GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

1471/14/FR
WP 223

Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets

adopté le 16 septembre 2014

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL,

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de la directive précitée,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

RÉSUMÉ

L'internet des objets (IdO) est sur le point d'être intégré dans la vie des citoyens européens. La viabilité de bon nombre de projets dans l'IdO reste à confirmer mais il commence à exister des «objets intelligents», qui surveillent nos maisons, nos voitures, notre environnement de travail et nos activités physiques, et qui communiquent avec eux. Aujourd'hui déjà, des dispositifs connectés répondent avec succès aux besoins des citoyens de l'UE sur les vastes marchés de la quantification de soi et de la domotique. L'IdO recèle donc d'importantes opportunités de développement pour un grand nombre d'entreprises innovantes et créatives de l'UE, qu'elles soient grandes ou petites, qui opèrent sur ces marchés.

Le groupe de travail «Article 29» souhaite qu'il soit répondu à ces attentes, dans l'intérêt tant des citoyens que de l'industrie de l'UE. Toutefois, les avantages escomptés doivent également se plier aux nombreux défis en matière de respect de la vie privée et de la sécurité pouvant être associés à l'IdO. Beaucoup de questions se posent en ce qui concerne la vulnérabilité de ces dispositifs, souvent déployés en dehors d'une structure informatique traditionnelle et dépourvus d'une sécurité suffisante intégrée. Les pertes de données, une infection par un logiciel malveillant, mais aussi l'accès non autorisé aux données à caractère personnel, une utilisation intrusive de l'électronique vestimentaire ou une surveillance illicite constituent autant de risques auxquels les parties prenantes à l'IdO doivent apporter une réponse pour attirer d'éventuels utilisateurs finals de leurs produits ou services.

Au-delà de la conformité légale et technique, ce qui est en jeu en réalité, c'est la conséquence que cela peut avoir sur la société au sens large. Les organisations qui privilégient le respect de la vie privée et la protection des données dans le développement des produits seront bien placées pour garantir que leurs produits et services sont conformes aux principes de respect de la vie privée dès la conception et sont paramétrés par défaut de manière à favoriser la protection de la vie privée conformément aux attentes des citoyens de l'UE.

Pour le moment, cette analyse n'a été formulée qu'en termes très généraux par un certain nombre de régulateurs et de parties prenantes dans l'UE et ailleurs. Le groupe de travail «Article 29» a décidé d'aller plus loin en adoptant le présent avis. De la sorte, il entend contribuer à l'application uniforme du cadre juridique de la protection des données dans l'IdO ainsi qu'au développement d'un niveau de protection élevé des données à caractère personnel dans l'UE. La conformité à ce cadre est essentielle pour relever les défis juridiques, techniques mais aussi, puisqu'il se fonde sur la qualification de la protection des données en tant que droit humain fondamental, les défis sociétaux décrits ci-dessus.

Le présent avis identifie donc les principaux risques pour la protection des données qui résident dans l'écosystème de l'IdO avant de donner des orientations quant à la façon dont le cadre juridique de l'UE doit être appliqué dans ce contexte. Le groupe de travail est favorable à ce que les parties prenantes intègrent dans leurs projets les garanties les plus élevées possibles pour les utilisateurs individuels. Plus particulièrement, les utilisateurs doivent garder le contrôle total de leurs données à caractère personnel pendant toute la durée de vie du produit et, lorsque les organisations ont besoin de leur consentement pour procéder au traitement des données, ledit consentement doit être totalement éclairé, donné librement et spécifique. Afin de les aider à répondre à cet objectif, le groupe de travail a conçu un ensemble exhaustif de recommandations pratiques adressées aux différentes parties prenantes concernées (fabricants de dispositifs, développeurs d'application, plateformes sociales, autres destinataires des données, plateformes de données et organismes de normalisation) de manière à les aider à conformer leur produits et services aux exigences du respect de la vie privée et de la protection des données.

En effet, il est essentiel, pour soutenir la confiance et l'innovation et, partant, le succès sur ces marchés, d'autonomiser les personnes en veillant à ce qu'elles soient informées, libres et protégées. Le groupe de travail est fermement convaincu que les parties prenantes qui répondent à ces attentes détiendront un avantage concurrentiel particulièrement solide sur les autres acteurs dont les modèles d'entreprise consistent à laisser leurs clients ignorer dans quelle mesure leurs données sont traitées et partagées et à les enfermer dans leurs écosystèmes.

Compte tenu des importants défis en matière de protection des données que pose l'IdO, le groupe de travail «Article 29» continuera de surveiller son évolution. À cette fin, il reste ouvert à une coopération avec d'autres régulateurs et législateurs sur ces questions. Il reste également ouvert à la discussion avec des représentants de la société civile ainsi que des entreprises concernées, en particulier lorsque ces parties prenantes opèrent en tant que responsable du traitement des données ou sous-traitant chargé du traitement des données au sein de l'UE.

INTRODUCTION

La notion d'internet des objets (IdO) désigne une infrastructure dans laquelle des milliards de capteurs intégrés dans des dispositifs courants, quotidiens – des «objets» en tant que tels ou des choses liées à d'autres objets ou personnes – sont conçus pour enregistrer, traiter, conserver et transférer des données et, comme ils sont associés à des identifiants uniques, interagir avec d'autres dispositifs ou systèmes par un réseau. Étant donné que l'IdO se fonde sur le principe du traitement approfondi des données par ces capteurs, qui sont conçus pour communiquer discrètement et échanger des données de manière continue, il est étroitement lié à l'informatique dite «omniprésente» et «ubiquitaire».

Les parties prenantes de l'IdO visent à offrir de nouvelles applications et de nouveaux services par la collecte et la recombinaison de ces données relatives aux personnes – que ce soit afin de mesurer les données spécifiques à l'environnement de l'utilisateur «uniquement» ou afin d'observer et analyser spécifiquement ses habitudes. En d'autres termes, l'IdO implique généralement le traitement de données qui concernent des personnes physiques identifiées ou identifiables et, par conséquent, sont considérées comme des données à caractère personnel au sens de l'article 2 de la directive de l'UE sur la protection des données.

Le traitement de ces données dans ce contexte suppose l'intervention coordonnée d'un nombre significatif de parties prenantes (à savoir les fabricants de dispositifs – agissant également parfois comme plateformes de données; les agrégateurs de données ou courtiers en information; les développeurs d'applications; les plateformes sociales; les prêteurs ou loueurs de dispositifs, etc.). Les rôles respectifs de ces parties prenantes seront examinés plus en détail dans l'avis. Ces différentes parties prenantes peuvent être impliquées pour diverses raisons, à savoir pour fournir des fonctionnalités supplémentaires ou des interfaces de contrôle faciles à utiliser, qui permettent la gestion de paramètres techniques et relatifs à la vie privée, ou parce que l'utilisateur aura généralement accès à ses données collectées via une interface en ligne distincte. En outre, une fois que les données sont entreposées à distance, elles peuvent être partagées avec d'autres parties, parfois sans que la personne concernée n'en ait connaissance[1]. Le cas échéant, la transmission ultérieure de ses données est donc imposée à l'utilisateur qui ne peut l'empêcher sans désactiver la plupart des fonctionnalités du dispositif. Par suite de cette chaîne d'actions, l'IdO peut mettre les fabricants de dispositifs et leurs partenaires commerciaux en position de créer ou d'avoir accès à des profils d'utilisateurs très détaillés.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

À la lumière de ce qui précède, le développement de l'IdO pose clairement de nouveaux défis importants en matière de protection des données à caractère personnel et de respect de la vie privée[2]. En effet, en l'absence de contrôle, certaines évolutions de l'IdO pourraient aller jusqu'à développer une forme de surveillance des personnes qui pourrait être considérée comme illégale dans le cadre du droit de l'Union. L'IdO soulève également d'importantes préoccupations en matière de sécurité, étant donné que les incidents de sécurité peuvent entraîner des risques considérables en matière de respect de la vie privée pour les personnes dont les données sont traitées dans de tels contextes.

Le groupe de travail «Article 29» a dès lors décidé de publier le présent avis afin de contribuer à l'identification et au suivi des risques liés à ces activités, où les droits fondamentaux des citoyens de l'UE sont en jeu.

[2] Le présent avis doit être lu conjointement avec de précédents avis adoptés par le groupe de travail en 2014, à savoir ses avis sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif (WP211) et sur la surveillance (WP 215).

1. Portée de l'avis: attention particulière pour trois développements de l'IdO

À ce stade, il est impossible de prédire avec certitude la mesure dans laquelle l'IdO se développera. Cela tient en partie au fait que la question de savoir comment la transformation de toutes les données éventuellement collectées dans l'IdO en quelque chose d'utile, et partant commercialement viable, reste largement ouverte. La convergence et les synergies éventuelles de l'IdO avec d'autres développements technologiques tels que l'informatique en nuage et l'analyse prédictive qui, à ce stade, ne concernent que les développements sur les marchés émergents, ne sont pas claires non plus.

Le groupe de travail «Article 29» a dès lors décidé de se concentrer essentiellement, dans le présent avis, sur trois développements spécifiques de l'IdO (informatique vestimentaire, quantification de soi et domotique) qui 1) sont en interface directe avec l'utilisateur et 2) correspondent à des dispositifs et services qui sont effectivement utilisés, et qui se prêtent donc à une analyse conformément aux lois sur la protection des données. Le présent avis ne traite donc pas spécifiquement des applications B2B et de questions plus globales telles que les «villes intelligentes», les «transports intelligents» ainsi que les développements M2M («machine à machine»). Néanmoins, les principes et recommandations du présent avis peuvent s'appliquer en dehors de son champ d'application strict et couvrent ces autres développements dans l'IdO.

1.1 **Informatique vestimentaire**

L'informatique vestimentaire fait référence aux objets et vêtements du quotidien, tels que les montres et les lunettes, dans lesquels des capteurs ont été inclus afin d'étendre leurs fonctionnalités. Les objets vestimentaires sont susceptibles d'être adoptés rapidement car ils étendent l'utilité des objets du quotidien qui sont familiers à la personne – d'autant plus qu'il est difficile de les différencier des objets similaires non connectés. Ils peuvent intégrer des caméras, des microphones et des capteurs capables d'enregistrer et de transférer des données au fabricant du dispositif. En outre, la disponibilité d'un API pour les dispositifs vestimentaires (par exemple, Android Wear[3]) permet également la création d'applications par des tiers qui peuvent donc avoir accès aux données collectées par ces objets.

