PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Lignes directrices sur la protection des données Questions éthiques et juridiques dans la recherche et l'innovation en matière de TIC.

INTERNET DES OBJETS (IdO)

Cette œuvre est protégée par une licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Ce projet a reçu un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne sous la convention de subvention n° 788039. Ce document ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

IdO : Exigences éthiques et juridiques en matière de protection des données

Iñigo de Miguel Beriain (UPV/EHU)

Aliuska Duardo (UPV/EHU), Álvaro Anaya Rojas, Gerardo Pérez Laguna & María Carmen González Tovar (Everis Ciberseguridad)

Les versions préliminaires de ce document ont été révisées par Federica Lucivero (chercheuse senior en éthique et données chez Ethox et au Wellcome Centre for Ethics and Humanities (Big Data Institute) et Irene Kamara (professeur adjoint en gouvernance de la cybersécurité au TILT).

Révisé par Fruzsina Molnar-Gabor, Heidelberger Akademie der Wissenschaften (Allemagne) et membre du Groupe européen d'éthique des sciences et des nouvelles technologies de la Commission européenne.

Enfin validé par Iñaki Pariente, ancien directeur de l'Agence basque de protection des données.

Introduction

Cette section de nos "Lignes directrices sur la protection des données ELI dans la recherche et l'innovation en matière de TIC" (ci-après "les lignes directrices") fournit aux développeurs et aux innovateurs de l'internet des objets (IdO) des conseils sur les mesures à prendre pour se conformer aux exigences légales liées au développement d'outils IdO en termes de protection des données. Elles visent à contribuer à atténuer les problèmes éthiques et juridiques dans ce domaine. Il va sans dire que cette partie des lignes directrices (comme l'ensemble de celles-ci) ne constitue pas une interprétation autorisée de la réglementation, mais des recommandations de bonnes pratiques.

Cette partie des lignes directrices ne peut être comprise que dans le contexte de l'ensemble de l'outil (les lignes directrices). Plusieurs concepts ne sont pas abordés dans ce document, car ils sont traités dans d'autres sections ; nous y avons fait référence

lorsque cela était nécessaire (les références sont surlignées en jaune). Toutes les sections sont disponibles sur un site web interactif

Clause de non-responsabilité

Cette partie des lignes directrices a été rédigée à une époque où le règlement sur la vie privée et les communications électroniques n'avait pas encore été approuvé. Il se peut qu'au moment de l'utilisation de cet outil, le règlement soit en vigueur. Si tel est le cas, il faudra tenir compte des changements éventuels que cela a pu entraîner dans le cadre réglementaire. Jusqu'à l'entrée en vigueur du règlement "vie privée et communications électroniques", une situation fragmentée existera. En effet, les autorités de contrôle sont désormais confrontées à une situation où les interactions entre la directive "vie privée et communications électroniques" et le RGPD coexistent et posent des questions quant aux compétences, aux tâches et aux pouvoirs des autorités de protection des données dans les domaines qui déclenchent l'application à la fois du RGPD et des lois nationales transposant la directive "vie privée et communications électroniques".

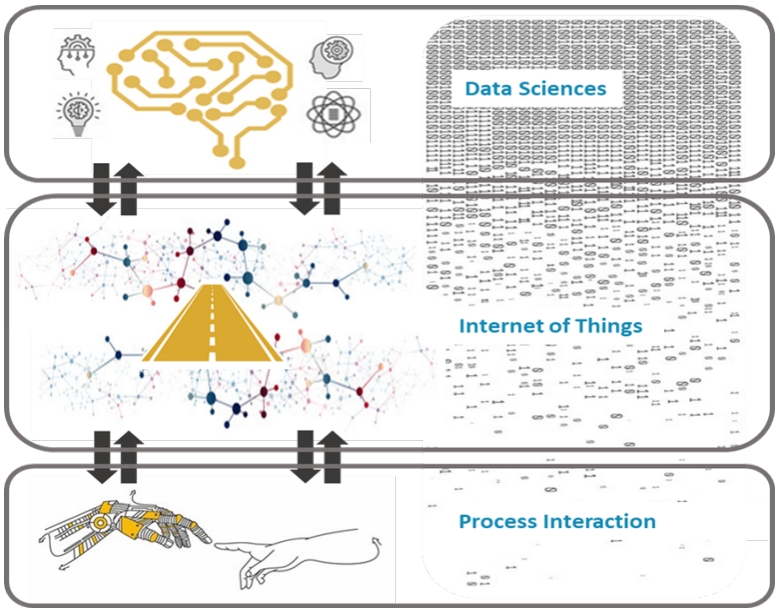
Préface

Il y a quelques années, le groupe de travail Article 29 a déclaré que "le concept d'Internet des objets (IdO) fait référence à une infrastructure dans laquelle des milliards de capteurs intégrés dans des appareils courants et quotidiens - des "objets" en tant que tels, ou des objets liés à d'autres objets ou individus - sont conçus pour enregistrer, traiter, stocker et transférer des données et, étant donné qu'ils sont associés à des identifiants uniques, interagir avec d'autres appareils ou systèmes en utilisant des capacités de mise en réseau". [804]

Quant à aujourd'hui, omniprésent, envahissant, *internet de tout,* sont quelques-uns des qualificatifs utilisés pour décrire l'IdO. Ces adjectifs visent à illustrer que l'interconnexion entre le monde physique et le monde virtuel se produit et peut se produire à tous les niveaux. Les technologies IdO nouvelles et émergentes comprennent, entre autres : les systèmes de transport intelligents, les appareils de santé connectés, les drones, la communication sans fil 5G, etc. Même les aspects quotidiens les plus triviaux de notre vie commencent à être imprégnés par l'IdO. Des machines à café "intelligentes" aux applications mobiles qui nous permettent de percevoir des odeurs.

[804] Groupe de travail A29, Avis 8/2014 sur l'évolution récente de l'Internet des objets, 2014, à l'adresse : https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

L'IdO est une technologie particulière qui entretient des liens étroits avec les technologies traditionnelles de Data Science, mais qui présente également de nombreuses différences dont il faut tenir compte lors de la définition d'un modèle de développement. La vitesse de génération des données est l'une des plus grandes différences entre l'IdO et les technologies traditionnelles de Data Mining. Bien que ces technologies puissent devenir complémentaires, le traitement dynamique des données englobe les réseaux partagés pour effectuer une analyse et une réponse en temps réel, comme l'IdO le fait contre une analyse de grands volumes de données statiques.



Paysage de l'IdO et des sciences des données

Ce succès dans le domaine du traitement des données présente également une complexité dans le développement de nouvelles technologies, c'est pourquoi il est essentiel de définir des processus pour faciliter le développement et la mise en œuvre des applications IdO. Disposer de modèles qui aident les développeurs TIC à comprendre le cadre juridique de la protection des données, et qui permettent d'identifier, de classer et de définir les tâches nécessaires pour aborder le traitement dès le début du développement des solutions, donne la possibilité d'atteindre une mise en œuvre plus efficace et structurée.

Il serait impossible de couvrir toutes les implications éthiques et juridiques de tout système IdO dans une directive. La qualification d'IdO s'applique à beaucoup de choses différentes. Premièrement, les appareils eux-mêmes (compteurs de pas, traqueurs de sommeil, appareils domestiques "connectés" tels que thermostats, détecteurs de

fumée, lunettes ou montres connectées, etc.) Ensuite, les terminaux des utilisateurs (par exemple, les smartphones ou les tablettes) sur lesquels des logiciels ou des applications ont été préalablement installés pour à la fois surveiller l'environnement de l'utilisateur grâce à des capteurs intégrés ou des interfaces réseau, et pour ensuite envoyer les données collectées par ces dispositifs aux différents responsables du traitement des données concernés. En outre, des outils logiciels sont nécessairement utilisés pour faire fonctionner ces systèmes.

Il serait difficile d'aborder toutes les questions liées à ce vaste cadre. Ainsi, notre travail propose un modèle simplifié qui permet d'aider les développeurs de systèmes IdO à répondre aux exigences de protection des données personnelles établies par la Charte européenne des droits de l'homme, le RGPD et les outils réglementaires complémentaires. Néanmoins, les parties prenantes, notamment les concepteurs, les fabricants, les propriétaires de réseaux et les spécialistes du marketing, doivent tenir compte des lois et des directives éthiques applicables à chaque développement spécifique, qu'il s'agisse de systèmes mécaniques ou de systèmes d'information et de communication, liés à leur système IdO concret.

À cette fin, le présent chapitre des lignes directrices tente d'offrir aux développeurs de TIC une vision systématique et simplifiée de la manière de satisfaire aux exigences légales de la législation européenne sur la protection des données. Cela se fait sans négliger les directives éthiques, en ajoutant aux produits IdO la valeur de "donner du pouvoir aux individus en les tenant informés, libres et en sécurité"[805] . En ce sens, le présent document s'inspire largement des considérations de l'avis 8/2014 du groupe de travail "Protection des données" sur l'évolution récente de l'internet des objets[806] ; du document de travail des services de la Commission intitulé "Advancing the Internet of Things in Europe"[807] ; et de la recommandation sur la sécurité de base de l'IdO dans le

805 Selon le groupe de travail Article 29 sur la protection des données, c'est "la clé pour soutenir la confiance et l'innovation, et donc pour réussir sur ces marchés". Avis 8/2014 du groupe de travail Article 29 sur la protection des données Op. Cit.

806 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088. Consulté en novembre 2020). Bien que cet avis soit antérieur à l'entrée en vigueur de l'actuel RGPD, nous considérons que les évaluations faites à l'époque par le groupe de travail sont toujours valables. Cet avis fournit les clés éthico-juridiques pour garantir la vie privée, sans entraver le développement de l'IdO.

807 Document de travail des services de la Commission Faire progresser l'Internet des objets en Europe, accompagnant le document Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Numériser l'industrie européenne Tirer pleinement parti d'un marché unique numérique. Commission européenne N5(19 AVRIL 2016) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110&qid=1610616372730 (Accès déc. 2020).

contexte des infrastructures d'information critiques[808] . **Il est à noter que ces documents sont soumis, dans la plupart des États membres, à un cadre réglementaire particulier et représentent un sujet réglementaire différent des domaines couverts par les autres lignes directrices. En outre, les développeurs de TIC doivent toujours garder à l'esprit que la réglementation européenne sur l'IdO changera probablement dans les prochains temps. Il est toujours recommandé de consulter leurs DPD au sujet des changements possibles et des particularités nationales.**

1 Compréhension du projet

Dans cette première partie, nous donnerons quelques conseils généraux sur la manière d'aborder le développement d'un système IdO dans les premières étapes de son cycle de production, c'est-à-dire lorsqu'il n'est encore guère plus qu'une idée qui n'a pas encore été mise en œuvre. Il est important de les garder à l'esprit si vous voulez garantir la mise en œuvre de politiques de protection des données dès la conception (voir la section "Protection des données dès la conception et par défaut" dans les "Concepts principaux", partie II des présentes lignes directrices).

Les conseils essentiels sont les suivants :

- Assurez-vous que votre projet est compatible avec le cadre de protection des données.
- Mettez en œuvre un programme de formation aux questions éthiques et juridiques pour les développeurs IdO.
- Définissez les rôles joués par tous les agents impliqués dans le traitement.
- Soutenez l'engagement des utilisateurs finaux

1.1 Assurez-vous que votre projet est compatible avec le cadre de protection des données.

Avant de commencer le développement d'un système IdO, les développeurs doivent avoir clairement à l'esprit ses objectifs principaux et ses éventuels objectifs secondaires et utilisations. Il peut arriver qu'un tel objectif ne soit pas compatible avec les normes

808 Recommandation de sécurité de base pour l'IdO dans le contexte des infrastructures d'information critiques, ENISA 12 (2017), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. (Consulté en novembre 2020)

éthiques et juridiques de l'UE (comme, par exemple, la **Charte des droits fondamentaux** de l'**Union européenne)**. Si le système prive ou réduit la capacité des personnes concernées à prendre librement des décisions concernant leur vie, s'il prend des décisions concernant les libertés fondamentales sans aucune forme de contrôle humain ou de possibilités de recours, si le système est fondé sur la nécessité de créer une sorte de dépendance, etc.

Il se peut aussi que l'objectif du système IdO implique une utilisation disproportionnée des données à caractère personnel, ce qui va à l'encontre du principe de minimisation et rend difficile le respect du cadre juridique applicable. En outre, les développeurs doivent également garder à l'esprit que le traitement des données dans l'IdO peut également concerner des personnes qui ne seront pas des abonnés ou des utilisateurs de leur technologie[809] . Ce scénario crée des risques liés au fait que certaines personnes concernées pourraient ne pas être conscientes que leurs données sont traitées. En outre, "si le responsable du traitement envisage un "modèle" dans lequel il prend uniquement des décisions automatisées ayant un impact élevé sur les personnes sur la base de profils établis à leur sujet et qu'il ne peut pas s'appuyer sur le consentement de la personne, sur un contrat avec elle ou sur une loi l'autorisant, le responsable du traitement ne doit pas poursuivre."[810] Enfin, les développeurs doivent évaluer si le projet est acceptable selon les normes éthiques, bien qu'il soit conforme aux obligations légales.

En résumé, les développeurs doivent analyser soigneusement l'impact possible de la technologie et les mesures appropriées à concevoir pour garantir la protection des données, la vie privée et les autres droits, tels que définis par la Charte des droits fondamentaux de l'**Union européenne et le cadre juridique connexe En ce qui concerne la protection des données et la vie privée, si l'analyse montre que le traitement ne sera pas acceptable sur la base de la Charte des droits fondamentaux** de l'**Union européenne, du RGPD et du cadre ePrivacy, le projet ne doit pas être approuvé.**

Encadré 1 : Les lunettes intelligentes

Le WP Art. 29 attire l'attention sur cette question avec l'exemple suivant : "les dispositifs portables comme les 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 européen de s'appliquer à de telles situations. L'application des règles de l'UE en matière de protection des données n'est pas conditionnée par la propriété d'un appareil ou d'un terminal, mais par le traitement des données à caractère personnel lui-même."

809 Art. 29 Op. cit. p. 13.

810 Ibid. p.30.

Si les développeurs sont prêts à créer un tel dispositif, ils doivent être conscients du fait que le RGPD exige un traitement équitable et licite de toutes les données personnelles recueillies. Cela inclut, entre autres, la condition d'une base juridique valide pour un traitement, la limitation de la finalité, la minimisation des données, la limitation de la conservation des données, la qualité et la sécurité des données, les droits des personnes concernées et la supervision indépendante. Le RGPD introduit également le principe de responsabilité comme une obligation primordiale de s'efforcer de respecter pas seulement la lettre de la loi. Il fournit également des instruments et des outils concrets pour parvenir à la responsabilisation, avec une approche fondée sur le risque mise en œuvre notamment dans les analyses d'impact sur la protection des données (AIPD), la protection des données dès la conception et par défaut, la nomination d'un délégué à la protection des données ainsi que le respect des codes de conduite et des mécanismes de certification existants.

Les développeurs doivent prendre en compte toutes ces questions essentielles dès les premières étapes du développement de leur projet, afin d'éviter des efforts inutiles, si la conformité au cadre juridique de la protection des données ne peut être garantie.

