EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 4/2015

Vers une nouvelle éthique numérique

Données, dignité et technologie

11 septembre 2015

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE 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». Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec pour mission spécifique d'être plus constructifs et proactifs. 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 fait suite au précédent avis du CEPD sur le règlement général sur la protection des données qui visait à aider les principales institutions de l'UE à trouver un consensus sur un ensemble de règles réalisables et tournées vers l'avenir qui renforce les droits et les libertés des personnes physiques. Dans le présent avis, comme il l'avait fait dans l'avis sur la santé mobile publié début 2015, le CEPD aborde le défi du passage en «mode numérique» de la protection des données – le troisième objectif de la stratégie du CEPD – en «visant à adapter les principes de protection des données au monde numérique», compte tenu également des projets de l'UE concernant le marché unique numérique. L'avis est conforme à l'approche du groupe de travail «Article 29» sur les aspects liés à la protection des données de l'utilisation des nouvelles technologies, comme l'«Internet des objets», à laquelle le CEPD a contribué en tant que membre à part entière du groupe.

Dignity	**Dignité**
Future oriented rules and enforcement	**Des règles et une mise en œuvre orientées vers l'avenir**
Empowered individuals	**L'autonomisation des personnes**
Accountable controllers	**Des responsables des traitements de données responsables**
Innovative privay engineering	**Une ingénierie innovante en matière de protection de la vie privée**
Ethics	**Éthique**

«La dignité humaine est inviolable. Elle doit être respectée et protégée.»

Article 1er, Charte des droits fondamentaux de l'UE

Les droits fondamentaux au respect de la vie privée et à la protection des données personnelles sont devenus plus importants qu'ils ne l'ont jamais été pour la protection de la dignité humaine. Ils sont consacrés dans les traités de l'UE et dans la Charte des droits fondamentaux de l'UE. Ils permettent aux personnes physiques de développer leur propre personnalité, de mener une vie indépendante, d'innover et d'exercer leurs autres droits et libertés. Les principes de protection des données définis dans la Charte de l'UE – caractère nécessaire, proportionnalité, équité, minimisation des données, limitation de la finalité, consentement et transparence – s'appliquent aux traitements de données dans leur ensemble, à la collecte des données et à leur utilisation.

Si la technologie ne doit pas dicter les valeurs et les droits; la relation entre ces éléments ne doit pas non plus être réduite à une fausse dichotomie. La révolution numérique est porteuse de promesses d'améliorations en matière de santé, d'environnement, de développement international et d'efficacité économique. Conformément aux projets de l'UE concernant un marché unique numérique, l'informatique dématérialisée, l'«Internet des objets», les mégadonnées et d'autres technologies sont considérés comme des éléments clés de la compétitivité et de la croissance. Les modèles d'affaire exploitent de nouvelles capacités de collecte massive, de transmission instantanée, de combinaison et de réutilisation d'informations à caractère personnel en vue de finalités qui n'avaient pas été prévues et dont la justification est exposée dans des politiques de protection de la vie privée longues et peu compréhensibles. Cette situation fait peser de nouvelles pressions sur les principes de protection des données, et appelle une nouvelle réflexion sur la manière dont ces principes sont appliqués.

Dans l'environnement numérique qui est le nôtre aujourd'hui, le respect de la loi ne suffit pas; nous devons examiner la dimension éthique du traitement de données. Le cadre réglementaire de l'UE accorde déjà une certaine marge de manœuvre pour l'adoption de décisions et l'application de garanties souples et définies au cas par cas dans le cadre du traitement d'informations à caractère personnel. La réforme du cadre réglementaire constituera un progrès appréciable. Mais il existe d'autres questions, plus profondes, concernant l'incidence que les tendances qu'il est possible d'observer dans une société axée sur les données ont sur la dignité, la liberté individuelle et le fonctionnement de la démocratie.

Ces questions ont des implications en termes d'ingénierie, philosophiques, juridiques et morales. Le présent avis souligne certaines tendances technologiques majeures qui pourraient supposer un traitement d'informations à caractère personnel inacceptable ou qui pourraient interférer avec le droit au respect de la vie privée. Il décrit un «écosystème de la protection des mégadonnées» comportant quatre volets, destiné à relever le défi du numérique: un effort collectif, sous-tendu par des considérations éthiques.

(1) Une réglementation relative aux traitements de données orientée vers l'avenir et le respect des droits à la vie privée et à la protection des données.
(2) L'adoption des décisions de traiter des informations à caractère personnel par des responsables du traitement responsables.
(3) Une ingénierie et une conception des produits et services liés au traitement de données tenant compte du respect de la vie privée.

(4) L’autonomisation des personnes physiques.

Le contrôleur européen de la protection des données souhaite stimuler une discussion ouverte et éclairée au sein et en dehors de l’UE, à laquelle participeraient la société civile, les concepteurs, les entreprises, les universitaires, les autorités publiques et les autorités de régulation. Le nouveau comité d’éthique européen en matière de protection des données que nous allons établir au sein du CEPD aidera à définir une nouvelle éthique numérique qui permettra de mieux comprendre la manière dont la technologie peut bénéficier à la société et à l’économie en renforçant les droits et les libertés des personnes physiques.

TABLE DES MATIÈRES

1. L'omniprésence des données: tendances, opportunités et défis

Des volumes toujours croissants d'informations à caractère personnel sont collectés et traités selon des modalités de plus en plus opaques et complexes. Le déploiement progressif des ordinateurs dans les entreprises et les administrations publiques dans les années 1980 a conduit à la perception largement répandue que les pratiques de gouvernements et d'entreprises puissants en matière de traitement de données à caractère personnel réduisaient les personnes physiques au seul statut de personnes concernées et constituaient une menace pour les droits et libertés fondamentaux. Ce qui distingue la vague actuelle de technologies de l'information et de la communication intégrée est son omniprésence et sa puissance.

L'an dernier, il a été annoncé que la planète comptait davantage de dispositifs connectés que d'êtres humains.[1] Les progrès en matière de capacité des processeurs[2], de stockage et de bande de transmission se traduisent par un affaiblissement progressif des contraintes techniques qui pèsent sur le traitement d'informations à caractère personnel. On s'attend à ce que l'«Internet des objets» et les analyses de mégadonnées convergent avec l'intelligence artificielle, le traitement du langage naturel et les systèmes biométriques pour doter des applications de capacités d'apprentissage de la machine en vue de l'acquisition d'un niveau avancé d'intelligence. Les gouvernements et les entreprises sont en mesure d'aller au-delà de l'«exploration de données» pour parvenir à une «exploration de la réalité» qui pénètre l'expérience quotidienne, la communication, voire la pensée.[3] Alors que la société s'adapte aux exigences du marché numérique, des efforts renouvelés sont mis en œuvre pour enseigner la programmation aux jeunes enfants.[4] L'exploitation de ces tendances dans un secteur dans lequel l'UE est un consommateur de premier plan mais est à la traîne s'agissant de la prestation de services est un thème récurrent de la stratégie pour le marché unique numérique de la Commission.[5]

En dépit de leur actualité, ces tendances et nombre des notions utilisées aujourd'hui sont vagues et se chevauchent. En vue de contribuer à la stimulation d'un débat, nous souhaitons souligner des tendances spécifiques qui, bien que nous ne prétendions évidemment pas à l'exhaustivité, soulèvent, de notre point de vue, les questions éthiques et pratiques les plus importantes pour l'application des principes de protection des données.

1.1 Mégadonnées

Les «mégadonnées»[6] renvoient à la pratique consistant à combiner d'énormes volumes d'informations émanant de sources diverses et à les analyser, en utilisant le plus souvent des algorithmes d'autoapprentissage pour éclairer la prise de décisions. Ces informations n'ont pas toujours un caractère personnel: les données générées par des capteurs à des fins de surveillance des phénomènes naturels ou atmosphériques comme le temps ou la pollution, ou à des fins de surveillance des aspects techniques de processus de fabrication, ne se rapportent pas à «une personne physique identifiée ou identifiable».[7] Mais l'une des valeurs les plus importantes des mégadonnées pour les entreprises et les gouvernements découle de la surveillance des comportements *humains*, aux niveaux collectif et individuel, et réside dans leur potentiel prédictif.[8]

L'une des conséquences est l'émergence d'un modèle de revenus pour les sociétés de l'Internet qui repose sur le suivi de l'activité en ligne en vue d'optimiser la valeur économique des transactions pour les prestataires de services, s'agissant non seulement de la publicité ciblée, mais aussi des conditions et des tarifs des polices d'assurance, des prêts et d'autres types de relations contractuelles. Dans le marché concurrentiel de l'attention des

utilisateurs, la plupart des personnes n'est pas consciente de l'ampleur considérable de ce suivi.[9] Ces «mégadonnées» devraient être considérées comme des données à caractère personnel, même dans les cas où il a été fait application de techniques d'anonymisation: il est de plus en plus facile de déduire l'identité d'une personne de la combinaison de données prétendument «anonymes» et d'autres ensembles de données, y compris d'informations à la disposition du public, par exemple sur les médias sociaux.[10] Lorsque ces données sont commercialisées, particulièrement dans le cadre d'échanges transfrontaliers et entre juridictions, la responsabilité du traitement des informations devient floue et difficile à établir ou à faire appliquer au titre de la législation en matière de protection des données, en particulier en l'absence de normes internationales.