1.2 **Quantification de soi**

Les objets de la quantification de soi sont conçus pour être régulièrement portés par les personnes qui souhaitent enregistrer des informations concernant leurs propres habitudes et styles de vie. Par exemple, une personne pourrait souhaiter porter un traqueur de sommeil chaque nuit pour avoir une vue d'ensemble de ses rythmes de sommeil. D'autres dispositifs se concentrent sur le suivi des mouvements, tels que les compteurs d'activités qui mesurent et rapportent continuellement des indicateurs quantitatifs liés aux activités physiques des personnes, tels que les calories brûlées ou les distances parcourues, notamment.

Certains objets mesurent en outre le poids, le pouls et d'autres indicateurs de santé. En observant les tendances et les changements de comportement au fil du temps, il est possible d'analyser les données collectées afin d'en déduire des informations qualitatives relatives à la santé, y compris des appréciations sur la qualité et les effets de l'activité physique, basées sur des seuils prédéfinis et la présence probable de symptômes de maladie, dans une certaine mesure.

Les capteurs de la quantification de soi doivent souvent être portés dans des conditions spécifiques pour extraire les informations pertinentes. Par exemple, un accéléromètre placé sur la ceinture d'une personne concernée, avec les algorithmes appropriés, pourrait mesurer les mouvements de l'abdomen

[3] http://developer.android.com/wear/index.html

(données brutes), extraire des informations concernant le rythme respiratoire *(données agrégées et informations extraites)* et afficher le niveau de stress de la personne concernée *(données affichables)*. Sur certains dispositifs, seules ces dernières informations sont notifiées à l'utilisateur mais le fabricant du dispositif ou le prestataire du service peut avoir accès à beaucoup plus de données pouvant être analysées à un stade ultérieur.

La quantification de soi pose un défi en ce qui concerne les types de données collectées qui sont liées à la santé, et donc potentiellement sensibles, ainsi que la large collecte de telles données. En effet, étant donné que cette évolution s'attache à motiver les utilisateurs à rester en bonne santé, elle a de nombreux liens avec l'écosystème de la santé en ligne. Or, des recherches récentes ont contesté l'exactitude réelle des mesures et des conclusions tirées de ces mesures[4].

1.3 **Automatisation de l'habitat («domotique»)**

Aujourd'hui, les dispositifs IdO peuvent être placés dans des bureaux ou des habitations, sous la forme d'ampoules, de thermostats, de détecteurs de fumée, de baromètres, de machines à laver ou de fours «connectés», pouvant être contrôlés à distance sur l'internet. Par exemple, les objets contenant des capteurs de mouvements sont capables de détecter et enregistrer le moment où un utilisateur est chez lui, quels sont ses modèles de déplacement, et peuvent lancer des actions pré-identifiées spécifiques (par exemple, allumer la lumière ou modifier la température de la pièce). La plupart des dispositifs d'automatisation de l'habitat sont constamment connectés et peuvent retransmettre les données au fabricant.

À l'évidence, la domotique pose des défis spécifiques en matière de protection des données et de respect de la vie privée, étant donné qu'une analyse des profils d'utilisation dans un tel contexte est susceptible de révéler des détails, des habitudes ou des choix sur le style de vie des habitants ou simplement leur présence à domicile.

Les trois catégories de dispositifs répertoriés ci-dessus illustrent la plupart des principales questions en matière de respect de la vie privée qui sont liées à l'IdO dans son état actuel. Il convient de noter, cependant, que ces catégories ne sont pas exclusives: par exemple, un dispositif «vestimentaire» tel qu'une montre intelligente pourrait servir au suivi du rythme cardiaque, à savoir à une évaluation de la quantification de soi.

2. Défis relatifs au respect de la vie privée et à la protection des données liés à l'internet des objets

Le groupe de travail «Article 29» a décidé de publier le présent avis spécifique parce que l'IdO pose un certain nombre de défis importants en matière de respect de la vie privée et de protection des données, dont certains sont nouveaux et d'autres plus traditionnels mais accrus eu égard à l'augmentation exponentielle du traitement des données qu'implique son évolution. L'importance de l'application du cadre juridique de la protection des données de l'UE et les recommandations pratiques correspondantes ci-dessous doivent être considérées à la lumière de ces défis.

2.1 **Absence de contrôle et asymétrie de l'information**

Par suite de la nécessité de fournir des services omniprésents de manière discrète, les utilisateurs peuvent, en pratique, se retrouver sous la surveillance d'un tiers. Il peut en résulter des situations dans lesquelles l'utilisateur peut perdre tout contrôle sur la diffusion de ses données, selon que la collecte et le traitement de ses données sont ou non réalisés de manière transparente.

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

De façon plus générale, l'interaction entre les objets, entre les objets et les dispositifs des personnes, entre les personnes et d'autres objets et entre les objets et les systèmes de gestion entraînera la génération de flux de données pouvant difficilement être gérés avec les outils classiques utilisés pour assurer la protection adéquate des intérêts et des droits des personnes concernées. Par exemple, contrairement à d'autres types de contenu, les données amenées par l'IdO peuvent ne pas être adéquatement révisables par la personne concernée avant la publication, ce qui entraîne indéniablement un risque d'absence de contrôle et d'auto-exposition excessive pour l'utilisateur. De même, la communication entre les objets peut être déclenchée automatiquement ainsi que par défaut, sans que la personne n'en ait conscience. En l'absence de possibilité de contrôler efficacement la façon dont les objets interagissent ou de définir les frontières virtuelles en définissant des zones actives ou non actives pour des objets spécifiques, il deviendra extrêmement difficile de contrôler les flux de données générés. Il sera encore plus difficile de contrôler leur utilisation ultérieure et, partant, de prévenir un éventuel détournement d'usage. La question du manque de contrôle, qui concerne également d'autres évolutions techniques telles que l'informatique en nuage ou les mégadonnées, est encore plus difficile lorsque l'on songe que ces différentes technologies émergentes peuvent être utilisées conjointement.

2.2 **Qualité du consentement de l'utilisateur**

Dans de nombreux cas, l'utilisateur peut ne pas avoir conscience du traitement des données effectué par des objets spécifiques. Un tel manque d'informations constitue un obstacle significatif à la démonstration d'un consentement valide en vertu du droit de l'Union, étant donné que la personne concernée doit être informée. En pareilles circonstances, le consentement ne peut être invoqué en tant que base juridique pour le traitement des données correspondant en vertu du droit de l'Union.

Des dispositifs vestimentaires tels que les montres intelligentes ne sont pas non plus perceptibles[5]: la plupart des observateurs pourraient ne pas distinguer une montre normale d'une montre connectée, alors que cette dernière pourrait cependant intégrer des caméras, des microphones et des capteurs de mouvements capables d'enregistrer et de transférer des données sans que les personnes en aient conscience et consentent encore moins à un tel traitement. Cela pose la question de l'identification du traitement des données par l'informatique vestimentaire, laquelle pourrait être résolue en envisageant une signalisation appropriée qui serait effectivement visibles par les personnes concernées.

En outre, du moins dans certains cas, la possibilité de renoncer à certains services ou caractéristiques d'un dispositif IdO est davantage une notion théorique qu'une alternative réelle. De telles situations conduisent à se demander si le consentement de l'utilisateur au traitement des données sous-jacent peut être considéré comme libre, et donc valide, en vertu du droit de l'Union.

En outre, les mécanismes classiques utilisés pour obtenir le consentement des personnes peuvent être difficiles à appliquer dans l'IdO, entraînant un consentement de «faible qualité», basé sur une absence d'informations ou sur l'impossibilité matérielle de donner un consentement précis, conforme aux préférences exprimées par les personnes. Dans la pratique, il semble que les dispositifs des capteurs ne soient généralement conçus ni pour fournir des informations par eux-mêmes, ni pour offrir un mécanisme valide permettant d'obtenir le consentement de la personne. Or, de nouvelles façons d'obtenir le consentement valide de l'utilisateur doivent être envisagées par les parties prenantes de

[5] Comme décrit dans l'avis 02/2013 sur les applications destinées aux dispositifs intelligents, l'informatique vestimentaire met également en exergue des défis résultant de la collecte continue de données provenant de tiers situés à proximité immédiate et pendant des périodes prolongées.

l'IdO, y compris en mettant en œuvre des mécanismes de consentement par l'intermédiaire des dispositifs eux-mêmes. Des exemples spécifiques, tels que l'anonymisation et l'intermédiation et les *sticky policies* (politiques adhésives) sont mentionnés ci-après dans le présent document.

2.3 **Conclusions tirées des données et recentrage du traitement original**

L'augmentation du volume de données générées par l'IdO en combinaison avec des techniques modernes liées à l'analyse des données et au recoupement peuvent prêter aux données des utilisations secondaires, liées ou non à la finalité du traitement original. Des tiers sollicitant l'accès aux données collectées par d'autres parties peuvent donc souhaiter utiliser ces données à des fins totalement différentes.

Des données en apparence anodines, collectées par un dispositif (par exemple l'accéléromètre et le gyroscope d'un smartphone) peuvent alors être utilisées pour déduire d'autres informations ayant une signification totalement différente (par exemple, les habitudes de conduite de la personne). Cette possibilité de tirer des conclusions à partir de telles données «brutes» doit être associée aux risques classiques analysés en ce qui concerne la fusion de capteurs, un phénomène bien connu en informatique[6].

La quantification de soi illustre également la quantité d'informations pouvant être tirée des capteurs de mouvements par l'agrégation et l'analyse avancée. Ces dispositifs utilisent souvent des capteurs élémentaires pour recueillir des données brutes (par exemple, les mouvements de la personne concernée) et se fondent sur des algorithmes sophistiqués pour extraire des informations sensibles (par exemple, le nombre de pas) et en déduire des informations potentiellement sensibles qui seront présentées à l'utilisateur final (par exemple, sa condition physique).