En outre, une idée claire du projet aidera à déterminer, dès les premières étapes du développement, d'autres questions juridiques relevant de la législation sur la protection des données, telles que la nécessité éventuelle de transferts internationaux de données, l'existence de responsables conjoints du traitement ou de sous-traitants, qui doivent être soigneusement sélectionnés, ou les mesures de sécurité et organisationnelles visant à minimiser les risques.

Ce document analysera plus en détail les principales obligations en matière de protection des données.

1.2 Mettre en œuvre un programme de formation aux questions éthiques et juridiques pour les développeurs IdO et les autres parties prenantes concernées.

L'un des principaux problèmes des systèmes IdO est qu'ils utilisent des données personnelles provenant de personnes autres que les utilisateurs finaux des appareils qui interagissent entre eux. En outre, ils fournissent souvent aux responsables du traitement de grands ensembles de données par le biais de l'agrégation de données recueillies auprès d'agents individuels. Ces circonstances brouillent en quelque sorte la relation entre le responsable du traitement et les personnes concernées. Les responsables du traitement ne savent tout simplement pas qui sont les personnes concernées qui fournissent certaines des données collectées par les dispositifs. Cela peut avoir des conséquences en termes de respect des normes de protection des données. Par exemple, il est difficile d'informer les personnes concernées du traitement si les responsables du

traitement ne savent pas qui sont les personnes concernées. En effet, le scénario est difficile, puisque ces personnes concernées pourraient être identifiées, même si un effort raisonnable était fait.

Il est primordial que les employés clés aient une connaissance aussi complète que possible des implications juridiques de leur travail, afin d'éviter tout traitement de données illicite non souhaité ou, en général, tout manquement au règlement sur la protection des données. En outre, les employés et les autres parties prenantes doivent prendre conscience des conséquences éthiques et sociales découlant du traitement des données personnelles par des moyens technologiques. [811]

Les développeurs IdO doivent être en mesure de comprendre les implications de leur action, tant pour les individus que pour la société, et être conscients de leurs responsabilités en apprenant à faire preuve d'une attention et d'une vigilance continues.[812] Cela aidera les développeurs IdO à prendre correctement en compte les questions éthiques et juridiques. En ce sens, **une formation optimale de tous les agents** impliqués dans le projet (développeurs, programmeurs, codeurs, data scientists, ingénieurs, chercheurs, etc.) avant son démarrage pourrait être l'un des outils les plus efficaces pour économiser du temps et des ressources en termes de conformité aux réglementations sur la protection des données.

Ainsi, la mise en œuvre de programmes de formation de base comprenant au moins les principes fondamentaux de la Charte des droits fondamentaux (en particulier, en ce qui concerne le rôle de la vie privée en tant que catalyseur d'autres droits tels que la non-discrimination ou la liberté idéologique), les principes exposés à l'article 5 du RGPD, la nécessité d'une base juridique pour le traitement (y compris les contrats entre les parties), les conséquences pratiques des principes de protection des données dès la conception et par défaut, et autres. Des sources utiles sont par exemple disponibles auprès de l'Agence des droits fondamentaux[813] , de l'IEEE et de ses lignes directrices en matière d'éthique[814] , et de la Commission européenne[815] . Si la formation n'est pas possible, la mise en œuvre des conseils d'un **expert externe** dès le début du projet pourrait être une alternative acceptable.

---

811 CNIL (2017) Comment l'humain peut-il garder la main ? Les questions éthiques soulevées par les algorithmes et l'intelligence artificielle. Commission nationale de l'informatique et des libertés, Paris, p.55. Disponible sur : www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf (consulté le 15 mai 2020).

812 Ibid. p.55.

813 https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition et
814 https://ethicsinaction.ieee.org/
815 https://ec.europa.eu/justice/smedataprotect/index_en.htm

1.3 Définir les rôles de protection des données joués par tous les agents impliqués dans le traitement : détermination des responsables du traitement et des sous-traitants.

L'un des plus gros problèmes des systèmes IdO est qu'ils utilisent souvent différents appareils, avec leurs propres caractéristiques. Cela crée des problèmes importants en termes de répartition des rôles entre les différents responsables du traitement impliqués. D'un autre côté, il est évident qu'un responsable du traitement confiera souvent certaines des tâches techniques à un sous-traitant, qui pourrait même impliquer un sous-sous-traitant dans ces tâches. Dans la pratique, cependant, il y aura des moments où il sera difficile de s'assurer que le sous-traitant n'agit pas réellement en tant que responsable du traitement ou responsable du traitement conjoint.

Les développeurs IdO devraient faire de leur mieux pour éviter ces problèmes, car le règlement sur la protection des données exige une réponse claire à la question "qui est responsable de ce traitement ?" pour garantir une protection efficace et complète des droits et libertés des personnes concernées. Ainsi, une exigence clé d'une politique adéquate de protection des données dès la conception est de **clarifier dès le début qui sont les responsables du traitement et les sous-traitants de données, afin de s'assurer que la responsabilité légale est comprise.**

Afin d'atteindre cet objectif**, des accords écrits entre tous les agents impliqués dans le développement de l'outil doivent être conclus et documentés.** Ceux-ci devraient inclure des spécifications claires sur les responsabilités assumées par tous les participants. La promotion d'une interaction continue entre toutes les DPD impliquées pourrait être une excellente option. Des organes et des outils de contrôle ad hoc peuvent être adoptés pour garantir une surveillance sans faille du traitement effectué par les participants. Voir l'encadré ci-dessous.

En outre, certaines parties peuvent rédiger des contrats en se positionnant dans un rôle différent de celui qui leur est réellement applicable. Par exemple, une partie prenante peut prétendre être un sous-traitant afin d'éviter certaines obligations de contrôle, et même signer un contrat. Cependant, la réalité fait loi ici et, indépendamment de ce que disent les parties, leur rôle devra être défini en fonction de leurs actes. En ce sens, la jurisprudence de l'UE[816] tend à élargir le concept de responsable du traitement et de responsable du traitement conjoint, réduisant ainsi la place des purs sous-traitants. À cet égard, il arrivera souvent que toutes les parties impliquées partagent un certain degré de responsabilité et deviennent des responsables du traitement conjoints pour les parties

[816] Voir : Arrêt de la Cour (grande chambre) du 5 juin 2018.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH.
Demande de décision préjudicielle auprès du Bundesverwaltungsgericht. Affaire C210-16, à l'adresse : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0210

Encadré 2 : Gérer des scénarios complexes de responsabilités en matière de données

Le projet de recherche Synchronicity, financé par l'UE, visait à créer un écosystème harmonisé pour les solutions de villes intelligentes basées sur l'IdO, où les fabricants de dispositifs IdO, les intégrateurs de systèmes et les fournisseurs de solutions peuvent innover et se concurrencer ouvertement. Ainsi, il utilisait beaucoup de données personnelles fournies par différentes sources. Dans ce contexte, "il est apparu assez clairement que les responsable du traitement des données de facto étaient les villes elles-mêmes. Ce sont elles qui contrôlent quelles données sont collectées et dans quel but. En même temps, le projet avait la responsabilité collective de s'assurer que ses activités de recherche étaient également conformes au règlement. Coordination de la protection des données - Modèle mezzanine Si plusieurs responsables du traitement des données peuvent être impliqués, la coordination entre eux au niveau du projet doit être assurée et garantie. C'est ce que Synchronicity a expérimenté en mettant en place un comité de protection des données (CPD) regroupant les délégués à la protection des données (DPD) de chaque ville intelligente, présidé par un coordinateur de la protection des données du projet (CPDP) au niveau du projet. Selon la loi, les villes restent les responsables formels du traitement des données sous leur contrôle et elles en sont directement responsables. Cependant, la mise en place du CPD permet une coordination étroite et un partage d'expérience pour s'assurer que le projet dans son ensemble est conforme à la réglementation, ainsi que pour identifier et atténuer les risques potentiels qui pourraient avoir un impact sur les partenaires."

Suivant ce critère, les rôles et les responsabilités dans le projet ont été répartis comme suit :

Au niveau du DPD de la ville

x Fonctions et responsabilités du DPD, y compris la protection des données et le contrôle de la conformité au RGPD.

x Identification de la collecte des données personnelles, y compris l'identification des responsables du traitement et des sous-traitants de données.

x Analyse de l'impact sur la protection des données (AIPD)

Au niveau du projet

x Coordination de la politique de protection des données

x Information du public et contact

x Rapports et protection des données Gestion des questions

(Voir : https://www.monica-project.eu/wp-content/uploads/2020/06/Personal-DataProtection-for-IoT-Deployments-final-MI.pdf, p. 11)

des activités de traitement impliquant ces différentes parties. À partir de là, chaque partie aura sa propre responsabilité indépendante et distincte.

1.4 Promouvoir l'engagement des utilisateurs finaux

Étant donné que l'IdO implique l'utilisation de données à caractère personnel provenant de différents types de personnes concernées, il est fortement recommandé, dans la mesure du possible, d'entendre la voix des représentants des collectifs impliqués afin de s'assurer que les politiques de protection des données dès la conception sont conformes à leurs intérêts, droits et libertés. L'organisation de quelques **discussions préliminaires**

avec ces représentants, lorsqu'ils existent, garantit la mise en œuvre d'un cadre ascendant qui pourrait être très utile à cette fin.

Liste de contrôle : Compréhension du projet

 Le développement de l'IdO ne favorise pas les scénarios qui ne sont pas compatibles avec les valeurs fondamentales et le cadre juridique de l'UE.

 Le développement de l'IdO n'implique pas une utilisation disproportionnée des données personnelles (le traitement n'est pas contraire au principe de minimisation).

 Le responsable du traitement peut s'assurer que des bases légales appropriées pour le traitement des données s'appliqueront à toutes les activités de traitement des données requises.

 Le responsable du traitement peut s'assurer que les membres clés de l'équipe qui traitent les données à caractère personnel ont reçu une formation adéquate sur les questions de protection des données et/ou que des outils d'évaluation adéquats ont été mis en œuvre.

 Les rôles joués par tous les différents agents impliqués dans l'outil IdO ont été identifiés de manière adéquate et le responsable du traitement peut en apporter la preuve (une déclaration ou un accord a été signé, par exemple).

 Lorsqu'il y en a, les représentants des principaux collectifs concernés par le traitement des données ont été consultés sur les caractéristiques de l'outil IdO.

2 Licéité : Choisir une base juridique

Selon le RGPD, un traitement licite nécessite une base juridique. Si le traitement comprend le type d'activités qui sont incluses dans la directive "vie privée et communications électroniques" (et dans le futur règlement "vie privée et communications électroniques"), les dispositions prises par ce nouvel outil s'appliqueront dès qu'il sera adopté. Un IdO doit pouvoir distinguer les différents individus utilisant le même système afin qu'ils ne puissent pas prendre connaissance des activités des autres sans une base juridique justifiant ce traitement (très probablement le consentement). La confiance entre les acteurs doit reposer sur l'authentification de chaque outil IdO avant la communication et l'accès aux données. La prévention de l'accès d'objets et d'utilisateurs non autorisés à un système peut renforcer la confidentialité, et donc la confiance des utilisateurs. **La définition de la base juridique qui s'applique à ce traitement est donc essentielle, pour garantir la licéité du**

traitement. À l'heure actuelle, il existe plusieurs bases juridiques pour le traitement des données qui pourraient s'appliquer à l'IdO. Il s'agit du consentement, de l'exécution d'un contrat, de l'intérêt légitime et, bien sûr, de l'intérêt public, lorsque nous parlons de recherche scientifique et d'innovation.

Le projet de règlement ePrivacy[817] considère le consentement comme la principale base légale du traitement des données dans le contexte des communications électroniques, une circonstance qui s'applique, par exemple, dans le cas des dispositifs IdO connectés au web. Toutefois, lorsqu'un responsable du traitement cherche à traiter des données à caractère personnel qui sont en fait nécessaires à l'exécution d'un contrat, alors le consentement n'est pas la base licite la plus recommandable et le traitement doit être fondé sur l'article 6, paragraphe 1, point b).

L'intérêt légitime, quant à lui, est la base juridique la plus souple pour le traitement, mais on ne peut pas supposer qu'il sera toujours le plus approprié. L'ICO a estimé qu'elle est probablement la plus appropriée lorsque les responsables du traitement utilisent les données des personnes d'une manière à laquelle elles s'attendent raisonnablement et qui a un impact minimal sur la vie privée, ou lorsqu'il existe une justification impérieuse pour le traitement.[818] Toutefois, il se peut que les critères utilisés par les autorités chargées de la protection des données des États membres de l'UE soient très différents. Il est donc préférable de demander à votre DPD de se prononcer sur cette question.

Une question préliminaire : n'oubliez pas que le traitement des données des catégories spéciales est interdit !

Avant de traiter des données, les responsables du traitement doivent s'assurer qu'il ne s'agit pas de données de catégories particulières. Si ce n'est pas le cas, ils doivent se rappeler que l'article 9.1 du RGPD oppose son veto à un tel traitement, sauf si l'une des circonstances décrites à l'article 9.2 s'applique. En outre, les responsables du traitement doivent garder à l'esprit que la plupart de ces circonstances (le consentement est une exception) exigent que ce traitement soit effectué sur la base du droit de l'Union ou des États membres qui prévoit des mesures appropriées et spécifiques pour sauvegarder les droits et libertés de la personne concernée. Ces garanties peuvent être la pseudonimisation, le secret professionnel, voire des mécanismes plus complexes si un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale est prévu (voir article 46 du RGPD).

817 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

818 ICO : Intérêts légitimes, à l'adresse : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

2.1 Consentement

Le consentement est la base juridique la plus traditionnelle pour le traitement des données. En outre, le projet de règlement sur la vie privée en ligne[819] considère le consentement comme la principale base du traitement légal des données dans le contexte des communications électroniques, une circonstance qui s'applique, par exemple, dans le cas des dispositifs IdO connectés au web. Le consentement, cependant, ne s'appliquera que si certaines conditions sont remplies. Si le consentement est utilisé comme base légale pour le traitement des données, **les développeurs doivent s'assurer que le dispositif qu'ils créent inclut la nécessité d'exiger le consentement préalable des utilisateurs pour le traitement de manière spécifique, informée et granulaire et assurer la documentation adéquate de ce consentement**.

Selon l'EDPB, la granularité signifie qu'"un service peut impliquer plusieurs opérations de traitement pour plus d'une finalité. Dans ce cas, les personnes concernées devraient être libres de choisir la finalité qu'elles acceptent, plutôt que de devoir consentir à un ensemble de finalités de traitement. Dans un cas donné, plusieurs consentements peuvent être justifiés pour commencer à offrir un service, conformément au RGPD."[820]

La granularité "ne devrait pas seulement concerner les catégories de données collectées, mais aussi le moment et la fréquence auxquels les données sont capturées, ainsi que les différentes finalités pour lesquelles ces données seront traitées. À l'instar de la fonction "ne pas déranger" sur les smartphones, les appareils IdO devraient proposer une option "ne pas collecter" pour programmer ou désactiver rapidement les capteurs."[821]

Il doit être parfaitement clair que le consentement de la personne concernée ne peut être obtenu librement par l'acceptation obligatoire de conditions générales, ni par des possibilités d'opt-out.[822] Ainsi, les dispositifs doivent être conçus de manière à ce que le consentement soit granulaire et que les utilisateurs aient la possibilité de renoncer à certains services ou fonctionnalités d'un IdO. Les utilisateurs ne doivent pas être pénalisés ou avoir un accès dégradé aux capacités du système s'ils décident de ne pas l'utiliser (lors d'une interaction avec un autre système) ou s'ils décident de ne pas utiliser un service spécifique intégré au système.

