à s'engager dans un débat responsable en vue de prendre les mesures appropriées.

Le présent avis fait la distinction entre le principe général de «respect de la vie privée dès la conception», qui englobe une dimension éthique conforme aux principes et aux valeurs de la Charte des droits fondamentaux de l'Union, et les obligations juridiques particulières prévues par l'article 25 du RGPD que nous appellerons «protection des données dès la conception» et «protection des données par défaut».

L'avis retrace brièvement l'histoire du principe de respect de la vie privée dès la conception, des recherches initiales sur les technologies de protection de la vie privée au RGPD. Il analyse aussi le contenu de l'article 25 et sa relation avec les autres articles. Il s'intéresse également à d'autres éléments de la législation de l'Union qui font référence au respect de la vie privée dès la conception. Il présente en outre certaines modalités de mise en œuvre en dehors de l'Union.

Dans une vue d'ensemble de l'état des connaissances, l'avis donne des exemples de méthodes en vue de déterminer les exigences en matière de respect de la vie privée et de protection des données et de les intégrer aux processus d'ingénierie de la vie privée afin de mettre en œuvre les garanties technologiques et d'organisation adéquates. Certaines de ces méthodes définissent des objectifs en matière de protection des données directement à partir des principes de respect de la vie privée et de protection des données, tels que ceux du RGPD, ou les déduisent à partir d'objectifs intermédiaires opérationnels. D'autres méthodes reposent sur la gestion des risques. Le processus de conception et d'exploitation doit prendre en considération l'ensemble du cycle de vie d'un service ou d'un produit, de la planification initiale à la suppression du service/du produit. La vue d'ensemble technologique inclut aussi des efforts de normalisation afin d'intégrer les exigences en matière de respect de la vie privée dans la conception des systèmes et l'état des connaissances relatives aux technologies renforçant la protection de la vie privée.

Il existe un besoin de faire progresser l'état des connaissances et le recours aux solutions renforçant la protection de la vie privée. Si les recherches se multiplient, ainsi que les initiatives consacrées au développement de la discipline de l'ingénierie de la vie privée, cela reste insuffisant pour susciter un changement dans l'efficacité de la protection des personnes et de leurs données à caractère personnel. Les organisations ne peuvent retirer que des avantages de l'adoption d'une approche fondée sur le respect de la vie privée dès la conception. Les

politiques qui encouragent les technologies et les stratégies renforçant la protection de la vie privée doivent s'inscrire dans les priorités de l'Union et les administrations publiques doivent montrer l'exemple. L'initiative IPEN sera un instrument pour encourager les parties concernées au niveau international à recourir aux technologies renforçant la protection de la vie privée.

Les initiatives en matière de respect de la vie privée dès la conception doivent être considérées dans le contexte plus vaste de l'intégration des considérations éthiques dans la conception technologique, suivant les conclusions du récent rapport du groupe consultatif sur l'éthique du CEPD.

Dans le présent avis, le CEPD formule un certain nombre de recommandations à l'intention des institutions de l'Union:

- garantir une solide protection de la vie privée, notamment le respect de la vie privée dès la conception, dans le règlement «vie privée et communications électroniques»;
- favoriser le respect de la vie privée dans tous les cadres juridiques qui influencent la conception de la technologie, en multipliant les mesures d'incitation et en justifiant les obligations, notamment les règles de responsabilité appropriées;
- encourager l'introduction et l'adoption d'approches fondées sur le respect de la vie privée dès la conception et de PET dans l'Union et au niveau des États membres au moyen de mesures de mise en œuvre et d'initiatives stratégiques appropriées;
- garantir des compétences et des ressources pour la recherche et l'analyse dans le domaine de l'ingénierie de la vie privée et des PET au niveau de l'Union, par l'ENISA ou d'autres entités;
- favoriser la mise au point de nouvelles pratiques et de nouveaux modèles d'entreprise au moyen des instruments de recherche et de développement technologique de l'Union;
- aider les administrations publiques nationales et de l'UE à intégrer les exigences appropriées en matière de respect de la vie privée dès la conception dans les marchés publics;
- soutenir la mise en place d'un inventaire et d'un observatoire de «l'état des connaissances» en matière d'ingénierie de la vie privée et de PET et de leur état d'avancement.

Le CEPD:

- continuera à encourager le respect de la vie privée dès la conception, dans les cas appropriés en coopération avec d'autres autorités chargées de la protection des données au sein du Comité européen de protection des données (EDPB);
- soutiendra l'application coordonnée et effective de l'article 25 du RGPD et des dispositions y afférentes;
- donnera des directives aux responsables du traitement des données concernant la bonne application du principe défini dans la base juridique; et
- avec les autorités chargées de la protection des données de l'Autriche, de l'Irlande et du Schleswig-Holstein, lancera un concours pour la conception d'une application respectueuse de la vie privée dans le domaine de la santé mobile.

La coordination et la mise en commun des capacités technologiques des autorités chargées de la protection des données sont essentielles pour favoriser la protection des données dès la conception et par défaut. La coopération au sein de l'EDPB, ainsi que du groupe de travail international sur la protection des données dans les télécommunications (IWGDPT, «groupe de Berlin»), est nécessaire.

Les retours d'information concernant le présent avis préliminaire sont les bienvenus.

La conférence internationale des commissaires à la protection des données et de la vie privée 2018 constituera une étape majeure dans les discussions sur l'éthique numérique en général et sera l'occasion de mieux définir la voie à suivre en matière de respect de la vie privée dès la conception.

TABLE DES MATIÈRES

1. Le respect de la vie privée dès la conception et par défaut: une possibilité de protéger efficacement les personnes

1.1 Pourquoi un avis sur «le respect de la vie privée dès la conception»

1. Au début de l'année 2018, le débat public sur le traitement des données à caractère personnel au moyen de technologies de l'information et de la communication de pointe a fait l'objet d'une attention sans précédent. Les commissions parlementaires mènent ou envisagent de mener des enquêtes au Parlement européen[1], au Congrès des États-Unis[2] et au sein des parlements nationaux d'États membres de l'Union tels que le Royaume-Uni[3], l'Allemagne[4] et la France[5]. Á l'instard du grand public, les membres de ces parlements[6], veulent comprendre comment leurs données à caractère personnel sont traitées et utilisées dans le cadre du suivi des activités des citoyens en ligne et du traitement des données à caractère personnel collectées. Les auditions des dirigeants d'entreprises technologiques jouent un rôle central dans ces enquêtes.

2. Malgré l'intérêt massif des médias, le public n'a encore connaissance que du «sommet de l'iceberg»[7] en ce qui concerne le suivi et le ciblage. Le CEPD a analysé l'utilisation des données à caractère personnel à des fins de manipulation en ligne dans son récent avis[8] et a formulé des recommandations sur l'application de la législation en matière de protection des données, l'analyse commune et la coopération des organismes de réglementation entre les secteurs, l'autoréglementation et l'autonomisation des individus. L'avis note aussi que les découvertes récentes soulignent l'importance de concevoir les technologies de manière à ce qu'elles favorisent l'exercice pratique et effectif des droits fondamentaux, au lieu d'être exclusivement motivées par les intérêts économiques des entreprises.

3. Le présent avis repose sur de nombreuses années de travail des experts en matière de respect de la vie privée et de technologie sur le rôle de la conception technologique en vue de garantir le droit fondamental au respect de la vie privée. Il dresse le bilan des évolutions juridiques et technologiques dans le monde et présente des recommandations concernant les mesures qui permettront de faire progresser le respect de la vie privée et la protection des données dès la conception. Si les observations concernant la manipulation en ligne mettent en évidence l'urgence d'une nouvelle approche en matière de conception de la technologie, et si les systèmes utilisés sur l'internet jouent un rôle central, la nécessité de garantir que les droits fondamentaux sont pris en considération dans le cadre du développement technologique s'applique à tous les outils de traitement des données, quels que soient les plates-formes et les domaines d'application utilisés.

«Respect de la vie privée dès la conception» ou «protection des données dès la conception»?

4. Dans le cadre du présent avis, nous utilisons le terme «respect de la vie privée dès la conception» pour désigner la notion générale recouvrant les mesures technologiques destinées à garantir le respect de la vie privée qui a pris de l'ampleur dans le débat international ces dernières décennies. En revanche, nous utilisons le terme «protection des données dès la conception» et «protection des données par défaut» pour désigner les obligations juridiques particulières établies par l'article 25 du RGPD[9]. Si les mesures prises au titre de ces obligations contribueront aussi à atteindre l'objectif plus général de «respect

de la vie privée dès la conception», nous estimons qu'un spectre plus large d'approches peut être pris en considération pour atteindre l'objectif de «respect de la vie privée dès la conception», qui comporte une dimension visionnaire et éthique, conforme aux principes et aux valeurs consacrés dans la Charte des droits fondamentaux de l'Union.

Est-ce la technologie qui façonne la société, ou la société qui façonne la technologie?

5. La technologie est liée à l'évolution de l'humanité depuis les premiers outils fabriqués par l'homme. Les avancées technologiques ont fortement influencé l'évolution des sociétés humaines, souvent pour le meilleur, parfois pour le pire. Les règles qui régissent nos sociétés, tant sous la forme de lois contraignantes que sous la forme de normes sociales, sont aussi fortement influencées par la technologie. La protection des données est un bon exemple de cette interaction, car la naissance de cette notion juridique est liée au développement et à la popularisation des ordinateurs d'abord, et, plus récemment, de l'internet. Les termes programmatiques du 2ème considérant de la directive relative à la protection des données[10] («*considérant que les systèmes de traitement de données sont au service de l'homme*») et du 4ème considérant du RGPD («*[l]e traitement des données à caractère personnel devrait être conçu pour servir l'humanité*») illustrent parfaitement ce point. L'exemple de la protection des données montre la complexité de l'interaction entre la technologie et les règles: si la notion de protection des données elle-même a été élaborée en réaction à la puissance émergente de l'informatique dans l'administration et dans les entreprises, il a fallu plusieurs décennies pour que l'obligation d'intégrer des garanties de protection des données dans la conception technologique devienne une obligation juridique explicite.

6. En 1989, deux développements ont marqué le début d'une transformation qui a fait de l'internet l'infrastructure de communication dominante qu'il est aujourd'hui. Si, pendant ses 20 premières années d'existence, l'internet a essentiellement été utilisé par des institutions scientifiques et de recherche civiles et militaires, la connexion aux services de messagerie électronique existants a permis d'ouvrir celui-ci à une utilisation commerciale publique. La même année, le système hypertexte réparti proposé par Sir Tim Berners-Lee, qui utilise des liens et des URL, a jeté les bases du World Wide Web et de son potentiel apparemment illimité d'organiser les informations et de les rendre accessibles à l'échelle mondiale.

7. Tant l'internet que le World Wide Web ont été développés et modifiés sans interruption au cours des 29 dernières années, et leur taille, leur potentiel et leurs capacités continuent de croître. Les témoins de connexion, les langages de script, les formats audiovisuels compressés, les moteurs de recherche, les protocoles de diffusion, les plates-formes de réseaux sociaux, les dispositifs mobiles intelligents, les outils de suivi, d'analyse et de profilage ont favorisé de nouveaux modes d'utilisation et de nouvelles manières de faire des affaires. Si de nombreux avantages sont évidents, de sérieuses craintes quant à leur incidence sur les droits fondamentaux et les fondements mêmes et le fonctionnement des sociétés démocratiques se font de plus en plus sentir. La perte de contrôle sur les données à caractère personnel, la diffusion de «fake news» et de publicité politique ciblée, sur la base de l'analyse et de l'évaluation de données à caractère personnel, comptent parmi les problèmes récemment mis en évidence[11]. Dans son discours prononcé en 2018 à l'occasion de l'anniversaire du WWW, Sir Tim Berners-Lee fait observer que plus de la moitié de la population mondiale aura accès au web, mais que le web est à présent contrôlé par une poignée de puissantes entreprises plates-formes qui ont le pouvoir de décider quelles idées et innovations sont mises en œuvre, excluant la majeure partie de la population mondiale

des décisions quant à son développement et faisant dans le même temps de la publicité le principal moteur du web[12].

8. Si nos parlements et nos sociétés poursuivent leurs travaux pour déterminer comment remédier à ces problèmes, les nouvelles évolutions technologiques sont susceptibles de susciter une modification encore plus grande et plus profonde de la communication humaine et de l'interaction sociale. Le traitement de volumes énormes d'informations, les mégadonnées, est en constante augmentation. L'internet des objets en est encore au tout début de son déploiement et le nombre d'appareils connectés devrait être multiplié par dix au moins, se faisant plus présents non seulement dans les foyers et dans les villes, mais aussi dans le corps humain lui-même[13]. La transition du développement de l'intelligence artificielle de domaines spécialisés pointus à une application générale ne fait que commencer. La technologie de la *blockchain* est encouragée pour tout un éventail d'utilisations, notamment le traitement des données à caractère personnel. Les décisions d'affaires et d'ingénierie concernant le futur développement de ces technologies qui sont prises aujourd'hui auront vraisemblablement des effets à long terme pour nous-mêmes et nos descendants.

9. Nous avons observé un effort fructueux de façonner la technologie en fonction des objectifs sociétaux sous la forme des principes de durabilité élaborés ces dernières décennies en vue de préserver les ressources naturelles[14]. Comme en droit de l'environnement, la technologie doit être conçue et appliquée tout au long de son cycle de vie de manière compatible avec les valeurs et les droits fondamentaux qui déterminent nos sociétés démocratiques. Cette expérience nous inspire la confiance qu'il est possible de prendre le contrôle de la technologie pour le meilleur de l'humanité. La recherche dans l'histoire de la technologie a montré que «*la technologie n'est ni bonne ni mauvaise, et elle n'est pas non plus neutre*»[15], que son évolution n'est pas soumise à un déterminisme intrinsèque et qu'elle peut être façonnée: «*[b]ien que la technologie puisse être un élément capital dans de nombreux enjeux publics, les facteurs non techniques prévalent dans les décisions stratégiques liées à la technologie*»[16]. Ces dernières années, le CEPD a encouragé une analyse des exigences éthiques générales dans le contexte des travaux du groupe consultatif sur l'éthique[17] mis sur pied en 2015.