Une telle tendance renferme des défis spécifiques. En effet, si l'utilisateur ne voyait aucune objection à partager les informations originales pour un objectif spécifique, il peut ne pas souhaiter partager ces informations secondaires qui pourraient être utilisées à des fins totalement différentes. Par conséquent, il est important qu'à chaque niveau (qu'il s'agisse des données brutes, extraites ou affichées), les parties prenantes de l'IdO s'assurent que les données sont utilisées à des fins qui soient toutes compatibles avec l'objectif original du traitement et que ces fins sont connues de l'utilisateur.

2.4 **Mise en évidence intrusive de comportements et profilage**

Même si différents objets collectent séparément des éléments d'information isolés, un volume suffisant de données collectées et ensuite analysées peut révéler des aspects spécifiques des habitudes, des comportements et des préférences de la personne. Comme indiqué ci-dessus, le fait de générer des connaissances à partir de données banales, voire anonymes, sera facilité par la prolifération des capteurs et favorisera d'importantes capacités de profilage.

En outre, l'analyse fondée sur des informations recueillies dans un environnement IdO pourrait permettre la détection de schémas encore plus détaillés et complets de la vie et du comportement d'une personne.

En effet, cette tendance est susceptible d'exercer un impact sur la façon dont la personne se comporte en réalité, de la même façon qu'il a été démontré que l'utilisation intensive de la télévision en circuit fermé (CCTV) a eu une influence correspondante sur le comportement du citoyen dans les espaces

[6] La fusion des capteurs consiste à combiner les données des capteurs ou les données issues de sources diverses afin d'obtenir de meilleures informations, plus précises que celles que fourniraient ces sources isolément.

publics. Avec l'IdO, cette surveillance potentielle pourrait à présent atteindre la sphère la plus privée de la vie des personnes, jusqu'à leur domicile. Cela incitera la personne à s'abstenir d'un comportement inhabituel afin d'éviter la détection de ce qui pourrait être perçu comme des anomalies. Une telle évolution serait très intrusive dans la vie privée et l'intimité des personnes et doit être très étroitement surveillée.

2.5 **Limitations de la possibilité de rester anonyme lors de l'utilisation des services**

Le développement complet des capacités de l'IdO pourrait exercer une pression sur les possibilités actuelles d'utilisation anonyme des services et limiter, de façon générale, la possibilité de passer inaperçu.

Par exemple, les objets vestimentaires conservés à proximité immédiate des personnes concernées entraînent la disponibilité d'une série d'autres identifiants, telles que les adresses MAC d'autres dispositifs qui pourraient être utiles pour générer une empreinte permettant la géolocalisation des personnes concernées. La collecte de multiples adresses MAC de multiples dispositifs dotés de capteurs contribuera à la création d'empreintes uniques et d'identifiants plus stables que les parties prenantes de l'IdO pourront attribuer à des personnes spécifiques. Ces empreintes et identifiants pourraient être utilisés pour une série d'objectifs, dont l'analyse de localisation[7] ou l'analyse des modèles de mouvements des foules et des personnes.

Une telle évolution doit être associée au fait que ces données peuvent être ultérieurement combinées à d'autres données provenant d'autres systèmes (par exemple, CCTV ou historique d'utilisation d'internet).

En pareils cas, certaines données de capteurs sont particulièrement vulnérables aux attaques de réidentification.

À la lumière de ce qui précède, il est évident qu'il sera de plus en plus difficile de rester anonyme et de préserver sa vie privée sur l'IdO. L'évolution de l'IdO entraîne d'importantes préoccupations en matière de protection des données et de respect de la vie privée à cet égard.

2.6 **Risques pour la sécurité: sécurité contre efficacité**

L'IdO pose plusieurs problèmes de sécurité étant donné que les contraintes de sécurité et de ressources forcent les fabricants de dispositifs à tenir compte de l'efficacité des batteries et de la sécurité des dispositifs. En particulier, on ne sait pas encore clairement quel compromis les fabricants de dispositifs trouveront entre la mise en œuvre des mesures de confidentialité, d'intégrité et de disponibilité à tous les niveaux de la séquence de traitement et la nécessité d'optimiser l'utilisation des ressources informatiques – et de l'énergie – par les objets et les capteurs.

Il existe dès lors un risque que l'IdO transforme un objet du quotidien en une cible potentielle en matière de respect de la vie privée et de sécurité des informations tout en répartissant ces cibles beaucoup plus largement que la version actuelle de l'internet. Des dispositifs connectés moins sécurisés peuvent représenter de nouveaux moyens d'attaque efficaces, parmi lesquels des moyens de surveillance aisés, des violations de données entraînant le vol ou la compromission de données à

[7] L'analyse de localisation désigne l'analyse du nombre de personnes qui sont présentes en un certain lieu à un moment donnée et la durée pendant laquelle elles y demeurent.

caractère personnel qui peuvent avoir des effets considérables sur les droits des consommateurs et la perception par la personne de la sécurité de l'IdO.

Les dispositifs et plateformes IdO sont également censés échanger des données et les enregistrer sur les infrastructures des prestataires de services. Par conséquent, la sécurité de l'IdO ne doit pas être envisagée uniquement sous l'angle de la sécurité des dispositifs mais aussi sous celui des liens de communication, de l'infrastructure de stockage et d'autres contributions de cet écosystème.

De même, la présence de différents niveaux de traitement dont la conception technique et la mise en œuvre sont assurées par différentes parties prenantes ne garantit pas la coordination adéquate entre toutes ces parties prenantes et peut entraîner l'existence de points faibles pouvant être mis à profit pour exploiter les vulnérabilités.

Par exemple, la plupart des capteurs actuellement sur le marché ne permettent pas d'établir un lien crypté pour les communications étant donné que les exigences informatiques auront un impact sur un dispositif limité par la faible puissance des batteries. En ce qui concerne la sécurité de bout en bout, le résultat de l'intégration des composants physiques et logiques fournis par un ensemble de parties prenantes différentes ne garantit que le niveau de sécurité offert par le composant le plus faible.

3. Applicabilité du droit de l'UE au traitement des données à caractère personnel dans l'IdO

3.1 Législation applicable

Le cadre juridique pertinent pour évaluer les problèmes de respect de la vie privée et de protection des données posés par l'IdO dans l'UE comprend la directive 95/46/CE ainsi que des dispositions spécifiques de la directive 2002/58/CE telle que modifiée par la directive 2009/136/CE.

Ce cadre s'applique lorsque les conditions de son applicabilité, telles qu'énoncées à l'article 4 de la directive 95/46/CE, sont réunies. Le groupe de travail a fourni des orientations détaillées concernant l'interprétation des dispositions de l'article 4, à savoir dans son avis 8/2010[8] sur le droit applicable.

Plus particulièrement, conformément à l'article 4, paragraphe 1, point a), de la directive, les dispositions nationales d'un État membre sont applicables aux traitements de données à caractère personnel lorsque le traitement est effectué «dans le cadre des activités d'un établissement» du responsable du traitement sur le territoire de l'État membre. Cette notion d'établissement dans le cadre de l'économie d'internet a été récemment interprétée de manière très large par la Cour de justice européenne[9].

Les dispositions nationales d'un État membre sont également applicables lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté mais recourt à des moyens situés sur le territoire dudit État membre [article 4, paragraphe 1, point c)]. Par conséquent, même lorsqu'une partie prenante de l'IdO qui est considérée comme un responsable du traitement en vertu de la directive 95/46/CE n'est pas établie dans l'UE au sens de l'article 4, paragraphe 1, point a) (qu'elle soit impliquée dans le développement, la distribution ou l'exploitation de dispositifs de l'IdO), elle restera susceptible d'être assujettie au droit de l'Union dans la mesure où elle traite des données collectées à l'aide de «moyens» d'utilisateurs situés dans l'UE.

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_fr.pdf
[9] Arrêt de la Cour (grande chambre) du 13 mai 2014 dans l'affaire C-131/12 (points 45 à 60)

En effet, tous les objets qui sont utilisés pour recueillir et ensuite traiter les données de la personne dans le cadre de la prestation de services dans l'IdO sont considérés comme des moyens au sens de la directive. Cette qualification s'applique manifestement aux dispositifs proprement dits (podomètres, traqueurs de sommeil, dispositifs domestiques «connectés» tels que thermostats, détecteurs de fumée, lunettes ou montres connectées, etc.). Elle s'applique également aux terminaux des utilisateurs (par exemple, smartphones ou tablettes) sur lesquels des logiciels ou des applications ont été précédemment installés à la fois pour surveiller l'environnement de l'utilisateur par des capteurs intégrés ou des interfaces de réseaux et ensuite envoyer les données collectées par ces dispositifs aux divers responsables du traitement impliqués.

L'identification du rôle des différentes parties prenantes impliquées dans l'IdO sera essentielle pour qualifier leur statut juridique en tant que responsables du traitement des données, et donc identifier la législation nationale applicable au traitement qu'elles mettent en œuvre, ainsi que leurs responsabilités respectives. La détermination du rôle des parties participant à l'IdO fera l'objet d'une analyse plus détaillée plus bas au point 3.3.

3.2 La notion de données à caractère personnel

Le droit de l'Union s'applique au traitement des données à caractère personnel tel que défini à l'article 2 de la directive 95/46/CE. Le groupe de travail a fourni des orientations détaillées concernant l'interprétation de cette notion, à savoir dans son avis 4/2007 sur le concept de données à caractère personnel[10].

Dans le contexte de l'IdO, il arrive souvent qu'une personne puisse être identifiée sur la base de données qui proviennent d'«objets». En effet, ces données peuvent révéler le style de vie d'une personne ou d'une famille spécifique – par exemple, les données générées par la commande centralisée de l'éclairage, du chauffage, de la ventilation et de la climatisation.