1.2 L'«Internet des objets»

De nombreux dispositifs connectés à l'Internet sont devenus communs, comme les téléphones intelligents, les tablettes, les distributeurs de billets et les appareils d'enregistrement sur des vols. D'ici 2020, la connectivité devrait devenir une caractéristique standard, avec 25 milliards de dispositifs connectés (contre 4,8 milliards en 2015) dans des domaines allant de la télémédecine aux véhicules et des compteurs intelligents à toute une gamme de nouveaux dispositifs fixes et mobiles nécessaires destinés à permettre la création des villes intelligentes.[11]

Ces capteurs fourniront des informations avec une immédiateté et un niveau de détail que les offices de statistiques et les instituts de sondage ne peuvent pas atteindre aujourd'hui. Cependant, ces informations ne seront pas nécessairement plus précises et elles pourraient même être potentiellement trompeuses.[12] Les connections entre appareils dans le domaine automobile, qui devraient atteindre 1,8 milliard en 2022, pourraient réduire les accidents et la pollution, augmenter la productivité et renforcer l'autonomie des personnes âgées et des personnes handicapées.[13] Les objets «portables», comme les vêtements et les montres, traiteront les informations à caractère personnel de la même manière que les autres dispositifs connectés. Ils pourront détecter la présence de caillots de sang et surveiller la condition physique et la cicatrisation des plaies; les tissus connectés pourraient offrir une protection dans les environnements extrêmes, par exemple lors des opérations de lutte contre les incendies. Ces dispositifs téléchargeront directement les données à caractère personnel dans des espaces de stockage dématérialisés, reliés à des réseaux sociaux et susceptibles de faire l'objet d'une diffusion publique; il sera ainsi possible d'identifier des utilisateurs et de contrôler le comportement et les déplacements de personnes physiques et de foules.[14]

La manière dont ces informations seront traitées pourrait avoir une incidence non seulement sur la vie privée des utilisateurs des dispositifs, y compris lors d'une utilisation sur le lieu de travail, mais également sur les droits des tiers qui seront observés et enregistrés par le dispositif. Bien que l'on dispose de peu de preuves de l'existence d'une discrimination effective, il est clair que l'énorme volume d'informations à caractère personnel collectées par l'«Internet des objets» présente un grand intérêt en tant qu'outil d'optimisation des bénéfices au moyen de la mise en place d'une tarification plus personnalisée fondée sur le comportement de la personne suivie, particulièrement dans le secteur de l'assurance maladie.[15] D'autres règles spécifiques à certains domaines seront également remises en question, par exemple dans les cas où des dispositifs impliquant le traitement de données sur la santé ne sont pas considérés, techniquement, comme des dispositifs médicaux et ne relèvent pas du champ d'application de la réglementation.[16]

1.3 Informatique ambiante

L'informatique ambiante ou informatique invisible renvoie à une technologie clé qui sous-tend l'«Internet des objets». L'une de ses applications les plus évidentes réside dans les «maisons intelligentes» et les «bureaux intelligents» composés de dispositifs dotés de capacités de traitement d'informations sophistiquées et qui promettent de parvenir à une meilleure efficacité énergétique et de permettre aux personnes, qui seront mieux informées, d'agir sur leur consommation à distance (même si ce point dépend du degré d'autonomie du résidant par rapport au propriétaire ou au gestionnaire du bâtiment). Il conviendra d'établir clairement qui est responsable de la finalité et des moyens du traitement des données à caractère personnel liées à des applications d'informatique ambiante, non seulement pour protéger les droits fondamentaux des personnes physiques, mais également pour répartir de manière appropriée les responsabilités en vue d'assurer le respect des exigences générales en matière de sécurité des systèmes.

1.4 L'informatique dématérialisée

L'informatique dématérialisée est définie comme une technologie centrale habilitante permettant d'exploiter des puissances d'analyse et d'exploration approfondies et de collecter et d'analyser des mégadonnées et le flux de données issues de «l'Internet des objet». À l'heure actuelle, elle est utilisée par un cinquième environ des personnes physiques et des entreprises établies dans l'UE.[17]. Elle permet de concentrer des données issues de la multitude de dispositifs de l'«Internet des objets» et elle repose sur la disponibilité et la connectivité d'énormes volumes de données situés dans des espaces de stockage et des installations de traitement de données à grande échelle répartis à travers le monde.[18] On estime qu'une adoption plus large de l'informatique dématérialisée[19] par les secteurs privé et public se traduirait potentiellement par une augmentation de 449 milliards d'EUR du PIB de l'UE28 (0,71 % du PIB total de l'UE).

Le contrôle des informations à caractère personnel est souvent réparti entre le client et le prestataire de services d'informatique dématérialisée et la responsabilité de la conformité aux obligations en matière de protection des données n'est pas toujours claire. Ceci pourrait signifier qu'en pratique, la protection fournie est insuffisante. Ces obligations sont indépendantes de l'**emplacement physique de l'installation de stockage des données. En outre**, même si elle constitue uniquement une technologie de base sur laquelle repose les applications commerciales, l'infrastructure d'informatique dématérialisée elle-même peut devenir une infrastructure critique et accroître les déséquilibres en termes de pouvoir de marché. En effet, 30 % des entreprises ont fait part récemment de difficultés rencontrées pour résilier un abonnement ou pour changer de prestataire.[20]

1.5 Modèles d'affaire dépendants des données à caractère personnel

Ces technologies ont permis l'émergence de nouveaux modèles d'affaire qui se fondent non seulement sur des informations générées par la prestation de services mais également sur des informations issues d'autres sources, comme la présence sur les médias sociaux, pour évaluer les risques et la solvabilité et optimiser les bénéfices. Les plateformes de mise en relation de vendeurs et d'acheteurs, qui permettent de partager et de redistribuer des produits, des services, des compétences et des actifs, constituent aujourd'hui un modèle d'affaire de premier plan. Ces plateformes, souvent désignées par les expressions «économie du partage», «consommation collaborative» ou plateformes de commerce en ligne et mobiles de pair à pair[21], peuvent offrir des rendements économiques classiques, injecter de la compétitivité sur

les marchés et réduire les déchets. Leur valeur à l'échelle mondiale devrait quadrupler dans les années à venir, passant de 26 milliards USD à 110 milliards USD.[22] Ces modèles d'affaire axés sur les données génèrent déjà des bénéfices énormes dans les activités de partage de véhicules et de location de maisons et dans les domaines de la technologie financière et des prêts sociaux. Les sondages indiquent que les consommateurs apprécient leur caractère apparemment plus accessible et pratique.[23]

La fiabilité de ces plateformes repose généralement sur la réputation de l'utilisateur, le contrôle par les pairs et la vérification de l'identité. Ces éléments pourraient potentiellement être considérés comme des facteurs de renforcement de la transparence et de la responsabilité, mais pas nécessairement en relation avec le fournisseur de la plateforme lui-même. De grands acteurs de ces marchés ont été critiqués au motif qu'ils cacheraient des données liées à la réputation aux utilisateurs personnes physiques précis auxquels ces informations se rapportent. Il existe un risque énorme que des personnes physiques puissent être exclues de la prestation de services sur la base d'une réputation fondée sur des données inexactes que ces personnes ne peuvent pas remettre en cause et dont elles ne peuvent pas demander la suppression. Le fait de se fonder sur des données issues de sources multiples remet également en cause le principe de la minimisation des données prévu par le droit de l'UE. La portée de l'incidence que ces modèles d'affaire reposant sur la technologie actuels et à venir auront sur les personnes physiques et sur la société mérite une réflexion approfondie.[24]

1.6 Drones et véhicules autonomes

À l'heure actuelle, les drones, ou aéronefs semi-autonomes, sont principalement utilisés à des fins militaires. Cependant, ils le sont de plus en plus à des fins de surveillance, de cartographie, de transport, de logistique et de sécurité publique, par exemple pour contenir des incendies.[25] Les photographies, vidéos et autres données à caractère personnel collectées par les drones peuvent être échangées par l'intermédiaire des réseaux de télécommunications. Leur utilisation risque de conduire à de graves ingérences dans la vie privée et d'avoir un effet dissuasif sur la liberté d'expression. La question se pose de savoir comment leur conception et leur utilisation pourraient être réglementées de manière efficace pour permettre aux personnes concernées d'exercer leur droit d'accès aux données capturées par ces machines.