---

819 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

820 EDPB, Lignes directrices 05/2020 sur le consentement au titre du règlement 2016/679, adoptées le 4 mai 2020, à l'adresse : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

821 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

822 Groupe de travail Article 29 (2011) Avis 13/2011 sur les services de géolocalisation sur les appareils mobiles intelligents Adopté le 16 mai 2011. 881/11/FR WP 185, P. 13, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

Les dispositifs et les applications doivent toujours être conçus pour informer les utilisateurs et les non-utilisateurs du traitement des données, par exemple via l'interface physique du dispositif ou en diffusant un signal sur un canal sans fil. **Indépendamment de l'existence d'une relation contractuelle et même de la base juridique du traitement, toute personne concernée, qu'elle soit utilisatrice ou non-utilisatrice, doit être informée et en mesure d'exercer ses droits (la seule exception est le droit d'opposition, qui n'est pas applicable si la base juridique du traitement est le consentement).** [823] La possibilité de retirer le consentement doit être garantie dès le moment où les données sont collectées et les personnes concernées doivent être informées de cette possibilité.

La gestion des consentements nécessite une conformité préalable avec les principes de protection des données dès la conception et par défaut. Comme l'a indiqué Wachter, il est fortement recommandé aux développeurs IdO de définir des autorisations d'accès "**non seulement pour les utilisateurs, mais aussi pour les "objets" qui cherchent à accéder aux données d'un utilisateur ou à les traiter pour le compte de l'utilisateur ou d'un tiers".** Ces autorisations d'accès doivent respecter les préférences de l'utilisateur en matière de confidentialité. La gestion des identités combinée à un contrôle d'accès basé sur les rôles, par exemple, permet de vérifier l'identité et d'autoriser les demandes d'actions ou les dispositifs des utilisateurs en fonction du rôle qui leur est attribué par le système, ce qui garantit que seules les actions autorisées pour un rôle spécifique (par exemple, la collecte, la transmission ou le traitement de données) peuvent être effectuées au cours d'une session. Les administrateurs ou les utilisateurs peuvent définir ces autorisations, offrant ainsi différentes approches pour protéger les préférences subjectives des utilisateurs en matière de vie privée."[824]

823 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

824 Wachter, Sandra, Défis normatifs de l'identification dans l'Internet des objets : Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, Volume 34, Issue 3, 2018, pages 436-449.

Encadré 3 : Politiques collantes et mandataires de la vie privée

Un meilleur contrôle du traitement des données pourrait être garanti par l'utilisation d'une approche basée sur les politiques dites "collantes", qui peuvent favoriser le respect du cadre de protection des données en intégrant aux données elles-mêmes des informations sur les conditions et les limites de l'utilisation des données. Ainsi, ces politiques pourraient définir le contexte d'utilisation des données, les finalités, les politiques d'accès des tiers et une liste d'utilisateurs de confiance.

Un moyen alternatif/complémentaire d'offrir à la personne concernée un contrôle réel sur la manière dont les données doivent être traitées lors de l'interaction avec les capteurs en lui permettant d'exprimer ses préférences, y compris l'obtention et la révocation du consentement et les choix de limitation de la finalité, pourrait être basé sur l'utilisation de **mandataires pour la protection de la vie privée.** Prises en charge 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 des paires de capteurs et de politiques, les demandes de tiers pour la collecte ou l'accès aux données des capteurs seraient autorisées, limitées ou simplement rejetées.

Source : Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

Afin d'éviter les risques de surveillance secrète, l'ancien groupe de travail Article 29 estime qu'il est essentiel que le **dispositif prévienne que la fonction de partage des données est "activée", par exemple au moyen d'une icône visible en permanence**.[825] En effet, envisager une signalisation appropriée qui serait réellement visible par les personnes concernées pourrait être particulièrement important lorsque nous avons affaire à des wearables. Tous les dispositifs IdO devraient informer les personnes concernées non utilisatrices dont les données sont collectées de ce traitement, y compris de toutes les informations pertinentes le concernant. Les responsables du traitement doivent faire de leur mieux pour s'assurer que ces informations sont fournies, même si, en pratique, cela peut être difficile. **Des outils adéquats doivent être mis en œuvre pour garantir le respect de la préférence des personnes concernées non utilisatrices de ne pas voir leurs données collectées par le dispositif.**

825 Groupe de travail Article 29 (2011) Avis 13/2011 sur les services de géolocalisation sur les appareils mobiles intelligents Adopté le 16 mai 2011. 881/11/EN WP 185, P. 13, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf. Voir l'affaire LaLiga, à l'adresse : https://asociaciondpd.com/wp-content/uploads/2019/07/PS-00326-2018_ORI.pdf. Un résumé en anglais est disponible à l'adresse suivante : https://iapp.org/news/a/spanish-dpa-fines-la-liga-250k-euros-for-alleged-gdpr-violations/

Si le dispositif IdO intègre des **outils fournis par des tiers** et que le consentement est la base légale la plus appropriée, les développeurs IdO doivent être conscients du fait que ces outils doivent être installés sur la base d'un consentement préalable (même si cette pratique n'est pas largement suivie dans certains secteurs). Par conséquent, le groupe de travail "Article 29" a déclaré que "comme cet accès est soumis à l'obligation d'obtenir le consentement préalable de l'utilisateur, ce consentement doit être clairement donné, spécifique et informé. La pratique montre toutefois que, souvent, les demandes d'autorisation faites par les développeurs d'applications tierces n'affichent pas suffisamment d'informations pour que le consentement de l'utilisateur soit considéré comme spécifique et suffisamment éclairé, et donc valable au regard du droit communautaire". [826]

Enfin, et c'est important, le groupe de travail Article 29 a recommandé que les fournisseurs d'applications ou de services cherchent à **renouveler le consentement individuel** (même lorsqu'il n'y a pas de changement dans la nature du traitement) après une période de temps appropriée. Par exemple, il peut ne pas être valable de continuer à traiter des données personnelles lorsqu'une personne n'a pas utilisé activement le service au cours des 12 mois précédents. Même lorsqu'une personne a utilisé le service, il convient de lui **rappeler au moins une fois par an** (idéalement plus souvent, notamment lorsque la nature du traitement le justifie) la nature du traitement de ses données personnelles. Ainsi, le développeur pourrait envisager la possibilité d'incorporer dans le dispositif ou le système un outil capable d'envoyer une demande à l'utilisateur et de regagner (ou non) son consentement pour poursuivre le traitement. **Toutefois, il s'agit davantage d'une recommandation que d'une exigence légale absolue.** En tout état de cause, la personne concernée doit avoir à sa disposition un moyen facile de retirer son consentement, à tout moment, sans effet rétroactif.

Le **consentement général** peut être acceptable, mais uniquement si certaines circonstances concrètes s'appliquent, par exemple : il est difficile ou improbable de prévoir comment ces données seront traitées à l'avenir ; le consentement général utilisé pour le traitement de catégories spéciales de données est compatible avec la réglementation nationale ; lorsque le consentement général est utilisé, les personnes concernées ont la possibilité de retirer leur consentement et de choisir de participer ou non à certaines recherches ou à certaines parties de celles-ci. En outre, certaines **garanties doivent être mises en œuvre (voir encadré 4).**

Encadré 4 : Consentement général et garanties supplémentaires

L'autorité allemande de protection des données a dressé une liste de garanties

826 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

supplémentaires à mettre en œuvre en cas de consentement large dans le cadre de projets de recherche.[827] Ces garanties, qui peuvent être adaptées de manière appropriée à d'autres circonstances, sont les suivantes :

1. Garanties pour assurer la transparence :
   - Utilisation de règlements d'utilisation ou de plans de recherche qui illustrent les méthodes de travail prévues et les questions qui doivent faire l'objet du projet de recherche.
   - Évaluation et documentation de la question de savoir pourquoi, dans ce projet de recherche particulier, une spécification plus détaillée des objectifs de la recherche n'est pas possible.
   - Créer un site web pour informer les participants aux études sur les études en cours et futures.
2. Des garde-fous pour instaurer la confiance :
   - Vote positif d'un comité d'éthique avant l'utilisation des données à des fins de recherche ultérieure.
   - Évaluation de la possibilité de travailler avec un consentement dynamique ou de la possibilité pour une personne concernée de refuser son consentement ou de s'y opposer avant que les données puissent être utilisées pour de nouvelles questions de recherche (en fonction de la base légale de ce traitement ultérieur des données).
3. Garanties de sécurité :
   - Aucun transfert de données vers des pays tiers dont le niveau de protection des données est inférieur.
   - Mesures supplémentaires concernant la minimisation des données, le cryptage, l'anonymisation, la pseudonymisation ou la mise en œuvre de mesures de sécurité.
   - Mise en œuvre de politiques spécifiques pour limiter l'accès aux données personnelles.

Il est important de noter que si le traitement des données à caractère personnel est nécessaire au traitement, de telle sorte que le traitement ne peut avoir lieu sans les données, ou qu'un certain service ne peut être offert sans le traitement, le consentement

827 DSK, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs "bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. avril 2019, à l'adresse : www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf (consulté le 20 mai 2020). La traduction anglaise provient d'un beau résumé des mesures qui peut être consulté ici : www.technologylawdispatch.com/2019/04/privacy-data-protection/german-dpas-publish-resolution-on-concept-of-broad-consent-and-the-interpretation-of-certain-areas-of-scientific-research/.

peut ne pas être la base légale la plus efficace. En effet, les personnes concernées peuvent toujours avoir le droit de retirer leur consentement à tout moment. Dans les cas où l'activité dépend des données, le retrait du consentement peut déclencher l'incapacité de satisfaire le service. En fonction de toutes les autres circonstances entourant l'activité de traitement, dans ces cas, d'autres bases légales peuvent être plus appropriées, comme la nécessité d'exécuter un contrat.

En outre, les personnes concernées doivent avoir la possibilité de retirer tout consentement préalable donné à un traitement de données spécifique et de s'opposer au traitement des données les concernant. L'exercice de ce droit doit être possible sans aucune contrainte technique ou organisationnelle et les outils fournis pour enregistrer ce retrait doivent être accessibles, visibles et efficaces.

Selon le groupe de travail Article 29, "les régimes de retrait devraient être très fins et couvrir :

(1) Toute donnée collectée par une chose spécifique (par exemple, demander que la station météorologique cesse de collecter l'humidité, la température et les sons) ;

(2) Un type spécifique de données collectées par n'importe quoi (par exemple, un utilisateur devrait pouvoir interrompre la collecte de données par tout dispositif enregistrant le son, qu'il s'agisse d'un tracker de sommeil ou d'une station météorologique) ;

(3) Un traitement de données spécifique (par exemple, les utilisateurs pourraient exiger que leur podomètre et leur montre cessent de compter leurs pas). En outre, étant donné que les "objets connectés" portables sont susceptibles de remplacer des articles existants qui fournissent des fonctionnalités habituelles, les responsables du traitement des données devraient offrir une option permettant de désactiver la fonctionnalité "connectée" de l'objet et de le faire fonctionner comme l'objet original, non connecté (c'est-à-dire désactiver la fonctionnalité connectée de la montre intelligente ou des lunettes).

Le groupe de travail a déjà précisé que les personnes concernées devraient avoir la possibilité de "retirer continuellement (leur) consentement, sans avoir à quitter le service fourni"[828] .

Liste de contrôle : consentement

 Les responsables du traitement sont en mesure de démontrer que, après avoir mis en balance les circonstances du traitement, ils ont conclu que le consentement est la base

828 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur l'évolution récente de l'Internet des objets (SEP 16, 2014), p. 20, à l'adresse : https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

juridique la plus appropriée pour le traitement.

 Les responsables du traitement demandent le consentement des personnes concernées de manière libre, spécifique, informée et non équivoque, conformément à l'article 7 du RGPD.

 Les responsables du traitement ont informé les personnes concernées de leur droit de retirer leur consentement à tout moment.

 Lorsque le consentement général est utilisé pour le traitement de catégories spéciales de données compatible avec la réglementation nationale.

 Lorsque le consentement général est utilisé, les personnes concernées ont la possibilité de retirer leur consentement et de choisir de participer ou non à certains projets et parties de ceux-ci.

 Le déséquilibre des pouvoirs entre les responsables du traitement et les personnes concernées ne fait pas obstacle au libre consentement. Ceci est particulièrement important dans un contexte tel que le cadre du travail.

 Les responsables du traitement demandent aux personnes de s'inscrire activement.

 Les responsables du traitement n'utilisent pas de cases pré-cochées ou tout autre type de consentement par défaut.

 Les responsables du traitement utilisent un langage clair et simple, facile à comprendre.

 Les responsables du traitement précisent quels types de données ils veulent, pourquoi ils les veulent, ce qu'ils vont en faire et pendant combien de temps les données seront traitées.

 Les responsables du traitement donnent des options distinctes ("granulaires") pour consentir séparément à différentes finalités et types de traitement.

 Les responsables du traitement établissent un lien entre les éléments de données ou les catégories de données qui seront traités pour chaque finalité.

 Les responsables du traitement ont informé les personnes concernées de leur droit de retirer leur consentement à tout moment et de la manière de le faire.

 Les responsables du traitement veillent à ce que les personnes puissent refuser de consentir sans préjudice dans leur accès au service.

 Les responsables du traitement évitent de faire du consentement une condition préalable à un contrat de prestation de service si les données ne sont pas nécessaires à l'exécution de ce service.

2.2 Exécution d'un contrat

Parfois, les données peuvent être traitées sur la base de l'article 6.1(b) du RGPD : le traitement des données à caractère personnel est licite lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. La portée de cette base juridique est limitée par le critère de "nécessité", qui exige un lien direct et objectif entre le traitement lui-même et les finalités de l'exécution contractuelle attendue de la personne concernée. En effet, cette base juridique ne légitime que les traitements qui sont effectivement nécessaires à ce but. Au contraire, si le traitement n'est pas effectivement nécessaire à l'exécution d'un contrat, ce traitement ne peut avoir lieu que s'il repose sur une autre base juridique appropriée.[829]

Ainsi, l'**idée de nécessité est clé pour déterminer si cette base juridique est applicable au traitement ou non.** L'EDBP a adopté en 2019 ses lignes directrices sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, qui sont particulièrement pertinentes pour cette question.[830] Selon ces lignes directrices, l'utilisation des données pourrait être nécessaire à l'exécution d'un contrat avec une personne concernée, ou afin de prendre des mesures précontractuelles à la demande d'une personne concernée.

Il est important de noter que le concept de ce qui est "nécessaire à l'exécution d'un contrat" n'est pas simplement une évaluation de ce qui est permis par ou écrit dans les termes d'un contrat. Le concept de nécessité implique plusieurs **exigences**.