10. L'Union a adopté des dispositions spécifiques concernant la définition des solutions technologiques lorsqu'il y a traitement de données à caractère personnel. Depuis le 25 mai 2018, date à laquelle le RGPD[18] est devenu pleinement applicable, la protection des données dès la conception et la protection des données par défaut ne sont plus seulement des desiderata ou des bonnes pratiques recommandées, mais bien des obligations juridiques pleinement exécutoires que toutes les personnes qui traitent des données à caractère personnel en vertu du droit de l'Union doivent respecter. Nous devons maintenir la dynamique afin que cette nouvelle obligation puisse concrétiser et renforcer l'efficacité de la protection promise par le RGPD, et qu'elle ne soit pas interprétée de manière trop étroite.

11. Le présent avis du CEPD vise à contribuer à ce processus en sensibilisant les parties concernées et en encourageant la création de valeur publique et de bien-être sociétal, et il invite les parties concernées pertinentes (les responsables politiques nationaux et de l'UE, les organismes de réglementation de la protection des données et autres, les milieux académiques, les fournisseurs de technologie, les organisations publiques et privées chargées du traitement de données à caractère personnel et les personnes dont les données sont traitées) à entamer un débat responsable afin de prendre les bonnes décisions en gardant

à l'esprit non seulement l'avancée de la technologie et ses capacités infinies, mais aussi les droits fondamentaux en jeu, parmi lesquels le respect de la vie privée et la protection des données à caractère personnel.

12. Si l'article 25 du RGPD représente une étape importante sur la voie de la conception et de l'exploitation responsables de la technologie, et si la manière dont ce nouveau principe juridique est mis en œuvre et appliqué sera un facteur essentiel de réussite pour l'ensemble du nouveau cadre juridique de protection des données, le présent avis ne contient néanmoins pas d'analyse juridique complète de l'article 25 du RGPD[19], ni d'instructions étape par étape[20] pour permettre aux organisations de se conformer à l'article 25. Il vise plutôt à déterminer les éléments essentiels qui sont susceptibles de faciliter la compréhension du principe essentiel et de ses conséquences pour toutes les parties concernées, en véhiculant des messages clairs dans un langage simple afin de favoriser un débat fructueux. Des instructions détaillées concernant l'article 25 peuvent être attendues de la part des autorités de contrôle et de l'EDPB.

1.2 Historique du respect de la vie privée dès la conception

13. Dans le passé, de nombreuses organisations percevaient le respect de la vie privée et la protection des données comme une question essentiellement liée à la conformité juridique, souvent limitée au simple processus formel de publication de politiques de confidentialité extensives couvrant toute éventualité potentielle et réagissant aux incidents de façon à minimiser le préjudice causé à leurs propres intérêts. Autrement dit, pour de nombreuses organisations, la protection des données se limitait à une «façade» avec très peu d'incidence sur les objectifs ou pratiques de l'organisation ou sur la protection des personnes concernées.

14. La **difficulté de traduire les principes juridiques en exigences concrètes** et la nécessité d'une approche réellement pluridisciplinaire[21] pour faire face aux problèmes liés au respect de la vie privée ont contribué à élargir le fossé entre une discipline de conformité juridique gérée par des juristes, d'une part, et un processus d'innovation dynamique mené par les dirigeants d'entreprise et les ingénieurs, de l'autre, qui sont en définitive responsables de la conception et de la mise en œuvre des procédés et des systèmes qui régissent le fonctionnement réel de l'organisation.

15. Dans ce contexte, l'idée que l'évolution technologique n'est pas seulement la cause de la multiplication des préoccupations en matière de respect de la vie privée, mais qu'elle fait aussi partie de la solution, est née pas plus tard que lors de la codification des principes de respect de la vie privée en bonnes pratiques et en lois, soit à partir des années 70. David Chaum et d'autres[22] ont mené des recherches technologiques initiales clairement axées sur les préoccupations en matière de respect de la vie privée, avec des contributions concernant la minimisation des données, les transactions et communications anonymes, ainsi que les technologies de protection de la vie privée dans les relevés statistiques. Les améliorations dans les technologies de la communication, la sécurité informatique (y compris les cadres conceptuels conçus pour autonomiser l'utilisateur final des systèmes de TIC avec davantage d'autodétermination dans le domaine de la vie privée et de la sécurité[23]), dans les communications anonymes et dans la cryptographie ont ouvert la voie au développement de ce qui s'est ensuite fait connaître sous le nom de technologies renforçant la protection de la vie privée (PET)[24], une famille de solutions technologiques axées sur la minimisation des risques pour la vie privée des personnes.

16. Ni la sécurité ni le respect de la vie privée n'ont cependant réellement été intégrés en tant qu'exigences primaires dans le développement et l'expansion de l'internet et du WWW, et la priorité a été donnée à la fonctionnalité, à l'extensibilité et à l'ouverture. Après les révélations sur les programmes de surveillance massive par les agences nationales de sécurité en 2013[25], l'*Internet Engineering Task Force* (IETF)[26] a fait une déclaration[27] reconnaissant que «*l'ampleur du suivi dont il a récemment été fait état est surprenante. Une telle ampleur n'a pas été envisagée lors de la conception de nombreux protocoles internet...*» Des travaux visant à intégrer davantage le respect de la vie privée dans les protocoles internet ont ensuite été lancés avec la réunion de l'IETF à Vancouver en novembre 2013.

17. Le terme «respect de la vie privée dès la conception» a à l'origine été utilisé par Ann Cavoukian alors qu'elle était commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada. Selon son concept, la protection de la vie privée dès la conception peut être divisée en «sept principes fondamentaux»[28], qui soulignent la nécessité d'être proactif en prenant en considération les exigences de protection de la vie privée dès la phase de conception et tout au long du cycle de vie des données, qui doivent être «*intégrées dans la conception et l'architecture des systèmes informatiques et des pratiques commerciales... sans en diminuer la fonctionnalité...*», avec le respect de la vie privée comme paramètre par défaut, la sécurité de bout en bout, y compris la sécurité de la destruction des données, et une forte transparence soumise à une vérification indépendante. Le principe du respect de la vie privée par défaut a été défini comme le deuxième principe fondamental, qui établit que le respect de la vie privée dès la conception nécessite de «*garantir que les données à caractère personnel sont automatiquement protégées dans tout système informatique ou toute pratique commerciale. Si une personne ne fait rien, sa vie privée reste néanmoins protégée. Aucune action n'est requise de la part de la personne afin de protéger sa vie privée – cette protection est intégrée au système, par défaut*». Cette déclaration est une définition opérationnelle puissante du principe de respect de la vie privée par défaut, où la personne n'est pas tenue de s'efforcer de protéger sa vie privée lorsqu'elle utilise un service ou un produit, mais bénéficie «automatiquement» (aucun comportement actif requis) du droit fondamental au respect de la vie privée et à la protection des données à caractère personnel.

18. Certains éléments du principe de respect de la vie privée dès la conception figuraient déjà dans la directive 95/46/CE relative à la protection des données[29] (ci-après, «la directive»), abrogée par le RGPD. Le 46ème considérant de la directive souligne comment les mesures techniques et d'organisation à prendre pour protéger les droits et libertés des personnes dont les données sont traitées doivent s'appliquer «*tant au moment de la conception qu'à celui de la mise en œuvre du traitement...*».

19. La «résolution sur le respect de la vie privée dès la conception» adoptée lors de la 32e conférence des commissaires à la protection des données et de la vie privée en octobre 2010[30] représente un jalon dans la reconnaissance du principe en tant qu'«*élément essentiel de la protection fondamentale de la vie privée*». La conférence a invité les autorités chargées de la protection des données à encourager le respect de la vie privée dès la conception dans la «*formulation des politiques et de la législation dans leurs domaines de compétence respectifs*».

20. Dans sa réponse à la consultation publique de la Commission européenne pour la réforme de la protection des données, le groupe de travail «Article 29» (WP29)[31] a exigé

l'introduction du principe de respect de la vie privée dès la conception dans le nouveau cadre législatif, car «*si les dispositions susmentionnées de la directive contribuent à promouvoir la prise en compte du respect de la vie privée dès la conception, elles n'ont, en pratique, pas suffi à garantir l'intégration du respect de la vie privée dans les TIC*», et a aussi demandé «*un paramétrage par défaut favorable au respect de la vie privée*». Le WP29 a poursuivi en recommandant que ce «*principe [soit] contraignant pour les concepteurs et producteurs de technologies ainsi que pour les responsables du traitement des données... Ils devraient avoir l'obligation de prendre en compte la protection technologique des données dès la phase de planification des procédures et des systèmes technologiques d'information».*

21. Dans son «Avis sur la promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée» de mars 2010[32], le CEPD a pleinement approuvé le principe de respect de la vie privée dès la conception comme instrument essentiel pour renforcer la confiance dans les technologies de l'information et a réalisé une analyse complète assortie de recommandations spécifiques. Nous avons indiqué comment le principe devrait avoir été intégré dans la législation générale et sectorielle sur la protection des données à caractère personnel (notamment les réseaux sociaux, l'internet des objets, les dispositifs RFID et les navigateurs). Nous avons aussi formulé des recommandations sur la manière d'encourager la mise en œuvre du principe dans les produits et services informatiques, après avoir admis que les PET n'avaient pas vraiment percé sur le marché et après avoir analysé les raisons potentielles de cet échec, notamment le manque de mesures d'incitation économiques et d'appui institutionnel, et la demande insuffisante de la part des utilisateurs.

22. Si le respect de la vie privée dès la conception a connu des avancées significatives au niveau juridique, technologique et conceptuel, il est encore loin d'avoir déployé tout son potentiel pour la protection des droits fondamentaux des personnes. Les sections suivantes du présent avis donnent une vue d'ensemble des développements pertinents et recommandent des efforts supplémentaires.

2. La protection des données dès la conception et par défaut dans le droit de l'Union européenne

2.1 L'article 25 du RGPD

23. L'article 25[33] du RGPD, intitulé «Protection des données dès la conception et protection des données par défaut» [34], dispose que le responsable du traitement[35] met en œuvre, tant lors de la phase de conception du traitement qu'au moment de son exécution, des mesures techniques et organisationnelles appropriées qui sont destinées à intégrer les garanties en matière de protection des données de façon effective afin de se conformer au règlement et de protéger les droits fondamentaux des personnes dont les données sont traitées. Ces mesures sont définies compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés de ces personnes. L'article indique que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement peuvent être traitées. L'article conclut que des mécanismes de certification approuvés peuvent servir à démontrer le respect des exigences énoncées[36].

24. L'exigence de protection des données dès la conception et par défaut de l'article 25 complète la responsabilité du responsable du traitement prévue à l'article 24, une disposition essentielle du RGPD. Cet article définit «qui fait quoi» pour protéger les personnes et leurs données à caractère personnel et indique qu'une approche fondée sur les risques est adoptée pour déterminer ce qu'il convient de faire à cet effet. Plus précisément, il dispose que le responsable du traitement «*met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément...*» à la loi. Ces mesures sont conçues «*compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques*».

25. Celles-ci comprennent les règles de l'article 32, qui exigent un cadre de gestion des risques pour la sécurité informatique et des mesures en vue de réduire les risques pour les personnes dont les données sont traitées en sécurisant ces données de manière adéquate. Il est utile de rappeler que, tandis que les mesures définies à l'article 32 sont simplement celles qui ciblent un des principes de protection des données de l'article 5[37], à savoir «l'intégrité et la confidentialité», l'article 24 fait référence à l'application de tous les principes de protection des données et au respect de l'ensemble du RGPD.

26. Dans le contexte de la responsabilité du responsable du traitement qui vise à s'assurer et à être en mesure de démontrer la conformité avec la loi, l'article 25 cible les mesures techniques et organisationnelles requises par l'article 24, en insistant sur certaines dimensions de leur processus de mise en œuvre déjà implicitement présentes à l'article 24 et en en ajoutant d'autres et les rendant toutes obligatoires. Nous décrivons ces dimensions dans les paragraphes suivants.

Les différentes dimensions de l'obligation de protection des données dès la conception

27. La première dimension est la reconnaissance du fait que le traitement des données à caractère personnel, partiellement ou entièrement pris en charge par des systèmes informatiques, devrait toujours être le **résultat d'un projet de conception**. L'article 25 impose d'envisager des garanties[38] tant lors de la phase de conception que lors de la phase opérationnelle, **ciblant ainsi l'ensemble du cycle de vie du projet**[39] et citant clairement la **protection des personnes et de leurs données à caractère personnel parmi les exigences de projet**.

28. La deuxième dimension est l'**approche fondée sur la gestion des risques** en vue de sélectionner et de mettre en œuvre des **mesures** pour une protection effective. Les **ressources à protéger sont les personnes** dont les données sont traitées et en particulier leurs libertés et droits fondamentaux[40]. À cet égard, il n'y a pas d'indication de mesures obligatoires[41]. Le législateur donne néanmoins des indications concernant ces facteurs (nature, portée, contexte et finalités du traitement) dont l'organisation doit tenir compte au moment de choisir les mesures appropriées.

29. Dans le même temps, l'organisation est chargée de choisir les garanties parmi celles disponibles (selon l'«état des connaissances») et examine leurs coûts parmi les éléments conduisant à la décision finale, pondérés par rapport aux risques pour les personnes. Ces deux facteurs, l'état des connaissances de la technologie disponible et les coûts de mise en œuvre des mesures, ne doivent pas être interprétés de manière à ce que les mesures choisies

ne réduisent pas suffisamment les risques existants et à ce que la protection ne soit pas suffisante.

30. La troisième dimension est la nécessité que **ces mesures soient appropriées et effectives**. Le caractère effectif est à mesurer par rapport à la finalité de ces mesures: s'assurer et être en mesure de démontrer la conformité avec le RGPD, mettre en œuvre les principes de protection des données et protéger les droits des personnes dont les données sont traitées. En particulier, l'article 25 dispose que ces mesures sont destinées «*à mettre en œuvre les principes relatifs à la protection des données [...] de façon effective*». Ces principes relatifs à la protection des données, énoncés à l'article 5, peuvent être considérés comme les **objectifs à atteindre**. Ils ont été retenus par le législateur comme fondement de la protection des personnes lors du traitement de leurs données et ils sont complétés dans le RGPD par des règles plus détaillées (c'est-à-dire les informations à fournir aux personnes et leurs droits en tant que «personnes concernées»[42], qui sont détaillés dans le principe de «transparence»; ou les obligations de sécurité de l'article 32) ou par d'autres instruments de responsabilité, tels que les devoirs de documentation de l'article 30, qui sont essentiels à ces principes. Cela signifie qu'appliquer ces principes/atteindre ces objectifs de façon effective, tel qu'expliqué plus en détail dans la législation par d'autres dispositions, garantirait la protection escomptée des données à caractère personnel.