Pour ce qui est de la voie terrestre, les véhicules autonomes ou voitures sans conducteur vont modifier la manière dont les déplacements individuels sont utilisés et organisés, et pourrait brouiller la distinction entre transports publics et transports privés. On estime que d'ici 2035, l'Europe comptera 12 millions de véhicules pleinement autonomes et 18 millions de véhicules partiellement autonomes, parmi les adopteurs précoces.[26] Les algorithmes de conduite des véhicules automobiles, comme ceux utilisés par l'option programmée en cas de collision inévitable, dicteront des décisions susceptibles de concerner directement l'intégrité physique, voire la vie ou la mort, de personnes physiques. Ces applications nécessitent à l'évidence de déterminer clairement qui assume la responsabilité et qui doit rendre des comptes en matière de contrôle et de sécurité des données; elles soulèvent également un certain nombre de questions éthiques.

1.7 Tendances susceptibles de présenter une incidence plus importante, à plus long terme

La **bioimpression tridimensionnelle** d'éléments organiques, qui utilise des copies de cellules de patients et des «biobandes» de collagène (à savoir, des données sensibles en

application du droit de l'UE) pour fixer des rangées successives de cellules vivantes, devrait être bientôt disponible.[27] Elle faciliterait la fourniture d'éléments anatomiques humains sur mesure et serait particulièrement précieuse dans les zones les plus pauvres et dans les zones sortant d'une période de conflit dans le monde entier. La bioimpresion soulève des questions évidentes en matière d'éthique médicale, de protection de la propriété intellectuelle et de protection du consommateur mais également, dès lors qu'elle repose sur le traitement de données intimes et sensibles relatives à la santé des personnes physiques, en matière d'application des règles de protection des données.

L'**intelligence artificielle**, comme la robotique, renvoie à une exigence technologique applicable aux machines autonomes fixes et mobiles. L'amélioration de ces machines va offrir un immense potentiel allant au-delà de leur application actuelle. Les ordinateurs dotés de capacités d'apprentissage approfondi apprennent tout seuls à effectuer des tâches en traitant de grands ensembles de données, grâce (notamment) à des réseaux de neurones qui semblent imiter le cerveau. Les chercheurs et les entreprises visent à améliorer l'apprentissage sans supervision. Les algorithmes sont déjà en mesure de comprendre et traduire différentes langues, de reconnaître des images, d'écrire des articles de presse et d'analyser des données médicales.[28] Les médias sociaux fournissent des volumes importants d'informations à caractère personnel que les personnes physiques elles-mêmes ont déjà indexées de manière efficace. Il pourrait s'agir de l'élément final d'une série d'améliorations cognitives destinées à renforcer les capacités du cerveau humain, comme le papier ou le boulier, ou intégrées dans des machines autonomes, des robots, mais le moment est venu d'examiner les ramifications plus larges pour les personnes physiques et la société.[29]

2. Un écosystème de protection des mégadonnées

Aujourd'hui, l'UE a l'occasion de montrer la voie en indiquant la manière dont les gouvernements, les autorités de régulation, les responsables de traitements de données, les concepteurs, les développeurs et les personnes physiques peuvent agir conjointement pour renforcer les droits et pour orienter, et non pas bloquer, l'innovation technologique. Comme il a été relevé par un commentateur[30], les tendances décrites dans cette deuxième partie ont «creusé l'écart entre ce qui est possible et ce qui est autorisé par la loi». Contrairement à ce que certains ont prétendu, le respect de la vie privée et la protection des données constituent l'un des fondements d'un environnement numérique durable et dynamique, et non un obstacle à cet environnement. Les autorités chargées de la protection des données indépendantes comme le CEPD jouent un rôle clé pour dissiper ce type de légendes et pour répondre aux préoccupations réelles des personnes physiques qui craignent de perdre tout contrôle sur leurs informations à caractère personnel.[31]

La prochaine génération de données à caractère personnel sera probablement encore moins accessible aux personnes auxquelles ces données se rapportent. La responsabilité de la mise en forme d'un marché unique numérique durable est nécessairement répartie entre plusieurs acteurs, mais elle se caractérise également par l'existence d'une interdépendance, à la manière d'un écosystème, dès lors qu'elle suppose une interaction efficace entre les développeurs, les entreprises et les autorités de régulation dans l'intérêt des personnes physiques. Dans la présente partie, nous présentons la contribution que ces quatre acteurs fondamentaux peuvent apporter.

2.1 Une réglementation axée sur l'avenir

Nous avons récemment exhorté l'UE à saisir l'occasion historique qui lui est offerte de mettre en place des règles relatives au traitement des informations à caractère personnel plus simples, qui resteront pertinentes le temps d'une génération.[32] Les négociations sur le règlement général sur la protection des données et sur la directive relative à la protection des données dans les domaines policier et judiciaire sont en phases finales, et l'attention va bientôt se porter sur l'avenir de la directive «vie privée et communications électroniques» et sur le nouveau règlement régissant le traitement des données à caractère personnel par les institutions et les organes de l'UE eux-mêmes. Le coût économique de la collecte et du stockage de données est désormais presque négligeable et dès lors, c'est aux autorités chargées de la protection des données qu'il reviendra d'assurer l'application cohérente de ces règles afin d'éviter le «danger moral» d'un traitement des données excessif.[33]

Dans la stratégie pour le marché unique numérique, la Commission reconnaît le lien existant entre le contrôle d'importants volumes de données et le pouvoir de marché. Elle partage la conviction, que nous avons exprimée dans notre avis préliminaire de 2014 sur la «[v]ie privée et [la] compétitivité à l'ère de la collecte de données massives», qu'il est nécessaire de parvenir à une plus grande cohérence entre les autorités de régulation. L'UE dispose déjà des outils nécessaires pour corriger les déséquilibres de pouvoir sur le marché numérique: à titre d'exemple, les procédures en matière d'ententes et de positions dominantes en cours devant la Commission européenne constituent une reconnaissance de la prédominance des appareils mobiles pour accéder à l'Internet. Il est possible de parvenir à une mise en œuvre plus holistique dans le cadre juridique existant, par exemple au moyen d'un centre de compensation de l'UE permettant aux autorités de contrôle d'examiner si des affaires spécifiques peuvent soulever des questions de conformité aux règles applicables en matière de concurrence, de consommation et de protection des données, par exemple:

- en exigeant une plus grande transparence concernant le prix – financier ou autre – d'un service, ce qui pourrait éclairer et faciliter l'analyse d'affaires de concurrence[34], et
- en identifiant les cas de discrimination par les prix déloyale fondée sur des données de qualité médiocre et sur un profilage et des corrélations déloyaux.[35]

Un dialogue plus étroit entre les autorités de régulation des différents secteurs pourrait permettre de répondre aux demandes croissantes de mise en place de partenariats mondiaux à même de créer des «communs» de données ouvertes dans lesquels des données et des idées, comme des statistiques et des cartes, pourraient circuler, être mises à disposition et être échangées dans l'intérêt général, avec moins de risques de surveillance, afin de donner aux personnes physiques davantage d'influence sur les décisions qui les concernent.[36]

2.2 Des responsables des traitements de données responsables

La responsabilité nécessite la mise en place de politiques et de systèmes de contrôle internes qui assurent la conformité et fournissent des preuves pertinentes, en particulier aux autorités de contrôle indépendantes.