- **Premièrement**, le sous-traitant doit identifier la finalité concrète du traitement, car dans le cadre d'une relation contractuelle, il peut y avoir une variété de finalités de traitement et toutes ne sont pas nécessaires à l'exécution d'un contrat ou pour effectuer des démarches précontractuelles. Ainsi, les finalités concrètes à légitimer via cette base juridique doivent être clairement spécifiques et communiquées à la personne concernée, conformément aux obligations de limitation des finalités et de transparence du responsable du traitement. Si, par exemple, ces finalités sont nécessaires à d'autres fins commerciales du responsable du traitement, mais pas à l'exécution spécifique du contrat avec la personne concernée, elles pourraient être légitimes en vertu de la base juridique de l'intérêt légitime ou du consentement, mais pas en vertu de l'exécution d'un contrat. En outre, bien entendu, il arrive que le traitement ne soit couvert par aucune base juridique et doive donc être évité.

829 Lignes directrices du groupe de travail Article 29 sur le consentement au titre du règlement 2016/679 (WP259), approuvées par l'EDPB, page 19.

830 Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées Adoptées le 9 avril 2019, à l'adresse : https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

- **Deuxièmement,** il faut garder à l'esprit que **trois conditions principales doivent être remplies pour évaluer que cette base juridique s'applique dans un contrat concret**, à savoir : (a) un contrat existe, (b) le contrat est valable en vertu du droit national des contrats applicable, et (c) le traitement est objectivement nécessaire à l'exécution du contrat. Cette dernière partie est particulièrement importante : **objectivement nécessaire** signifie que ce besoin est lié à "une finalité qui fait partie intégrante de la fourniture de ce service contractuel à la personne concernée". Le traitement des données de paiement pour la facturation du service en fait partie. **Le responsable du traitement doit être en mesure de démontrer comment l'objet principal du contrat spécifique avec la personne concernée ne peut, en fait, être réalisé si le traitement spécifique des données à caractère personnel en question n'a pas lieu**. Le point important ici est le lien entre les données à caractère personnel et les opérations de traitement concernées, et l'exécution ou la non-exécution du service fourni dans le cadre du contrat." [831] En d'autres termes, le fait que le traitement des données à caractère personnel soit inclus comme une obligation dans un contrat ne le rend pas "nécessaire à l'exécution d'un contrat" au sens de la législation sur la protection des données. Ainsi, **si le responsable du traitement introduit dans le contrat une condition qui oblige la personne concernée à autoriser le traitement, même si ce traitement n'est pas strictement nécessaire à l'exécution du contrat, la base juridique n'est pas applicable à ce scénario.** S'il existe des alternatives réalistes et moins intrusives, le traitement n'est pas "nécessaire"." [832]
- Enfin, les responsables du traitement doivent toujours se rappeler que les **principes de limitation de la finalité et de minimisation des données sont particulièrement pertinents lorsqu'un responsable du traitement utilise "l'exécution d'un contrat" comme base juridique du traitement des données**, car les contrats de services en ligne (qui sont les services typiques liés aux dispositifs IdO) ne sont généralement pas négociés sur une base individuelle.

---

831 Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées Adoptées le 9 avril 2019, à l'adresse : https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

832 Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées Adoptées le 9 avril 2019, à l'adresse : https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

Encadré 5 : Le profilage peut-il être considéré comme nécessaire à l'exécution d'un contrat ?

L'EDPB a reconnu que la **personnalisation du contenu** peut constituer un élément essentiel ou attendu de certains services, et **peut** donc **être considérée comme nécessaire à l'exécution du contrat** avec l'utilisateur du service dans certains cas. La question de savoir si un tel traitement peut être considéré comme un aspect intrinsèque d'un service dépendra de la nature du service fourni, des attentes de la personne concernée moyenne à la lumière non seulement des conditions de service mais aussi de la manière dont le service est promu auprès des utilisateurs, et de la possibilité de fournir le service sans personnalisation. Lorsque la personnalisation du contenu n'est pas objectivement nécessaire à l'objectif du contrat sous-jacent, par exemple lorsque la livraison de contenu personnalisé est destinée à accroître l'engagement de l'utilisateur envers un service mais ne fait pas partie intégrante de l'utilisation du service, les responsables du traitement des données doivent envisager une autre base légale, le cas échéant.

Au contraire, la **publicité comportementale** et le suivi et le profilage associés des personnes concernées **ne peuvent pas être fondés sur l'exécution d'une base juridique contractuelle**, pas même lorsque cette publicité finance indirectement la fourniture du service. Ce traitement est distinct de la finalité objective du contrat entre l'utilisateur et le prestataire de services, et n'est donc pas nécessaire à l'exécution du contrat en question. Par conséquent, les responsables du traitement doivent utiliser d'autres bases juridiques telles que le consentement ou l'intérêt légitime s'ils souhaitent procéder de cette manière.

Source : Lignes directrices 2/2019 de l'EDPB sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées Adoptées le 9 avril 2019, à l'adresse : https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.

Liste de contrôle : exécution d'un contrat

 Les responsables du traitement sont en mesure de démontrer que, après avoir évalué les circonstances en jeu, ils ont conclu que l'exécution d'un contrat est la base juridique la plus appropriée pour le traitement.

 Les responsables du traitement peuvent démontrer que le traitement est **objectivement nécessaire à l'exécution du contrat**. A cette fin, ils ont répondu à ces questions :

- Quelle est la nature du service fourni à la personne concernée ? Quelles sont ses caractéristiques distinctives ?
- Quelle est la raison d'être exacte du contrat (c'est-à-dire sa substance et son objet fondamental) ?
- Quels sont les éléments essentiels du contrat ?
- Quelles sont les perspectives et les attentes mutuelles des parties au contrat ? Comment le service est-il promu ou annoncé à la personne concernée ? Un

utilisateur ordinaire du service s'attendrait-il raisonnablement à ce que, compte tenu de la nature du service, le traitement envisagé ait lieu afin d'exécuter le contrat auquel il est partie ?

 Les responsables du traitement ont informé les personnes concernées de la nécessité de traiter leurs données sur cette base juridique.

 Si des catégories spéciales de données doivent être traitées, les responsables du traitement ont identifié une exception au veto inclus dans l'article 9.1 du RGPD à l'article 9.2.

 Lorsque le consentement général est utilisé, les personnes concernées ont la possibilité de retirer leur consentement et de choisir de participer ou non à certaines recherches et parties de celles-ci.

 Les responsables de traitement n'étendent pas cette base juridique au traitement des données qui ne sont pas strictement nécessaires à l'exécution du contrat.

 Les responsables de traitement sont conscients que l'inclusion d'une condition pour signer le contrat qui implique un traitement de données ne justifie pas que ce traitement soit nécessaire à l'exécution du contrat.

2.3 Intérêt légitime

L'intérêt légitime est l'une des six bases légales pour le traitement des données à caractère personnel énoncées à l'article 6, paragraphe 1, du RGPD. Cette base juridique exige que les intérêts légitimes du responsable du traitement ou de tout tiers auquel les données sont communiquées prévalent sur les intérêts, les libertés et les droits fondamentaux des personnes concernées qui exigent la protection des données à caractère personnel (article 6, paragraphe 1, point f)). Pour vérifier que c'est bien le cas, les responsables du traitement doivent procéder à un ***test de mise en balance***, en suivant les lignes directrices du groupe de travail Article 29[833] (voir le "Test de mise en balance", sous la rubrique "Principaux outils et actions", dans la partie II des présentes lignes directrices). Bien entendu, comme pour les autres bases légales du traitement, même si l'intérêt légitime prévaut et que l'évaluation conclut que le traitement peut avoir lieu, les droits de la personne concernée ne s'appliquent toujours pas (voir "Droits de la personne concernée" dans la partie II des présentes lignes directrices). En outre, des garanties et des mesures d'atténuation adéquates visant à minimiser les risques et à assurer la protection de la vie privée des personnes concernées doivent être mises en

833 A29WP, Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement au titre de l'article 7 de la directive 95/46/CE. Avril 2014, p. 24. À l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consulté le 05 janvier 2020

œuvre chaque fois que possible, en particulier lorsque l'évaluation conclut à un risque élevé pour les droits des personnes concernées.

Liste de contrôle : intérêt légitime

 Les responsables de traitement ont vérifié que l'intérêt légitime est la base la plus appropriée.

 Les responsables de traitement ont vérifié que le traitement est nécessaire et qu'il n'existe pas de moyen moins intrusif pour parvenir au même résultat.

 Les responsables de traitement ont procédé à un test d'équilibre et sont convaincus que les intérêts de la personne ne l'emportent pas sur ces intérêts légitimes.

 Les responsables du traitement n'utilisent les données des individus que de la manière dont ils le feraient.

 Les responsables du traitement n'utilisent pas les données des personnes d'une manière qu'elles trouveraient intrusive ou qui pourrait leur porter préjudice, sauf si nous avons une très bonne raison.

 Si les responsables du traitement prévoient le traitement des données des enfants, ils ont pris des précautions supplémentaires pour s'assurer qu'ils protègent leurs intérêts.

 Les responsables de traitement ont envisagé des mesures de sauvegarde pour réduire l'impact lorsque cela est possible.

 Les responsables de traitement ont mis en place des outils adéquats pour garantir les droits des personnes concernées.

 S'ils ont identifié un impact significatif sur la vie privée, ils ont examiné s'ils devaient également mener une AIPD.

 Les responsables du traitement incluent des informations sur nos intérêts légitimes dans leurs informations sur la vie privée.

2.4 L'intérêt public et le cadre de la recherche scientifique

Selon l'article 6 (e) du RGPD, le traitement est licite s'il est nécessaire à l'exécution d'une tâche effectuée dans l'intérêt public. En outre, la recherche scientifique pourrait bien servir à éviter le veto sur les catégories spéciales de traitement des données inclus dans l'article 9.1 du RGPD. Toutefois, dans ce cas, conformément à l'article 9.2(j), le

traitement doit être fondé sur le droit de l'UE ou d'un État membre et doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour sauvegarder les droits fondamentaux et les intérêts de la personne concernée (voir " Traitement des données à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ", "Concepts principaux", partie II des présentes lignes directrices). Néanmoins, les développeurs IdO devraient toujours considérer qu'il n'est pas nécessairement vrai que toute recherche scientifique implique un intérêt public. En effet, "il est difficile à l'heure actuelle, voire impossible, de considérer un "intérêt public substantiel" comme une base pour le traitement de données sensibles à des fins de recherche scientifique" si un État membre n'a pas produit de réglementation spécifique à cet effet. Ainsi, les développeurs IdO devraient analyser le cadre juridique de leur pays concret.

D'autre part, il faut se rappeler que l'article 5, point b), du RGPD établit le principe de limitation de la finalité, en vertu duquel les données ne peuvent être traitées pour des finalités autres que les données spécifiques initiales (voir "Protection des données et recherche scientifique", dans "Concepts principaux", partie II des présentes lignes directrices).

Si le développement d'un système IdO peut être considéré comme de la recherche scientifique, le droit de l'Union ou des États membres peut prévoir des dérogations aux droits visés aux articles 15 (droit d'accès), 16 (droit de rectification), 18 (droit à la limitation du traitement) et 21 RGPD (droit d'opposition), toujours sous réserve de certaines conditions et garanties (article 89, paragraphe 2).

Liste de contrôle : utilisation des données pour la recherche scientifique

 Les responsables de traitement ont vérifié que leur projet s'inscrit bien dans le concept de recherche scientifique.

 Les responsables de traitement ont consulté leur DPD sur l'utilisation de cette exception à l'interdiction du traitement des données de catégories particulières.

 Les responsables de traitement ont consulté le cadre juridique national sur ce sujet.

 Les responsables du traitement ont mis en œuvre les garanties et les mesures organisationnelles consacrées pour s'aligner sur l'article 89 du RGPD et la réglementation nationale correspondante.

 Les responsables de traitement ont documenté toutes les informations concernant ce problème.

3 Capacité d'action humaine (prise de décision automatisée et profilage)

L'un des problèmes inhérents à l'IdO est que cette technologie **peut difficilement éviter de promouvoir le profilage et le traitement automatisé des données.** Cela crée des problèmes importants en termes de protection des données. Comme l'a déclaré le groupe de travail Article 29, "contrairement à d'autres types de contenu, les données poussées par l'IdO peuvent ne pas être examinées de manière adéquate par la personne concernée avant leur publication, ce qui génère indéniablement un risque de manque de contrôle et d'auto-exposition excessive pour l'utilisateur. En outre, la communication entre les objets peut être déclenchée automatiquement ainsi que par défaut, sans que l'individu en soit conscient. En l'absence de la possibilité de contrôler efficacement la manière dont les objets interagissent ou de pouvoir définir des frontières virtuelles en définissant des zones actives ou non actives pour des choses spécifiques, il deviendra extraordinairement difficile de contrôler le flux de données généré. Il sera encore plus difficile d'en contrôler l'utilisation ultérieure et d'éviter ainsi les dérives fonctionnelles. Cette question du manque de contrôle, qui concerne également d'autres développements techniques comme le cloud computing ou le big data, est encore plus difficile quand on pense que ces différentes technologies émergentes peuvent être utilisées en combinaison."[834] En effet, il faut garder à l'esprit que l'IdO nécessite souvent de relier des ensembles de données provenant de différents appareils afin d'obtenir des informations détaillées sur la vie privée des utilisateurs, et de faire des hypothèses et des prédictions sur leur comportement. Ces pratiques ne sont pas contraires à la protection des données, à condition qu'elles respectent strictement la réglementation applicable. Cependant, il est souvent difficile de garantir ce respect.

En outre, ce scénario permet de combiner plusieurs données qui, à elles seules, peuvent fournir peu d'informations sur la personne concernée. Certaines de ces données peuvent même être anonymisées. Cependant, **leur combinaison finit souvent par créer un nouveau scénario**, dans lequel les données personnelles et notamment les catégories spéciales de données personnelles. **Celles-ci sont généralement appelées données déduites**, c'est-à-dire "toutes les données à caractère personnel qui ont été créées par le responsable du traitement dans le cadre du traitement des données, par exemple par un processus de personnalisation ou de recommandation, par une catégorisation ou un profilage des utilisateurs effectué sur la base des données à caractère personnel fournies

834 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

par la personne concernée (données observées ou brutes)[835] . Il s'**agit également de données à caractère personnel, ce qui signifie qu'elles sont soumises au RGPD et à la réglementation applicable en matière de protection des données**.

3.1 Traitement automatisé des données personnelles, profilage, prise de décision automatisée : comprendre les différences

Un responsable du traitement doit faire la distinction entre tous ces concepts, car ils ont des implications juridiques différentes. Ils sont clairement liés, mais pas du tout équivalents, et le principal résultat juridique concerne la question de savoir si un certain traitement relève ou non de l'article 22 du RGPD.

En effet, la casuistique peut être très variée : il peut y avoir un traitement automatisé des données sans profilage ; cependant, le profilage peut également servir de support à des processus décisionnels automatisés ; de plus, le profilage peut servir de base à des processus décisionnels entièrement automatisés ; mais les processus décisionnels automatisés peuvent être effectués avec ou sans profilage préalable. Par exemple, tout traitement automatisé de données à caractère personnel n'implique pas nécessairement un profilage. En outre, la création d'un profil d'utilisateur n'implique pas toujours un profilage. Un profil d'utilisateur peut inclure des informations telles que le nom d'utilisateur et les caractéristiques observées sans créer ou déduire de nouvelles données, ni associer à une personne des connaissances dérivées d'autres données ou processus analytiques.