En outre, il est possible que même les données relatives aux personnes qui sont destinées à n'être traitées qu'après la mise en œuvre des techniques de pseudonymisation, voire d'anonymisation, doivent être considérées comme des données à caractère personnel. En fait, le grand volume de données traitées automatiquement dans le contexte de l'IdO entraîne des risques de ré-identification. Sur ce point, le groupe de travail fait référence aux évolutions pertinentes décrites dans son récent avis sur les techniques d'anonymisation, qui aide à identifier ces risques et formule des recommandations quant à la mise en œuvre de ces techniques[11].

3.3 Parties prenantes de l'IdO en tant que responsables du traitement des données basées dans l'UE

La notion de responsable du traitement et son interaction avec la notion de sous-traitant sont essentielles dans l'application de la directive 95/46/CE, étant donné qu'elles conditionnent les responsabilités respectives des diverses organisations impliquées dans la mise en œuvre d'un traitement des données eu égard aux règles de l'UE en matière de protection des données. Les parties prenantes peuvent se reporter à l'avis 1/2010 du groupe de travail sur les notions de «responsable du

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf

[11] Avis 05/2014 sur les techniques d'anonymisation, adopté le 10 avril 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

traitement» et de «sous-traitant»[12] qui fournit des orientations sur l'application de cette notion à des systèmes complexes avec de multiples acteurs, où de nombreux scénarios impliquent des responsables du traitement et des sous-traitants, seuls ou conjointement, avec différents degrés d'autonomie et de responsabilité.

En effet, la mise en œuvre de l'IdO implique fortuitement l'intervention conjointe de multiples parties prenantes – telles que les fabricants de dispositifs, les plateformes sociales, les applications de tiers, les prêteurs ou loueurs de dispositifs, les courtiers en information[13] ou les plateformes de données.

Le maillage complexe des parties prenantes impliquées requiert/suppose la nécessité d'une attribution précise des responsabilités légales parmi elles en ce qui concerne le traitement des données à caractère personnel des personnes, sur la base des spécificités de leurs interventions respectives.

3.3.1 Fabricants de dispositifs

Les fabricants de dispositifs dans l'IdO ne se bornent pas à vendre des articles physiques à leurs clients ou des produits blancs à d'autres organisations. Ils peuvent également avoir élaboré ou modifié le système d'exploitation «de l'objet» ou installé un logiciel déterminant sa fonctionnalité globale, y compris les données et la fréquence de la collecte, quand et à qui les données doivent être transmises pour quels objectifs (par exemple, des entreprises pourraient tarifer l'assurance de leur personnel sur la base des données notifiées par les traqueurs qu'elles leur font porter[14]). La plupart d'entre eux collectent et traitent effectivement des données à caractère personnel qui sont générées par le dispositif, pour des finalités et des moyens qu'ils ont totalement déterminés. Ils sont donc considérés comme des responsables du traitement des données en vertu du droit de l'Union.

3.3.2 Plateformes sociales

Les personnes concernées sont encore plus susceptibles d'utiliser les objets connectés lorsqu'elles peuvent partager ces données publiquement ou avec d'autres utilisateurs. Plus particulièrement, les utilisateurs de dispositifs de la quantification de soi ont tendance à partager des données avec d'autres sur les réseaux sociaux afin d'encourager une forme d'émulation au sein du groupe.

Un tel partage de données collectées et agrégées par des «objets» sur des réseaux sociaux aura souvent lieu automatiquement, une fois que l'utilisateur aura configuré l'application en ce sens. Ainsi, la capacité de partage appartient généralement aux paramètres par défaut standard fournis par le fabricant.

L'agrégation de ces rapports sur des plateformes sociales signifie que des responsabilités spécifiques en matière de protection des données s'appliquent désormais à ces plateformes. Ces données étant introduites sur ces plateformes par l'utilisateur, lorsqu'elles sont traitées par les réseaux sociaux à des fins différentes, qu'ils ont eux-mêmes déterminées, ces réseaux sont considérés comme des responsables du traitement de plein droit, en vertu du droit de l'Union. Par exemple, un réseau social

[12] Avis 01/2010 sur les notions de «responsable du traitement» et de «sous-traitant» adopté le 16 février 2010 (WP 169) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_fr.pdf

[13] Les courtiers en information achètent les données des entreprises afin d'établir une liste de personnes appartenant à une même catégorie ou un même groupe. Ces catégories et groupes sont établis par les courtiers en information mais peuvent refléter des caractéristiques démographiques, des revenus ou l'intérêt manifesté pour un sujet ou un produit spécifique.

[14] Avec des dispositifs de suivi, les employeurs peuvent suivre la santé des travailleurs http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

pourrait utiliser les informations collectées par un podomètre pour conclure qu'un utilisateur spécifique est un coureur régulier et lui présenter des publicités sur des chaussures de course. Les conséquences de cette qualification ont été détaillées dans l'avis du groupe de travail «Article 29» sur les réseaux sociaux.[15]

3.3.3 Développeurs d'applications de tiers

De nombreux capteurs exposent les interfaces de programmation pour faciliter le développement des applications. Pour utiliser ces applications, les personnes concernées doivent installer des applications de tiers qui leur permettent d'accéder à leurs données, telles que mémorisées par le fabricant de dispositifs. L'installation de ces applications revient souvent à donner un accès aux données au développeur de l'application au moyen de l'interface de programmation.

Certaines applications peuvent récompenser les utilisateurs d'objets spécifiques; par exemple, une application élaborée par une compagnie d'assurance maladie pourrait récompenser les utilisateurs d'«objets» de quantification de soi, ou une compagnie d'assurance habitation pourrait élaborer une application spécifique pour s'assurer que les alarmes incendie de ses clients sont correctement configurées. À moins que ces données ne soient correctement anonymisées, un tel accès constitue un traitement en vertu de l'article 2 de la directive 95/46/CE, de sorte que le développeur d'application qui a organisé cet accès aux données doit être considéré comme un responsable du traitement en vertu du droit de l'Union.

Ces applications sont traditionnellement installées sur la base d'une démarche volontaire. En effet, étant donné qu'un tel accès est soumis à l'obligation d'obtenir le consentement préalable de l'utilisateur, ce consentement doit être clairement donné, spécifique et éclairé. La pratique montre, cependant, que souvent les demandes d'autorisation faites par des développeurs d'applications de tiers ne présentent pas les informations suffisantes pour que le consentement de l'utilisateur soit considéré comme spécifique et suffisamment éclairé, et donc valide en vertu du droit de l'Union (voir ci-dessous).

3.3.4 Autres tiers

D'autres tiers que les fabricants de dispositifs et les développeurs d'applications de tiers pourraient utiliser les dispositifs IdO afin de recueillir et traiter des informations sur les personnes. Par exemple, les compagnies d'assurance pourraient souhaiter donner des podomètres afin de surveiller la fréquence à laquelle elles font de l'exercice[16] et adapter leurs primes d'assurance en conséquence.

Contrairement aux fabricants de dispositifs, ces tiers n'ont aucun contrôle sur le type de données collectées par l'objet. Or, ils sont considérés comme responsables du traitement des données pour ce traitement, dans la mesure où ils collectent et stockent les données générées par ces dispositifs IdO à des fins spécifiques qu'ils ont eux-mêmes déterminées.

Exemple: Une compagnie d'assurance lance un nouveau défi et offre un podomètre aux souscripteurs qui souhaitent demander des prix moins élevés. Les souscripteurs qui acceptent l'offre reçoivent un podomètre configuré et enregistré par la compagnie. Alors que les souscripteurs peuvent accéder aux données enregistrées par leur podomètre, les dispositifs eux-mêmes appartiennent à «FeelGood», qui a

[15] Avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009 (WP 163) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_fr.pdf

[16] Les employeurs peuvent suivre la santé des travailleurs au moyen de dispositifs de suivi, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

également accès aux données de ses souscripteurs. Dans ce contexte, les souscripteurs doivent être considérés comme les personnes concernées et se voir accorder l'accès à leur compte sur l'application de comptage des pas, tandis que la compagnie d'assurance est considérée comme le responsable du traitement.

3.3.5 Plateformes de données IdO

En raison d'une absence de normalisation et d'interopérabilité, l'Internet des Objets est parfois perçu comme un «Intranet des Objets» dans lequel chaque fabricant a défini son propre ensemble d'interfaces et format de données. Les données sont alors hébergées dans des environnements cloisonnés, ce qui empêche effectivement les utilisateurs de transférer (voire de combiner) leurs données d'un dispositif à un autre.

Or, les smartphones et les tablettes sont devenus les passerelles naturelles des données collectées au moyen de nombreux dispositifs IdO vers l'internet. Par conséquent, les fabricants ont progressivement développé des plateformes qui visent à héberger les données collectées au moyen de ces différents dispositifs afin de centraliser et simplifier leur gestion.

Ces plateformes peuvent également être considérées comme des responsables du traitement en vertu de la législation de l'UE sur la protection des données, lorsque l'élaboration de ces services implique en réalité que ces plateformes collectent les données à caractère personnel des utilisateurs à des fins propres.

3.4 Les personnes physiques en tant que personnes concernées: abonnés, utilisateurs, non-utilisateurs

Les abonnés et, de manière plus générale, les utilisateurs de l'IdO sont considérés comme des personnes concernées en vertu du droit de l'UE. Si les données qu'ils collectent et mémorisent sont exclusivement utilisées à des fins personnelles ou domestiques, ils relèvent de l'«exemption domestique» visée dans la directive 95/46/CE[17]. Toutefois, dans la pratique, le modèle d'entreprise de l'IdO implique que les données de l'utilisateur sont systématiquement transférées aux fabricants de dispositifs, développeurs d'application et autres tiers qui sont considérés comme responsables du traitement. L'«exemption domestique» sera dès lors d'une application limitée dans le contexte de l'IdO.

Le traitement des données dans l'IdO peut également concerner des personnes qui ne sont ni des abonnés ni des utilisateurs effectifs de l'IdO. Par exemple, des dispositifs vestimentaires tels que des lunettes intelligentes sont susceptibles de collecter des données sur d'autres personnes concernées que le propriétaire du dispositif. Il est important de souligner que ce facteur n'empêche pas le droit de l'Union de s'appliquer à de telles situations. L'application des règles européennes en matière de protection des données n'est pas conditionnée par la propriété d'un dispositif ou d'un terminal mais par le traitement des données à caractère personnel proprement dites, quelle que soit la personne concernée par ces données.