Nous avons plaidé en faveur de l'élimination de toute bureaucratie dans la législation en matière de protection des données, au moyen de la réduction des exigences de documentation non nécessaire afin de laisser une plus grande place à l'initiative plus responsable des

entreprises, soutenue par les orientions des autorités chargées de la protection des données. Le principe selon lequel les données à caractère personnel doivent être traitées uniquement de manière compatible avec la réalisation de la ou des finalités pour lesquelles elles sont collectées est fondamental pour assurer le respect des attentes légitimes des personnes physiques. À titre d'exemples, les codes de conduite, les vérifications, la certification et une nouvelle génération de clauses contractuelles et de règles d'entreprise contraignantes peuvent contribuer à l'établissement d'une confiance robuste à l'égard du marché numérique. Les personnes et entités responsables de la gestion d'informations à caractère personnel doivent se montrer beaucoup plus dynamiques et proactives et s'abstenir de suivre la tendance, dite de la «boîte noire», consistant à appliquer des pratiques commerciales secrètes et opaques tout en exigeant une transparence toujours plus importante de la part des clients.[37]

2.3 Une ingénierie tenant compte du respect de la vie privée

L'innovation humaine a toujours été le produit des activités de groupes sociaux spécifiques et de contextes spécifiques, reflétant généralement les normes sociétales de l'époque concernée.[38] Cependant, les décisions en matière de conception technologique ne devraient pas dicter nos relations sociétales et la structure de nos communautés, mais plutôt soutenir nos valeurs et nos droits fondamentaux.

L'UE devrait développer et promouvoir des techniques et des méthodologies d'ingénierie qui permettent de mettre en œuvre des technologies de traitement des données dans le parfait respect de la dignité et des droits des personnes physiques. Les ingénieurs systèmes et les ingénieurs spécialisés en logiciels doivent comprendre les principes de respect de la vie privée dès la conception et les appliquer de manière plus satisfaisante aux nouveaux produits et services, tout au long des étapes de conception, et aux technologies. La responsabilité doit s'appuyer sur des activités de recherche et développement plus poussées concernant des méthodes et outils destinés à assurer la réalisation de vérifications précises et à apprécier la conformité des responsables de traitements et des sous-traitants aux règles applicables, par exemple en associant à chaque donnée à caractère personnel des «métadonnées» décrivant les exigences en matière de protection des données.

Les solutions d'ingénierie devraient donner aux personnes physiques qui le souhaitent la possibilité de préserver leur vie privée et leur liberté par l'anonymat. L'UE devrait promouvoir la conception et la mise en œuvre d'algorithmes qui masquent les identités et les données agrégées afin d'exploiter le pouvoir prédictif des données tout en protégeant la personne physique.[39]

Aujourd'hui, nous devons établir les bases nécessaires pour aborder ces tâches en réunissant des développeurs et des experts de la protection des données de différents secteurs au sein de grands réseaux, comme l'Internet Privacy Engineering Network (IPEN), qui contribuent à un échange interdisciplinaire fructueux d'idées et d'approches.

2.4 L'autonomisation des personnes

Un environnement de «prosommateurs»

Les personnes physiques ne sont pas de simples objets passifs que la loi doit protéger contre l'exploitation. Les tendances dans le domaine numérique décrites ci-dessus offrent des occasions positives de renforcement du rôle de la personne physique. À titre d'exemple, désormais, les gens sont à la fois producteurs et consommateurs de contenus et de services, et ils pourraient de plus en plus être considérés comme assumant la responsabilité conjointe,

avec les prestataires de services, du traitement de données, sauf si ce traitement est effectué à des fins exclusivement «domestiques»[40] (la notion de «prosommateurs» est apparue pour décrire cette évolution[41]). Dans le même temps, les monnaies virtuelles permettent aux utilisateurs de bénéficier de l'anonymat et de contourner toute vérification des transactions par des tiers et elles conduisent ainsi à la réduction des coûts de transaction applicables lors du paiement de produits et services acquis à l'étranger. Par ailleurs, l'anonymat qu'offrent ces monnaies virtuelles et le fait que celles-ci relèvent de la compétence de plusieurs territoires (ou, comme on pourrait le faire valoir, d'*aucun territoire*) rendent les personnes physiques vulnérables à des actes de fraudes et aux activités de marchés criminels qu'il est difficile d'identifier et sur lesquels il est difficile d'enquêter. Outre les obligations qui incombent aux autorités de régulation, aux entreprises et aux ingénieurs, il revient également aux citoyens de se montrer attentifs, alertes et critiques et de s'informer lorsqu'ils prennent des décisions, que ce soit dans un environnement en ligne ou hors ligne.[42]

Consentement

En outre, contrairement à la pensée traditionnelle, il n'est pas possible d'expliquer tous les comportements humains par des principes économiques qui reposent sur le postulat selon lequel les êtres humains sont parfaitement rationnels et sont sensibles aux incitations économiques.[43] Ce point est pertinent pour examiner le rôle à venir du consentement de la personne physique au traitement d'informations personnelles la concernant. Conformément au droit de l'UE, pour la plupart des traitements, le consentement ne constitue pas le seul fondement légitime. Même lorsque le consentement joue un rôle important, il n'exonère pas les responsables du traitement de la responsabilité de l'utilisation qu'ils font des données, en particulier dans les cas où les personnes concernées ont donné leur consentement général au traitement de leurs données en vue d'une vaste gamme de finalités.

Contrôle et «propriété» des données

Les personnes physiques doivent être en mesure de contester les erreurs et les biais inéquitables découlant de la logique utilisée par les algorithmes pour établir des hypothèses et des prévisions. À titre d'illustration, aux États-Unis, dans une étude portant sur près de 3 000 rapports de solvabilité concernant 1 000 consommateurs, il a été constaté que 26 pour cent des rapports comportaient des erreurs «importantes» suffisamment graves pour avoir une incidence sur la cote de solvabilité des consommateurs et, en conséquence, sur le coût d'obtention d'un crédit.[44]

Les données sont souvent considérées comme une ressource, comme le pétrole, destinée à être commercialisée, idéalement entre des parties à la transaction disposant du même degré élevé d'information.[45] Les clients ne sont pas suffisamment rémunérés en contrepartie des informations à caractère personnel commercialisées, et certaines personnes ont plaidé en faveur d'un modèle de propriété des données. Cependant, il est difficile de garantir un contrôle absolu sur les données à caractère personnel – d'autres préoccupations apparaîtront, comme l'intérêt public et les droits et libertés des tiers. Le contrôle est nécessaire mais il n'est pas suffisant.[46] Cependant la dignité humaine demeure une constante et, conformément au droit de l'UE, l'analogie de la propriété ne saurait s'appliquer en tant que telle aux données à caractère personnel qui sont liées de manière intrinsèque à des personnalités individuelles. Il n'existe aucune disposition dans la législation de l'UE en matière de protection des données permettant à une personne physique de renoncer à ce droit fondamental.

Une autre méthode pour permettre aux personnes physiques de mieux contrôler leurs données, qui peut y accéder et pour quelle finalité, pourrait consister à utiliser des espaces de stockage de données personnels ou «coffres-forts de données».[47] Cette notion d'«espace de stockage personnel» suppose des mécanismes de sécurité à même de garantir que seules les entités auxquelles la personne concernée a accordé son autorisation peuvent accéder aux données, et que ces entités ne peuvent accéder qu'aux données pour lesquelles l'autorisation leur a été accordée. Les espaces de stockage de données personnels seraient très efficaces dans le cas des informations actuelles et constamment mises à jour, comme les données géospatiales ou les signes de vie. Au-delà des garanties techniques, les utilisateurs de données seraient tenus de respecter les règles relatives au partage et à l'utilisation des données. Le pouvoir le plus efficace dont dispose un consommateur pour exercer une influence sur le marché des services mis à sa disposition réside dans la concurrence et dans la possibilité d'utiliser un autre service. Il a été prouvé que le fait d'assurer la portabilité des connexions, y compris des identifiants et des informations de contact, constitue un puissant catalyseur pour la concurrence et a effectivement conduit à la réduction des prix à la consommation lorsque le marché des télécommunications a été libéralisé. La portabilité des données, à savoir la possibilité factuelle et pratique de transférer la plupart de ses propres données d'un fournisseur de service à un autre, est un point de départ efficace pour établir les conditions d'un véritable choix offert aux consommateurs.

3. La dignité au cœur d'une nouvelle éthique numérique

Les différents éléments constitutifs de cet écosystème doivent être sous-tendus par un cadre éthique. Le CEPD considère qu'un plus grand respect et la protection de la dignité humaine pourraient constituer le contrepoids à la surveillance omniprésente et à l'asymétrie des pouvoirs auxquelles les personnes physiques sont actuellement confrontées. La dignité devrait se trouver au cœur d'une nouvelle éthique numérique.