Le tableau suivant montre les différences entre ces concepts[836] :

Concept	**Définition**	**Exemple**
Traitement automatisé des données à caractère personnel	Le RGPD s'applique au "traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier" (article 2 du RGPD).	Traitement effectué par les caméras photo qui imposent des amendes liées au dépassement de la vitesse autorisée. Stockage des données dans un formulaire Excel permettant de les trier automatiquement par date, nom, etc.

835 A29WP, Lignes directrices sur le droit à la portabilité des données, à l'adresse : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/right-data-portability_en.

836 Ce tableau a été construit sur la base des distinctions faites par Jorge García ici : https://jorgegarciaherrero.com/decisiones-automatizadas-profiling-inteligencia-artificial-que-son/#De_que_hablamos_cuando_hablamos_de_profiling_en_que_se_diferencia_el_profiling_de_las_decisiones_automatizadas_del_art_22.

Profilage	Il est défini par le RGPD comme "consistant à utiliser des données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant la performance au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique." Le profilage se compose de trois éléments: - le traitement automatisé des données ; - les données personnelles ; et - il doit avoir pour but d'évaluer des aspects personnels concernant une personne physique.	Les photos prises par les appareils photo sont incluses dans un fichier correspondant au conducteur qui subit l'amende. Elles sont utilisées pour durcir les sanctions en cas de récidive ou de mauvaises habitudes de conduite.
Processus de décision entièrement automatisés de l'article 22 du RGPD.	Il s'agit de décisions prises et exécutées sans intervention humaine décisive, avec des effets juridiques ou qui affectent de manière significative et similaire les personnes concernées.	Le système de caméras est conçu pour déclencher l'envoi automatique d'une sanction personnalisée en fonction de l'historique des sanctions, du comportement du contrevenant avant l'action sanctionnée, de l'âge du véhicule, de la vitesse moyenne des autres conducteurs à ce moment-là, etc.

3.2 Avoir une bonne connaissance du cadre juridique relatif au profilage

Le profilage a été défini à l'art. 4 du RGPD comme "toute forme de traitement automatisé de données à caractère personnel qui implique l'utilisation de données à

caractère personnel pour évaluer des aspects spécifiques d'une personne, notamment pour analyser ou prédire des aspects liés à la performance professionnelle, à la situation financière, à la santé, aux préférences personnelles, aux intérêts, à la fiabilité, au comportement, à la localisation ou aux déplacements de cette personne".

En principe, le **profilage peut apporter aux utilisateurs des avantages importants**, puisqu'il pourrait accroître l'efficacité du système, économiser des ressources ou contribuer à fournir un meilleur service. Par exemple, le profilage par une télévision intelligente pourrait nous aider à trouver des séries qui correspondent bien à nos préférences sans passer beaucoup de temps à les chercher par nous-mêmes. Toutefois, il est également clair qu'il pourrait servir à des fins plus obscures et discriminatoires, qui comportent des risques importants pour les droits et libertés des personnes" et peuvent "perpétuer les stéréotypes existants et la ségrégation sociale" en l'absence de garanties appropriées.

La prudence concernant le profilage doit être particulièrement adoptée lorsque les responsables du traitement commencent à mélanger les données. **Le rapprochement de différents types de données à caractère personnel peut révéler des informations sensibles sur les personnes.** Parfois, ces processus aboutissent même à traiter des données personnelles de catégories spéciales de manière inaperçue. Par exemple, le fait de mélanger des catégories de données non spéciales, telles que des données sur les préférences, la localisation et les connexions aux médias sociaux, peut permettre de déduire avec un haut degré de réussite l'orientation sexuelle des personnes ou leurs croyances religieuses. Cela peut se produire sans que les personnes concernées en aient conscience. Il va sans dire que ces conséquences doivent être soigneusement évitées.

Afin d'aborder ces questions, les développeurs d'IA devraient avoir une bonne connaissance de l'article 22 du RGPD. Cette clause stipule que "les personnes concernées ont le droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques les concernant ou les affecte de manière significative de façon similaire." Sur cette base, il y a quelques considérations importantes à faire.

- Premièrement, l'interdiction de la "prise de décision entièrement automatisée" ne s'applique que lorsque la décision fondée sur une telle technologie "**a un effet juridique sur quelqu'un ou l'affecte de manière significative de façon similaire**". Les lignes directrices de l'EDPB citent à titre d'exemple : le rejet d'un processus de sélection, le refus d'un crédit ou d'une assurance, ou l'application de prix différents à un même groupe. Il n'est pas nécessaire que cela affecte un grand nombre de personnes. Dans d'autres situations, il n'est pas toujours évident pour le responsable du traitement d'évaluer si le processus décisionnel entièrement automatisé crée des effets significatifs. Dans ces cas, nous recommandons de demander conseil au DPD.

- Deuxièmement, il faut garder à l'esprit qu'**il n'y a pas de "décision fondée uniquement sur un traitement automatisé" si la décision est examinée par un être humain qui "tient compte d'autres facteurs pour prendre la décision finale"**. Si un être humain ne fait que ratifier ce qu'un outil énonce, cela ne compterait pas comme une intervention humaine en tant que telle. L'élément humain doit avoir suffisamment de pouvoir pour rectifier la recommandation de l'outil. Parmi les facteurs d'évaluation, on peut citer le nombre de fois où l'humain s'écarte de la recommandation automatisée, si la personne dispose d'une autonomie au sein de l'organisation pour prendre la décision, et quels autres facteurs sont pris en compte par la personne qui ne sont pas inclus dans le modèle automatisé.
- En outre, l'article 22(2) introduit quelques exceptions à cette interdiction générale du profilage ou de la prise de décision automatisée. En effet, les lignes directrices publiées par l'A29WP déclarent que l'**interdiction ne s'applique pas si le profilage ou la prise de décision automatisée est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;** autorisé par le droit de l'Union ou des États membres auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la protection des droits et libertés et des intérêts légitimes de la personne concernée (mesures techniques et organisationnelles, garanties, etc.) ; ou est fondé sur le consentement explicite de la personne concernée. C'est-à-dire que dans ces trois circonstances, les processus décisionnels entièrement automatisés sont autorisés. Par exemple, un service consistant à proposer des contenus médias personnalisés en fonction de vos préférences déclarées et de vos données de consommation, nécessitera nécessairement un profilage. Si la "nécessité" peut être prouvée, le profilage entièrement automatisé sera autorisé.

Par conséquent, le profilage ou la prise de décision automatisée peuvent être acceptables si l'une de ces circonstances s'applique, à condition que le traitement ne contrevienne pas au règlement sur la protection des données de toute autre manière possible. Cependant, même dans ces cas, des actions supplémentaires devraient être intégrées. Les développeurs IdO doivent être particulièrement prudents s'ils traitent des catégories spéciales de données déduites par les systèmes. L'article 22, paragraphe 4, contient des limitations quant à l'utilisation de catégories spéciales de données pour une prise de décision ou un profilage entièrement automatisé. Dans ce cas, l'art. 22 doit être appliqué conformément à l'art. 9 du RGPD. Plus précisément, lorsqu'il s'agit de catégories particulières de données, les décisions entièrement automatisées ne sont autorisées qu'avec le consentement explicite de la personne concernée (art. 9, paragraphe 1, point a)) ou pour des raisons d'intérêt public important, sur la base de la législation existante (art. 9, paragraphe 1, point g)). Par exemple, un responsable du traitement souhaite créer des profils de citoyens pour déduire les risques de contracter un virus et prévenir une pandémie. À cette fin, différentes sources de données doivent être mélangées, y compris des données relatives à la santé. Cela pourrait être considéré comme nécessaire à la protection d'un intérêt public important. En outre, il doit exister une législation européenne ou nationale autorisant ce traitement. Si toutes ces circonstances sont réunies, l'art. 9, paragraphe 2, point g), est applicable, et le responsable du traitement peut donc bénéficier de l'exception prévue à l'art. 22(4) autorisant ce profilage entièrement automatisé.

Dans tous les cas, toutes les autres obligations et garanties doivent être remplies. Par exemple, les obligations d'information, l'évaluation d'un AIPD, etc. En outre, l'art. 22(3) contient des garanties supplémentaires qui doivent être observées lors de la prise de certaines décisions entièrement automatisées, comme le droit d'obtenir une intervention humaine, d'exprimer le point de vue de la personne concernée et de contester la

Encadré 6 : Profilage des effets négatifs et analyse inférentielle

Méthodes possibles de surveillance et de profilage pouvant entraîner des problèmes de confidentialité et de discrimination dans les systèmes IdO :

- le profilage par inférence de données, que ce soit sur la base de celles fournies en premier lieu par le sujet des données ou d'autres sources de données (par exemple, le comportement de navigation sur Internet) ;
- le profilage en reliant les ensembles de données de l'IdO ;
- le profilage qui se produit lorsque les données sont partagées avec des tiers qui combinent les données avec d'autres ensembles de données (par exemple, les fournisseurs de produits, l'assistance technique).

décision. Les personnes concernées devraient être informées de toutes ces informations et des droits et actions correspondants qu'elles pourraient intégrer.

Encadré 7 : Déduire des données. Exemple

"La société X a développé une application qui, en analysant les données brutes des signaux d'électrocardiogramme générés par des capteurs commerciaux couramment disponibles pour les consommateurs, est capable de détecter des schémas de dépendance aux drogues. Le moteur de l'application peut extraire des caractéristiques spécifiques des données brutes de l'ECG qui, selon les résultats d'enquêtes précédentes, sont liées à la consommation de drogues. Le produit, compatible avec la plupart des capteurs du marché, pourrait être utilisé comme une application autonome ou par le biais d'une interface web nécessitant le téléchargement des données. Très probablement, le consentement explicite sera la base légale la mieux adaptée pour ce traitement."

Source : Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

Comme indiqué précédemment, le processus de profilage est "souvent invisible pour la personne concernée". Il fonctionne en créant des données dérivées ou déduites sur les individus. Les individus ont des niveaux de compréhension différents et peuvent trouver difficile de comprendre les techniques complexes impliquées dans les processus de profilage et de prise de décision automatisée". [837]

3.3 Introduire des mesures de protection et minimiser les risques

La prise de décision et le profilage entièrement automatisés sont des activités de traitement sensibles qui doivent être prises avec précaution. Les responsables du traitement doivent en être conscients et agir en conséquence afin d'identifier les risques, de les réduire et de mettre en place des garde-fous et des garanties.

Nous venons de mentionner l'existence de droits des personnes concernées liés à ces traitements et reconnus à l'article 22.3, à savoir le droit d'obtenir une intervention humaine, d'exprimer le point de vue de la personne concernée et de contester la décision.

En outre, les responsables du traitement doivent informer de manière simple, transparente et complète de l'existence de processus automatisés et d'activités de

837 Groupe de travail Article 29 (2017) Lignes directrices sur la prise de décision individuelle automatisée et le profilage aux fins du règlement 2016/679. Adopté le 3 octobre 2017, tel que révisé en dernier lieu et adopté le 6 février 2018. Commission européenne, Bruxelles, p.9. Disponible à l'adresse : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

profilage lorsqu'ils relèvent de la définition de l'article 22 du RGPD. L'information doit également s'étendre à une explication de la logique impliquée dans le processus et à l'existence des droits susmentionnés.

Les informations sur la logique d'un système et les explications des décisions doivent donner aux individus le contexte nécessaire pour décider si, et pour quels motifs, ils souhaitent demander une intervention humaine. Dans certains cas, des explications insuffisantes peuvent inciter les individus à recourir inutilement à d'autres droits. Les demandes d'intervention, l'expression de points de vue ou les contestations sont plus susceptibles de se produire si les individus estiment ne pas avoir une compréhension suffisante de la manière dont la décision a été prise.[838]

En outre, l'article 35(3) (a) du RGPD stipule l'obligation pour le responsable du traitement de réaliser une AIPD dans le cas d'une évaluation systématique et extensive d'aspects personnels concernant des personnes physiques qui est basée sur un traitement automatisé, y compris le profilage, et sur laquelle sont fondées des décisions produisant des effets juridiques concernant la personne physique ou l'affectant de manière significative de façon similaire. Les responsables du traitement doivent savoir que chaque pays a désormais soumis à l'EDPB sa liste des cas dans lesquels une AIPD est requise. Si le responsable du traitement se trouve dans l'EEE, cette liste doit également être vérifiée localement.[839] (Conformément à l'article 37, paragraphe 1, point b) et paragraphe 5 du RGPD, les responsables du traitement doivent désigner un délégué à la protection des données lorsque "les activités principales du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, en raison de leur nature, de leur portée et/ou de leurs finalités, nécessitent un suivi régulier et systématique des personnes concernées à grande échelle".

Les responsables du traitement sont également tenus de conserver un registre de toutes les décisions prises par un outil d'IA dans le cadre de leurs obligations en matière de responsabilité et de documentation. Ce registre doit également indiquer si une personne a demandé une intervention humaine, a exprimé un point de vue, a contesté la décision et si une décision a été modifiée à la suite de cette intervention[840] (voir la section "Responsabilité" dans les "Principes" de la partie II des présentes lignes directrices).

838 ICO (2020) Guidance on the AI auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.94. Disponible à l'adresse : https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf.

839 EDPB (2019) Analyse d'impact sur la protection des données. Conseil européen de la protection des données, Bruxelles. Disponible à l'adresse : https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-DPIA_es .

840 ICO (2020) Guidance on the AI auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.94-95. Disponible à l'adresse : https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf .

Voici quelques actions supplémentaires qui pourraient être extrêmement utiles pour éviter la prise de décision automatisée : [841]

- Prenez en compte les exigences du système nécessaires pour soutenir une révision humaine significative **dès la phase de conception.** En particulier, les exigences d'interprétabilité et la conception d'une interface utilisateur efficace pour soutenir les examens et les interventions humaines. Cela peut en effet être considéré comme une obligation contraignante pour les responsables du traitement, conformément au principe de la protection des données dès la conception.

- Concevoir et dispenser une formation et un soutien appropriés aux examinateurs humains. Il s'agit notamment de comprendre quelles sont les variables sur lesquelles repose le modèle de prise de décision ou de profilage et, surtout, quelles sont les variables qui ne sont pas prises en compte dans le modèle. Ces éléments peuvent être essentiels pour repérer les spécificités d'une personne concernée qui font d'elle une aberration dans le modèle ou dont les circonstances justifient une décision différente.

- Donnez au personnel l'autorité, les incitations et le soutien appropriés pour répondre aux préoccupations des personnes ou les transmettre à un échelon supérieur et, si nécessaire, annuler la décision de l'outil d'IA. Par exemple, si les réviseurs humains subissent des pressions organisationnelles ou des conséquences professionnelles négatives s'ils s'écartent de la décision automatisée, leur autorité et leur indépendance seront mises en danger.

Liste de contrôle : Prise de décision et profilage automatisés

 Le responsable du traitement informe les utilisateurs du type de données qui sont collectées et traitées ultérieurement par les capteurs IdO, des autres types de données qu'ils reçoivent de sources externes et de la manière dont elles seront traitées et combinées.

 Les systèmes IdO peuvent faire la distinction entre les différents individus qui utilisent le même appareil, de sorte qu'ils ne puissent pas prendre connaissance des activités des autres sans une base juridique appropriée.

 Les responsables du traitement collaborent avec les organismes de normalisation et les plateformes de données pour soutenir un protocole commun permettant d'exprimer des préférences en ce qui concerne la collecte et le traitement des données par les responsables du traitement, en particulier lorsque des dispositifs non intrusifs

841 Ibid, p.95.

collectent ces données.