31. La quatrième dimension est l'obligation d'**intégrer les garanties définies au traitement**. Le RGPD comprend des garanties visant à protéger les personnes dont les données sont traitées par des moyens qui sont «extérieurs» au traitement lui-même, tels que les avis de protection des données, par exemple. Cette dimension se concentre plutôt sur la nécessité de protéger les personnes en protégeant directement leurs données et la façon dont elles sont gérées.

32. L'ensemble des quatre dimensions sont d'importance égale et deviennent partie intégrante de l'obligation de responsabilité, et seront soumises au contrôle des autorités de contrôle de la protection des données compétentes, dans les cas appropriés.

L'obligation de protection des données par défaut

33. Suivant l'application du principe de protection des données dès la conception, l'organisation doit, par défaut, ne traiter que les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique définie conformément à la loi et communiquée aux personnes concernées en toute transparence. Si l'on peut faire valoir que cette obligation est déjà implicite dans les principes de «limitation des finalités» et de «minimisation des données»[43] dans les phases tant de conception que d'exécution[44], la règle explicite insiste néanmoins sur l'importance de prendre des mesures techniques pour répondre aux attentes des personnes dont les données sont traitées, de ne pas traiter leurs données à d'autres fins que ce que le produit ou le service est fondamentalement et strictement censé faire, désactivant ainsi par défaut toute autre utilisation, par exemple au moyen de paramètres de configuration[45].

34. Une partie de la valeur ajoutée de la disposition relative à la protection des données par défaut est aussi le développement du principe de minimisation des données et l'extension au principe de limitation de la conservation. L'article 25, paragraphe 2, explique comment l'obligation de ne traiter par défaut que les données à caractère personnel qui sont nécessaires «*s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité...*». L'article

établit alors une obligation précise en illustrant le principe général au moyen d'une utilisation particulière: les organisations mettent en place des mesures afin d'empêcher que les données à caractère personnel soient rendues publiques par défaut.

Le rôle des «sous-traitants» et les devoirs pertinents des responsables du traitement

35. Les prestataires de services en faveur d'une organisation qui traitent des données à caractère personnel pour le compte de ladite organisation sont considérés comme des «sous-traitants»[46] dans le RGPD. Il incombe à l'organisation/au responsable du traitement de choisir des contractants/des sous-traitants qui sont en mesure de les aider à respecter la loi[47], et donc aussi les obligations de protection des données dès la conception et par défaut.

36. Cela oblige indirectement les sous-traitants à concevoir et appliquer les procédés et les technologies de manière à permettre à l'organisation responsable de protéger les personnes et leurs données selon une approche fondée sur la protection des données dès la conception et par défaut.

L'article 25 et les développeurs de produits et de technologies

37. Une sérieuse limitation des obligations de l'article 25 est qu'elles s'appliquent uniquement pour imposer une obligation aux responsables du traitement et pas aux développeurs des produits et des technologies utilisés pour traiter les données à caractère personnel. L'obligation pour les fournisseurs de produits et de technologies ne figure pas dans les dispositions de fond du RGPD. Le 78ème considérant[48] prévoit cependant que «*[l]ors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données...*». L'application de l'article 25 nécessiterait donc que le fournisseur conçoive ses produits de manière à permettre au responsable du traitement de mettre en place toutes les mesures nécessaires pour protéger les personnes et leurs données, et de les configurer de manière à ce que par défaut, sans aucune intervention de l'utilisateur, aucune donnée à caractère personnel ne soit collectée, ou seulement celles qui sont strictement nécessaires pour permettre au produit de fonctionner comme il est censé le faire.

L'article 25 et les administrations publiques

38. L'article 25 s'applique à tous les types d'organisations faisant office de responsables du traitement, y compris les administrations publiques qui, étant donné leur rôle consistant à servir l'intérêt public, devraient donner l'exemple en protégeant les libertés et les droits fondamentaux des personnes. Le RGPD souligne le rôle de protection des données dès la conception et par défaut lorsque les administrations publiques doivent identifier leurs fournisseurs de produits et de services au 78ème considérant , selon lequel «*[l]es principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics*». Les administrations publiques sont appelées à se positionner à l'avant-garde et à appliquer ces principes de manière responsable, prêtes à démontrer leur mise en œuvre, si nécessaire, à l'autorité de contrôle compétente.

Analyse d'impact relative à la protection des données

39. L'article 35 du RGPD prévoit une analyse d'impact relative à la protection des données (AIPD) obligatoire lorsque le traitement est «*susceptible[s] d'engendrer un risque élevé pour les droits et libertés des personnes physiques...*». Cette obligation complète l'**approche fondée sur la gestion des risques obligatoire** de l'article 24 lorsque l'organisation estime que le niveau de risque pour les personnes dont les données sont traitées est élevé[49]. L'AIPD constitue un excellent outil de responsabilité et les organisations auraient intérêt à adopter aussi cette approche dans les cas où elle n'est pas obligatoire[50].

40. Dans ses lignes directrices sur l'AIPD[51], le WP29 indiquait qu'elle servait de garantie en matière de protection des données dès la conception, car elle devait «*être effectuée avant le traitement...*». Cette exigence est conforme aux principes de protection des données dès la conception et de protection des données par défaut[52]. La gestion des risques en matière de protection des données est au cœur de l'approche fondée sur le respect de la vie privée dès la conception et par défaut.

2.2 Le respect de la vie privée dès la conception et la protection des données dès la conception dans les règles sectorielles de l'Union

41. Outre le RGPD, il existe plusieurs dispositions dans le droit sectoriel de l'Union qui ont trait aux principes de respect de la vie privée dès la conception et par défaut.

La directive «vie privée et communications électroniques» et la directive RED

42. Les principes de respect de la vie privée dès la conception et par défaut n'apparaissent pas explicitement dans les dispositions de fond de la directive «vie privée et communications électroniques»[53]. Le 30ème considérant indique cependant que «*[l]es systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires...*». Il s'agit d'une recommandation aux fournisseurs de services **et de produits** de communication électronique publics afin qu'ils conçoivent ces services de manière à respecter le principe de minimisation des données.

43. Le 46ème considérant dispose que «*[l]a protection des données à caractère personnel et de la vie privée de l'utilisateur de services de communications électroniques accessibles au public devrait être indépendante de la configuration des différents éléments nécessaires à la fourniture du service...*» et rappelle donc la nécessité d'une protection globale. Il poursuit en énonçant qu'«*[i]l peut, par conséquent, être nécessaire d'adopter des mesures exigeant que les fabricants de certains types d'équipements utilisés pour les services de communications électroniques intègrent dans leurs produits des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés*» et fait explicitement référence aux mesures à adopter conformément à la directive 1999/5/CE[54] concernant les équipements hertziens et les équipements terminaux de télécommunications. La directive 2014/53/UE[55], qui abroge cette dernière, et remplace les règles pertinentes pour les équipements radioélectriques, prévoit explicitement en son article 3, paragraphe 3, point e), que certains équipements radioélectriques «*sont construits...*» de telle sorte qu'ils comportent «*des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés*». On peut observer, également dans cette obligation, une référence à la **phase d'ingénierie des produits**.

44. L'avis du CEPD[56] sur la proposition de la Commission de remplacer la directive «vie privée et communications électroniques»[57] par le nouveau règlement «vie privée et communications électroniques» est cohérent avec l'approche du 78ème considérant du RGPD et propose pour le secteur «*l'obligation, pour les fournisseurs de matériel et de logiciels, de mettre en œuvre des paramètres par défaut qui protègent les dispositifs des utilisateurs finaux contre tout accès non autorisé à des informations ou tout stockage d'informations dans leurs dispositifs*». Cette obligation concernerait **les fournisseurs de matériel et de logiciels pour tous types de services de communication**, y compris la messagerie instantanée, la voix sur IP, et les communications de données à caractère personnel parmi les «objets» sur l'internet des objets et les opérateurs de sites web. Cette disposition renforcerait considérablement le niveau de protection et donnerait à tous les fournisseurs de services de communication électronique une réelle possibilité de se conformer à la législation et non de rejeter toute allégation de protection insuffisante en pointant du doigt l'absence de fournisseurs adéquats. Cela constituerait aussi une référence en vue d'une possible extension d'une disposition analogue dans d'autres secteurs.

Règlement eIDAS

45. Le règlement eIDAS[58] constitue le cadre pour la fourniture de services d'identification et de confiance électronique sur le marché unique numérique de l'Union. Comme la fourniture de ces services nécessite le traitement de données à caractère personnel par le fournisseur de services, le règlement contient des références à la directive sur la protection des données. Outre le respect des principes de protection des données, le règlement fait aussi explicitement référence au respect de la vie privée dès la conception en tant que principe devant être soutenu par le cadre d'interopérabilité eIDAS. La mise en œuvre technique des services eIDAS devrait être guidée par un cadre d'interopérabilité commun qui applique le principe de respect de la vie privée dès la conception[59]. Il conviendrait cependant d'ajuster les mesures mises en œuvre au titre du règlement eIDAS afin de développer ce potentiel.

Systèmes intelligents de mesure et réseaux intelligents pour l'énergie et le gaz: un cas de coréglementation

46. Pour le secteur de l'énergie, et plus précisément pour l'introduction des systèmes intelligents de mesure dans l'Union, la validité du principe de protection des données dès la conception a été justifiée de manière plus détaillée. En 2012, la Commission a publié une recommandation[60] relative à la préparation de l'introduction des systèmes intelligents de mesure sur les marchés de l'électricité et du gaz afin de fournir aux États membres des directives sur la protection des données dès la conception et par défaut et sur l'application des principes de protection des données. La recommandation a établi que les États membres devraient adopter et appliquer un modèle d'analyse de l'impact sur la protection des données («modèle AIPD») et ensuite veiller à ce que les opérateurs du réseau et les opérateurs des systèmes intelligents de mesure prennent les mesures techniques et d'organisation adéquates pour garantir la protection des données à caractère personnel conformément au modèle AIPD. Le modèle a été préparé par l'industrie avec l'aide de la Commission et en coordination avec celle-ci, et il a été soumis par deux fois au WP29 pour avis. Il a été annexé à une recommandation de la Commission adoptée en octobre 2014[61].

47. Le 17ème considérant de la recommandation concernant le modèle AIPD explique: «*[u]n tel modèle devrait faciliter l'application du principe de la protection des données dès la conception en encourageant les responsables du traitement à réaliser une analyse d'impact sur la protection des données dès que possible, leur permettant ainsi d'anticiper les incidences potentielles sur les droits et libertés des personnes concernées et de mettre en*

œuvre des garanties strictes. Ces mesures devraient faire l'objet d'un suivi et d'un examen par le responsable du traitement des données tout au long du cycle de vie de l'application ou du système». Cette approche est conforme au **rôle central du processus de gestion des risques dans le cadre de la protection des données**, tel qu'indiqué au point 39, et à la nécessité de tenir compte des **exigences de respect de la vie privée lors des premières phases et tout au long du cycle de vie** d'un projet, tel que souligné au point 27.

48. La recommandation 2012/148/UE a aussi donné lieu à l'initiative visant à recenser les meilleures techniques disponibles[62] en matière de cybersécurité et de respect de la vie privée des systèmes intelligents de mesure sur la base de dix exigences fonctionnelles minimales. Par «meilleures techniques disponibles» (MTD) [63], on entend «*le stade de mise en œuvre le plus efficace et le plus avancé des activités et de leurs méthodes d'exploitation, indiquant la capacité concrète de techniques particulières à constituer, en principe, la base sur laquelle s'appuyer pour se conformer au cadre de l'Union régissant la protection des données. Elles servent à prévenir ou à limiter les risques d'atteinte à la vie privée, aux données à caractère personnel et à la sécurité»*.

49. Au sens de l'article 25 du RGPD, le catalogue des MTD correspond à une indication de l'état des connaissances pour les mesures techniques et organisationnelles, qui prend en considération l'efficacité des mesures, la maturité de la technique et les coûts de mise en œuvre. De plus, les MTD axées sur le respect de la vie privée peuvent aussi être considérées comme des PET.

50. Nous pensons que certains éléments des travaux entrepris dans le secteur des systèmes intelligents de mesure, et en particulier l'approche qui consiste à réaliser un inventaire des meilleures techniques disponibles en matière de respect de la vie privée, pourraient contribuer à opérationnaliser le respect de la vie privée dès la conception dans différents secteurs technologiques.

3. La dimension internationale du respect de la vie privée dès la conception

51. L'adoption des principes de respect de la vie privée et de protection des données dès la conception et par défaut n'est pas seulement un concept de l'Union européenne: une part significative de son développement a eu lieu de l'autre côté de l'Atlantique. Les sept principes fondamentaux[64], tels que relayés par les commissaires à la protection de la vie privée dans la déclaration de Jérusalem[65], et la recherche dans le domaine des PET et des efforts en vue de concevoir des systèmes et des procédés conformes aux exigences de respect de la vie privée, ont influencé les directives en la matière et la définition des bonnes pratiques et des normes émergentes partout dans le monde. Le respect de la vie privée dès la conception a récemment été proposé comme principe à intégrer à d'autres législations nationales[66].

52. Parmi les exemples de pays dans lesquels l'approche fondée sur le respect de la vie privée dès la conception et par défaut a été largement suggérée par les autorités compétentes figurent le Canada, l'Australie[67] et les États-Unis, souvent parallèlement à l'utilisation des analyses d'impact sur le respect de la vie privée, désignée comme «la» mesure méthodologique qui permet à l'approche globale d'être appliquée au cours des premières phases du projet et utilisée pour faire apparaître les exigences à imposer via l'évaluation des risques en matière de protection des données. L'approche a bénéficié du fait que la portée

de l'analyse d'impact sur le respect de la vie privée va souvent au-delà de la stricte protection des données à caractère personnel pour englober la notion pluridisciplinaire et contextuelle plus large de respect de la vie privée et même d'autres droits fondamentaux comme objectifs.