4. Obligations pesant sur les parties prenantes de l'IdO

Les parties prenantes de l'IdO considérées comme responsables du traitement (seules ou conjointement avec d'autres) en vertu du droit de l'Union doivent satisfaire aux différentes obligations qui pèsent sur elles en application de la directive 95/46/CE et des dispositions pertinentes de la directive 2002/58/CE le cas échéant. Le présent avis traite uniquement de l'application des dispositions qui méritent une

[17] Voir avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009 (WP 163)

attention spécifique dans ce contexte, mais cette portée limitée n'exclut pas l'application des autres dispositions restantes.

4.1 Application de l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques»

L'article 5, paragraphe 3, de la directive 2002/58/CE est applicable aux situations dans lesquelles une partie prenante de l'IdO stocke ou obtient l'accès à des informations déjà stockées sur un dispositif IdO, dans la mesure où les dispositifs IdO sont considérés comme un «équipement terminal» au sens de cette disposition[18]. Cette disposition exige que l'abonné ou l'utilisateur concerné consente à ce stockage ou accès pour que ces actions soient légitimes, à moins qu'elles ne soient «strictement nécessaires à la fourniture d'un service expressément demandé par l'abonné ou l'utilisateur»[19]. Cette exigence est particulièrement importante étant donné que des parties prenantes autres que l'utilisateur ou l'abonné peuvent avoir accès aux données sensibles à caractère privé qui sont stockées sur cet équipement terminal[20].

L'exigence de consentement à l'article 5, paragraphe 3, concerne principalement le fabricant de dispositifs, mais aussi toutes les parties prenantes qui souhaitent avoir accès à ces données brutes agrégées stockées dans cette infrastructure. Cela s'applique également à tout responsable du traitement des données qui souhaite enregistrer des données supplémentaires sur le dispositif d'un utilisateur.

En pareilles circonstances, les parties prenantes de l'IdO doivent s'assurer que la personne concernée a effectivement consenti à ce stockage et/ou accès après avoir obtenu des informations claires et détaillées du responsable du traitement concernant, notamment, les objectifs du traitement.

Par conséquent, le consentement de l'utilisateur doit avoir été obtenu avant d'accéder aux informations pouvant être utilisées pour générer une empreinte de tout dispositif (y compris les dispositifs vestimentaires). Le groupe de travail a déjà publié des orientations sur la notion de consentement pour les témoins de connexion (*cookies*) ou des technologies de suivi similaires dans son document de travail 02/2013 (WP-208) et il fournira de nouvelles orientations sur cette question dans son futur avis sur l'empreinte.

Exemple: Un podomètre enregistre le nombre de pas effectués par son utilisateur et enregistre ces informations dans sa mémoire interne. L'utilisateur a installé une application sur son ordinateur pour télécharger directement le nombre de pas à partir de son dispositif. Si le fabricant du dispositif souhaite télécharger les données provenant des podomètres sur ses serveurs, il doit obtenir le consentement de l'utilisateur en vertu de l'article 5, paragraphe 3, de la directive 2002/58/CE.

Une fois que le fabricant du dispositif a téléchargé les données sur ses serveurs, il conserve uniquement les données agrégées concernant le nombre de pas par minute. Une application sollicitant l'accès à ces données, dans la mesure où elle est stockée sur le serveur du fabricant de dispositifs, n'est alors pas soumise à l'article 5, paragraphe 3, de la directive «Vie privée et communications électroniques» mais aux dispositions de la directive 95/46/CE relative au caractère légitime de ce nouveau traitement.

[18] La notion d'«équipement terminal» à l'article 5, paragraphe 3, doit être comprise de la même manière que celle d'«équipement» à l'article 4, paragraphe 1, point c).
[19] Avis 02/2013 sur les applications destinées aux dispositifs intelligents (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf
[20] Voir considérant 25 de la directive 2002/58/CE

En outre, le propriétaire d'un dispositif IdO et la personne dont les données seront suivies (la personne concernée) pourraient être des personnes différentes. Cette situation peut donner lieu à une application distribuée de l'article 5, paragraphe 3 de la directive 2002/58/CE et de la directive 95/46/CE.

Exemple: Un service de location de voitures installe un dispositif intelligent de suivi des véhicules dans ses voitures de location. Bien que le service de location de voitures soit considéré comme le propriétaire/abonné du dispositif/service de suivi, la personne qui loue la voiture est considérée comme l'utilisateur du dispositif. L'article 5, paragraphe 3, exige dès lors du fabricant de dispositif qu'il obtienne (au moins) le consentement de l'utilisateur du dispositif, en l'espèce la personne qui loue la voiture. En outre, la légitimité du traitement des données à caractère personnel relatives aux personnes qui louent des voitures sera soumise aux exigences distinctes de l'article 7 de la directive 95/46/CE.

4.2 **Base juridique pour le traitement (article 7 de la directive 95/46/CE)**

Les parties prenantes de l'IdO qui sont considérées comme responsables du traitement (voir la section 4.3 ci-dessus) doivent satisfaire aux exigences visées à l'article 7 de cette directive pour que le traitement des données à caractère personnel soit licite. Ces exigences s'appliquent à certaines de ces parties prenantes, outre l'application de l'article 5, paragraphe 3, lorsque le traitement en cause va au-delà du stockage de, ou de l'obtention de l'accès aux informations stockées dans l'équipement terminal de l'utilisateur/abonné[21].

Dans la pratique, trois bases juridiques sont pertinentes dans ce contexte.

Le consentement [article 7, point a)], est la première base juridique qui doit en principe être invoquée dans le contexte de l'IdO, que ce soit par les fabricants de dispositifs, les plateformes sociales ou de données, les prêteurs de dispositifs ou les tiers développeurs. Le groupe de travail a également publié, à plusieurs reprises, des orientations sur l'application simultanée des exigences de l'article 7, point a), et de l'article 5, paragraphe 3, de la directive 2002/58/CE[22]. Les conditions pour qu'un tel consentement soit valide en vertu du droit de l'Union ont également été précisées dans un précédent avis du groupe de travail[23].

L'article 7, point b), prévoit également que le traitement est licite s'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. La portée de cette disposition est limitée par le critère de «nécessité», qui exige un lien direct et objectif entre le traitement proprement dit et les objectifs de l'exécution contractuelle attendue de la personne concernée.

Troisièmement, l'article 7, point f), permet le traitement des données à caractère personnel lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée – notamment son droit au respect de la vie

[21] Concernant l'articulation de l'article 5, paragraphe 3, et de l'article 7, point a), voir notamment l'avis 02/2013 sur les applications destinées aux dispositifs intelligents, adopté le 27 février 2013 (WP202) - (pages 14 et suivantes) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf et l'avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP217) – (p. 26, 32 et 46)

[22] Avis WP202, pages 14 et suivantes.

[23] Avis 15/2011 sur la définition du consentement, adopté le 3 juillet 2011 (WP187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf

privée en ce qui concerne le traitement des données à caractère personnel –, qui appellent une protection au titre de l'article 1er paragraphe 1.

Dans son arrêt rendu dans l'affaire *Google Spain*[24], la Cour de justice de l'Union européenne a fourni des orientations substantielles sur l'interprétation de cette disposition, outre celles déjà fournies dans les précédentes affaires jointes ASNEF et FECEMD (C-468/10 et C-469/10). Dans le contexte de l'IdO, le traitement des données à caractère personnel d'une personne est susceptible de porter gravement atteinte à ses droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque, sans les dispositifs IdO, les données n'auraient pu être interconnectées ou seulement avec une grande difficulté. De telles situations peuvent se présenter lorsque les données collectées concernent l'état de santé, le domicile ou l'intimité de la personne, sa localisation et de nombreux autres aspects de sa vie privée. À la lumière de la gravité potentielle de cette interférence, il est clair qu'un tel traitement peut difficilement se justifier par l'intérêt économique poursuivi par une partie prenante dans ce traitement. D'autres intérêts poursuivis par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées doivent intervenir[25].

Exemple: Dans le cadre d'un plan visant à promouvoir l'utilisation des transports publics et réduire la pollution, le conseil municipal souhaite réglementer le stationnement dans le centre-ville en imposant des restrictions d'accès ainsi que des frais de stationnement. Le montant des frais dépend de divers paramètres, dont le type de moteur (diesel, essence, électrique) et l'âge du véhicule. Lorsqu'un véhicule approche d'un emplacement de parking libre, un capteur peut lire la plaque d'immatriculation afin de calculer, après vérification avec une base de données, la surtaxe ou la remise à appliquer automatiquement conformément à des critères prédéfinis. En l'espèce, le traitement des informations relatives à la plaque d'immatriculation pour déterminer le montant peut satisfaire l'intérêt légitime du responsable du traitement. Un traitement ultérieur, tel que l'obtention d'informations – non anonymisées – concernant la circulation des véhicules dans l'espace restreint exigerait l'application d'une autre base juridique.

4.3 **Principes relatifs à la qualité des données**

Considérés conjointement, les principes consacrés à l'article 6 de la directive 95/4/CE constituent une pierre angulaire de la législation européenne en matière de protection des données.

Les données à caractère personnel doivent être collectées et traitées loyalement et licitement. Le principe de loyauté exige spécifiquement que les données à caractère personnel ne soient jamais collectées et traitées sans que la personne n'en ait réellement conscience. Cette exigence est d'autant plus importante en ce qui concerne l'IdO que les capteurs sont en réalité conçus pour être discrets, c'est-à-dire aussi invisibles que possible. Or, les responsables du traitement agissant dans l'IdO (en premier lieu les fabricants de dispositifs) doivent informer toutes les personnes situées à proximité géographique ou numérique des dispositifs connectés lorsque des données qui se rapportent à elles ou à leur environnement sont collectées. Le respect de cette disposition va au-delà d'une stricte exigence légale: une collecte loyale fait partie des attentes les plus cruciales de l'utilisateur en ce qui concerne l'IdO, notamment l'informatique vestimentaire.