 Les responsables du traitement ont activé des entités locales de contrôle et de traitement (les "personal privacy proxies") permettant aux utilisateurs d'avoir une vision claire des données collectées par leurs appareils et facilitant le stockage et le traitement local sans avoir à transmettre les données au fabricant de l'appareil.

 Les systèmes IdO fournissent :

- une vue d'ensemble de quelles données personnelles ont été divulguées à quel contrôleur de données et en vertu de quelles politiques ;
- un accès en ligne aux données personnelles et à la manière dont elles ont été traitées ;
- des capacités de contre-profilage aidant l'utilisateur à anticiper la manière dont ses données correspondent à des profils de groupes pertinents, ce qui peut avoir une incidence sur les opportunités ou les risques futurs (cela n'est pas exigé par la loi, mais recommandé).

 Les systèmes IdO offrent des choix granulaires lors de l'octroi de l'accès aux applications. La granularité ne concerne pas seulement la catégorie de données collectées, mais aussi le moment et la fréquence à laquelle les données sont capturées. À l'instar de la fonction "ne pas déranger" sur les smartphones, les dispositifs IdO devraient proposer une option "ne pas collecter" pour programmer ou désactiver rapidement les capteurs.
 Le profilage et la prise de décision automatisée n'ont lieu que lorsqu'une base légale s'applique et que des garanties adéquates ont été mises en œuvre. Des mécanismes permettant d'en informer toutes les personnes concernées ont été mis en place.

 Les responsables du traitement ont effectué une AIPD.

 Les responsables du traitement ont consulté une DPD sur le traitement.

 Les responsables du traitement se sont assurés que toutes les garanties prévues par l'article 22 du RGPD ont été mises en œuvre de manière adéquate.

 Les responsables du traitement se sont assurés que toutes les personnes intervenant dans le profilage et le traitement automatique des données ont reçu une formation adéquate sur les questions de la protection des données.

 Les responsables du traitement ont documenté toutes les informations concernant ce problème.

4 Loyauté et transparence

La loyauté est un principe essentiel du RGPD. On peut dire que l'ensemble de la protection des données, et donc le RGPD, concerne la loyauté envers les personnes

concernées. Le RGPD peut être considéré comme précisant ce que signifie concrètement le terme *"loyauté"*. Dans le cas des TIC, il s'agit principalement d'éviter que personne ne soit exclu de la possibilité de bénéficier des outils, c'est-à-dire que tout le monde ait les mêmes droits fondamentaux et les mêmes opportunités de profiter des avancées technologiques. De même, il ne doit pas y avoir de discrimination sur la base des aspects fondamentaux de notre identité qui sont inaliénables, tels que le sexe, la race, l'âge, l'orientation sexuelle, l'origine nationale, la religion, la santé et le handicap, etc. En d'autres termes, en termes d'IdO, la loyauté est principalement liée à la nécessité de rendre les outils faciles à utiliser pour ceux qui ne sont pas particulièrement compétents dans les technologies numériques et d'éviter que le système ne crée une discrimination en introduisant des biais injustes (voir la sous-section "Loyauté" dans "Léicité, loyauté et transparence" dans "Concepts principaux", partie II des présentes lignes directrices).

La transparence, en revanche, est essentielle pour aider les personnes concernées à avoir confiance dans les systèmes et dispositifs IdO. En effet, les exigences de transparence sont clairement liées au principe de loyauté, car plus il est difficile pour l'utilisateur de comprendre le système IdO, plus la différence entre les différents types d'utilisateurs est grande. La transparence montre que le responsable du traitement agit de manière responsable. En revanche, le manque de transparence générale (et de droits à l'information en particulier) est contraire aux obligations du RGPD et peut entraîner des amendes élevées pour le responsable du traitement. Elle s'applique à tous les éléments pertinents pour un système IdO : les données, le système et les processus par lesquels il est conçu et exploité, l'interaction avec d'autres systèmes IdO, l'utilisation (ou non) d'outils d'IA, la réalisation de profilage ou de prise de décision automatique, etc. En outre, cela revient à savoir qui : qui est le responsable du traitement, à qui les données sont divulguées, qui est le DPD (s'il y en a un), etc.

La transparence est décrite dans le RGPD sous la forme d'exigences détaillées concernant les informations qui doivent être fournies par le responsable du traitement aux personnes concernées et aux autorités de contrôle. L'objectif de la transparence est d'informer les personnes concernées dès le départ de l'existence du traitement et de ses principales caractéristiques, conformément aux articles 12 à 14. D'autres informations (telles que les données concernant la personne concernée) sont disponibles sur demande (lors de l'exercice d'un droit d'accès ou d'un droit à la portabilité des données, par exemple). Les personnes concernées doivent également être informées de certains événements, notamment des violations de données (dans le cas où la personne concernée est exposée à un risque élevé). De toute évidence, la transparence est une condition préalable à la détection et à l'intervention en cas de non-conformité (voir "Transparence" dans la section "Licéité, loyauté et transparence" des "Concepts principaux", partie II des présentes lignes directrices).

Dans le cas de l'IdO, les responsables du traitement doivent garder à l'esprit qu'il est difficile de garantir la transparence aux personnes concernées, en raison d'un certain nombre de facteurs qui entravent cet objectif. Tout d'abord, il faut considérer qu'un système IdO interagit généralement avec d'autres, traitant de nombreuses données personnelles. En effet, "comme l'IdO repose sur le principe du traitement extensif des données par le biais de ces capteurs conçus pour communiquer de manière discrète et échanger des données de manière transparente, il est étroitement lié aux notions d'informatique "envahissant" et "ubiquitaire"."[842] En effet, dans le cas de l'IdO, les capteurs sont en réalité conçus pour être non intrusifs, c'est-à-dire aussi invisibles que possible. Par conséquent, dans de nombreux cas, la personne concernée n'est pas consciente du traitement des données en raison d'un manque d'informations disponibles. Dans d'autres cas, les informations disponibles ne sont pas synonymes de transparence et de sensibilisation pour les personnes concernées. Dans ces cas, en plus d'une formulation informative, la transparence peut signifier l'utilisation d'icônes lorsque des données telles que la localisation sont collectées, et la désactivation de ces icônes lorsque les données ne sont pas collectées. Les responsables du traitement doivent évaluer ce que signifie la transparence dans leur développement et leur dispositif spécifiques.

En outre, "une fois les données stockées à distance, elles peuvent être partagées avec d'autres parties, parfois sans que la personne concernée en ait conscience. Dans ces cas, la transmission ultérieure de leurs données est donc imposée à l'utilisateur qui ne peut l'empêcher sans désactiver la plupart des fonctionnalités de l'appareil."[843] Cette situation peut être renforcée par les données de plus en plus courantes stockées à l'intérieur de l'appareil. Dans ce cas, les données ne quittent pas l'appareil, ce qui renforce toute la transparence, le contrôle des personnes concernées sur leurs données et, selon le cas, la sécurité.

En outre, les systèmes IdO utilisent souvent des outils d'intelligence artificielle. Comme exposé en détail dans la section correspondante, ces outils souffrent souvent de divers types d'opacité, ce qui empêche le respect adéquat des exigences de transparence (voir "Transparence", dans la partie IV (IA) des présentes lignes directrices).

Enfin, mais c'est important, les développeurs IdO doivent garantir la transparence en utilisant un certain nombre d'**outils complémentaires.** La désignation d'un DPD, qui sert ensuite de point de contact unique pour les demandes des personnes concernées, est une excellente option. Préparer des registres de traitement adéquats pour les autorités de

842 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

843 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

contrôle, ou réaliser des AIPD, sont également des mesures fortement recommandées pour promouvoir la transparence. Entreprendre des analyses qui évaluent l'efficacité et l'accessibilité des informations fournies aux personnes concernées contribue à garantir la mise en œuvre efficace de ce principe. Ou encore, prévoir l'interopérabilité entre différents systèmes afin que les personnes concernées puissent exercer la portabilité ou prévoir des moyens faciles de télécharger ses données et d'exercer soi-même un droit d'accès.

4.1 Faites de votre mieux pour éviter d'élargir la division numérique

L'IdO est une technologie complexe qui implique l'utilisation de nombreux systèmes IdO différents. Certains traitements sont effectués automatiquement et il faut beaucoup d'attention et de compétences pour être conscient des implications de toutes les actions entreprises par les outils. Ainsi, il arrive souvent que seul un groupe sélectif bénéficie de certains produits concrets basés sur les technologies IdO, principalement les personnes ayant un niveau d'éducation ou des revenus plus élevés, un fort soutien social, les jeunes, etc.[844] D'autres groupes, tels que les personnes âgées, les groupes à faible revenu ou à faible niveau d'éducation, les personnes handicapées, etc. peuvent ainsi être exclus de l'adoption de la technologie. Ces circonstances créent un scénario injuste, qui est particulièrement inacceptable si nous parlons d'outils qui peuvent être utilisés pour permettre aux citoyens d'accéder aux services publics.

Afin de minimiser cette discrimination numérique injuste, les développeurs IdO devraient prendre certaines mesures qui pourraient bien servir à aider tout le monde à accéder à l'outil, en mettant en œuvre des **fonctionnalités supplémentaires ou des interfaces de contrôle faciles à utiliser qui permettent de gérer les paramètres techniques et de confidentialité.** Par exemple, la conception de conditions d'utilisation claires et de systèmes de contrôle IdO conviviaux devrait être un objectif important. En général, la **complexité doit être évitée dans la mesure du possible**. Si cela n'est pas possible, des instructions faciles à comprendre doivent être écrites ou enregistrées et être accessibles aux utilisateurs de la manière la plus conviviale possible. "L'utilisation des affordances des dispositifs IdO pour créer de nouvelles interactions par le biais de méthodes de livraison telles que les vidéos, l'audio et le retour d'informations à partir de gestes tels que l'agitation des mains ou les lumières et sons clignotants peut redéfinir les mécanismes de consentement et s'éloigner de la domination des conditions contractuelles formelles."[845]

---

844 Van Deursen, A. J. A. M. , &Mossberger, K. (2018). N'importe quoi pour n'importe qui ? Une nouvelle fracture numérique dans les compétences liées à l'internet des objets. *Politique et Internet*, *10*(2), 122-140.

845 Urquhart, L., Sailaja, N. & McAuley, D. Réaliser le droit à la portabilité des données pour l'Internet domestique des objets. *Pers Ubiquit Comput* 22, 317-332 (2018).

Le système IdO doit être conçu de manière à faciliter la traduction des préférences et des besoins des utilisateurs dans l'outil, de manière distribuée et coopérative, afin que des décisions appropriées soient prises concernant les ressources contrôlées. Il est fortement recommandé de fournir un soutien actif qui permette aux utilisateurs de l'IdO de profiter du système**. Une meilleure convivialité réduira la demande de compétences techniques, tandis qu'une meilleure compréhensibilité réduira les besoins en compétences d'ordre supérieur.** Cela inclut, bien entendu, la décision de partager certaines données ou d'autoriser le traitement et la prise de décision automatisée. En outre, si l'outil IdO doit intégrer des outils conçus par des tiers (des applications, par exemple), les développeurs devraient opter pour ceux qui fonctionnent le mieux afin d'éviter la discrimination numérique.

4.2 Éviter les biais

Les biais créent des préjudices et des discriminations à l'encontre de certains groupes ou de certaines personnes. Le préjudice peut également résulter de l'exploitation intentionnelle des biais (des consommateurs) ou de la pratique d'une concurrence déloyale, telle que l'homogénéisation des prix par le biais de la collusion ou d'un marché non transparent. Les systèmes IdO pourraient contribuer à exacerber cette terrible situation de **deux façons :** par l'incorporation d'outils d'IA biaisés dans le système IdO ou par la constitution d'ensembles de données biaisés grâce à une collecte inadéquate des données produites par les personnes concernées. Si l'utilisation de ces données alimente le profilage ou la prise de décision automatisée, cela pourrait avoir des conséquences sociales inacceptables.

Ainsi, les développeurs IdO devraient intégrer certaines actions afin d'éviter les biais injustes provoqués par l'utilisation de l'IA. D'une part, ils ne devraient intégrer à leur outil que des dispositifs ou des outils d'IA qui peuvent démontrer une absence de biais. Des outils tels que l'audit algorithmique éthique devraient être mis en œuvre pour signaler les discriminations. Des dispositifs d'audit interne devraient être envisagés pour se prémunir contre la discrimination des groupes protégés, mais aussi pour protéger les victimes de discriminations non anticipées.[846] D'autre part, le système IdO doit être conçu de manière à ce que la prise de décision automatisée sur la base des données recueillies soit en mesure d'éviter les biais. Cela pourrait se faire en utilisant les outils généralement utilisés dans l'IA à cette fin (voir la section "Loyauté" dans la partie IV sur l'IA des présentes lignes directrices).

Il est important de mentionner que l'IdO peut également être à l'origine de biais importants dus aux **inexactitudes** provoquées par le mode de fonctionnement de ces

846 Wachter, Sandra, Défis normatifs de l'identification dans l'Internet des objets : Privacy, profiling, discrimination, et le RGPD, Computer Law & Security Review, Volume 34, Issue 3, 2018, pages 436-449.

systèmes. Par exemple, les personnes concernées pourraient fournir des données incorrectes ou ne pas comprendre pleinement les conséquences si leur comportement est constamment surveillé. Cela peut entraîner une violation du principe de précision lorsque la situation aurait pu être évitée ou résolue par le responsable du traitement si elle avait été prise en compte. De même, le traitement des données peut également entraîner des biais inattendus car les relations potentielles entre les catégories de données, révélées uniquement par l'agrégation et la mise en relation d'ensembles de données disparates, peuvent ne pas être connues au moment de la collecte des données. Il se peut que, si les systèmes utilisent ces données pour établir des profils, des inexactitudes puissent entraîner des recommandations biaisées, par exemple. Afin d'éviter un tel scénario, une évaluation critique de la provenance des données est nécessaire. À cette fin, des mesures organisationnelles doivent être mises en œuvre pour garantir la précision et la fiabilité des données collectées, tout en respectant le droit des utilisateurs de ne pas divulguer des informations privées (par exemple, en confirmant la précision d'un registre).

4.3 Fournir des informations adéquates afin d'assurer la transparence

Les systèmes IdO sont généralement des outils complexes qui traitent de nombreuses données à caractère personnel en lien avec d'autres systèmes IdO ou par des outils incorporés à l'appareil. Cela crée un scénario complexe, car, comme l'a indiqué le GT Article 29, "l'interaction entre les objets, entre les objets et les dispositifs des individus, entre les individus et d'autres objets, et entre les objets et les systèmes dorsaux entraînera la génération de flux de données qui peuvent difficilement être gérés avec les outils classiques utilisés pour assurer une protection adéquate des intérêts et des droits des personnes concernées."

Les responsables du traitement doivent être conscients que, même si cela peut être difficile à atteindre, les personnes concernées doivent être en mesure de comprendre comment, et dans quel but, le système IdO utilise leurs données personnelles pour fonctionner et prendre ses décisions. En général, cela signifie que les **développeurs IdO doivent intégrer dans le système des fonctionnalités capables de fournir ces connaissances de la manière la plus simple possible**. L'explicabilité - c'est-à-dire la capacité d'expliquer les processus techniques d'un système IdO et la logique des décisions qu'il prend - est essentielle dans le cas de l'IdO, en particulier s'il intègre un outil d'intelligence artificielle (voir la section "Transparence" dans la partie IV des présentes lignes directrices, "Exigences en matière d'intelligence artificielle pour les innovateurs et les développeurs").