3.1 Dignité et données

À la suite de la révolution industrielle des 18e et 19e siècles, le mouvement des droits de l'homme a cherché à garantir le bien social général en réduisant les obstacles au respect de la personne physique. Avec la Charte des droits fondamentaux, et à la suite de la Déclaration universelle des droits de l'homme et de la Convention européenne de sauvegarde des droits de l'homme, l'UE a désormais pris comme point de départ l'inviolabilité de la dignité humaine. La dignité de la personne humaine n'est pas seulement un droit fondamental en soi, mais constitue également un fondement sur lequel reposent les autres droits et libertés, y compris les droits au respect de la vie privée et à la protection des données personnelles.[48] Les violations de la dignité peuvent inclure l'objectivation, lorsqu'une personne est traitée comme un outil au service des finalités poursuivies par un tiers.[49] Le respect de la vie privée fait partie intégrante de la dignité humaine et le droit à la protection des données a été conçu initialement, dans les années 1970 et 1980, comme un moyen de compenser le risque d'érosion du respect de la vie privée et de la dignité en conséquence de la réalisation de traitements de données à grande échelle. En Allemagne, le droit à l'«autonomie informationnelle» a été fondé sur les droits à la dignité personnelle et au libre développement de la personnalité prévus aux articles 1 et 2 de la Constitution allemande.[50]

Cependant, au début du 21e siècle, les personnes physiques sont de plus en plus tenues de divulguer un volume bien plus important d'informations à caractère personnel sur l'Internet pour pouvoir prendre part à des activités de natures sociale, administrative et commerciale, et la mesure dans laquelle elle peuvent refuser cette divulgation est encore plus limitée. Toutes

les activités s'effectuent potentiellement toujours en ligne, ce qui fait peser une pression énorme sur la notion de consentement libre et éclairé. Des «fragments numériques» sont recueillis chaque minute et combinés pour classer les personnes physiques en temps réel afin de créer des profils multiples et parfois contradictoires. Ces profils peuvent être diffusés en quelques microsecondes à l'insu des personnes physiques, et utilisés pour fonder des décisions importantes les concernant.

Les profils utilisés pour prédire le comportement des personnes font peser un risque de stigmatisation, de renforcement des stéréotypes existants, de ségrégation sociale et culturelle et d'exclusion[51], et cette «intelligence collective» nuit au choix individuel et à l'égalité des chances. Ces «bulles de filtrage» ou «chambres d'écho personnelles» pourraient finir par étouffer la créativité, l'innovation et les libertés d'expression et d'association qui ont précisément permis aux technologies numériques de prospérer.

Dans le même temps, il est fait usage d'un état d'exception continu pour des motifs de «sécurité» pour justifier la stratification multiple de techniques intrusives destinées à surveiller l'activité des personnes physiques.[52] La compréhension de ce «cliquet de surveillance» nécessite d'envisager les effets globaux à plus long terme sur la société et les comportements.

L'UE, aux côtés des pays tiers, doit examiner sérieusement les mesures à prendre pour veiller à ce que ces valeurs ne soient pas respectées uniquement sur le papier alors que, dans les faits, elles seraient neutralisées dans le cyberespace. L'UE en particulier dispose actuellement d'une «fenêtre critique» avant l'adoption massive de ces technologies pour inscrire ces valeurs dans les structures numériques qui définiront notre société.[53] Ceci nécessite une nouvelle appréciation du point de savoir si les avantages que les nouvelles technologies peuvent apporter dépendent vraiment de la collecte et de l'analyse des informations personnellement identifiables de milliards de personnes physiques. Cette appréciation pourrait permettre de mettre les développeurs au défi de concevoir des produits qui dépersonnalisent en temps réel d'énormes volumes de données non organisées, rendant ainsi plus difficile, voire impossible, de distinguer une personne physique donnée.

Nous reconnaissons d'ores et déjà que certains traitements de données, par exemple ceux portant sur les données génétiques, doivent non seulement faire l'objet d'une réglementation, mais également être soumis à une évaluation au regard de préoccupations sociétales plus larges, par exemple par des comités d'éthique. Du fait de leur nature même, les données génétiques se rapportent non seulement à une personne physique, mais également à ses ascendants et descendants. Les données génétiques ne servent pas seulement à identifier les relations familiales; des éléments repérés dans les gènes d'une personne physique peuvent également fournir des informations sur ses parents et sur ses enfants, et conduire les responsables du traitement à prendre des décisions qui auront une incidence sur les chances dont ces personnes disposeront au cours de leur vie avant même leur naissance. La concentration potentielle de données à caractère personnel génétiques dans les mains de quelques acteurs géants du marché a des incidences pour l'économie de marché et pour les personnes concernées. Le fait de dépendre de façon croissante d'un système mondial de collecte et d'analyse d'un flux ininterrompu de données pourrait se traduire par une plus grande vulnérabilité de la société et de l'économie à des failles de sécurité et à des attaques malveillantes sans précédent.

Le cadre existant pourrait échouer si nous n'abordons pas l'avenir avec une réflexion novatrice. Il existe une demande et une nécessité croissantes de considérer la personne

concernée comme une personne à part entière, et non pas uniquement comme un consommateur ou un utilisateur. Les autorités chargées de la protection des données, qui sont réellement indépendantes, ont un rôle crucial à jouer pour empêcher qu'à l'avenir, les personnes physiques soient définies par des algorithmes et leurs variations constantes. Ces autorités doivent disposer des outils nécessaires pour exercer un «devoir de diligence» à l'égard des personnes physiques et de leur dignité en ligne. Les notions et les principes traditionnels de respect de la vie privée et de protection des données comportaient déjà des éléments d'éthique à des fins de protection de la dignité, comme en matière d'emploi et de santé. Mais les tendances actuelles ont ouvert un chapitre entièrement nouveau, et il est nécessaire d'étudier si les principes sont suffisamment robustes pour l'ère numérique.[54] La notion de données à caractère personnel elle-même est susceptible de connaître une évolution radicale, dès lors que la technologie permet, de façon croissante, de ré-identifier des personnes physiques à partir de données supposément anonymes. En outre, l'apprentissage des machines et la combinaison des intelligences humaine et artificielle viendront saper les concepts de droits et de responsabilité de la personne physique.

3.2 Un comité consultatif européen en matière d'éthique

Il ne s'agit pas de dresser un tableau alarmant de dystopie. Des discussions sont déjà en cours dans les sphères juridique, politique, économique, sociale, scientifique et même religieuse.[55] Les approches simplistes qui donnent un avantage unilatéral au bénéfice économique ou à la surveillance à des fins de sécurité ne sont probablement pas plus utiles qu'une application trop restrictive de la législation existante qui viendrait étouffer l'innovation et le progrès. En conséquence, le CEPD propose une analyse approfondie, large et multidisciplinaire en vue de fournir des recommandations et d'éclairer le débat sociétal sur la manière dont une société libre et démocratique doit relever le défi technologique.

Dans sa Stratégie[56], le CEPD s'est engagé à développer une approche éthique de la protection des données, dans le cadre de laquelle «la faisabilité, l'utilité ou la rentabilité ne sont pas synonymes de durabilité» et qui reconnaît «la suprématie de la responsabilisation sur le respect mécanique de la lettre de la loi». Nous entendons aller au-delà de la communauté des fonctionnaires de l'UE, des avocats et des spécialistes du domaine informatique et consulter des personnes éminentes qui ont les compétences nécessaires pour apprécier les implications à moyen et long termes de l'évolution technologique et des réponses apportées par la réglementation. Dans les mois à venir, nous allons établir au sein de notre institution indépendante un groupe consultatif externe sur la dimension éthique de la protection des données qui sera chargé d'étudier les relations entre les droits de l'homme, la technologie, les marchés et les modèles d'affaire au 21^{e} siècle.

Notre comité consultatif en matière d'éthique sera composé d'un groupe restreint de personnalités éminentes des domaines de l'éthique et de la philosophie, de la sociologie, de la psychologie, de la technologie et de l'économie, qui bénéficieront le cas échéant du soutien d'autres experts disposant de connaissances et d'une expertise dans des secteurs comme la santé, le transport et l'énergie, l'interaction sociale et les médias, l'économie et la finance, la gouvernance et la démocratie et la sécurité et la surveillance. Ces personnes seront invitées à examiner les implications éthiques au sens large de la manière dont les données à caractère personnel sont conçues et utilisées, et leurs délibérations seront rendues les plus transparentes possibles.

4. Conclusion: le moment est venu d'approfondir la discussion

Le respect de la vie privée et la protection des données constituent une partie de la solution, et non pas le problème. Pour le moment, la technologie est contrôlée par les humains. Il n'est pas aisé de qualifier clairement ces évolutions potentielles de positives ou négatives, souhaitables ou nuisibles, avantageuses ou préjudiciables, et ce d'autant moins qu'un certain nombre de tendances potentielles devra être examiné dans son contexte. Il revient aux décideurs politiques, aux développeurs de technologies, aux développeurs d'activités commerciales et à chacun d'entre nous d'examiner de manière sérieuse si, et le cas échéant de quelle manière, nous souhaitons influencer l'évolution de la technologie et de son application. Mais il est tout aussi important que l'UE examine d'urgence les questions de l'éthique et de la place que la dignité humaine doit occuper dans les technologies de l'avenir.