Exemple: Un dispositif relatif à la santé utilise une petite lumière pour surveiller la façon dont le sang coule dans les veines et obtenir des informations sur le rythme cardiaque. Le dispositif inclut un autre

[24] Arrêt de la Cour (grande chambre) du 13 mai 2014 dans l'affaire C-131/12 (points 74 et suivants).
[25] Avis WP217

capteur qui mesure le niveau d'oxygène dans le sang, mais aucune information n'est disponible sur cette collecte de données, ni sur le dispositif, ni sur l'interface de l'utilisateur. Même si le capteur d'oxygène dans le sang est pleinement fonctionnel, il ne peut être activé sans informer d'abord l'utilisateur. Un consentement explicite sera requis pour activer ce capteur.

Le principe de limitation de la finalité implique que les données ne peuvent être collectées que pour des finalités spécifiques, explicites et légitimes. Tout autre traitement qui serait incompatible avec ces finalités originales serait illicite en vertu du droit de l'Union. Ce principe vise à permettre aux utilisateurs de savoir comment et pour quelles finalités leurs données seront utilisées et de décider de confier ou non leurs données à un responsable du traitement. Ces finalités doivent être définies *avant* que le traitement des données n'ait lieu, ce qui exclut des modifications soudaines des conditions essentielles du traitement. Cela suppose que les parties prenantes de l'IdO aient une bonne vue d'ensemble de leur dossier avant de commencer à collecter des données à caractère personnel.

De même, les données collectées sur la personne concernée doivent être strictement nécessaires pour la finalité spécifique précédemment déterminée par le responsable du traitement (le principe de la «minimisation des données»). Les données qui ne sont pas nécessaires à cette fin ne doivent pas être collectées et stockées «au cas où» ou parce qu'elles «pourraient être utiles plus tard». Certaines parties prenantes considèrent que le principe de minimisation des données peut limiter des opportunités potentielles de l'IdO et donc être un obstacle pour l'innovation au motif qu'une analyse exploratoire visant à trouver des corrélations et tendances non évidentes pourrait révéler des avantages potentiels du traitement des données. Le groupe de travail ne peut partager cette analyse et insiste sur le fait que le principe de la minimisation des données joue un rôle essentiel pour la garantie des droits en matière de protection des données conférés aux personnes par le droit de l'Union, de sorte qu'il doit être respecté en tant que tel[26]. Ce principe implique spécifiquement que lorsque des données à caractère personnel ne sont pas nécessaires pour fournir un service précis sur l'IdO, la personne concernée doit au moins se voir offrir la possibilité d'utiliser le service de façon anonyme.

L'article 6 exige également que les données à caractère personnel collectées et traitées dans le contexte de l'IdO ne soient pas conservées plus longtemps que nécessaire pour la réalisation de la finalité pour laquelle les données ont été collectées ou traitées ultérieurement. Ce critère de la nécessité doit être appliqué par chaque partie prenante lors de la fourniture d'un service spécifique sur l'IdO, étant donné que les finalités de leur traitement respectif peuvent en réalité être différentes. Par exemple, des données à caractère personnel communiquées par un utilisateur lorsqu'il s'abonne à un service spécifique sur l'IdO doivent être supprimées dès que l'utilisateur met un terme à son abonnement. De même, les informations supprimées par l'utilisateur sur son compte ne doivent pas être conservées. Lorsqu'un utilisateur n'utilise pas le service ou l'application pendant une certaine période, le profil de l'utilisateur doit être paramétré comme étant inactif. Après une autre période, les données doivent être supprimées. L'utilisateur doit être informé avant que ces mesures ne soient prises, par tout moyen dont dispose la partie pertinente concernée.

[26] En tout état de cause, une recherche exploratoire n'est jamais opérée de façon totalement aléatoire dans la pratique: l'objectif général de toute recherche est traditionnellement défini, à tout le moins en partie, ne serait-ce que pour des motifs organisationnels et budgétaires. Il est difficile de concevoir que le traitement de données pour une recherche spécifique soit compatible avec la finalité originale de la collecte des données, ce qui le rend alors contraire au droit de l'Union.

4.4 **Traitement des données sensibles (article 8)**

Des applications dans l'IdO peuvent traiter des données à caractère personnel pouvant révéler une origine raciale ou ethnique, des opinions politiques ou des convictions philosophiques, une appartenance syndicale, un état de santé ou des orientations sexuelles, qui sont effectivement considérées comme des «données sensibles» méritant une protection particulière au sens de l'article 8 de la directive 95/46/CE. Dans la pratique, l'application de l'article 8 aux données sensibles dans l'IdO exige que les responsables du traitement obtiennent le consentement explicite de l'utilisateur, à moins que la personne concernée n'ait elle-même rendu les données publiques.

Une telle situation est susceptible de se présenter dans des contextes spécifiques tels que les dispositifs de quantification de soi. Dans ces situations, les dispositifs concernés enregistrent essentiellement des données relatives au bien-être de la personne. Ces données ne constituent pas nécessairement des données sur la santé en tant que telles, mais elles peuvent rapidement fournir des informations sur la santé de la personne étant donné qu'elles sont enregistrées dans le temps et permettent donc de tirer des conclusions de leur variabilité sur une période donnée. Les responsables du traitement doivent prévoir ce changement possible de qualification et prendre des mesures adéquates en conséquence.

Exemple: La société X a développé une application qui, en analysant les données brutes des signaux d'un électrocardiogramme générés par des capteurs commerciaux couramment disponibles pour les consommateurs, est capable de détecter des schémas d'addiction aux drogues. Le moteur de l'application peut extraire des caractéristiques spécifiques des données brutes de l'ECG qui, selon de précédents résultats d'examen, sont liées à la consommation de drogues. Le produit, compatible avec la plupart des capteurs sur le marché, pourrait être utilisé en tant qu'application autonome ou au moyen d'une interface en ligne exigeant le chargement des données. Le consentement explicite de l'utilisateur doit être recueilli pour traiter les données à cette fin. Le respect de cette exigence de consentement peut être satisfait aux mêmes conditions et au même moment que lorsque le consentement est recueilli auprès de la personne concernée en vertu de l'article 7, point a).

4.5 **Obligations de transparence (articles 10 et 11)**

Outre l'exigence d'une collecte loyale des données visée à l'article 6, point a), les responsables du traitement doivent communiquer des informations spécifiques aux personnes concernées en application des articles 10 et 11: l'identité du responsable du traitement, les finalités du traitement, les destinataires des données, l'existence de leurs droits d'accès et du droit de s'opposer (lequel inclut des informations sur la façon de déconnecter l'objet afin de prévenir la divulgation d'autres données).

En fonction des applications, ces informations pourraient être fournies, par exemple, sur l'objet lui-même, à l'aide de la connectivité sans fil pour diffuser les informations, ou en utilisant la localisation au moyen de tests de proximité respectueux de la vie privée effectués par un serveur centralisé afin d'informer les utilisateurs qui sont situés près du capteur.

Ces informations doivent en outre être fournies de manière claire et compréhensible, conformément au principe du traitement loyal. Par exemple, le fabricant de dispositifs pourrait imprimer sur des objets équipés de capteurs un code QR ou code flash décrivant le type de capteurs et les informations qu'ils saisissent ainsi que les finalités de ces collectes de données.

4.6 **Sécurité (article 17)**

L'article 17 de la directive relative à la protection des données prévoit que le responsable du traitement «*doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données*

à caractère personnel» et que «*le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer*».

En conséquence, toute partie prenante considérée comme responsable du traitement des données reste pleinement responsable de la sécurité du traitement des données. Si des lacunes en matière de sécurité entrainant des violations du principe de sécurité résultent d'une conception ou maintenance inadéquate des dispositifs utilisés, cela engage la responsabilité du responsable du traitement. En ce sens, il est nécessaire pour ces responsables du traitement de procéder à des évaluations de la sécurité des systèmes dans leur ensemble, y compris au niveau des composants, en appliquant les principes de la sécurité des composants. Dans le même ordre d'idée, l'utilisation d'une certification pour les dispositifs ainsi que l'alignement sur des normes de sécurité reconnues au niveau international doivent être mis en œuvre afin d'améliorer la sécurité globale de l'écosystème de l'IdO.

Les sous-traitants qui conçoivent et fabriquent des composants de matériel pour le compte d'autres parties prenantes, sans effectivement traiter de données à caractère personnel, ne peuvent, à strictement parler, être tenus pour responsables en vertu de l'article 17 de la directive 95/46/CE en cas de violation de la protection des données en raison d'une lacune dans la sécurité de ces dispositifs. Toutefois, ces parties prenantes jouent un rôle clé dans le maintien de la sécurité de l'écosystème de l'IdO. Les parties prenantes qui supportent des responsabilités directes en matière de protection des données à l'égard des personnes concernées doivent s'assurer que ces sous-traitants sont effectivement liés par des normes de sécurité élevées en ce qui concerne le respect de la vie privée lors de la conception et de la fabrication de leurs produits.

Comme mentionné précédemment, des mesures de sécurité doivent être mises en œuvre en tenant compte des contraintes opérationnelles spécifiques des dispositifs IdO. Par exemple, aujourd'hui, la plupart des capteurs ne sont pas en mesure d'établir un lien crypté en raison de la priorité accordée à l'autonomie physique du dispositif ou à la maîtrise des coûts.

En outre, les dispositifs opérant dans l'IdO sont difficiles à sécuriser, tant pour des raisons techniques que pour des raisons commerciales. Étant donné que leurs composants utilisent généralement une infrastructure de communication sans fil et se caractérisent par des ressources limitées en termes d'énergie et de puissance informatique, les dispositifs sont vulnérables aux attaques physiques, à l'écoute clandestine ou aux attaques secrètes. Les technologies les plus communes actuellement utilisées – à savoir les infrastructures à clés publiques – ne sont pas facilement supportées par les dispositifs IdO étant donné que la plupart des dispositifs ne disposent pas de la puissance informatique nécessaire pour faire face aux tâches de traitement requises. L'IdO implique une chaîne logistique complexe, avec de multiples parties prenantes assumant différents degrés de responsabilité. Une atteinte à la sécurité pourrait trouver ses origines chez n'importe laquelle de ces parties, notamment compte tenu des environnements M2M basés sur l'échange de données entre dispositifs. Par conséquent, il convient de prendre en considération la nécessité d'utiliser des protocoles sécurisés et légers, pouvant être utilisés dans des environnements à faibles ressources.