À cet égard, le groupe de travail Article 29 a déclaré que "les méthodes permettant de donner des informations, d'offrir un droit de refus ou de demander le consentement

doivent être aussi conviviales que possible. En particulier, les politiques d'information doivent se concentrer sur des informations compréhensibles par l'utilisateur et ne doivent pas se limiter à une politique générale de confidentialité sur le site web des responsables du traitement.[847] À cet égard, les responsables du traitement doivent tenir compte des spécificités du dispositif IdO, à la lumière de problèmes tels que les petits écrans qui peuvent rendre la lecture des politiques de confidentialité presque impossible, ou même l'absence totale d'écrans. Les systèmes à double couche pourraient être particulièrement utiles dans les scénarios où la quantité d'informations et leur complexité sont difficiles à gérer. Une première couche fournissant à l'utilisateur les informations essentielles et une seconde couche contenant des informations et des explications plus approfondies semblent raisonnables.

En général, les systèmes IdO doivent être en mesure de fournir une vue d'ensemble de "quelles données personnelles ont été divulguées à quel contrôleur de données et dans le cadre de quelles politiques ; de fournir un accès en ligne aux données personnelles et à la manière dont elles ont été traitées ; et de fournir des capacités de contre-profilage aidant l'utilisateur à anticiper la manière dont ses données correspondent aux profils de groupes pertinents, ce qui peut affecter les opportunités ou les risques futurs".[848] Si le responsable du traitement "prévoit" d'effectuer un traitement à des fins autres que celles pour lesquelles les données ont été collectées, il doit informer au préalable les utilisateurs ou les personnes concernées de ce nouveau traitement, en fournissant des informations et en se conformant à toutes les autres exigences, telles que l'existence d'une base juridique pour cette nouvelle finalité ou la réalisation d'une évaluation de compatibilité. Sur la base des obligations ci-dessus, et en les appliquant spécifiquement à l'IdO, une première couche d'information doit être fournie aux utilisateurs avant qu'ils ne commencent à utiliser le dispositif. En outre, les exigences en matière d'information stipulent que des informations complètes doivent être fournies avant le début du traitement, de sorte que les utilisateurs doivent avoir un moyen d'y accéder avant d'enregistrer ou d'accéder au dispositif IdO.

Selon le RGPD, les informations qu'un système IdO doit fournir aux personnes concernées varient selon que ces informations ont été obtenues auprès d'elles ou déduites par le système.

- Si les données sont obtenues directement auprès de la personne concernée (art. 13 du RGPD)

Le responsable du système IdO doit informer l'utilisateur, avant le traitement, de l'identité du responsable du traitement, des coordonnées du DPD, des finalités

847 Groupe de travail Art 29 sur la protection des données (2014) Avis 8/2014 sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

848 Weber, Rolf H., " Internet of Things : Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618, 625 ; de même, Tene et Polonetsky (n 18).

spécifiques du traitement ; de la base juridique du traitement et, le cas échéant, des intérêts légitimes sur lesquels se fonde le traitement [849] , des bases juridiques applicables à chaque finalité ; des destinataires ou catégories de destinataires des données ; de l'existence de transferts internationaux ; le cas échéant, les délais de conservation des données ou les critères utilisés pour déterminer ces délais ; les modalités d'exercice des droits des personnes concernées et le droit d'introduire une réclamation auprès de l'autorité de contrôle ; et dans le cas de décisions automatisées, y compris le profilage, le responsable du traitement doit fournir des informations pertinentes sur la logique impliquée et les conséquences attendues de ce traitement pour la personne concernée.

- Si les données personnelles ne sont pas obtenues auprès de l'utilisateur (art. 14 du RGPD)

Dans ce cas, si les données personnelles sont obtenues auprès d'un tiers, le responsable du système IdO doit informer l'utilisateur des dispositions de l'art. 13 du RGPD, et communiquer les informations concernant l'origine ou la source des données, spécifiquement si elles proviennent de sources accessibles au public. À cet égard, les responsables du traitement doivent garder à l'esprit que le concept de "sources accessibles au public" n'est pas une liste exhaustive mais plutôt une liste étroite, et qu'il n'inclut pas les médias sociaux ou Internet. Les informations doivent être fournies dans un délai d'un mois "au plus tard" à l'utilisateur de l'IdO.

Liste de contrôle : loyauté et transparence[850]

Loyauté

 Les responsables du traitement ont mis en œuvre des fonctionnalités ou des interfaces de contrôle faciles à utiliser qui permettent de gérer les paramètres techniques et de confidentialité.

 Les systèmes IdO ont été conçus de manière à faciliter que les préférences et les besoins des utilisateurs soient traduits à l'outil de manière distribuée et coopérative afin que des décisions appropriées concernant les ressources contrôlées soient prises.

 Les responsables du traitement ont mis en place des mesures adéquates pour éviter les biais provoqués par l'utilisation d'outils d'IA.

849 N'oubliez pas que, selon la jurisprudence récente de l'autorité espagnole de protection des données, l'APED, les intérêts qui servent de fondement à la base juridique de l'art. 6.1.f du RGPD ne seraient pas les mêmes que les finalités du traitement.

850 Toutes ces exigences ne sont pas des exigences légales *stricto sensu*, mais elles peuvent toutes être considérées comme des exigences éthiques.

 Les responsables du traitement ont mis en place des mesures pour éviter de collecter des ensembles de données biaisées.

Transparence

 Les systèmes IdO fournissent :

- une vue d'ensemble de quelles données personnelles ont été divulguées à quel contrôleur de données, dans le cadre de quelles politiques ;
- un accès en ligne aux données personnelles et à la manière dont elles ont été traitées ;
- des capacités de contre-profilage aidant l'utilisateur à anticiper la manière dont ses données correspondent à des profils de groupes pertinents, ce qui peut avoir une incidence sur les opportunités ou les risques futurs.

 Si les données à caractère personnel ont été fournies directement par la personne concernée, les responsables du traitement ont fourni toutes les informations énumérées à l'article 13 du RGPD.

 Si les données personnelles n'ont pas été fournies par la personne concernée, les responsables du traitement ont fourni toutes les informations énumérées à l'article 14 du RGPD.

 Si les données à caractère personnel sont fournies directement par la personne concernée, les informations sont fournies avant le traitement et, au plus tard, au moment où elles sont collectées auprès de la personne concernée.

 Si les données personnelles ne sont pas fournies par la personne concernée, les informations sont fournies :

- dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais au plus tard dans un délai d'un mois ;
- si les données à caractère personnel doivent être utilisées pour la communication avec la personne concernée, au plus tard au moment de la première communication avec cette personne ;
- si une communication à un tiers est envisagée, au plus tard lors de la première communication des données à caractère personnel.

 L'information est fournie de manière concise, transparente, intelligible et facilement accessible. Elle est claire et expurgée dans un langage simple.

 Les responsables du traitement ont documenté toutes les informations concernant ces problèmes.

5 Gouvernance des données : principes de minimisation, de limitation de la finalité et de limitation du stockage.

Le principe de minimisation stipule que les données à caractère personnel doivent être **adéquates**, **pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées. D'autre part, selon l'article 5, paragraphe 1, point e), du RGPD, les données à caractère personnel doivent être "conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées". Enfin, la limitation de la finalité signifie que les données à caractère personnel ne peuvent pas être traitées à des fins autres que celles stipulées dans la politique de confidentialité lors de la collecte des données, sauf si ces fins correspondent à des activités d'archivage d'intérêt public, à des fins de recherche scientifique et historique ou à des fins statistiques.

La combinaison de ces trois principes crée un outil normatif combiné qui doit être strictement suivi par les développeurs IdO. En général, les responsables du traitement des données[851] doivent rendre explicites les finalités du traitement : "divulguées, expliquées ou exprimées sous une forme intelligible". Conformément au principe de minimisation des données, ils doivent également identifier la quantité minimale de données personnelles nécessaires pour atteindre leurs objectifs. En outre, en ce qui concerne le principe de responsabilité, les responsables du traitement doivent être en mesure de démontrer qu'ils ne collectent et ne conservent que les données à caractère personnel nécessaires et qu'elles ne sont utilisées que pour les finalités spécifiques qui ont été informées en vertu d'une base juridique adéquate.

En résumé, la définition d'objectifs clairs pour le développement de l'IdO permettra de s'assurer que les données personnelles à traiter le seront :

- adéquates : suffisantes pour atteindre l'objectif fixé ;
- pertinentes : car elles doivent avoir un lien rationnel avec l'objectif ;
- limitées à ce qui est nécessaire : elles ne doivent pas détenir plus de données que celles nécessaires à la finalité déclarée.

Les responsables du traitement ne doivent pas oublier que, si les dispositifs traitent les données à des fins autres que celles pour lesquelles elles ont été collectées, une base

851 Il est important d'identifier qui est le "responsable de données" ; les développeurs sont rarement le "responsable de données" puisqu'ils ne sont pas responsables de l'objectif commercial, cette tâche incombant à la direction de l'entreprise.

juridique légitimant ce traitement sera nécessaire, à moins que la nouvelle utilisation des données soit compatible avec la finalité pour laquelle les données personnelles ont été initialement collectées, conformément à l'article 6.4 du RGPD. La possibilité de faire usage de l'exception à cette règle liée au traitement à des fins de recherche doit être soigneusement analysée avant tout traitement. Une consultation avec le DPD est fortement recommandée.

5.1 Principe de minimisation

Le principe de minimisation stipule que les données à caractère personnel doivent être **adéquates**, **pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées (voir "Minimisation des données", dans la section "Principes" de la partie II des présentes lignes directrices). En termes simples, il s'agirait de réduire autant que possible la quantité, les catégories et la granularité des données à caractère personnel traitées. Cela signifie qu'il ne sera pas possible de collecter des données à caractère personnel qui ne seront pas traitées simplement pour que le responsable du traitement puisse les avoir et les utiliser à l'avenir, soit pour les finalités déclarées, soit pour de nouvelles finalités. Malheureusement, ce principe est parfois en tension avec la logique de la technologie IdO. Parfois, l'inférence de données et le profilage sont nécessaires aux fins du système, mais ils multiplient la quantité de données impliquées dans le traitement. En outre, la plupart des systèmes IdO traitent de nombreuses données personnelles entre des dispositifs qui sont souvent sous le contrôle de sous-traitants alternatifs et/ou impliquent des tiers.

Il existe certains moyens d'éviter les scénarios envahissants. Si la finalité du traitement peut être obtenue sans avoir besoin d'informations identifiables, les données doivent être rendues anonymes dès que possible. En principe, les systèmes IdO **devraient promouvoir l'utilisation de données anonymes, en particulier si ces données sont partagées avec d'autres appareils**. "Comme on ne peut guère éviter la possibilité d'établir des profils personnels étendus, l'anonymisation des données est importante dans le contexte du partage des données."[852] En principe, cela semble faisable, mais en pratique, cela pourrait être difficile à atteindre. Comme l'a déclaré l'AEPD, "La liaison des dispositifs IdO à des identifiants uniques, doublée de liens étroits entre certains dispositifs et leurs utilisateurs, rend pratiquement impossible l'utilisation anonyme de ces données, et le risque de réidentification monte en flèche. Par exemple, de nombreux dispositifs nécessitent l'enregistrement de l'utilisateur ou incluent des identifiants uniques de publicité, tels que les Smart TV. La présence d'identifiants uniques dans les appareils mobiles est un fait avéré, et ces appareils sont largement utilisés pour interagir

852 Rolf H Weber, 'Internet of Things : Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618.

avec les appareils IdO et les faire fonctionner."[853] Ainsi, les **responsables du traitement ne devraient pas présumer que leurs processus d'anonymisation serviraient bien à préserver la vie privée des personnes concernées. En effet, ils devraient effectuer des AIPD et des évaluations des risques pour s'assurer de cette idée (voir la responsabilité dans cette partie des lignes directrices)**.

À cet égard, les responsables du traitement doivent être conscients que la saisie de données à caractère personnel qui sont ensuite rendues anonymes constitue un traitement de données à caractère personnel, tant que ces données n'ont pas achevé le processus d'anonymisation, aussi bref que soit ce délai. En outre, l'anonymisation est un traitement, ce qui signifie qu'il ne peut être licite que si une base juridique s'applique. L'intérêt légitime ou le consentement sont les candidats les plus prometteurs. Une fois les données rendues anonymes, le traitement ne doit plus être conforme aux exigences de la protection des données à caractère personnel. Il peut encore relever des règles relatives à la vie privée en ligne, mais de manière plus diluée.

Une alternative à l'anonymisation proprement dite est l'utilisation de **données agrégées (l'agrégation est parfois considérée comme un outil d'anonymisation)**. Cela devrait être possible dans la plupart des systèmes IdO, puisque la plupart des valeurs de données que nous traitons sont une forme d'agrégation, même si cela n'est pas forcément évident puisqu'elle peut être effectuée de manière "invisible" par un capteur ou une méthode de collecte de données. L'agrégation est une manière de **substituer plusieurs éléments de données par un seul**. Les exemples les plus frappants proviennent des statistiques et comprennent la moyenne, la médiane, le minimum et le maximum. Dans le contexte de la protection des données, il convient de distinguer deux types d'agrégation (voir "Minimisation des données" dans la section "Principes", partie II des présentes lignes directrices) :

- Agrégation d'éléments de données relatifs à une **seule personne** : En prenant par exemple le revenu mensuel moyen d'une personne sur une année, on réduit le contenu des informations relatives à cette personne.
- Agrégation d'éléments de données relatifs à une **multitude de personnes** : Prendre par exemple le revenu annuel moyen d'un groupe de personnes réduit également le contenu global de l'information (minimisation des données). En outre, cela affaiblit également le degré d'association entre un élément de données et une personne donnée. Ce type d'agrégation est donc également pertinent pour la limitation du stockage.

Lorsque l'objectif peut être atteint en utilisant des données agrégées, il convient de le faire. Dans ces circonstances, personne d'autre que la personne concernée ne devrait

853 AEPD, " **IdO (I) : Qu'est-ce que l'IdO et quels risques comporte-t-il ?", à l'adresse : https://www.aepd.es/en/prensa-y-comunicacion/blog/iot-%20and-which-risks-does-it-entail.**

accéder aux données brutes, à moins qu'une raison pertinente ne s'applique. La transformation des données brutes en données agrégées devrait être possible dans l'outil IdO, de sorte que la matière première quittant l'appareil reste le minimum strictement nécessaire. Ces données agrégées devraient être dans un format standardisé."[854] Quoi qu'il en soit, les responsables du traitement doivent être conscients du fait que la collecte de données et leur suppression au bout d'un petit laps de temps, même de quelques millisecondes, constitue toujours un traitement de données à caractère personnel et que le respect total des règles de protection des données est requis.

Si la finalité du traitement ne peut être obtenue qu'en traitant des données à caractère personnel, ces données peuvent toujours être rendues pseudonymes. Cela relèvera toujours des règles de protection des données et de la vie privée, mais constitue une bonne mesure de sécurité et renforce la responsabilité.