53. Un rapport de 2012[68] publié par la *Federal Trade Commission* (FTC) américaine proposait le respect de la vie privée dès la conception parmi les trois principaux concepts[69] d'un nouveau cadre qui «*intégrerait l'ensemble des principes des pratiques équitables en matière de traitement des informations, mis à jour pour le XXI^e siècle*»[70]. Le respect de la vie privée dès la conception «*doit être une chose à laquelle un ingénieur ou un développeur de sites pense instinctivement lorsqu'il écrit du code ou élabore un nouveau produit. Le respect de la vie privée doit être considéré comme une partie intégrante du processus d'innovation... cela aide à décharger les consommateurs du fardeau de la protection de la vie privée... Trop souvent, la protection de la vie privée repose sur la notion que les consommateurs peuvent lire et comprendre le jargon juridique des interminables politiques de protection de la vie privée. Le nouveau cadre de la FTC vise à s'éloigner de cette vision irréaliste de la protection de la vie privée*»[71].

54. Le cadre de la FTC est différent du RGPD par son champ d'application[72] et sa nature juridique[73], et quelques différences substantielles peuvent être trouvées dans l'interprétation juridique de certains des principes de respect de la vie privée qu'il vise à appliquer (par exemple, la licéité dans les principes de protection des données de l'article 5 du RGPD, y compris le test de nécessité stricte du traitement des données). Néanmoins, la définition du respect de la vie privée dès la conception de la FTC peut être considérée comme assez analogue (sur le plan méthodologique et même sur le fond, dans une large mesure) à ce qui se trouve dans le droit de l'Union dans toutes ses dimensions, telles que présentées dans la section 2.1, et elle est clairement formulée en vue de l'application pratique du principe.

55. Si le cadre de la FTC et d'autres initiatives y afférentes ont contribué au développement conceptuel du respect de la vie privée dès la conception et des moyens technologiques, les développements législatifs n'ont pas suivi, et ils n'ont donc pas eu l'impact profond et de grande envergure qu'ils auraient pu avoir avec l'engagement total du législateur.

56. Plus récemment, le *National Institute of Standards and Technology* (NIST), une agence du ministère américain du commerce, a publié un rapport interne comprenant une introduction aux notions d'ingénierie de la vie privée et de gestion des risques pour les systèmes fédéraux américains[74]. Il s'agit là d'une grande nouveauté dans le paysage des directives fournies par les gouvernements ou les autorités chargées de la protection des données, car le document comprend un modèle de risque pour la protection de la vie privée et une méthode en vue de mettre en œuvre les exigences en matière de respect de la vie privée dans le cadre de l'ingénierie des systèmes qui traitent les données à caractère personnel. Les documents du NIST sont considérés comme des normes pour les systèmes d'information fédéraux américains et doivent être respectés par les agences fédérales[75]. Le programme d'ingénierie de la vie privée du NIST se poursuit[76].

4. Concevoir et exécuter des procédures et des systèmes tout en protégeant les données à caractère personnel

4.1 Opérationnaliser le respect de la vie privée et la protection des données dès la conception et par défaut

57. La législation de l'Union en matière de protection des données et les autres cadres relatifs au respect de la vie privée, tels que les principes des pratiques équitables en matière de traitement des informations[77] ou les lignes directrices de l'OCDE[78], précisent généralement des objectifs à atteindre sans donner de directives quant à la manière d'y parvenir en pratique. L'application du principe de respect de la vie privée dès la conception peut aider à régler ce problème, car il se traduit en directives pratiques, afin de:

    1. définir une méthode en vue d'intégrer les exigences en matière de respect de la vie privée et de protection des données dans le cadre de projets visant à élaborer et à exécuter un procédé, une procédure ou un système qui traite des données à caractère personnel;

    2. mettre en évidence et mettre en œuvre les mesures techniques et organisationnelles adéquates à intégrer dans ces procédés, procédures et systèmes afin de protéger les personnes et leurs données. L'innovation technologique peut être un outil à l'appui de ces mesures;

    3. intégrer le soutien au respect de la vie privée dans le cadre de gestion et de gouvernance de l'organisation, en déterminant les tâches à effectuer et en définissant et en affectant les ressources et les responsabilités.

58. Il y a longtemps que des méthodes sont en place pour définir les exigences applicables aux processus opérationnels et aux systèmes informatiques[79]. En particulier, il existe une interprétation commune du mode de préparation des exigences pour les systèmes informatiques et de nombreuses bonnes pratiques ont été proposées et adoptées par les universités et l'industrie. Généralement, les exigences sont réparties en exigences fonctionnelles et non fonctionnelles. Les exigences fonctionnelles sont celles qui définissent le principal objectif commercial et la particularité du système à mettre au point. Les exigences non fonctionnelles[80] s'appliquent à tous les systèmes et concernent les aspects horizontaux, tels que les besoins en matière de sécurité et le respect des législations applicables. Le respect de la vie privée et la protection des données doivent être considérés dans le cadre des exigences non fonctionnelles[81].

59. Pour de nombreuses raisons, cependant, le respect de la vie privée est souvent oublié ou seulement considéré a posteriori lors de la conception des systèmes. Parmi ces raisons figurent la notion contextuelle et souvent liée à la culture qu'est le respect de la vie privée et la difficulté de traduire le respect de la vie privée en exigences réalisables. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié une vaste analyse de l'état des connaissances en matière d'ingénierie de la vie privée dès la conception en décembre 2014[82].

4.2 Ingénierie de la vie privée et de la protection des données

Déterminer les exigences en matière de protection des données et sélectionner les mesures adéquates pour répondre aux exigences

60. Le mode de fonctionnement de certaines méthodes actuelles d'ingénierie de la vie privée consiste à définir des objectifs de protection des données directement à partir des principes de protection des données ou à définir des objectifs intermédiaires opérationnels qui permettent d'atteindre les objectifs originaux. D'autres méthodes sont plus explicitement axées sur une approche de gestion des risques, et elles définissent le risque lié au non-respect des principes de protection des données et y remédient ou évaluent directement les conséquences négatives potentielles pour les personnes.

61. Dans la section 2.1, nous indiquons que le RGPD considère ces principes comme des objectifs à atteindre, qui servent de «moyens indirects» de protéger les libertés et droits fondamentaux des personnes, indépendamment du niveau de risque. Dans le même temps, il adopte une approche «de précaution» et définit des garanties à mettre en œuvre en toutes circonstances sous certaines conditions (par exemple, des mesures de sécurité, des avis de violation des données à caractère personnel, etc.). Ce qu'il manque pour effectivement parvenir à la protection escomptée des personnes et leur octroyer les droits de protection des données établis, en raison du contexte, de la nature des données, du type de traitement, etc., est alors laissé à l'approche de gestion des risques. Cette approche permet aux organisations de mettre en évidence de nouvelles mesures et contribue à détailler et à intégrer ce qui est déjà obligatoire sur la base du risque pour les personnes.

62. Les méthodes de développement logiciel ont inspiré l'approche qui consiste à utiliser un catalogue de modèles de conception spécifiques pour élaborer des solutions aux problèmes de protection de la vie privée connus. Cet aspect est développé plus avant au point 72.

Exemples de méthodes existantes

63. Sur la base de la définition des objectifs en matière de respect de la vie privée et de protection des données, il est devenu possible d'élaborer des méthodes de conception dans lesquelles les exigences correspondantes peuvent être pleinement intégrées. Cette section présente brièvement ces méthodes, et le lecteur intéressé peut consulter les documents sources pour se faire une meilleure idée de la question.

64. Les six objectifs de protection pour l'ingénierie de la vie privée[83] constituent un cadre en vue de définir les garanties applicables aux systèmes d'information qui traitent des données à caractère personnel. Outre la triade classique de la sécurité informatique[84] que sont la «confidentialité», l'«intégrité» et la «disponibilité», trois objectifs supplémentaires[85] ont été ajoutés: la «non-associativité», la «transparence» et la «possibilité d'intervention». Dans ce contexte, la sécurité informatique ne cible pas les risques pour l'organisation mais plutôt les risques pour les droits des personnes. Toute approche habituelle connue dans la littérature sur la gestion des risques liés à la sécurité informatique peut être utilisée si les ressources à protéger sont clairement définies (les personnes).

65. La «non-associativité» concerne la capacité des informations d'être associées les unes aux autres et à une personne. L'anonymat relève clairement de cet objectif. La «transparence» implique que «*tout le traitement des données pertinent en matière de protection de la vie privée, y compris le cadre juridique, technique et organisationnel, puisse être compris et reconstruit à tout moment. Il s'agit par ailleurs d'une condition préalable à la*

responsabilité. Les méthodes types pour parvenir à la transparence ou favoriser celle-ci comprennent l'établissement de registres et de rapports, la documentation du traitement des données ou les avis aux utilisateurs». La «possibilité d'intervention» permet «*l'application effective des changements et des mesures correctives*» et est pertinente pour permettre aux personnes de jouir de leurs droits et aux autorités compétentes d'intervenir.

66. Ces objectifs sont interdépendants et aident à montrer, entre autres, que les mesures de protection de la vie privée pourraient entrer en conflit les unes avec les autres. Par exemple, l'établissement de registres des données à caractère personnel au service de la possibilité d'intervention accroît le risque de manquer l'objectif de «non-associativité» en créant un risque d'utilisation abusive des opérations d'établissement de registres. Pour compléter le tableau, ces objectifs pourraient être utilisés en combinaison avec une méthode afin d'obtenir des garanties en vue de les atteindre, et des efforts existent afin de créer un catalogue de mesures possibles au service de ces objectifs.

67. Le NIST américain[86] a défini l'ingénierie de la vie privée comme une «*discipline spécialisée de l'ingénierie des systèmes qui vise à supprimer les conditions susceptibles de créer des problèmes pour les personnes avec des conséquences inacceptables qui découlent du système lorsqu'il traite des PII*[87]. Le NIST considère l'ingénierie de la vie privée comme un ensemble de composants multiples dont les éléments fondateurs sont le cadre de gestion des risques et les objectifs d'ingénierie. Ils établissent un modèle de risque pour le respect de la vie privée et trois objectifs pour les systèmes de protection de la vie privée en plus des objectifs de sécurité classiques que sont toujours la confidentialité, l'intégrité et la disponibilité: la **prédictibilité**, la **gérabilité** et la **dissociabilité**. Les trois objectifs contribuent à concevoir des systèmes qui répondent aux principes de respect de la vie privée[88], tel qu'illustré dans le document de référence[89].

68. La «prédictibilité» vise à «*permettre aux personnes, propriétaires et opérateurs, de faire des hypothèses fiables concernant les PII et leur traitement par un système d'information*». Cela signifie intégrer des mécanismes afin de garantir aux parties concernées, preuves à l'appui, que les mesures nécessaires pour protéger les personnes et leurs données sont en place et effectives. Par exemple, concevoir un mécanisme qui permette la gestion du consentement et apporter la preuve de ce qui a été sélectionné permettrait de remplir l'objectif de prédictibilité. La «gérabilité» signifie «*donner la capacité d'une gestion granulaire des PII, y compris leur modification, leur effacement et le divulgation sélective*», des éléments essentiels à une bonne gestion des données à caractère personnel. La «dissociabilité» permet «*le traitement des PII ou des événements sans association aux personnes ou aux dispositifs au-delà des exigences opérationnelles du système*». Cet objectif de protection de la vie privée est clairement axé sur la minimisation des données à caractère personnel et sur une possible anonymisation.

69. Dans la méthode d'ingénierie de la vie privée du NIST, la prédictibilité se distingue comme une sorte de méta-objectif qui sert de base pour assurer la mise en œuvre effective des mesures, ainsi que la transparence et la responsabilité des solutions proposées à l'égard des parties concernées (personnes, autorités compétentes, société, etc.). Un exemple pratique de la manière de mettre cet objectif en œuvre consiste en des mesures telles que l'utilisation de la cryptographie pour apporter une preuve mathématique des faits.

70. Un autre exemple de méthode d'ingénierie de la vie privée, qui dans ce cas particulier insiste sur la dimension d'analyse des risques, est l'approche LINDDUN[90] élaborée à l'université KU Leuven. Elle implique de:

- créer un diagramme de flux de données sur la base de la description du système de haut niveau;

- cartographier les catégories de menaces pour le respect de la vie privée suivantes: associabilité, identifiabilité, non-répudiation, détectabilité, divulgation d'informations, ignorance, non-conformité, telles qu'identifiées par les méthodes, sur les éléments du diagramme;

- repérer les éléments des diagrammes du flux de données où ces menaces pourraient constituer un risque et procéder à une analyse des risques à l'aide de l'arborescence des menaces pour la vie privée fournie par la méthode. Les menaces sont ensuite classées par ordre de priorité sur la base d'une évaluation. LINDDUN n'indique pas comment effectuer l'évaluation des risques. Cela signifie que les critères permettant de classer les risques par ordre de priorité sont laissés à l'appréciation de l'organisation qui applique la méthode, ce qui lui donne une certaine flexibilité;

- sur la base des priorités établies, des stratégies de réduction des risques et des solutions spécifiques sont choisies en fonction de leur pertinence pour les menaces particulières. La méthode propose une taxonomie de stratégies de réduction des risques qui peut être intégrée et détaillée selon les besoins. Il y a ensuite lieu de sélectionner des PET afin d'appliquer efficacement ces stratégies.

71. La gestion des risques est au cœur de la méthode LINDDUN, complétée par un catalogue de stratégies de haut niveau neutres sur le plan technologique, à mettre en œuvre au moyen de mesures d'organisation et de solutions technologiques de pointe.

72. Une autre approche de la détermination des mesures de mise en œuvre des exigences en matière de respect de la vie privée consiste à établir des «modèles» afin de concevoir des solutions informatiques pour satisfaire aux exigences en matière de respect de la vie privée. Des «modèles de conception», tels que définis dans les méthodes de développement logiciel pour résoudre des problèmes récurrents[91], sont proposés en guise d'éléments constitutifs pour mettre en œuvre les mesures de protection de la vie privée dans les systèmes[92] dans le contexte d'une stratégie (et d'une tactique). Ces modèles sont ensuite mis en pratique dans les éléments constitutifs logiciels et soutenus par les PET. Des «stratégies de conception» pour les problèmes relatifs au respect de la vie privée courants sont mises en évidence[93] afin de décrire «*une approche fondamentale pour atteindre un objectif de conception donné*». Pour une meilleure modélisation, elles peuvent être divisées en couches d'abstraction supplémentaires plus spécifiques (par exemple, ce que l'on appelle des «tactiques», «*des approches du respect de la vie privée dès la conception qui contribuent à une stratégie globale*»).