Dans ce contexte, lorsque la capacité informatique réduite peut mettre en péril une communication sécurisée et efficace, le groupe de travail «Article 29» souligne le fait qu'il est d'autant plus important de respecter le principe de minimisation des données et de limiter le traitement des données à caractère personnel, en particulier leur stockage sur le dispositif, au minimum requis.

En outre, des dispositifs qui sont conçus pour permettre un accès direct via l'internet ne sont pas toujours configurés par l'utilisateur. Ils peuvent donc offrir une voie d'accès aisée aux intrus s'ils continuent à fonctionner avec les paramètres par défaut. Des pratiques de sécurité basées sur des restrictions de réseau, désactivant des fonctionnalités non critiques par défaut, empêchant l'utilisation de sources de mise à jour de logiciels non fiables (limitant donc les attaques de programmes malveillants basés sur une altération du code) pourraient contribuer à limiter l'impact et l'étendue d'éventuelles atteintes aux données. Ces protections du respect de la vie privée doivent être intégrées dès le départ, en application du principe du «respect de la vie privée assuré dès la conception».

En outre, l'absence de mises à jour automatiques entraîne de fréquentes vulnérabilités non corrigées qui peuvent être facilement découvertes par des moteurs de recherche spécialisés. Même dans les cas où les utilisateurs sont conscients des vulnérabilités affectant leurs propres dispositifs, ils peuvent ne pas avoir accès aux mises à jour du vendeur, que ce soit en raison des limitations du matériel ou de technologies désuètes, empêchant le dispositif de supporter des mises à jour logicielles. Si un fabricant de dispositifs doit cesser de supporter un dispositif, des solutions alternatives à ce soutien doivent être proposées (par exemple, l'ouverture du logiciel à la communauté des logiciels libres). Les utilisateurs doivent être informés que leurs dispositifs sont susceptibles de devenir vulnérables à des lacunes non corrigées.

Certains des systèmes auto-suiveurs (par exemple, podomètres, traqueurs de sommeil) sur le marché souffrent également de lacunes de sécurité permettant aux pirates de falsifier les valeurs observées qui sont notifiées aux applications et aux fabricants de dispositifs. Il est essentiel que ces dispositifs offrent des protections adéquates contre la falsification des données, notamment si les valeurs notifiées par ces capteurs ont une incidence directe sur les décisions en matière de santé des utilisateurs.

Enfin, et ce n'est pas le moins important, une politique adéquate de notification des atteintes aux données peut également contribuer à limiter les effets négatifs des vulnérabilités des logiciels et de la conception en diffusant des connaissances et en fournissant des orientations sur ces questions.

5. Droits de la personne concernée

Les parties prenantes de l'IdO doivent respecter les droits des personnes concernées conformément aux dispositions des articles 12 et 14 de la directive 95/46/CE et prendre des mesures organisationnelles en conséquence. Ces droits ne sont pas limités aux abonnés des services IdO ou aux propriétaires de dispositifs et concernent toute personne dont les données à caractère personnel sont traitées.

5.1 **Droit d'accès**

L'article 12, point a), prévoit que toute personne concernée a le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données.

Dans la pratique, dans l'IdO, les utilisateurs ont tendance à être enfermés dans des systèmes spécifiques. Les dispositifs envoient d'abord généralement les données au fabricant du dispositif, qui rend ensuite ces données accessibles à l'utilisateur au moyen d'un portail web ou d'une application. Cette conception permet aux fabricants de fournir des services en ligne qui optimisent les capacités des dispositifs, mais elle peut également empêcher les utilisateurs de choisir librement le service qui interagit avec leur dispositif.

En outre, aujourd'hui, les utilisateurs finals sont rarement en mesure d'avoir accès aux données brutes qui sont enregistrées par des dispositifs IdO. De toute évidence, ils ont un intérêt plus immédiat pour

les données interprétées que pour les données brutes qui peuvent ne pas avoir de sens pour eux. Or, l'accès à ces données pourrait s'avérer utile pour que les utilisateurs finals comprennent ce que le fabricant de dispositifs peut en conclure à leur sujet. De même, le recours à ces données brutes leur donnerait la capacité de transférer leurs données à un autre responsable du traitement et de changer de services – par exemple si le responsable du traitement original modifie sa politique en matière de respect de la vie privée, d'une manière qui ne les satisfait pas. Aujourd'hui, dans la pratique, ces personnes n'ont pas d'autre possibilité que de cesser d'utiliser leurs dispositifs étant donné que la plupart des responsables du traitement des données n'offrent pas cette fonctionnalité et ne donnent accès qu'à une version dégradée des données brutes stockées.

Le groupe de travail «Article 29» estime que de telles attitudes empêchent l'exercice efficace du droit d'accès accordé aux personnes par l'article 12, point a), de la directive 95/46/CE. Il estime que les parties prenantes de l'IdO devraient au contraire prendre des mesures pour permettre aux utilisateurs de faire observer efficacement ce droit et offrir aux utilisateurs une possibilité de choisir un autre service qui pourrait ne pas être proposé par le fabricant de dispositifs. Des normes d'interopérabilité pourraient être utilement élaborées à cet effet.

Il serait d'autant plus pertinent de prendre de telles mesures que le «droit à la portabilité», que le projet de règlement général sur la protection des données est susceptible de consacrer en tant que variante du droit d'accès, vise à mettre clairement fin aux situations d'«enfermement» de l'utilisateur[27]. Le législateur européen a pour ambition, sur ce point, de débloquer les obstacles à la concurrence et d'aider les nouveaux acteurs à innover sur ce marché.

5.2 **Possibilité de retirer son consentement et de s'opposer au traitement**

Les personnes concernées doivent avoir la possibilité de révoquer tout consentement préalable donnée à un traitement spécifique des données et de s'opposer au traitement de données les concernant. L'exercice de ces droits doit être possible sans aucune contrainte ni entrave technique ou organisationnelle et les outils fournis pour enregistrer ce retrait doivent être accessibles, visibles et efficaces.

Les systèmes de retrait doivent être détaillés et couvrir: 1) toutes données collectées par un objet spécifique (par exemple, pour demander que le baromètre cesse d'enregistrer l'humidité, la température et les sons); 2) un type spécifique de données collectées par tout objet (par exemple, un utilisateur doit pouvoir interrompre la collecte de données par tout dispositif enregistrant le son, qu'il s'agisse d'un traqueur de sommeil ou d'un baromètre); 3) un traitement spécifique de données (par exemple, un utilisateur pourrait exiger que tant son podomètre que sa montre cessent de compter ses pas).

En outre, étant donné que les «objets connectés» sont susceptibles de remplacer des articles existants qui offrent des fonctionnalités habituelles, les responsables du traitement devraient proposer une option pour désactiver la fonction «connectée» de l'objet et lui permettre de fonctionner comme l'article original non connecté (à savoir, désactiver la fonctionnalité liée à la montre ou aux lunettes

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

intelligentes). Le groupe de travail a déjà précisé que les personnes concernées devraient avoir la possibilité de «retirer (leur) consentement à tout moment, sans avoir à quitter» le service fourni[28].

Exemple: un utilisateur installe une alarme incendie connectée dans son appartement. L'alarme utilise un détecteur de présence, un détecteur de chaleur, un capteur ultrasonique et un capteur de luminosité. Certains de ces capteurs sont nécessaires pour détecter un incendie tandis que d'autres ne fournissent que des fonctions supplémentaires à propos desquelles l'utilisateur a été précédemment informé. L'utilisateur doit pouvoir désactiver ces fonctions pour utiliser seulement les détecteurs d'incendie, et donc déconnecter les capteurs utilisés pour fournir ces fonctions.

Il est intéressant de noter que certaines évolutions récentes dans ce domaine tentent d'autonomiser les personnes concernées en leur offrant un plus grand contrôle sur les fonctions de gestion du consentement, par exemple au moyen de politiques adhésives[29] ou l'anonymisation et l'intermédiation[30].

6. Conclusions et recommandations

Ci-après sont énumérées un certain nombre de recommandations jugées utiles par le groupe de travail afin de faciliter l'application des exigences légales de l'UE à l'IdO, répertoriées ci-dessus.

Les recommandations ci-après offrent uniquement des orientations qui s'ajoutent aux documents précédemment adoptés par le groupe de travail «Article 29».

À cet égard, le groupe de travail souhaite attirer une attention particulière sur ses précédentes recommandations concernant les applications et les dispositifs intelligents[31]. Étant donné que les smartphones font partie de l'environnement de l'IdO et que les deux écosystèmes impliquent un ensemble comparable de parties prenantes, les présentes recommandations sont directement pertinentes pour l'IdO. En particulier, les développeurs d'applications et les fabricants de dispositifs doivent fournir un niveau adéquat d'informations aux utilisateurs finals, offrir des dispositions simples de non-participation et/ou un consentement granulaire, le cas échéant. En outre, lorsque le consentement n'a pas été obtenu, le responsable du traitement doit anonymiser les données avant de les utiliser pour d'autres finalités ou de les partager avec d'autres parties.

[28] Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, adopté le 16 mai 2011 (WP185) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf

[29] À cet égard, le recours à une approche basée sur les «politiques adhésives» peut soutenir la conformité au cadre de protection des données en intégrant des informations sur les conditions et les limites d'utilisation des données dans les données proprement dites. Ces politiques pourraient donc fournir le contexte de l'utilisation des données, les finalités, les politiques concernant l'accès des tiers et une liste d'utilisateurs de confiance.

[30] Une façon d'offrir à une personne concernée un contrôle réel sur la façon dont les données doivent être traitées lors d'une interaction avec les capteurs en étant en mesure d'exprimer ses préférences, y compris l'obtention et la révocation du consentement et les choix de limitation de la finalité, pourrait être basée sur le recours à l'anonymisation et l'intermédiation. Soutenues par un dispositif, les demandes de données sont confrontées à des politiques prédéfinies régissant l'accès aux données sous le contrôle de la personne concernée. En définissant les couples de capteurs et de politiques, les demandes émanant des tiers pour la collecte ou l'accès aux données des capteurs seraient autorisées, limitées ou simplement rejetées.