Les principes de protection des données ont prouvé leur capacité à protéger les personnes physiques et leur vie privée contre les risques liés au traitement irresponsable de données. Mais les tendances actuelles pourraient nécessiter une approche entièrement nouvelle. Nous ouvrons donc un nouveau débat sur la mesure dans laquelle l'application des principes comme l'équité et la légitimité est suffisante. La communauté de la protection des données peut jouer un rôle nouveau en utilisant des outils existants, comme les contrôles préalables et les autorisations; en effet, aucun autre organisme ne dispose des moyens nécessaires pour examiner ces traitements de données. Le développement à une vitesse vertigineuse de la technologie, de l'innovation à l'échelle mondiale et de la connectivité des personnes nous fournit l'occasion d'attirer l'attention, de susciter l'intérêt et de parvenir à un consensus.

Avec le présent avis, nous espérons fournir un cadre pour une discussion plus large et plus approfondie sur la manière dont l'UE peut assurer l'intégrité de ses valeurs tout en bénéficiant pleinement des avantages des nouvelles technologies.

Fait à Bruxelles, le 11 septembre 2015.

(**signé**)

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

Notes

[1] Source: GSMA Intelligence.

[2] La «loi de Moore» selon laquelle le nombre de transistors qu'il est possible de fixer sur un microprocesseur double tous les 18 mois s'est généralement révélée exacte; Moore, Gordon E. (19.04.1965). «Cramming more components onto integrated circuits», *Electronics*. 22.08.2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, «Reality mining: sensing complex social systems», *Journal Personal and Ubiquitous Computing*, volume 10, numéro 4, mars 2006, p. 255 à 268. Shoshana Zuboff, dans l'article «Big Other: surveillance capitalism and the prospects of an information civilization», *Journal of Information Technology* (2015) 30, p. 75 à 89, écrit: «En conséquence de la médiation informatique généralisée, presque chaque aspect du monde est présenté dans une nouvelle dimension symbolique, les événements, les objets, les processus et les personnes devenant visibles, reconnaissables et susceptibles d'être partagés d'une manière tout à fait nouvelle». Zuboff envisage «la naissance d'une nouvelle architecture universelle» qu'elle désigne par le nom de «Big Other», un régime d'institutions en réseau omniprésent qui enregistre, modifie et réduit au statut de marchandises les expériences quotidiennes, du grille-pain aux organismes et de la communication à la pensée, le tout en vue d'établir de nouvelles possibilités de monétisation et de bénéfices»; p. 77 et 81.

[4] «BBC Micro Bit computer's final design revealed», 07.07.2015, http://www.bbc.com/news/technology-33409311 (consulté le 10.09.2015); «No assembler required: How to teach computer science in nursery school», *The Economist*, 01.08.2015.

[5] Aucune des dix premières sociétés du secteur de la technologie par la capitalisation boursière n'a son siège dans l'UE (huit sont des sociétés américaines, une a son siège en Chine et une à Taiwan), selon le «classement mondial des dix premières sociétés par la capitalisation boursière» établi par PWC, mise à jour du 31 mars 2015.

[6] «Les mégadonnées renvoient à la croissance exponentielle de la disponibilité et de l'utilisation automatisée d'informations: elles renvoient à de gigantesques ensembles de données numériques détenus par les sociétés, les gouvernements et d'autres grandes organisations, qui sont ensuite analysées de manière approfondie (d'où le nom "analyse") en utilisant des algorithmes informatiques»; avis nº 03/2013 du groupe de travail «Article 29» sur la limitation de la finalité. Dans un rapport de la Maison Blanche de 2014, les mégadonnées étaient décrites comme «la capacité technique croissante de recueillir, d'agréger et de traiter un volume, une vitesse et une variété de données toujours plus importants», voir «Big Data: Seizing Opportunities, Preserving Values», Bureau exécutif du Président («Podesta report»), mai 2014.

[7] La législation de l'UE définit les «données à caractère personnel» comme suit: «toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale»; article 2, point a), de la directive 95/46/CE. Cette définition est largement comparable à celles qui ont été adoptées par le Conseil de l'Europe dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (désignée par le nom de «Convention 108») et par l'OCDE dans ses Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Pour une analyse approfondie, voir avis du groupe de travail «Article 29» nº 04/2007 sur le concept de données à caractère personnel, WP136.

[8] Voir, à titre d'exemple, le discours prononcé par la présidente de la Commission fédérale du commerce des États-Unis en 2014: «La prolifération des dispositifs connectés, la diminution importante des coûts liés à la collecte, au stockage et au traitement d'informations et la capacité des courtiers en données et d'autres personnes de combiner des données collectées en ligne et hors ligne signifient que les entreprises peuvent accumuler des quantités virtuellement illimitées d'informations

concernant les consommateurs et les stocker indéfiniment. L'analyse prédictive permet à ces entités d'apprendre un nombre de choses surprenant sur chacun de nous en se fondant sur ces informations»; observations introductives d'Edith Ramirez, présidente de la Commission fédérale du commerce des États-Unis, «Big Data: A Tool for Inclusion or Exclusion?», Washington, DC, 15 septembre 2014. Selon Sandy Pentland, «la physique sociale est une science sociale quantitative qui décrit des connexions fiables et mathématiques entre, d'une part, les informations et le flux d'idées, et d'autre part, le comportement des personnes [...] elle nous permet de prédire la productivité de petits groupes, de services au sein d'entreprises et même de villes entières». Il s'agit d'un élément «nécessaire pour mettre en place de meilleurs systèmes sociaux» (p. 4 et 7) et pour «permettre (aux fonctionnaires, aux responsables du secteur industriel et aux citoyens) d'utiliser les outils des incitations des réseaux sociaux pour *établir de nouvelles normes de comportement*» (p. 189) (caractères italiques ajoutés); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Eurobaromètre spécial nº 431 sur la protection des données, juin 2015, et rapport de l'enquête «Public Perceptions of Privacy and Security in the Post-Snowden Era» du Pew Research Center de janvier 2014. Une étude a révélé qu'en moyenne, la consultation d'un site Internet donne lieu à 56 occurrences de collecte de données (Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). Il ressort du rapport 2014 de la Maison Blanche sur les mégadonnées que «la puissance de calcul et la sophistication sans précédent [...] créent une asymétrie entre les pouvoirs respectifs des personnes qui détiennent les données et de celles qui les communiquent intentionnellement ou par inadvertance»; «certains des défis les plus importants apparus au cours de cette enquête concernent la manière dont l'analyse des mégadonnées peut [...] créer un environnement de prise de décision d'une opacité telle que l'autonomie individuelle est noyée dans un ensemble d'algorithmes impénétrable».

[10] En utilisant les données anonymes publiques issues du recensement de 1990, il serait certainement possible d'identifier 87 % de la population des États-Unis au moyen du code postal à cinq chiffres de ces personnes associé à leur sexe et à leur date de naissance; voir Paul Ohm «Broken promises of privacy: responding to the surprising failure of anonymisation», *UCLA Law Review* 2010 et «Record linkage and privacy: issues in creating new federal research and statistical info», avril 2011. L'ADN est unique (sauf dans le cas des vrais jumeaux) et demeure identique tout au long de la vie. Il contient des informations sur l'appartenance ethnique et sur les prédispositions à certaines maladies et il permet d'identifier d'autres membres de la famille. En janvier 2013, des chercheurs ont été en mesure d'identifier des personnes physiques et des familles à partir de données relatives à l'ADN anonymes figurant dans des bases de données généalogiques accessibles au public; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. et Erlich, Y., *Science* 339, 321–324 (2013). Voir également «Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts», 23.06.2014, http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (consulté le 10.09.2015). Voir également avis nº 04/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel; avis nº 03/2013 du groupe de travail «Article 29» sur la limitation de la finalité; avis nº 06/2013 du groupe de travail «Article 29» sur la réutilisation des informations du secteur public (ISP) et des données ouvertes; et avis nº 05/2014 du groupe de travail «Article 29» sur l'anonymisation.

[11] Source: Gartner.

[12] Voir, à titre d'exemple, «What is the future of official statistics in the Big Data era?», the Royal Statistical Society, Londres, 19 janvier 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (consulté le 10.09.2015).

[13] Dix technologies qui pourraient changer nos vies. Impacts potentiels et conséquences des politiques, Unité de la prospective scientifique, Service de recherche du Parlement européen, janvier 2015.