Couvrir l'ensemble du cycle de vie des services et des produits, gouvernance et gestion au sein de l'organisation

73. Si certaines méthodes d'ingénierie de la vie privée sont essentiellement axées sur la phase des exigences ou sur les mesures à mettre en œuvre, l'ingénierie de la vie privée doit prendre en considération l'ensemble du cycle de vie d'un service ou d'un produit, de la planification initiale à l'élimination du service/du produit. Des structures et des procédures adéquates de gouvernance et de gestion au sein de l'organisation sont alors nécessaires pour permettre l'approche globale.

74. Un exemple de méthode axée sur l'ensemble du cycle de vie du projet est celui publié par le projet de recherche PRIPARE[94] qui propose des actions et des produits livrables complets en matière de respect de la vie privée à travers huit phases de projet, des considérations relatives à l'environnement et l'infrastructure de l'organisation, au démantèlement du système. D'autres directives utiles qui viennent d'être publiées sont disponibles dans une publication en ligne de l'autorité norvégienne chargée de la protection des données[95].

75. Le respect effectif de la vie privée dès la conception et par défaut signifie, par essence, que la protection des droits fondamentaux des personnes devient une des missions de l'organisation et qu'en conséquence, elle doit se refléter dans sa structure de gouvernance et de gestion, avec une répartition adéquate des tâches et responsabilités en matière de respect de la vie privée, de façon responsable. La principale responsabilité des exigences en matière de respect de la vie privée incombe à la direction; la mise en œuvre peut être déléguée aux services responsables de la conception et de l'exécution des systèmes pertinents. Les services informatiques et technologiques aident les propriétaires d'entreprises sur la base de leurs instructions et des bonnes pratiques en matière de respect de la vie privée dès la conception.

76. Le rôle des délégués au respect de la vie privée et à la protection des données est central et leur participation est cruciale dans une approche axée sur le respect de la vie privée dès la conception. Ils doivent faire partie du processus dès les premières phases, lorsque les organisations planifient les systèmes de traitement de données à caractère personnel, afin de pouvoir aider les directeurs, les propriétaires d'entreprises et les services informatiques et technologiques selon les besoins. Leurs compétences doivent correspondre à ces besoins.

77. Le CEPD a publié des lignes directrices pour la gouvernance informatique et la gestion informatique[96] afin d'aider les institutions de l'Union à tenir compte des exigences en matière de respect de la vie privée et de protection des données dans le développement et l'exécution des systèmes d'information, et la manière dont la gouvernance informatique d'une organisation peut être établie conformément au principe de responsabilité. Ces lignes directrices reposent sur les principes généralement applicables, même si elles sont ciblées sur les parties intéressant spécifiquement le CEPD.

Efforts de normalisation

78. Des efforts de normalisation sont en cours afin d'intégrer les exigences en matière de respect de la vie privée dans la conception des systèmes au sein de différentes organisations de normalisation et dans le cadre de différentes initiatives[97]. Ils prennent souvent les approches existantes de la gestion des risques pour la sécurité informatique comme modèles et les étendent et les modifient pour couvrir la gestion des risques pour la vie privée. Par exemple, l'ISO a publié des normes relatives à un cadre de respect de la vie privée (ISO/IEC 29100) et à une architecture de respect de la vie privée (ISO/IEC 29101) concernant les PII dans un environnement de technologies de l'information et de la communication. Leur travail inclut l'extension des normes ISO/IEC 27001 et 27002 sur la gestion de la sécurité de l'information à la gestion de la vie privée. Un autre exemple est la norme RFC 6973[98] publiée par l'IETF sur «les considérations relatives au respect de la vie privée pour les protocoles internet», qui vise à inclure les exigences en matière de respect de la vie privée dans les protocoles internet.

79. La normalisation du respect de la vie privée devrait aussi prendre de l'ampleur eu égard au rôle que les certifications pourraient jouer afin de démontrer la conformité avec le RGPD.

Les mécanismes de certification pourraient être utilisés pour démontrer la conformité avec le principe de protection des données dès la conception et par défaut[99].

80. En 2015, la Commission européenne a demandé aux[100] organisations européennes de normalisation[101], qui ont un accord de coopération[102] avec la Commission, de travailler sur «une approche du respect de la vie privée et de la protection des données dès la conception» et sur un «cadre de gestion du respect de la vie privée et de la protection des données» pour le secteur de la sécurité. En 2017, après l'adoption du RGPD, les organisations européennes de normalisation ont envisagé la possibilité d'un plan de travail plus vaste et plus articulé qui intègre le respect de la vie privée, la protection des données et la cybersécurité. Il inclut: une norme sur «la protection des données et le respect de la vie privée dès la conception et par défaut» qui prévoit des «*obligations pour les fabricants et/ou les fournisseurs de services*» de mettre en œuvre le principe «*...applicable à tous les secteurs professionnels, y compris le secteur de la sécurité*», ainsi que des rapports techniques sur les mises en œuvre particulières du principe[103], les initiatives sur la cybersécurité et le respect de la vie privée et la protection des données à l'appui de l'élaboration des politiques récente et en cours au niveau de l'Union[104]. Cette activité de normalisation peut servir de base au secteur et à toutes les parties concernées pour établir l'état des connaissances dans le domaine du respect de la vie privée dès la conception. C'est la raison pour laquelle il est crucial que son résultat soit conforme aux dispositions juridiques pertinentes afin qu'il contribue effectivement à garantir la bonne mise en œuvre du respect de la vie privée dès la conception[105].

4.3 Technologies renforçant la protection de la vie privée (PET)

81. Les technologies renforçant la protection de la vie privée, autrement dit les solutions technologiques particulières à certains problèmes relatifs au respect de la vie privée dans la conception des systèmes, ont précédé l'idée d'une approche d'ingénierie de la vie privée globale[106], et elles peuvent aujourd'hui être considérées comme des éléments constitutifs fondamentaux de qualité pour l'ingénierie de la vie privée. Une liste exhaustive des PET existantes dépasse le propos du présent document, mais nous pouvons renvoyer le lecteur vers des exemples pertinents, tels qu'une stratégie de conception appelée «accréditation sur la base d'attributs», ou «accréditation anonyme», qui donne aux personnes la possibilité de s'authentifier auprès d'un service sans divulguer leur identité complète, en ne divulguant de façon sélective, en toute sécurité, que les attributs qui sont strictement nécessaires dans ce contexte. Cela est possible grâce à des concepts cryptographiques spécifiques tels que les preuves à divulgation nulle de connaissance. À titre d'exemple, si un service est destiné aux adultes, les personnes doivent simplement divulguer de manière sûre et fiable qu'elles ont plus de 18 ans, sans divulguer au service leur âge et leurs autres attributs d'identité[107].

82. De nombreux développeurs, issus d'environnements commerciaux et non commerciaux, ont investi dans la mise à disposition d'outils et de services dotés de fonctionnalités renforçant la protection de la vie privée. Les domaines concernés sont les services de messagerie, qui proposent souvent un chiffrement complet de bout en bout et l'absence de serveurs centraux qui traitent ou conservent le contenu des communications ou les métadonnées. Leur popularité accrue, en particulier depuis 2013, a sans aucun doute contribué à l'adoption de normes de chiffrement analogues pour les outils de communication plus couramment utilisés. Un certain succès a aussi été observé dans des domaines tels que les moteurs de recherche. Des navigateurs populaires ont ajouté davantage de contrôles de la confidentialité, tels que des fonctionnalités *Do Not Track* (DNT)[108] et un contrôle des utilisateurs sur les fonctionnalités de suivi, et ils peuvent être améliorés grâce à de nombreux

modules complémentaires qui suppriment les tentatives de suivi ou limitent le profilage. Les infrastructures de communications, tels que les *mix networks*[109], ainsi que les systèmes d'exploitation complets, ont aussi été développés jusqu'à leur pleine utilisabilité. Les éléments du RGPD axés sur la technologie suscitent de nouvelles idées commerciales fondées sur la technologie, promouvant par exemple un mécanisme de consentement valable et la portabilité des données. Tous ces développements démontrent que la compétence technologique pour la mise en œuvre du respect de la vie privée dès la conception est disponible.

83. Les PET se sont développées au fil des ans, et des efforts ont été réalisés pour dresser un inventaire des technologies disponibles, comme le rapport de l'ENISA sur l'état des connaissances en matière de techniques de protection de la vie privée dans sa publication sur le respect de la vie privée dès la conception de décembre 2014[110]. Ce rapport a été complété par un autre rapport sur le respect de la vie privée dès la conception pour l'analyse des mégadonnées[111].

84. Ces dernières années, l'ENISA a continué d'analyser l'état des connaissances et a mis à disposition une méthode d'analyse de l'état de préparation et de la maturité des PET[112], une approche en vue d'évaluer les outils de protection de la vie privée en ligne et mobiles, ainsi que des recommandations à l'attention de toutes les parties concernées, des développeurs aux autorités compétentes, en vue de créer et de tenir un répertoire de maturité des PET adéquat et réunissant les conditions requises. Dans la dernière édition du rapport, l'ENISA recommande que les autorités compétentes et les organismes de réglementation encouragent «*le recours à l'outil en tant que répertoire en ligne des évaluations des PET, dans le contexte de l'application pratique du principe de protection des données dès la conception*», que la communauté des chercheurs le soutienne en «*participant activement en tant qu'évaluateurs et utilisateurs de la plate-forme, ainsi qu'en encourageant son utilisation*», et que la communauté des chercheurs, la Commission, les institutions de l'Union dans le domaine de la sécurité et du respect de la vie privée entreprennent d'améliorer la plate-forme.

85. Le CEPD continuera de s'appuyer sur les initiatives en cours de l'ENISA à travers ses propres futures actions afin de favoriser l'ingénierie de la vie privée. Le fait de disposer d'un outil d'évaluation fonctionnel, à jour et fondé sur la qualité peut aider à contrôler et à comparer le niveau de mise en œuvre du respect de la vie privée dès la conception et par défaut en permettant d'être au fait de l'état des connaissances en matière de PET.

86. Dans ses observations formelles[113] sur le paquet relatif à la cybersécurité de la Commission, le CEPD a souligné que l'ENISA était actuellement la seule institution au niveau de l'Union qui était dotée des compétences et des ressources nécessaires pour entreprendre des activités de recherche et de conseil spécialisées dans le domaine du respect de la vie privée et de la protection des données dès la conception et par défaut et sur les technologies renforçant la protection de la vie privée. Nous réitérons notre recommandation visant à maintenir et à améliorer cette fonction, sinon avec l'ENISA, avec une autre institution telle que le CEPD.

5. La technologie au service des êtres humains: tirer parti du respect de la vie privée dès la conception et par défaut

5.1 Faire avancer l'état des connaissances et le recours aux solutions renforçant la protection de la vie privée

La situation actuelle

87. L'analyse que nous avons réalisée en 2010 dans notre «avis sur la promotion de la confiance dans la société d'information par des mesures d'encouragement de la protection des données et de la vie privée» reste en grande partie valable aujourd'hui. Le recours aux produits et services commerciaux qui appliquent pleinement le concept du respect de la vie privée dès la conception et par défaut est limité. Par ailleurs, les révélations d'activités de surveillance d'État ont sensibilisé le public aux dangers de la collecte omniprésente et massive de données à caractère personnel à des fins de profilage. L'arrivée du RGPD a renforcé la sensibilité du public et a incité les entreprises à réorienter leur attention et leurs ressources sur le respect de la vie privée et la protection des données. Cette tendance devrait se poursuivre alors que le RGPD entre pleinement en vigueur et que des actions de mise en œuvre sont entreprises. L'attention politique actuelle pour le suivi commercial à des fins de profilage et de ciblage pourrait accroître la demande de services et de produits largement accessibles qui contribuent au respect de la vie privée dès la conception.

88. Les PET ont apporté leur contribution dans l'offre commerciale traditionnelle, notamment une plus grande adoption de la cryptographie pour la sécurité des données à caractère personnel (par exemple, la messagerie mobile avec chiffrement de bout en bout), l'utilisation du *Do Not Track*[114] et ses paramètres de non-suivi par défaut (même si ceux-ci ne sont pas souvent respectés et sont interprétés de différentes manières par les fournisseurs de services) ou l'application d'algorithmes de confidentialité différentielle[115] lors de la collecte de statistiques d'utilisation auprès des clients. Les moteurs de recherche respectueux de la vie privée semblent fonctionner de manière durable. D'autres services sont encore des offres de niche peu utilisées. La famille des produits et des services connue sous le nom de systèmes de gestion des informations personnelles (PIMS) offre aux utilisateurs la possibilité d'avoir davantage de contrôle sur leurs données en englobant des PET et une nouvelle structure de gouvernance des données, tirant souvent parti des nouveaux modèles d'affaires. Le CEPD a joint une évaluation de la situation et des recommandations en vue de mesures stratégiques à son avis sur les systèmes de gestion des informations personnelles [116].

89. Les universités et l'industrie, avec l'appui des associations de la société civile et de certaines autorités chargées du respect de la vie privée et de la protection des données, ont mené des recherches pertinentes dans des domaines tels que la science des données, la cryptographie, la physique quantique, l'intelligence artificielle et l'apprentissage automatique, ainsi que les sciences humaines. Les associations du domaine de l'ingénierie et de l'internet ont commencé à consacrer des ressources en bonne et due forme et à donner de la visibilité à l'ingénierie de la vie privée[117]. L'Union européenne a cofinancé de nombreux projets par l'intermédiaire des programmes-cadres pour la recherche et le développement technologique et d'autres initiatives stratégiques. C'est appréciable et encourageant, mais pas suffisant.

La voie à suivre

90. Il est essentiel de poursuivre les recherches tout en veillant à ce que les technologies de protection de la vie privée puissent atteindre un bon niveau de maturité et être introduites sur le marché sous la forme de technologies, produits et services abordables.

91. L'Union doit intégrer à ses priorités **des politiques qui encouragent les technologies et les stratégies renforçant la protection de la vie privée**. La commission LIBE du Parlement européen[118] débat actuellement sur son avis concernant le paquet de la Commission sur la cybersécurité. Elle a tenu compte de l'appel du CEPD à ne pas abandonner le soutien de l'Union en faveur de la recherche et de ses conseils stratégiques sur les PET, et elle envisage de modifier la proposition commune relative au règlement ENISA révisé en conséquence. Nous encourageons fortement le législateur européen à garantir un soutien continu aux PET en répartissant clairement les tâches et en allouant des ressources suffisantes à une entité adéquate.