[31] Avis 02/2013 sur les applications destinées aux dispositifs intelligents (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_fr.pdf

6.1 Recommandations communes à toutes les parties prenantes

- Des analyses de l'impact sur la vie privée doivent être effectuées avant le lancement de toute nouvelle application dans l'IdO. La méthodologie à suivre pour ces analyses de l'impact sur la vie privée peut être basée sur le cadre relatif à l'analyse de l'impact sur la vie privée et la protection des données que le groupe de travail «Article 29» a adopté le 12 janvier 2011 pour les applications RFID[32]. Lorsque cela est approprié/réalisable, les parties prenantes doivent envisager de mettre l'analyse pertinente à la disposition du grand public. Des cadres spécifiques d'analyse pourraient être élaborés pour des écosystèmes IdO particuliers (par exemple, les villes intelligentes).

- Beaucoup de parties prenantes de l'IdO ont seulement besoin de données agrégées et n'ont pas besoin des données brutes collectées par les dispositifs IdO. Les parties prenantes doivent supprimer les données brutes dès qu'elles ont extrait les données nécessaires à leur traitement des données. En principe, la suppression doit avoir lieu au point de collecte des données brutes le plus proche (par exemple, sur le dispositif même après le traitement).

- Chaque partie prenante dans l'IdO doit appliquer les principes du respect de la vie privée assuré dès la conception et du paramétrage par défaut favorable au respect de la vie privée.

- L'autonomisation de l'utilisateur est essentielle dans le contexte de l'IdO. Les personnes concernées et les utilisateurs doivent pouvoir exercer leurs droits et donc «avoir le contrôle» des données à tout moment, conformément au principe de l'autodétermination des données.

- Les méthodes pour fournir les informations, offrant un droit de refus ou sollicitant le consentement, doivent être rendues aussi conviviales que possible. En particulier, les politiques d'information et de consentement doivent se concentrer sur des informations compréhensibles pour l'utilisateur et ne doivent pas se limiter à une politique générale relative au respect de la vie privée sur le site internet des responsables du traitement.

- Les dispositifs et les applications doivent également être conçus de façon à informer les personnes concernées utilisatrices et non utilisatrices, par exemple au moyen de l'interface physique du dispositif ou par la diffusion d'un signal sur un canal sans fil.

6.2 Fabricants de systèmes d'exploitation et de dispositifs

- Les fabricants de dispositifs doivent informer les utilisateurs sur le type de données qui sont collectées par les capteurs et ensuite traitées, les types de données qu'ils reçoivent et la façon dont elles sont traitées et combinées.

- Les fabricants de dispositifs doivent pouvoir informer toutes les autres parties prenantes concernées dès qu'une personne concernée retire son consentement ou s'oppose au traitement des données.

- Les fabricants de dispositifs doivent fournir des choix granulaires lors de l'octroi de l'accès à leurs applications. La granularité ne doit pas seulement concerner la catégorie de données collectées mais aussi le moment et la fréquence à laquelle les données sont saisies. À l'instar de la fonctionnalité «ne pas déranger» sur les smartphones, les dispositifs IdO doivent proposer une option «ne pas collecter» pour programmer ou désactiver rapidement les capteurs.

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

- Afin de prévenir le suivi de la localisation, les fabricants de dispositifs doivent limiter la création d'empreinte par le dispositif en désactivant leurs interfaces sans fil lorsqu'ils ne sont pas utilisés ou doivent utiliser des identifiants aléatoires (tels que les adresses MAC aléatoires pour scanner les réseaux wifi) afin de prévenir l'utilisation d'un identifiant permanent aux fins de suivre la localisation.

- Afin de faire respecter le principe de transparence et de contrôle par l'utilisateur, les fabricants de dispositifs doivent fournir des outils permettant de lire, éditer et modifier les données localement avant qu'elles soient transférées à un responsable du traitement. En outre, les données personnelles traitées par un dispositif doivent être stockées dans un format permettant la portabilité des données.

- Les utilisateurs ont un droit d'accès à leurs données à caractère personnel. Ils doivent recevoir des outils leur permettant d'exporter facilement leurs données dans un format structuré et couramment utilisé. Par conséquent, les fabricants de dispositifs doivent fournir une interface conviviale pour les utilisateurs qui souhaitent obtenir des données agrégées et/ou des données brutes qu'ils stockent encore.

- Les fabricants de dispositifs doivent fournir des outils simples pour informer les utilisateurs et mettre à jour les dispositifs lorsque des vulnérabilités en matière de sécurité sont découvertes. Lorsqu'un dispositif devient obsolète et n'est plus actualisé, le fabricant de dispositifs doit en informer l'utilisateur et s'assurer qu'il a connaissance du fait que le dispositif ne sera plus mis à jour. Toutes les parties prenantes qui sont susceptibles d’être affectées par la vulnérabilité doivent également en être informées.

- Les fabricants de dispositifs doivent suivre un processus de sécurité dès le stade de la conception et consacrer certains composants aux primitives essentielles de cryptographie.

- Les fabricants de dispositifs doivent limiter autant que possible le volume de données qui quittent les dispositifs en transformant les données brutes en données agrégées directement sur le dispositif. Les données agrégées doivent se présenter dans un format normalisé.

- Contrairement aux smartphones, les dispositifs IdO peuvent être partagés par plusieurs personnes concernées, voire être loués (par exemple, les maisons intelligentes). Un paramètre doit être disponible pour différencier les différentes personnes utilisant le même dispositif afin qu'elles ne puissent être renseignées sur leurs activités mutuelles.

- Les fabricants de dispositifs doivent collaborer avec les organismes de normalisation et les plateformes de données afin de soutenir un protocole commun pour exprimer les préférences concernant la collecte et le traitement des données par les responsables du traitement, en particulier lorsque ces données sont collectées par des dispositifs discrets.

- Les fabricants de dispositifs doivent permettre aux entités locales de contrôle et de traitement (dites «d'anonymisation et d'intermédiation») de permettre aux utilisateurs d'avoir une vision claire des données collectées par leurs dispositifs et de faciliter le stockage et le traitement au niveau local sans devoir transmettre les données au fabricant du dispositif.

6.3 **Développeurs d'application**

- Des avis ou avertissements devraient être conçus afin de rappeler fréquemment aux utilisateurs que des capteurs collectent les données. Lorsque le développeur d'application ne dispose pas d'un

accès direct au dispositif, l'application doit envoyer périodiquement une notification à l'utilisateur pour l'informer qu'il enregistre encore des données.

- Les applications doivent faciliter l'exercice par les personnes concernées des droits d'accès, de modification et de suppression des informations personnelles collectées par les dispositifs IdO.

- Les développeurs d'application doivent fournir des outils afin que les personnes concernées puissent exporter des données brutes et/ou agrégées dans un format standard et utilisable.

- Les développeurs doivent accorder une attention particulière aux types de données qui sont traitées et à la possibilité de déduire des données à caractère personnel sensibles à partir de ces données.

- Les développeurs d'applications devraient appliquer un principe de minimisation des données. Lorsque la finalité peut être réalisée au moyen de données agrégées, les développeurs ne doivent pas avoir accès aux données brutes. De manière plus générale, les développeurs doivent suivre une approche de respect de la vie privée assuré dès la conception et réduire le volume des données collectées à celui requis pour fournir le service.

6.4 **Plateformes sociales**

- Les paramètres par défaut des applications sociales basées sur les dispositifs de l'IdO doivent demander aux utilisateurs de revoir, éditer et décider des informations générées par leur dispositif avant une publication sur les plateformes sociales.

- Les informations publiées par les dispositifs IdO sur les plateformes sociales doivent, par défaut, ne pas devenir publiques ou être indexées par des moteurs de recherche.

6.5 **Propriétaires de dispositifs IdO et destinataires supplémentaires**

- Le consentement à l'utilisation d'un dispositif connecté et au traitement de données résultant doit être éclairé et librement donné. Les utilisateurs ne doivent pas être économiquement sanctionnés ou avoir un accès moindre aux capacités de leurs dispositifs s'ils décident de ne pas utiliser le dispositif ou un service spécifique.

- La personne concernée dont les données sont traitées dans le cadre d'une relation contractuelle avec l'utilisateur d'un dispositif connecté (à savoir, un hôtel, une compagnie d'assurances ou un loueur de voitures) doit être en mesure de gérer le dispositif. Indépendamment de l'existence de toute relation contractuelle, toute personne concernée non utilisatrice doit être en mesure d'exercer ses droits d'accès et d'opposition.

- Les utilisateurs de dispositifs IdO doivent informer les personnes concernées non utilisatrices dont les données sont collectées de la présence des dispositifs IdO et du type de données collectées. Ils doivent également respecter la préférence de la personne concernée de ne pas voir ses données collectées par le dispositif.

6.6 **Organismes de normalisation et plateformes de données**

- Les organismes de normalisation et les plateformes de données doivent promouvoir des formats de données portables et interopérables ainsi que clairs et explicites afin de faciliter les transferts de données entre les différentes parties et aider les personnes concernées à comprendre quelles données sont réellement collectées à leur sujet par les dispositifs IdO.

- Les organismes de normalisation et les plateformes de données doivent non seulement se concentrer sur le format pour les données brutes mais aussi sur l'émergence de formats pour les données agrégées.

- Les organismes de normalisation et les plateformes de données doivent encourager des formats de données contenant aussi peu d'identifiants que possible afin de faciliter l'anonymisation correcte des données IdO.

- Les organismes de normalisation devraient développer des normes certifiées qui jetteraient les bases des garanties en matière de vie privée et de sécurité pour les personnes concernées.

- Les organismes de normalisation devraient élaborer des protocoles de cryptage et de communication légers adaptés aux spécificités de l'IdO, garantissant la confidentialité, l'intégrité, l'authentification et le contrôle de l'accès.