[14] Le programme de travail 2016-2017 d'Horizon 2020 de l'UE vient soutenir ces développements, notamment par la mise en place de pilotes à grande échelle destinés à examiner les préoccupations relatives à la protection de la vie privée et à l'éthique.

[15] Le secteur des assurances a été décrit comme «le modèle d'affaire natif pour l'Internet des objets»; «From fitness trackers to drones, how the "Internet of Things" is transforming the insurance industry», Business Insider 11.06.2015. La notion de discrimination par les prix existant en droit de la concurrence, tirée de l'article 102 du TFUE en application duquel il est interdit à une entreprise détenant une position dominante sur un marché d'«imposer de façon directe ou indirecte des prix d'achat ou de vente ou d'autres conditions de transaction non équitables», est extrêmement litigieuse; voir, à titre d'exemple, Damien Gerardin et Nicolas Petit Price «Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles» (juillet 2005), Global Competition Law Centre, collection de documents de travail, nº 07/05. Concernant les mégadonnées et leur capacité (non encore réalisée, selon les auteurs) à accélérer la mise en place de la tarification personnalisée, voir le rapport du bureau exécutif du président des États-Unis, «Big Data and Differential Pricing», février 2015, et une analyse récente dans laquelle il est conclu que la tarification personnalisée implique généralement le traitement de données à caractère personnel et doit donc respecter le principe de transparence prévu par le droit de la protection des données, en application duquel les sociétés sont tenues d'informer les personnes de la finalité du traitement de leur données à caractère personnel: si les sociétés personnalisent les prix, elles doivent l'indiquer. Et si une entreprise utilise un «cookie» pour reconnaître une personne, elle est tenue, en application de la directive «Vie privée et communications électroniques», d'informer la personne de la finalité de ce «cookie»; avant-projet de Frederik Borgesius «Online Price Discrimination and Data Protection Law». Disponible à l'adresse http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (consulté le 10.09.2015).

[16] Les dispositifs médicaux sont définis en droit de l'UE par la directive 93/42/CEE du Conseil, relative aux dispositifs médicaux modifiée par la directive 2007/47/CE du Parlement européen et du Conseil du 5 septembre 2007. Concernant les implications de la «santé mobile» en matière de protection des données, voir avis nº 1/2015 du CEPD.

[17] Selon Eurostat, 21 % des personnes physiques et 19 % des entreprises établies dans l'UE utilisent des services de stockage dématérialisé.

[18] «Si l'Internet mondial était un pays, il se placerait au 12e rang du classement des plus gros consommateurs d'énergie à l'échelle mondiale, quelque part entre l'Espagne et l'Italie. Ceci correspond à environ 1,1 % à 1,5 % de la consommation mondiale d'électricité (en 2010) et aux émissions de gaz à effet de serre annuelles de 70 à 90 grandes centrales électriques au charbon (500 mégawatts)». Natural Resources Defense Council, «Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers» 2014.

[19] Rapport de l'étude «SMART 2013/0043 – Uptake of Cloud in Europe».

[20] Source: Eurostat.

[21] Le terme «économie du partage» a été critiqué au motif qu'il serait trompeur: «The Sharing Economy Isn't About Sharing at All», Giana M. Eckhardt et Fleura Bardhi, *Harvard Business Review*, 28.01.2015.

[22] Rachel Botsman et Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Forum «Future of Privacy», «User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy», juin 2015.

[24] Voir atelier de travail du 9 juin 2015 de la Commission fédérale du commerce des États-Unis intitulé «Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy» https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (consulté le 10.09.2015).

[25] Concernant les implications des drones ou systèmes d'aéronefs télépilotés, voir avis du CEPD sur la communication de la Commission au Parlement européen et au Conseil intitulée «Une nouvelle ère de l'aviation. Ouvrir le marché de l'aviation à l'utilisation civile de systèmes d'aéronefs télépilotés, d'une manière sûre et durable», novembre 2014.

[26] Source: Boston Consulting Group.

[27] Gartner.

[28] Il a été indiqué que l'algorithme de reconnaissance faciale Facebook Deepface atteignait un taux de succès de 97 %, c'est-à-dire un taux supérieur à celui atteint par les personnes humaines; «DeepFace: Closing the Gap to Human-Level Performance in Face Verification», contribution publiée dans le compte rendu de la conférence «Computer Vision and Pattern recognition» de l'IEEE de juin 2014.

[29] Robo a été définie comme une «machine située dans le monde qui ressent, pense et agit»; Bekey, G., «Current trends in robotics: technology and ethics», dans «Robot Ethics – The ethical and social implications of robotics», *The MIT Press2*, 2012, p. 18. On estime que le nombre de robots de service vendus entre 2013 et 2016 atteindra 22 millions; IRF World Robotics Report, 2013. Concernant l'intelligence artificielle, voir «Rise of the Machines», *Economist*, 05.09.15 et le projet «Internet» du Pew Research Center de 2014. Une société exerçant son activité dans le domaine de l'intelligence artificielle a subordonné son acquisition par une société du secteur technologique de premier plan en 2014 à la mise en place d'un comité d'éthique et de sécurité et à l'interdiction de toute utilisation des travaux sur l'intelligence artificielle à des fins militaires ou de renseignement; Forbes, «Inside Google's Mysterious Ethics Board», 03.02.2014.

[30] Pentland, *Social physics*, p. 147

[31] Voir note 9 ci-dessus. Pentland, *Social Physics*, p. 153: «Il est possible de réaliser d'immenses progrès en matière de soins de santé, de transport, d'énergie et de sécurité... les principaux obstacles à l'atteinte de ces objectifs résident dans les préoccupations concernant le respect de la vie privée et dans le fait que nous ne sommes pas encore parvenus à un consensus sur l'arbitrage entre les valeurs personnelles et les valeurs sociales». Le débat intervenu autour de la pandémie du virus Ébola en Afrique de l'Ouest en 2014 est une illustration de la manière dont cette fausse dichotomie entre le respect de la vie privée et les besoins sociétaux s'établit. On observe une tendance à suivre des maladies et à mesurer leur durée au moyen d'enquêtes et de recensements qui deviennent facilement obsolètes et sur la base desquels il est difficile d'extrapoler pour prévoir les régions dans lesquelles les maladies apparaîtront à l'avenir. Il existe quelques exemples d'utilisation de «mégadonnées» pour suivre les épidémies de paludisme en Namibie et au Kenya, et, en 2009, pour suivre l'efficacité des avertissements sanitaires formulés par les pouvoirs publics au cours de la crise de la grippe porcine mexicaine. Les enregistrements d'appels passés à partir de téléphones mobiles, qui indiquent le relais de base qui a traité l'appel et qui peuvent fournir en temps réel la localisation et la destination approximatives des personnes, constituent l'une des sources de données. L'objectif n'est pas de réunir tous ces enregistrements – il n'est pas possible d'établir une distinction entre les interlocuteurs porteurs du virus Ébola et les autres. Une association à but non lucratif suédoise a établi une cartographie de la mobilité des populations en Afrique de l'Ouest, mais les données n'ont pas été utilisées car les opérateurs de téléphonie mobile ont refusé de les communiquer à des chercheurs externes en faisant valoir qu'ils devaient obtenir des instructions des gouvernements, lesquels ont fait part de préoccupations liées à de possibles atteintes à la vie privée qu'il n'était pas possible de justifier au titre du droit de l'UE; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola (consulté le 10.09.2015).

[32] Avis nº 3/2015 du CEPD.

[33] L'hypothèse selon laquelle, en matière de mégadonnées, «N=la totalité» renvoie à la nécessité d'examiner tous les éléments de données, et non pas uniquement un échantillon. Viktor Mayer-Schönberger et Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Le Lisbon Council et le Progressive Policy Institute ont fait valoir que l'optimisation de

la «densité numérique» – «le volume de données utilisées par habitant dans une économie» conduira à une plus grande prospérité; http://www.lisboncouncil.net/component/downloads/?id=1178 (consulté le 10.09.2015). Le Groupe de travail international sur la protection des données dans les télécommunications (désigné par le nom de «Groupe de Berlin») a proposé des dérogations aux principes de protection des données pour les mégadonnées; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (consulté le 10.09.2015). Le Forum économique mondial a appelé à se concentrer sur l'utilisation, et non pas sur la collecte, et à renoncer a l'exigence de consentement à la collecte de données à caractère personnel; «Unlocking the Value of Personal Data: From Collection to Usage», 2013.

[34] Voir avis préliminaire du CEPD sur la «[v]ie privée et [la] compétitivité à l'ère de la collecte de données massives».