92. **Une stratégie commune sur le respect de la vie privée dès la conception et les PET peut être un formidable levier en vue d'entamer un dialogue constructif aussi au niveau international.** Ces dernières années, le CEPD a lancé l'initiative IPEN[119] afin de combler l'écart entre les exigences juridiques et l'ingénierie de la vie privée en mettant en relation et en soulignant les initiatives d'ingénierie de la vie privée existantes et en encourageant des solutions de protection de la vie privée pour le public au moyen d'actions coordonnées. Si nous nous sommes jusqu'ici plus particulièrement intéressés aux acteurs de l'Union, nous avons organisé en novembre 2017 un atelier[120] conjointement avec le Future of Privacy Forum, l'ULD[121], la Carnegie Mellon University et la KU Leuven, lors duquel nous avons discuté de l'état des connaissances et des défis en matière d'ingénierie de la vie privée, plus particulièrement dans l'Union européenne et aux États-Unis. Les partenaires universitaires ont décidé de poursuivre les recherches sur les sujets mis en évidence lors de l'atelier et de combler les lacunes existantes dans les technologies de protection de la vie privée disponibles et abordables dans la coopération transatlantique[122]. Les premières publications universitaires pourraient être disponibles prochainement.

93. **Les administrations publiques devraient montrer l'exemple** en appliquant pleinement le principe de respect de la vie privée dès la conception et par défaut. Nous croyons fermement qu'il s'agit bel et bien de la voie à suivre, qui stimulerait indirectement une offre adéquate de la part des fournisseurs. Les conclusions de la déclaration de Tallinn sur les services publics numériques d'octobre 2017[123] indiquent que «*le développement des services publics numériques doit respecter, encourager et renforcer les libertés fondamentales des personnes, telles que la liberté d'expression, le respect de la vie privée et le droit à la protection des données à caractère personnel, et respecter les législations de l'Union en la matière, en particulier le règlement général sur la protection des données. [...] Nous veillerons à ce que les besoins en matière de sécurité de l'information et de respect de la vie privée soient pris en considération au moment de concevoir des solutions de technologies de l'information et des communications (TIC) pour les services publics et les administrations publiques, suivant une approche fondée sur les risques et à l'aide de solutions de pointe... Nous appelons la Commission à travailler conjointement avec nos pays afin d'élaborer des propositions quant à la manière d'utiliser davantage le financement de la recherche et du développement de l'Union pour développer des outils et des technologies de cybersécurité et de protection de la vie privée et les déployer dans l'administration publique – en 2018*». Le CEPD soutient cet appel et contribuera à cet objectif stratégique au moyen d'initiatives spécifiques en sa qualité de conseiller et de

superviseur pour les institutions de l'Union, dans le cadre desquelles des projets pilotes pourraient être pionniers pour des solutions viables. Nous invitons la Commission à utiliser ses programmes de financement, tels que ceux pour la recherche et le développement, les Fonds structurels et la coopération administrative, comme ISA[2], et à coordonner les initiatives stratégiques afin de développer le rôle du secteur public en tant que moteur de l'avancement de l'état des connaissances et du marché.

94. Un système de mesures d'incitation politiques et économiques (ces dernières en particulier pour les PME) devrait être coordonné au niveau de l'Union et au niveau national afin d'abaisser le seuil d'un «état des connaissances» économiquement viable dans l'intérêt des personnes et de la société au sens large. C'est particulièrement important dans le paysage actuel du commerce en ligne, axé sur les données, dans lequel les oligopoles actuels représentent un obstacle qui empêche les start-ups et les PME de planifier des investissements valables dans les PET[124].

95. Au moment de choisir des mesures techniques et organisationnelles pour la protection des données, ou d'évaluer les mesures prises par une organisation, le facteur financier joue un rôle. Les avantages que les organisations retirent de leurs investissements sont mis en balance avec les coûts. La protection des données à caractère personnel ne permet pas seulement de réduire leurs risques en matière de responsabilités, de dommages et de sanctions. Dans une société de plus en plus attentive à la manière dont l'utilisation des données peut avoir une incidence négative sur la vie des personnes et informée à cet égard[125], **un attachement convaincant et soutenu au respect de la vie privée dès la conception devrait être considéré comme un avantage concurrentiel**. Le rapport *Global Human Capital Trend* de 2018 de Deloitte[126] témoigne d'une nécessaire réorientation des entreprises vers l'«entreprise sociale», où le fait d'entretenir des relations positives avec différentes parties concernées, notamment les organismes de réglementation et les communautés «*est crucial pour maintenir la réputation d'une organisation... et pour cultiver la loyauté chez les clients*», et ainsi «*influencer sa réussite ou son échec par la suite*». La protection des droits et des intérêts des personnes à travers le respect de la vie privée dès la conception et par défaut peut grandement contribuer à cette clé du succès.

96. Nous **réitérons en particulier l'appel lancé aux entreprises afin qu'elles utilisent leurs ressources, leurs capacités et leur créativité pour inventer de nouveaux services et modèles d'entreprise qui accordent une place centrale aux personnes, maîtresses de leurs données**[127]**.** Comme nous l'avons déclaré sur le blogue de notre site web en commentant la procédure législative en cours concernant le règlement «vie privée et communications électroniques»[128], en référence aux pratiques de publicité comportementale complexes et à la technologie sous-jacente: «*le facteur qui limite le contrôle effectif par l'utilisateur n'est pas la technologie. Lorsque les intérêts des entreprises sont en jeu, nous observons des efforts colossaux et des réalisations incroyables en matière de développement des technologies*». Cette transition est essentielle pour concrétiser pleinement la mise en œuvre du respect de la vie privée et de la protection des données dès la conception.

5.2 Le respect de la vie privée dès la conception, un jalon pour le développement technologique axé sur les valeurs

97. Un nombre croissant d'acteurs et d'organisations ont lancé des initiatives visant à renforcer un élément de responsabilité sociale et éthique dans le développement et l'introduction des

technologies. Si le respect de la vie privée joue un rôle central dans ces initiatives, il est souvent accompagné d'autres droits fondamentaux et objectifs sociaux.

98. Tel qu'observé lors de la conférence CPDP 2018[129], il existe un sentiment très répandu, partagé par l'inventeur du web[130] et les initiés du secteur[131], selon lequel nous pourrions avoir perdu le contrôle de la technologie au service de l'humanité en tant que société et que l'essentiel de la technologie est plutôt déterminé par les intérêts commerciaux de quelques entreprises. Ce n'est pas simplement le respect de la législation en vigueur qui est en jeu, mais plutôt la dignité humaine[132] et nos libertés fondamentales de base, y compris le fondement de nos sociétés démocratiques. Les modèles d'affaires les plus répandus tirent parti de l'utilisation de nos données à caractère personnel et de la construction de représentations numériques qui nous réduisent nous-mêmes et nos personnalités à des objets d'influence et de manipulation. Cela peut avoir de lourdes conséquences sur nos vies, même lorsque nous n'interagissons pas en ligne, et changer la façon dont nous sommes perçus par les autres, changer la façon dont nous percevons les autres et le monde qui nous entoure, et avoir une incidence sur nos droits et nos libertés.

99. En 2015, le CEPD a publié un avis[133] sur la nécessité de compléter l'approche réglementaire par une éthique numérique, en vue d'encourager la conception et l'utilisation de nouvelles technologies à la lumière des valeurs humaines communes. Le groupe consultatif sur l'éthique[134] qui a été créé vient juste de conclure son mandat de deux ans et de publier un rapport final[135], qui analyse les principales difficultés en matière d'éthique numérique et indique les principaux caps et risques pour l'avenir: la confirmation de l'idée que la dignité humaine doit demeurer inviolable à l'ère numérique; que les personnes et leurs données sont deux notions inséparables; que la prise de décision fondée sur le profilage automatisé des mégadonnées peut être incompatible avec des sociétés démocratiques et créer une discrimination; que la marchandisation des données risque de donner lieu à un recentrage de la valeur des personnes vers les données à caractère personnel.

100. Notre appel à des fondements éthiques dans la technologie est partagé par d'autres parties concernées, notamment les acteurs technologiques, en particulier en ce qui concerne la croissance attendue des applications de l'intelligence artificielle et de la manière dont cela peut affecter nos vies dans de nombreux domaines. En avril 2016, l'*Institute of Electrical and Electronics Engineers* (IEEE) a lancé une initiative mondiale sur l'éthique et les systèmes autonomes et intelligents[136], un ambitieux projet d'orientation vers «*la mise en œuvre éthique des technologies intelligentes*». L'initiative a pour objectif d'«*intégrer les aspects éthiques du bien-être humain susceptibles de ne pas être automatiquement pris en considération dans la conception et la fabrication actuelles des technologies A/IS, et de redéfinir la notion de succès afin que le progrès humain puisse intégrer l'établissement des valeurs éthiques individuelles, communautaires et sociétales comme priorités de façon intentionnelle*». Un rapport reprenant les contributions de centaines de participants provenant du monde entier vise à faire avancer le débat public sur le sujet. Par ailleurs, des groupes de travail ont été créés afin de concevoir des normes pour intégrer les considérations éthiques dans certains contextes bien précis, y compris la protection de la vie privée et le traitement des données à caractère personnel par des systèmes autonomes prenant des décisions sans intervention humaine[137].

101. En 1989 déjà, l'IETF publiait un document[138] qui définissait toute perturbation dans l'utilisation prévue de l'internet comme éthiquement inacceptable, y compris le respect de la vie privée des utilisateurs. En octobre 2017, l'IETF a donné des directives détaillées sur

un protocole des droits de l'homme[139], considérées comme «... *le premier jalon d'un effort de recherche à plus long terme... L'internet n'est pas neutre sur le plan des valeurs... Ce document vise à 1) montrer la relation entre les protocoles et les droits de l'homme, 2) proposer des lignes directrices possibles pour protéger l'internet en tant qu'environnement propice aux droits de l'homme dans le futur développement des protocoles, d'une manière analogue au travail réalisé pour les considérations relatives au respect de la vie privée [RFC6973], et 3) sensibiliser la communauté des droits de l'homme et la communauté technique à l'importance du fonctionnement technique de l'internet et à son incidence sur les droits de l'homme*».

102. Les initiatives à l'appui du droit au respect de la vie privée peuvent servir de balises pour intégrer les principes éthiques dans la conception de l'internet et de la société axée sur la technologie pour l'ensemble des droits de l'homme. Le CEPD considère l'enthousiasme pour la mise en œuvre effective des principes de respect de la vie privée dès la conception et par défaut comme une occasion sans précédent de stimuler le respect pour l'éthique dans la technologie. Toutes les parties concernées ont une responsabilité importante; en particulier, les entreprises qui fondent leurs activités sur l'utilisation des données à caractère personnel et les autorités publiques sont appelées à façonner leurs opérations pour servir l'intérêt commun.

6. Recommandations et engagements

103. Nous voulons encourager un débat mature et pragmatique entre les parties concernées (responsables politiques, organismes de réglementation, industrie, universités et société civile) afin de parvenir à des décisions claires et réalistes pour concevoir une technologie au service des êtres humains. Dans le même temps, nous confirmons l'attachement du CEPD à une mise en œuvre effective du RGPD et en particulier du principe de protection des données dès la conception et par défaut. Dans ce contexte, le CEPD invite toutes les parties concernées à multiplier leurs efforts.

104. Le CEPD appelle le Parlement européen, le Conseil et la Commission européenne:

- à garantir une solide protection de la vie privée, y compris le respect de la vie privée dès la conception, dans le cadre du processus législatif en cours concernant le **règlement «vie privée et communications électroniques»**; il s'agit à la fois de favoriser le développement du marché des produits et services respectueux de la vie privée dans les communications et de créer de nouvelles possibilités de marché pour les entreprises européennes dont le respect de la vie privée est inscrit dans l'ADN;

- à encourager le respect de la vie privée au moment d'adapter ou de créer des cadres juridiques qui influencent la conception de la technologie, en multipliant les mesures d'incitation et en justifiant les obligations, y compris les règles de responsabilité adéquates, afin d'intégrer le respect de la vie privée dès la conception dans les produits et les services, par exemple dans le domaine des transports, de l'énergie, de la finance, des villes intelligentes et de l'internet des objets;

- à encourager la mise en place et l'adoption d'approches de protection de la vie privée dès la conception et de technologies renforçant la protection de la vie privée dans l'Union et au niveau des États membres au moyen de mesures de mise en œuvre appropriées et d'initiatives stratégiques;

- à garantir la disponibilité continue de compétences et de ressources pour la recherche et l'analyse sur l'ingénierie de la vie privée et les PET au niveau de l'Union, soit en maintenant la capacité et les missions actuelles de l'ENISA, soit en affectant des ressources suffisantes à d'autres entités;

- à favoriser l'élaboration de nouvelles pratiques et de nouveaux modèles d'entreprise au moyen des instruments de recherche et de développement technologique de l'Union, et plus particulièrement les pratiques et modèles émergents tels que l'intelligence artificielle, l'apprentissage automatique et la *blockchain*;

- à soutenir les initiatives stratégiques afin que les institutions de l'Union et les administrations publiques nationales montrent l'exemple et intègrent les exigences adéquates en matière de respect de la vie privée dès la conception dans les marchés publics, à l'aide de politiques de coopération des administrations; et

- à favoriser la mise en place d'un inventaire et d'un observatoire de l'«état des connaissances» de l'ingénierie de la vie privée et des PET et de leur avancement, et à sensibiliser les citoyens et les acteurs économiques et politiques à cet égard.

105. Le CEPD continuera aussi à encourager le respect de la vie privée dès la conception, le cas échéant en coopération avec d'autres autorités chargées de la protection des données au sein de l'EDPB:

- en soutenant l'application coordonnée et effective de l'article 25 du RGPD et des dispositions y afférentes, grâce à des actions de sensibilisation et autres actions de soutien, et

- en donnant des directives aux responsables du traitement des données concernant la bonne application du principe défini dans la base juridique.

106. Nous pensons qu'il est essentiel de coordonner et de joindre, dans la mesure du possible, les capacités technologiques des différentes autorités chargées de la protection des données afin de favoriser, de définir et d'évaluer un «état des connaissances» ambitieux pour la protection des données dès la conception et par défaut. Le CEPD invite ses collègues à travailler ensemble en ce sens dans le contexte de l'EDPB, ainsi que du groupe de travail international sur la protection des données dans les télécommunications [140] (IWGDPT, «groupe de Berlin»).

107. Le CEPD soutiendra directement les initiatives et les projets pilotes destinés à faire progresser l'ingénierie de la vie privée et les PET, en tirant parti des initiatives existantes et en encourageant une plus grande coordination au niveau de l'Union et la coopération au niveau international (par exemple transatlantique). Le réseau IPEN sera particulièrement pertinent à cet égard.

108. Avec les autorités chargées de la protection des données d'Autriche, d'Irlande et du Schleswig-Holstein, le CEPD est actuellement en train de préparer un concours concernant une application de santé mobile qui met en œuvre les principes de protection des données.

109. Avec cet avis, nous voulons contribuer à accorder une place importante au débat général sur l'intégration des exigences en matière de respect de la vie privée et d'éthique dans la conception des technologies. Les retours d'information concernant le présent avis

préliminaire sont les bienvenus. La conférence internationale des commissaires à la protection des données et de la vie privée 2018[141], organisée conjointement par le CEPD et l'autorité bulgare chargée de la protection des données, devrait être une étape importante dans le débat sur l'éthique numérique en général, et l'occasion de mieux définir la voie à suivre en matière de respect de la vie privée dès la conception, à titre de bon exemple d'approche fondée sur des valeurs à l'égard du développement technologique.

Bruxelles, le 31 mai 2018

Giovanni Buttarelli

Contrôleur européen de la protection des données

Notes

[1] Le Président du PE Tajani invite le PDG de Facebook: http://www.europarl.europa.eu/news/fr/agenda/briefing/2018-04-16/1/facebook-meps-to-discuss-misuse-of-eu-citizens-personal-data.

[2] Audition du PDG de Facebook au Sénat des États-Unis: https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf.

[3] Commission du numérique, de la culture, des médias et des sports de la Chambre des communes britannique: enquête sur les «fake news»: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/inquiries/parliament-2017/fake-news-17-19/.

[4] Parlement fédéral allemand, commission de la stratégie numérique, rapport https://www.bundestag.de/presse/hib/2018_03/-/548624.

[5] Résolution du Parlement français, http://www.assemblee-nationale.fr/15/pdf/propositions/pion0858.pdf.

[6] Le rapport Eurobaromètre spécial 431 publié en juin 2015 indiquait que plus de huit répondants sur dix avaient le sentiment de ne pas disposer d'un contrôle intégral sur leurs données à caractère personnel. Parmi ceux-ci, 31 % pensaient qu'ils n'avaient aucun contrôle sur celles-ci (http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf). Cette impression a récemment été confirmée par d'autres études menées par d'autres organisations. Par exemple, PwC a réalisé une enquête auprès de 2 000 Américains en 2017: https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/cybersecurity-protect-me.html. Seul un répondant sur dix déclarait qu'il avait le sentiment d'avoir totalement le contrôle sur ses données à caractère personnel.

[7] Giovanni Buttarelli sur CNN, 5 avril 2018: http://transcripts.cnn.com/TRANSCRIPTS/1804/05/qmb.91.html.

[8] Avis nº 3/2018 du CEPD sur la manipulation en ligne et les données à caractère personnel du 19 mars 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf.

[9] 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.

[10] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[11] Tim Berners-Lee, «Three challenges for the web, according to its inventor», Web Foundation, 12 mars 2017, https://webfoundation.org/2017/03/web-turns-28-letter/.

[12] Tim Berners-Lee, «The web is under threat. Join us and fight for it», Web Foundation, 12 mars 2018, https://webfoundation.org/2018/03/web-birthday-29/.

[13] Des données issues d'un stimulateur cardiaque ont été utilisées dans au moins une procédure judiciaire pour vérifier si les relevés du rythme cardiaque correspondaient au récit des événements par le suspect. https://www.forensicmag.com/news/2017/02/data-suspects-pacemaker-leads-arson-insurance-fraud-charges.

[14] Il existe de nombreuses recherches sur l'efficacité de la législation environnementale. La conclusion selon laquelle «*avec une quasi-certitude [...] les réglementations environnementales ont suscité les améliorations technologiques qui ont permis d'accroître la production manufacturière tout en réduisant les émissions*» est par exemple corroborée par Bryan C. Williamson, «Do Environmental Regulations Really Work?», dans: University of Pennsylvania, The Regulatory Review, 24 novembre 2016, https://www.theregreview.org/2016/11/24/williamson-do-environmental-regulations-really-work/.

[15] Melvin Kranzberg, Technology and History: «Kranzberg's Laws», dans : Technology and Culture, vol. 27, nº 3 (juillet 1986), pp. 544-560.

[16] Ibid.

[17] Voir: https://edps.europa.eu/data-protection/our-work/ethics_fr

[18] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

[19] Voir par exemple: Lina Jasmontaite, Irene Kamara, Gabriela Zanfir-Fortuna et Stefano Leucci, «*Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules*» EDPL vol. 4 (2018), à venir.

[20] Les autorités chargées de la protection des données et leurs organisations (WP29, EDPB) fourniront des instructions appropriées sur la mise en œuvre des dispositions du RGPD.

[21] Voir par exemple *Tsormpatzoudi, P., Berendt, B., & Coudert, F. (2016). Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity. Dans B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), Privacy Technologies and Policy. Third Annual Privacy Forum, APF 2015. Luxembourg, Luxembourg, 7-8 octobre 2015. Revised Selected Papers (pp. 199-212). Berlin etc.: Springer. LNCS 9484. © Springer*:

https://people.cs.kuleuven.be/~bettina.berendt/Papers/tsormpatzoudi_berendt_coudert_APF2015_with_bib_metadata.pdf.

[22] Deux exemples de solutions proposées sont exposés dans les documents suivants: «*Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–88, 1981*» et «*Security without identification: transaction systems to make big brother obsolete. Commun. ACM, 28(10):1030–1044, octobre 1985. http://doi.acm.org/10.1145/4372.4373.*».

[23] Ce paradigme a été appelé «sécurité multilatérale» et peut être trouvée dans son stade originaire dans des documents tels que «*Kai Rannenberg. Recent development in information technology security evaluation – the need for evaluation criteria for multilateral security. Dans Richard Sizer, Louise Yngström, Henrik Kaspersen, and Simone Fischer-Hübner, editors, Security and Control of Information Technology in Society – Proceedings of the IFIP TC9/WG 9.6 Working Conference. North-Holland Publishers, 1994.*».

[24] Une des définitions les plus adoptées du terme «technologie renforçant la protection de la vie privée» a été donnée par Borking, Blarkom et d'autres en 1995, qui les définissaient comme «*un système de mesures de TIC visant à protéger la confidentialité des informations en éliminant ou en réduisant au minimum les données à caractère personnel et en prévenant ainsi le traitement inutile ou non désiré des données à caractère personnel, sans perte de fonctionnalité du système d'information*».

[25] Voir par exemple «The Guardian - Revealed: how US and UK spy agencies defeat internet privacy and security»: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (consulté en dernier lieu le 22.2.2018).

[26] «L'*Internet Engineering Task Force*» (IETF) est une vaste communauté internationale ouverte de concepteurs de réseau, d'opérateurs, de prestataires de services, et de chercheurs qui s'intéressent à l'évolution de l'architecture de l'internet et au bon fonctionnement de l'internet. Il est ouvert à toute personne intéressée», extrait du site web de l'IETF: https://www.ietf.org/about/who/ (consulté en dernier lieu le 22.2.2018).

[27] «IETF news- Security and Pervasive Monitoring», 7 septembre 2013: https://www.ietf.org/blog/security-and-pervasive-monitoring/ (consulté en dernier lieu le 22.2.2018).

[28] Voir: https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf (consulté en dernier lieu le 21.2.2018). Les «sept principes fondamentaux» sont les suivants: 1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives. 2. Établir le respect de la vie privée comme paramètre par défaut. 3. Intégrer le respect de la vie privée dans la conception. 4. Assurer une fonctionnalité complète selon un paradigme à somme positive et non à somme nulle. 5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements. 6. Assurer la visibilité et la transparence, maintenir un processus ouvert. 7. Respecter la vie privée des utilisateurs, maintenir l'utilisateur au centre du processus.

[29] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995.

[30] Voir: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

[31] Le WP29 était composé de représentants de l'ensemble des autorités de contrôle de la protection des données de l'Union/de l'EEE. Il est basé sur les dispositions de l'article 29 de la directive 95/46/CE. Le RGPD l'a remplacé par l'EDPB.

[32] L'avis est disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_fr.pdf.

[33] ***Protection des données dès la conception et protection de la vie privée par défaut***

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au

moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

[34] Si les termes «respect de la vie privée» et «protection des données» sont utilisés dans des sens différents dans le cadre juridique de l'Union, nous utiliserons l'expression «respect de la vie privée dès la conception et par défaut» comme englobant aussi toute utilisation de l'expression «protection des données dès la conception et par défaut». De plus, lorsque nous parlons simplement de «respect de la vie privée dès la conception», cela n'exclut pas le «respect de la vie privée par défaut» mais souligne simplement la dimension «conceptuelle».

En référence à la Charte des droits fondamentaux de l'Union, le «respect de la vie privée» est normalement utilisé pour décrire le droit exprimé par l'article 7 («Respect de la vie privée et familiale») tandis que la «protection des données» est utilisée pour l'article 8 («Protection des données à caractère personnel»).

[35] Le RGPD définit le responsable du traitement comme «*la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...]*». Voir article 4.

[36] Ces mécanismes de certification doivent être approuvés en vertu de l'article 42. Une interprétation de cet article a été adoptée par le comité européen de protection des données (voir article 70 du RGPD).

[37] L'article 5 reprend tous les principes relatifs au traitement des données à caractère personnel. Il s'agit des principes de a) licéité, loyauté, transparence; b) limitation des finalités; c) minimisation des données; d) exactitude; e) limitation de la conservation; f) intégrité et confidentialité. Pour de plus amples détails, veuillez lire l'article dans son intégralité.

[38] Dans le présent document, les termes «garantie» et «mesure» sont utilisés de manière interchangeable.

[39] En général, dans les ouvrages consacrés à la gestion de projet, la «mise en œuvre/construction» du projet/système, à la suite de la conception et précédant son exécution, et le «rejet/la transition» d'un projet/système à la suite de son exécution sont aussi des phases claires d'un projet avec leurs exigences propres. Il n'y a néanmoins aucune raison de croire que le législateur ne voulait pas faire référence à l'ensemble du cycle de vie d'un projet en mentionnant simplement les phases de conception et d'exécution.

[40] Pour des exemples de libertés et droits fondamentaux à protéger, le 75^{éme} considérant du RGPD constitue une source précieuse et fiable.

[41] En réalité, un exemple est donné pour clarifier le concept, dans lequel la «pseudonymisation» est mentionnée comme garantie possible pour satisfaire au principe de «minimisation des données».

[42] Voir définition de «personne concernée» à l'article 4, paragraphe 1, du RGPD.

[43] Les principes de limitation des finalités et de minimisation des données sont décrits respectivement à l'article 4, paragraphe 1, points b) et c).

[44] Voir aussi «avis du CEPD sur le paquet de mesures pour une réforme de la protection des données» du 7 mars 2012, en particulier le point 180. Bien sûr, cet avis renvoie à la proposition originale de la CE COM/2012/011 final: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52012PC0011 . La formulation du principe de respect de la vie privée par défaut dans la proposition originale est très proche de celle du texte final.

[45] Par exemple, si j'utilise une application de partage de véhicules, je m'attends à ce que ma position géographique soit utilisée afin de pouvoir savoir où la voiture la plus proche est stationnée, et à ce que mes coordonnées soient utilisées afin de pouvoir être joignable dans le contexte de ce service. Cela ne signifie pas que, par défaut, ma position géographique et mes coordonnées doivent être envoyées à des vendeurs de bicyclettes locaux afin qu'ils puissent m'envoyer de la publicité et des offres.

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

[47] Voir article 28, paragraphe 1, du RGPD.

[48] Les «considérants» d'un texte juridique précèdent la liste des articles («dispositions de fond»). Ils ont pour objectif de donner un contexte et une justification aux articles et contiennent des recommandations et des explications supplémentaires pertinentes. Bien que seuls les articles soient juridiquement contraignants, les considérants sont néanmoins souvent utilisés pour interpréter le droit, notamment par les organismes de réglementation et les tribunaux.

[49] Les règles de l'article 35 du RGPD ont été complétées par les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) - wp248, publiées par le groupe de travail «Article 29» et disponibles à l'adresse suivante: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (consulté en dernier lieu le 20.2.2018).

[50] Voir comment ce concept est développé dans les directives provisoires du CEPD sur la documentation des opérations de traitement pour les institutions, organes et agences de l'Union européenne: https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en, en particulier la partie 1.

[51] Op. cit. dans la note de fin de document **Error! Bookmark not defined.**.

[52] Voir article 35, paragraphes 1 et 10, et considérants 90 et 93 du RGPD.

[53] 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, JO L 201 du 31.7.2002, p. 37, modifiée par la directive 2009/136/CE.

[54] Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité. JO L 91 du 7.4.1999, p. 10.

[55] Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE, JO L 153 du 22.5.2014, p. 62. Cette dernière est aussi appelée «directive RED».

[56] Avis du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement «vie privée et communications électroniques»), avril 2017, p. 23: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_fr.pdf (consulté en dernier lieu le 7.3.2018).

[57] 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) 10 final, 2017/0003 (COD). Cette proposition fait actuellement l'objet de la procédure législative ordinaire de l'Union.

[58] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JO L 257 du 28.8.2014, p. 73.

[59] Article 12, paragraphe 3, point c), du règlement eIDAS.

[60] Recommandation 2012/148/UE de la Commission du 9 mars 2012 relative à la préparation de l'introduction des systèmes intelligents de mesure (JO L 73 du 13.3.2012, p. 9):

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32012H0148&from=FR (consulté en dernier lieu le 1.3.2018).

[61] Recommandation 2014/724/UE de la Commission du 10 octobre 2014 concernant le modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure (JO L 300 du 18.10.2014, p. 63):

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014H0724&from=FR (consulté en dernier lieu le 1.3.2018). L'industrie a testé le modèle AIPD pendant deux ans et la Commission a réalisé une évaluation de la phase d'essai. Le modèle est à présent en cours de parachèvement suivant les résultats de l'évaluation, et eu égard aux nouvelles exigences du RGPD.