[35] L'article 21 de la Charte des droits fondamentaux interdite «toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle». Nombre de ces catégories de données («qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle») bénéficient d'une protection renforcée en application de l'article 8 de la directive 95/46/CE.

[36] Sur l'idée de «communs» numériques, voir «Ambition numérique: Pour une politique française et européenne de la transition numérique», Conseil français du numérique, juin 2015, p. 276; Bruce Schneier plaide pour la création, sur l'Internet, d'«espaces publics ne faisant l'objet d'aucun droit de propriété», comparables à des parcs publics, *Data and Goliath*, p. 188 et 189; Sandy Pentland se prononce en faveur de «communs de données publics», *Social Physics*, p. 179. Sur l'appréciation du caractère sûr de la publication d'ensembles de données agrégées sous la forme de données ouvertes, voir avis nº 06/2013 du groupe de travail «Article 29» sur la réutilisation des informations du secteur public et des données ouvertes.

[37] «Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent» http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Sur la transparence qualifiée, voir, à titre d'exemple, Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] «Derrière les technologies qui ont une incidence sur les relations sociales, on retrouve ces mêmes relations sociales», David Noble, «Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools», *Case Studies in the Labor Process*, éd. Andrew Zimbalist, 1979. Voir également Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 p. 89 et 90; et Zuboff, «Big Other» (cité à la note 3 ci-dessus).

[39] Avis nº 05/2014 sur les techniques d'anonymisation adopté le 10 avril 2014 (WP 216.)

[40] Concernant l'interprétation étroite de l'exception aux règles de protection des données qui s'applique aux activités entreprises à des fins exclusivement personnelles ou domestiques, voir CJUE, arrêt dans l'affaire C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů.*

[41] Le terme «prosommateur» a été inventé par Alvin Toffler dans l'ouvrage *The Third Wave*, 1980. Pour une discussion sur l'«environnement de prosommateurs» et la manière dont celui-ci devrait être réglementé, voir Ian Brown et Chris Marsden, *Regulating Code*, 2013.

[42] Avis du Groupe européen d'éthique des sciences et des nouvelles technologies adressé à la Commission européenne: «L'éthique des technologies de sécurité et de surveillance», avis nº 28, 20.05.2015, p. 74.

[43]Voir, à titre d'exemple, *Homer Economicus: The Simpsons and Economics*, éd. Joshua Hall, 2014.

[44] Selon la définition la plus conservatrice du mot «erreur», cela signifie que 23 millions d'Américains ont fait l'objet d'un rapport sur le consommateur comportant des erreurs importantes. Cinq pour cent des participants à l'étude avaient dans leur rapport des erreurs dont la correction conduisait à une amélioration de leur cote de solvabilité dans une mesure telle qu'ils pouvaient obtenir un crédit à un coût moindre; Commission fédérale du commerce des États-Unis, rapport au Congrès conformément à l'article 319 de la «Fair And Accurate Credit Transactions Act» de 2003, décembre 2012; Chris Jay Hoofnagle, «How the Fair Credit Reporting Act Regulates Big Data» (10 septembre 2013). Forum «Future of Privacy», atelier de travail «Big Data and Privacy: Making Ends Meet», 2013. Consultable sur le site Internet du SSRN: http://ssrn.com/abstract=2432955.

[45] Le Forum économique mondial considère les données comme un actif précieux de la personne physique dont les droits de possession, d'utilisation et de renonciation peuvent être cédés à des entreprises et à des gouvernements en échange de services. Voir également les discours récents du vice-président de la Commission, M. Ansip, par exemple le discours prononcé le 07.09.2015 lors de la réunion annuelle de Bruegel intitulé «Productivity, innovation and digitalisation – which global policy challenges?» [en français, «Productivité, innovation et numérisation – quels sont les défis en matière de politique mondiale?»]: «La propriété et la gestion des flux de données, l'utilisation et la réutilisation des données. La gestion et le stockage des données. Ces éléments sous-tendent des secteurs émergents importants comme l'informatique dématérialisée, l'Internet des objets et les mégadonnées.»

[46] «Alors, qui possède le droit d'utiliser des informations et des données qui ne lui appartiennent pas réellement? Il s'agit d'une question qui dépasse les frontières du commerce, de l'éthique et de la morale, et qui conduit à des questions de vie privée et de protection de la vie privée»; Al-Khouri, novembre 2012, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Voir également Margaret Jane Radin, «Incomplete Commodification in the Computerized World», *The Commodification of Information* 3, 17, éd. Niva Elkin-Koren & Neil Weinstock Netanel, 2002: «Le point de savoir si la protection de la vie privée est considérée comme un droit relevant des droits de l'homme, attaché aux personnes en vertu de leur individualité, ou bien comme un droit de propriété, à savoir quelque chose que les personnes peuvent posséder et contrôler, fait une grande différence. Les droits de l'homme sont supposés incessibles sur le marché, tandis que les droits de propriété sont supposés cessibles sur le marché».

[47] Le projet «Computer Science and Artificial Intelligence Lab's Crosscloud» du MIT, qui bénéficie du soutien de plusieurs entreprises établies dans l'Union européenne, vise «1) à faciliter le développement de logiciels pluriutilisateurs ("sociaux") utilisant uniquement le développement de la partie client et respectueux des droits et de la vie privée des utilisateurs, et 2) à donner aux utilisateurs la liberté de passer librement d'une application, d'une plateforme matérielle et d'un réseau social à un autre en conservant leurs données et leurs connexions sur les sites sociaux»; http://openpds.media.mit.edu/#architecture (consulté le 10.09.2015).

[48] Voir explication ad article 1er de la Charte des droits fondamentaux.

[49] Martha Nussbaum, «Objectification», *Philopsophy and Public Affairs* 24.04.1995.

[50] Arrêt du 15 décembre 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Voir avis du Groupe européen d'éthique des sciences et des nouvelles technologies sur l'éthique et la surveillance, p. 75. Une étude a suggéré qu'un algorithme de ciblage publicitaire était discriminatoire: en moyenne, les résultats des recherches renvoyaient les visiteurs masculins des sites d'offres d'emploi vers des annonces pour des postes mieux payés que les visiteurs féminins de ces mêmes sites; Carnegie Mellon University et International Computer Science Institute. Sur la tendance à utiliser une voix par défaut féminine pour les assistants numériques, voir, à titre d'exemple, Judy Wajcman, «Feminist theories of technology». *Cambridge Journal of Economics*, 34 (1), p. 143 à 152, 2010.

[52] Giorgio Agamben, *State of Exception*, 2005.

[53] Neil Richards, Neil et Jonathan King, «Big Data Ethics» (19 mai 2014), *Wake Forest Law Review*, 2014.

[54] BBC, «Information watchdog investigates "charity data sales"», 01.09.2015.

[55] Voir courrier du Future of Life Institute. Encyclique papale *Laudato Si:* «les dynamiques des moyens de communication sociale et du monde digital, [...] en devenant omniprésentes, ne favorisent pas le développement d'une capacité de vivre avec sagesse, de penser en profondeur, d'aimer avec générosité. Les grands sages du passé, dans ce contexte, auraient couru le risque de voir s'éteindre leur sagesse au milieu du bruit de l'information qui devient divertissement. Cela exige de nous un effort pour que ces moyens de communication se traduisent par un nouveau développement culturel de l'humanité, et non par une détérioration de sa richesse la plus profonde. La vraie sagesse, fruit de la réflexion, du dialogue et de la rencontre généreuse entre les personnes, ne s'obtient pas par une pure accumulation de données qui finissent par saturer et obnubiler, comme une espèce de pollution mentale. En même temps, les relations réelles avec les autres tendent à être substituées, avec tous les défis que cela implique, par un type de communication transitant par Internet. Cela permet de sélectionner ou d'éliminer les relations selon notre libre arbitre, et il naît ainsi un nouveau type d'émotions artificielles, qui ont plus à voir avec des dispositifs et des écrans qu'avec les personnes et la nature. Les moyens actuels nous permettent de communiquer et de partager des connaissances et des sentiments. Cependant, ils nous empêchent aussi parfois d'entrer en contact direct avec la détresse, l'inquiétude, la joie de l'autre et avec la complexité de son expérience personnelle. C'est pourquoi nous ne devrions pas nous étonner qu'avec l'offre écrasante de ces produits se développe une profonde et mélancolique insatisfaction dans les relations interpersonnelles, ou un isolement dommageable.»

[56] Voir action nº 4 de la Stratégie du CEPD pour la période 2015-2020, développer une dimension éthique de la protection des données.