[62]Voir: https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp4_bref_smart-metering_systems_final_deliverable.pdf (consulté en dernier lieu le 1.3.2018).

[63] La notion de MTD a été héritée du secteur industriel, où elle était utilisée dans la politique de réduction des émissions de gaz: https://www.eea.europa.eu/themes/air/links/guidance-and-tools/eu-best-available-technology-reference (consulté en dernier lieu le 1.3.2018).

[64] Voir note de fin de document 28.

[65] Voir note de fin de document 30.

[66] Voir, par exemple, propositions au Canada: https://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/communique-de-presse/9691065 (consulté en dernier lieu le 7.3.2018) et au Brésil: https://iapp.org/news/a/brazilian-general-bill-on-the-protection-of-personal-data/ (consulté en dernier lieu le 7.3.2018).

[67] Voir, par exemple, bureau du commissaire à l'information de l'État de Victoria: https://www.cpdp.vic.gov.au/menu-privacy/privacy-organisations/privacy-organisations-privacy-by-design (consulté en dernier lieu le 7.3.2018).

[68] «Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers»: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (consulté en dernier lieu le 7.3.2018).

[69] Les autres sont «le choix simplifié» et «la transparence».

[70] Remarques de la commissaire Edith Ramirez, conférence sur le respect de la vie privée dès la conception, Hong Kong, 13.6.2012: https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf (consulté en dernier lieu le 7.3.2018). Les principes des pratiques équitables en matière de traitement des informations (*Fair Information Practice Principles*, FIPP), ont été adoptés par le gouvernement américain à l'intention des agences fédérales lorsqu'elles traitent des informations personnellement identifiables. Ils pourraient essentiellement être résumés de la manière suivante: transparence, limitation de l'utilisation, accès et correction, qualité des données, et sécurité. Nombreux sont ceux qui considèrent les FIPP comme les éléments constitutifs d'origine des législations et des chartes relatives au respect de la vie privée dans le monde, y compris dans l'Union européenne.

[71] Voir note de fin de document 70.

[72] Voir https://www.ftc.gov/about-ftc (consulté en dernier lieu le 7.3.2018).

[73] Extrait de la même source que celle citée dans la note de fin de document 70: «*La FTC recommande aux entreprises d'adopter ces concepts en guise de bonnes pratiques de manière volontaire ou autoréglementaire. Nous avons aussi appelé le Congrès américain à promulguer une législation complète sur le respect de la vie privée fondée sur les idées contenues dans le cadre de la FTC*».

[74] «NISTIR 8062 - An Introduction to Privacy Engineering and Risk Management in Federal Systems»:

https:/doi.org/10.6028/NIST.IR.8062 (consulté en dernier lieu le 7.3.2018).

[75] Extrait de la source dans la note de fin de document 74: «*En juillet 2016, l'*Office of Management and Budget *(OMB) a publié une mise à jour de la circulaire nº A-130 qui impose aux agences d'appliquer le cadre de gestion des risques du NIST dans leurs programmes de protection de la vie privée. Cette mise à jour de l'OMB met aussi à présent l'accent sur la gestion des risques pour la vie privée au-delà de la seule conformité avec les lois, les réglementations et les politiques en matière de protection de la vie privée. Les agences devraient déjà utiliser les analyses d'impact sur le respect de la vie privée pour faire face aux risques pour la vie privée, mais il est plus difficile pour elles de le faire de façon systématique en l'absence de modèle qui permette d'appliquer un processus répétable et mesurable pour évaluer les risques pour la vie privée. La répétabilité est importante afin que le processus puisse être exécuté de façon systématique dans le temps (non pas que le résultat soit nécessairement le même à chaque fois). La mesurabilité est importante afin que les agences puissent démontrer l'efficacité des contrôles du respect de la vie privée dans le cadre de la réduction des risques pour la vie privée mis en évidence.*»

[76] https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

[77] Pour les principes des pratiques de traitement équitable des informations, voir la note de fin de document 70.

[78] Voir:
http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm.

[79] Pour un aperçu des méthodes d'élaboration des logiciels, voir:
https://en.wikipedia.org/wiki/Software_development_process.

[80] Pour un aperçu des exigences non fonctionnelles, voir: https://en.wikipedia.org/wiki/Non-functional_requirement (consulté en dernier lieu le 7.3.2018).

[81] L'exception est la situation où le principal objectif du système consiste à gérer les paramètres de protection de la vie privée (par exemple, le module complémentaire d'un navigateur destiné à empêcher d'être suivi).

[82] «Privacy and Data Protection by Design – from policy to engineering», ENISA, décembre 2014: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (consulté en dernier lieu le 7.3.2018).

[83] «Protection Goals for Privacy Engineering», Marit Hansen, Meiko Jensen et Martin Rost, 2015 IEEE CS Security and Privacy Workshops.

[84] Pour un aperçu des propriétés de la sécurité de l'information, voir: https://en.wikipedia.org/wiki/Information_security.

[85] A. Pfitzmann et M. Hansen, «A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management», 2010.

[86] Voir note de fin de document 74.

[87] Les PII, *Personally Identifiable Information*, sont des informations personnellement identifiables. Dans «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)», NIST Special Publication 800-122, avril 2010: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf (consulté en dernier lieu le 7.3.2018), les PII sont définies comme «*toute information qui peut être utilisée pour distinguer ou découvrir l'identité d'une personne, telle que le nom, le numéro de sécurité sociale, la date et le lieu de naissance, le nom de jeune fille de la mère, ou les données biométriques; et toute autre information qui est associée ou associable à une personne, telle que les informations médicales, éducationnelles, financières et professionnelles*». Les PII ne doivent pas être confondues avec les «données à caractère personnel» telles qu'elles sont définies à l'article 4, point 1, du RGPD.

[88] Dans ce cas, les principes de référence sont les principes des pratiques de traitement équitable des informations (voir note de fin de document 54).

[89] Voir note de fin de document 74, à la section 3.1.1.

[90] Voir https://distrinet.cs.kuleuven.be/software/linddun/ (consulté en dernier lieu le 7.3.2018). La méthode vient du groupe de recherche DistriNet de l'université KU Leuven.

[91] Un modèle de conception «constitue un mécanisme permettant d'améliorer les sous-systèmes ou les composants d'un système logiciel, ou les relations entre ceux-ci. Il décrit une structure récurrente de composants de communication qui résout un problème de conception général dans un contexte particulier», selon la définition originale datant de la fin des années 70.

[92] Un exemple de catalogue de modèles est disponible à l'adresse suivante: https://privacypatterns.eu (consulté en dernier lieu le 7.3.2018).

[93] Voir, par exemple, Michael Colesky, Jaap-Henk Hoepman, Christiaan Hillen, «A Critical Analysis of Privacy Design Strategies»: https://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf (consulté en dernier lieu le 7.3.2018).

[94] PRIPARE, «Handbook - Privacy and Security by Design Methodology»: http://prepareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf (consulté en dernier lieu le 7.3.2018).

[95] Datatilsynet, «Software development with Data Protection by Design and by Default»: https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/ (consulté en dernier lieu le 7.3.2018).

[96] CEPD, «Lignes directrices sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions de l'UE», mars 2018: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf (consulté en dernier lieu le 7.3.2018).

[97] Voir une liste (non exhaustive) des initiatives de normalisation dans le domaine du respect de la vie privée dans le wiki d'IPEN: https://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards#Privacy_Standards (consulté en dernier lieu le 7.3.2018).

[98] Voir: https://tools.ietf.org/html/rfc6973.

[99] Voir note de fin de document 36.

[100] Commission européenne (2015) M/530, décision d'exécution C(2015) 102 final de la Commission du 20.1.2015 relative à une demande de normalisation aux organisations européennes de normalisation concernant des normes européennes et des publications en matière de normalisation européenne pour la gestion du respect de la vie privée et de la protection des données à caractère personnel, conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil à l'appui de la directive 95/46/CE du Parlement européen et du Conseil et à l'appui de la politique industrielle en matière de sécurité de l'Union: http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548.

[101] Voir: https://ec.europa.eu/growth/single-market/european-standards/key-players_en.

[102] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32012R1025.

[103] Présentation lors de la conférence sur la cybersécurité CEN/CENELEC, 12 mars 2018, A. Guarino, K. Rannenberg:

ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/GUARINO_RANNENBERG_CEN-CLC_JTC8.pdf.

[104] Voir:
ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Walter-FUMY_Chair_CEN-CLC_JTC13.pdf.

[105] Voir aussi Kamara, I., «Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'», dans European Journal of Law and Technology, vol. 8, nº 1, 2017: http://ejlt.org/article/view/545/723#_edn20.

[106] Le *Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies* est attribué à des recherches remarquables dans le domaine des PET. https://petsymposium.org/award/index.php.

[107] Voir https://privacybydesign.foundation/en/ (projet IRMA): https://privacybydesign.foundation/irma-explanation/ pour une application de la technique.

[108] La fonctionnalité DNT telle qu'elle est mise en œuvre dans les clients web envoie au site internet un signal qui communique que le client ne veut pas être suivi. Le W3C a entrepris une initiative de normalisation appelée *Tracking Preference Expression*, qui est disponible à l'adresse suivante: http://www.w3.org/2011/tracking-protection/.

[109] Les *mix networks* sont des protocoles de communication conçus de manière à rendre très difficile le suivi des expéditeurs et des récepteurs des messages. Voir, par exemple, «George Danezis, University of Cambridge, Technical Report nº 594, 2004 - Designing and attacking anonymous communication systems»:

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-594.pdf.

Une entrée Wikipédia existe, qu'il peut être intéressant de consulter: https://en.wikipedia.org/wiki/Mix_network

[110] Voir note de fin de document 82.

[111] «Privacy by design in big data», ENISA, décembre 2015: https://www.enisa.europa.eu/publications/big-data-protection (consulté en dernier lieu le 7.3.2018).

[112] Le travail de l'ENISA sur les PET est disponible ici: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies (consulté en dernier lieu le 7.3.2018).

[113] *Formal comments of the EDPS on the Cybersecurity package*, 15 décembre 2017, https://edps.europa.eu/data-protection/our-work/publications/comments/cybersecurity-package_en.

[114] Voir note de fin de document 108.

[115] La confidentialité différentielle est un processus qui introduit du «bruit» dans les données à caractère personnel collectées afin qu'elles ne puissent pas être associées à des personnes identifiables tout en garantissant un certain niveau d'exactitude dans les calculs (par exemple, statistiques) réalisés à partir de ces données. Voir un exemple d'application dans des produits d'utilisation courante: https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf (consulté en dernier lieu le 9.3.2018). Les références aux produits commerciaux ne sont pas nécessairement cautionnées par le CEPD.

[116] Avis du CEPD sur les systèmes de gestion des informations personnelles, octobre 2016: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf (consulté en dernier lieu le 9.3.2018).

[117] À titre d'exemple à cet égard, l'IEEE a commencé à organiser, en marge de son symposium sur la sécurité et la protection de la vie privée, un atelier international sur l'ingénierie de la vie privée: http://www.ieee-security.org/TC/SPW2017/IWPE/program.html (consulté en dernier lieu le 9.3.2018).

[118] Projet d'avis de la commission des libertés civiles, de la justice et des affaires intérieures à l'intention de la commission de l'industrie, de la recherche et de l'énergie sur 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) [COM(2017)0477 –C8-0310/2017(COD)]: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-615.394&format=PDF&language=FR&secondRef=02 (consulté en dernier lieu le 9.3.2018).

[119] Voir: https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_fr (consulté en dernier lieu le 9.3.2018).

[120]Voir https://fpf.org/2017/08/30/privacy-engineering-research-gdpr-trans-atlantic-initiative/ (consulté en dernier lieu le 9.3.2018).

[121] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

[122] Voir panel à la CPDP 2018: https://www.youtube.com/watch?v=3S0CV2ujIVM (consulté en dernier lieu le 9.3.2018).

[123] *Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017*, http://ec.europa.eu/newsroom/document.cfm?doc_id=47559 (consulté en dernier lieu le 9.3.2018).

[124] Le CEPD contribue aux efforts dans ce sens, en particulier grâce à l'initiative Digital Clearinghouse: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_fr.

[125] Il peut être intéressant de lire cette réaction à la récente affaire Facebook-Cambridge Analytica: https://www.theguardian.com/technology/2018/apr/12/facebook-how-to-quit-delete-account-addiction-what-to-do.

[126] Le rapport peut être consulté à l'adresse suivante: https://www2.deloitte.com/content/dam/insights/us/articles/HCTrends2018/2018-HCtrends_Rise-of-the-social-enterprise.pdf.

[127] Voir avis du CEPD sur les systèmes de gestion des informations personnelles (note de fin de document 116) et en particulier la section 3.9.

[128] Voir: https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_fr

[129] Voir: https://edps.europa.eu/sites/edp/files/publication/18-01-25_privacy_by_design_privacy_engineering_cpdp_en_3.pdf (consulté en dernier lieu le 9.3.2018).

[130]Voir par exemple: http://www.wired.co.uk/article/is-the-internet-broken-how-to-fix-it (consulté en dernier lieu le 9.3.2018).

[131] Voir par exemple: https://www.theguardian.com/technology/2018/jan/13/mark-zuckerberg-tech-addiction-investors-speak-up (consulté en dernier lieu le 9.3.2018).

[132] Article 1er de la Charte des droits fondamentaux de l'Union européenne: *«La dignité humaine est inviolable. Elle doit être respectée et protégée.»*

[133] Avis du CEPD, Vers une nouvelle éthique numérique, Données, dignité et technologie, décembre 2015: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_fr.pdf (consulté en dernier lieu le 9.3.2018).

[134] Voir note de fin de document 26.

[135] https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[136] Voir: http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.

[137] Voir: https://ethicsinaction.ieee.org/.

[138] IETF RFC 1087 «Ethics and the Internet»: https://tools.ietf.org/html/rfc1087.

[139] IETF RFC 8280 «Research into Human Rights Protocol Considerations»: https://trac.tools.ietf.org/html/rfc8280.

[140] Les documents de travail de l'IWGDPT sont disponibles à l'adresse suivante: https://www.datenschutz-berlin.de/working-paper.html.

[141] Voir: https://edps.europa.eu/press-publications/press-news/press-releases/2017/2018-international-conference-data-protection-0_fr.