Il est important de souligner qu'un responsable du traitement ne doit pas créer, collecter et stocker des données "juste au cas où". En d'autres termes, les données sont stockées pour le cas où une nouvelle idée viendrait à surgir et nécessiterait ces données pour développer un projet différent. Dans ce cas, le stockage de données pendant une période plus longue que nécessaire et la réutilisation des données de manière illégale peuvent entraîner les amendes les plus élevées.

Dernier point, mais non des moindres, les développeurs IdO "devraient activer des entités de contrôle et de traitement locales (les fameux mandataires de la vie privée) permettant aux utilisateurs d'avoir une vision claire des données collectées par leurs appareils et facilitant le stockage et le traitement locaux sans avoir à transmettre les données au fabricant de l'appareil."[855]

5.2 Limitation de la finalité

Le principe de limitation de la finalité (voir la section "Limitation de la finalité" dans la partie II "Principes" des présentes lignes directrices) exige que les données à caractère personnel collectées et traitées dans le cadre de l'IdO ne soient traitées que pour la finalité pour laquelle elles ont été collectées.

Le responsable du traitement ne peut utiliser les données que pour les finalités ou objectifs qui ont été clairement et explicitement notifiés aux utilisateurs dans la politique de confidentialité. Les finalités non informées des données ne seront pas légitimes, et même celles qui sont mal informées. Par exemple, lorsque les informations fournies ne sont pas transparentes ou complètes, on peut affirmer que les finalités ne sont pas explicites.

854 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.
855 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

En outre, les finalités doivent être précisées. En d'autres termes, une formulation large et ouverte qui ne permet pas à une personne moyenne de comprendre toutes les finalités des données ne sera pas conforme à la loi.

Le principal problème est que les systèmes IdO collectent souvent de grandes quantités de données à des **fins vagues ou largement définies.** Comme l'a déclaré Watcher, "la fusion de capteurs ou la mise en relation d'ensembles de données existants mais non connectés auparavant, peut offrir de nouvelles possibilités d'analyse de données qui n'avaient pas été envisagées lorsque les données ont été collectées. Le profilage inférentiel invasif et imprévisible est rendu possible par les services d'identification qui relient les dispositifs et les données qu'ils collectent." [856] En conséquence, les responsables du traitement pourraient produire des données inférées sur la personne concernée qui ne sont pas liées aux finalités pour lesquelles les données ont été initialement collectées et auxquels la personne concernée n'a jamais consenti. En outre, les personnes concernées pourraient même ne pas être au courant de ce traitement. Pire encore, il se peut que les données soient traitées par des tiers à d'autres fins pour lesquelles la personne concernée n'a jamais donné son consentement.

Afin d'éviter un tel scénario, **les responsables du traitement doivent mettre en œuvre des outils capables de garantir que le traitement n'a lieu que si une base juridique s'applique.** L'utilité des données stockées pour la finalité prévue d'un produit ou d'un service particulier devra être périodiquement réévaluée pour éviter tout traitement illégal des données.

5.3 Limitation du stockage

Le principe de limitation de la conservation oblige les responsables du traitement à ne pas conserver les données à caractère personnel "plus longtemps que nécessaire pour les finalités pour lesquelles elles sont traitées" et à introduire des mesures de pseudonymisation et d'anonymisation qui réduisent/suppriment l'identifiabilité des personnes concernées lorsque l'identification n'est plus nécessaire pour ces finalités. Le problème ici est que les responsables du traitement pourraient être intéressés par le stockage de données plus nombreuses que nécessaire, pour des périodes plus longues que nécessaire, pour finalement utiliser les données stockées à des fins différentes. En outre, comme nous l'avons mentionné, les données sont parfois collectées et stockées "juste au cas où" elles pourraient servir à des utilisations imprévues.

Par conséquent, les périodes de stockage doivent être proportionnées aux finalités du traitement : "Pour définir les périodes de stockage (délais), il convient de prendre en compte des critères tels que la durée et la finalité de la recherche. Il convient de noter

856 Wachter, Sandra (2018). Le RGPD et l'Internet des objets : un modèle de transparence en trois étapes. Droit, innovation et technologie, 1-29. doi:10.1080/17579961.2018.1527479 .

que les dispositions nationales peuvent également stipuler des règles concernant la période de stockage."[857]

Les responsables du traitement doivent être conscients du fait que, même si le RGPD autorise la conservation pendant des périodes plus longues, bien qu'il **doive y avoir une raison bonne et réelle d'opter pour une telle période prolongée,** par exemple, lorsque la seule finalité est la recherche scientifique ultérieure (ou les autres circonstances mentionnées dans la liste rapprochée contenue dans l'art. 5.1(c) du RGPD comme l'archivage dans l'intérêt public, la recherche historique ou les fins statistiques) (voir la section "Protection des données et recherche scientifique" dans les "Concepts principaux" et la sous-section "Aspect temporel" dans la section "Limitation de la conservation" des "Principes", Partie II de ces Lignes directrices).

Afin d'éviter tout stockage illicite, un "test de nécessité" doit être effectué par chacune des parties prenantes à la fourniture d'un service spécifique sur l'IdO, car les finalités de leurs traitements respectifs peuvent en fait être différentes. Par exemple, les données à caractère personnel communiquées par les utilisateurs lorsqu'ils s'abonnent à un service spécifique sur l'IdO doivent être supprimées dès que les utilisateurs mettent fin à leur abonnement. De même, les informations supprimées par les utilisateurs dans leur compte ne doivent pas être conservées. Lorsqu'un utilisateur n'utilise pas le service ou l'application pendant une période définie, le profil de l'utilisateur doit être considéré comme inactif. Après une autre période, les données doivent être supprimées. L'utilisateur devrait être informé avant que ces mesures ne soient prises, par tous les moyens dont dispose la partie prenante concernée".[858]

En résumé, si les responsables du traitement n'ont pas besoin des données et qu'aucune raison juridique obligatoire ne les oblige à les conserver, ils doivent les rendre totalement anonymes ou les effacer. Les chercheurs devraient consulter leur DPD s'ils souhaitent conserver des données pendant une longue période et se renseigner sur la réglementation nationale applicable. Ce pourrait également être le moment idéal pour **envisager des délais d'effacement des différentes catégories de données et documenter ces décisions ou les appliquer de manière automatisée** (voir la section "Responsabilité" dans la partie "Principes", partie II des présentes lignes directrices).

Liste de contrôle : gouvernance des données

857 CEPD (2020) Lignes directrices 03/2020 sur le traitement des données relatives à la santé à des fins de recherche scientifique dans le cadre de l'épidémie COVID-19 Adoptées le 21 avril 2020. Contrôleur européen de la protection des données, Bruxelles, p.10. Disponible à l'adresse https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (consulté le 23 avril 2020).

858 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

Minimisation

 Les systèmes IdO utilisent des données anonymisées, en particulier si ces données sont partagées avec d'autres dispositifs, dans la mesure du possible.

 Si l'anonymisation n'est pas possible, les systèmes IdO optent pour l'agrégation des données dans un format standardisé.

 Les responsables du traitement ont veillé à ce que personne d'autre que la personne concernée ne puisse accéder aux données brutes, à moins qu'une base juridique ne légitime un tel traitement (et à condition qu'il soit nécessaire aux fins recherchées).

 Les responsables du traitement ont veillé à ce que la matière première quittant l'appareil reste le strict minimum nécessaire.

Limitation de la finalité

 Les responsables du traitement n'utilisent les données que pour les finalités pour lesquelles elles ont été collectées, sauf si une base juridique permet leur traitement illicite par des tiers.

 Le responsable du traitement informe de manière transparente sur ces finalités et sur la base juridique qui soutiendra chacune d'entre elles.

Limitation du stockage

 Les responsables du traitement ne conservent pas les données à caractère personnel pendant "plus longtemps que nécessaire pour les finalités pour lesquelles les données à caractère personnel sont traitées", selon le Necessity Toolkit du CEPD[859] .

 Les contrôleurs vérifient l'utilité des données stockées pour l'usage prévu d'un produit ou d'un service particulier, qui devra être réévalué périodiquement.

 Les données personnelles communiquées par les utilisateurs lorsqu'ils s'abonnent à un service spécifique sur l'IdO sont supprimées dès que les utilisateurs mettent fin à leur abonnement.

 Les informations supprimées par les utilisateurs dans leur compte ne sont pas conservées par le système IdO.

 Si une personne concernée et utilisateur n'utilise pas le système IdO pendant une période définie, son profil est défini comme inactif et, après une autre période, les

[859] https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

données sont supprimées.

 L'utilisateur est prévenu avant que ces mesures ne soient prises.

 Les responsables du traitement ont documenté toutes les informations concernant ces problèmes.

6 Droits des personnes concernées

Le chapitre III du RGPD prévoit un ensemble de droits que les personnes concernées peuvent exercer pour protéger leurs données personnelles. Bien que chaque droit comporte des détails et des questions spécifiques qui pourraient affecter et être affectés par la recherche et le développement des TIC (voir la section "Traitement à des fins de recherche scientifique" dans "Principaux outils et actions", partie II des présentes lignes directrices), ils partagent tous certaines caractéristiques générales concernant leur information transparente, leur communication et leurs modalités d'exercice (article 12 du RGPD). Dans cette section, nous analysons chaque droit spécifique à la lumière du développement d'un système IdO. Nous avons déjà analysé le droit à l'information (voir la section "Transparence" de cette partie des Lignes directrices) et le droit de ne pas être soumis à une prise de décision automatisée a été largement abordé dans la section "Capacité d'action humaine" de cette partie des Lignes directrices.

En général, la plupart de ces droits sont difficiles à mettre en œuvre dans le cas de l'IdO, en raison de la nature pure de la technologie, qui repose sur la vitesse élevée des données fournies par différents systèmes et dispositifs. Les techniques continues d'agrégation et de profilage, ainsi que la création continue de données déduites, contribuent à entraver les droits tels que l'accès, la portabilité et l'effacement. En outre, dans le cadre de l'IdO, il est assez courant de trouver différents responsables du traitement et sous-traitant des ensembles de données agrégées qui sont stockées par le biais de l'informatique en nuage dirigée par un superviseur, qui joue le rôle de responsables du traitement ou de sous-traitants conjoints.

Les contrats qui régissent ces interactions sont complexes et à plusieurs niveaux. Par conséquent, la répartition des rôles et des responsabilités devient difficile dans la pratique. Même si, en théorie, les contrats devraient clarifier toutes ces questions, "en réalité, ce sont les sous-traitants qui rédigent les clauses contractuelles standard et les instructions de traitement, car ils traitent les données pour le compte de nombreux responsables du traitement et ne disposent pas d'instructions de traitement distinctes pour chaque responsable du traitement. Il est donc difficile pour les responsables du traitement de se conformer aux exigences contractuelles et au principe de responsabilité

prévu par le RGPD, car ils ne sont pas pleinement conscients de tous les sous-traitants et sous-traitants secondaires. En outre, les relations contractuelles complexes à plusieurs niveaux entre les parties prenantes de l'IdO rendent plus difficile la revendication de la responsabilité d'un dommage causé aux personnes concernées par des dispositifs IdO ou des algorithmes analytiques."[860] En outre, certaines parties peuvent rédiger des contrats en se positionnant dans un rôle différent de celui qui s'applique réellement à elles (voir la section "Définir les rôles de protection des données joués par tous les agents impliqués dans le traitement : détermination des responsables du traitement et des sous-traitants" dans cette partie sur l'IdO).

Différents outils ont été proposés pour faire face à ces problèmes et l'approche du "système de gestion des informations personnelles" ("PIMS") a été promue par le contrôleur européen de la protection des données.[861] L'utilisation des techniques de blockchain pour concevoir des contrats intelligents fondés sur le RGPD qui tiennent compte de la vie privée afin d'améliorer la responsabilité des dispositifs IdO, qui sont des responsables du traitement ou des sous-traitants de données des utilisateurs, pourrait être une alternative adéquate, car ils n'ont pas besoin de contrôleur général ou de responsable des données. Cependant, la blockchain pourrait présenter des inconvénients en termes de droits et de libertés des personnes concernées, car le fait qu'ils soient propriétaires de nœuds en ferait des "responsables du traitement" et, par conséquent, ils auraient des obligations et des responsabilités en vertu du RGPD.[862]

Même s'il n'existe pas de solutions techniques définitives à ces questions complexes, les développeurs de l'IdO doivent faire de leur mieux pour s'assurer que les systèmes sont capables de respecter les droits et libertés des personnes concernées. Les domaines de la conception informatique tels que les technologies d'amélioration de la confidentialité (PETS), l'ingénierie de la confidentialité, la confidentialité utilisable et l'interaction des données humaines ont tous des méthodologies et des cadres à proposer.[863]

6.1 Droit d'accès

L'article 15 prévoit que les personnes concernées ont le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel les concernant sont

860 El-Gazzar, R., & Stendal, K. (2020). Examiner comment le RGPD défie les technologies émergentes. *Journal of Information Policy, 10*, 237-275. doi:10.5325/jinfopoli.10.2020.0237.

861 Contrôleur européen de la protection des données (2016) Avis sur les systèmes de gestion des informations personnelles vers une plus grande responsabilisation des utilisateurs dans la gestion et le traitement des données personnelles. Bruxelles. À l'adresse : https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf

862 Nicola Fabiano, Internet of Things and the Legal Issues related to the Data Protection Law, Athens Journal of Law - Volume 3, Issue 3, 2018, Pages 201-214 https://doi.org/10.30958/ajl.3-3-2 doi=10.30958/ajl.3-3-2 selon le nouveau règlement général européen sur la protection des données Par.

863 Urquhart, L., Sailaja, N. & McAuley, D. Réaliser le droit à la portabilité des données pour l'Internet domestique des objets. *Pers Ubiquit Comput* 22, 317-332 (2018).

ou ne sont pas traitées et, si tel est le cas, l'accès aux données à caractère personnel ainsi que certaines informations supplémentaires qui sont généralement fournies dans la politique de confidentialité (voir la section "Droit d'accès" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). En outre, à la demande des personnes concernées, le responsable du traitement doit leur fournir gratuitement une copie des données à caractère personnel traitées (des frais raisonnables destinés à couvrir les coûts administratifs peuvent être facturés pour toute autre copie demandée par la personne concernée). Dans le cas de l'IdO, cela pourrait se faire par le biais d'un portail web ou d'une application, puisque ces systèmes envoient généralement les données au fabricant de l'appareil, qui les conserve souvent dans des systèmes spécifiques. D'une part, cela permet à l'IdO de fournir des services en ligne qui tirent parti des capacités du dispositif, mais, d'autre part, cela peut également empêcher les utilisateurs de choisir librement le service qui interagit avec leur dispositif.

En outre, et comme l'a déclaré le groupe de travail Article 29, "les utilisateurs finaux sont rarement en mesure d'avoir accès aux données brutes qui sont enregistrées par les dispositifs IdO. Il est clair qu'ils ont un intérêt immédiat pour les données interprétées plutôt que pour les données brutes qui peuvent ne pas avoir de sens pour eux. Pourtant, l'accès à ces données peut s'avérer utile pour les utilisateurs finaux afin de comprendre ce que le fabricant du dispositif peut en déduire à leur sujet". [864]

Il est considéré que le droit d'accès couvre à la fois les données brutes et les données observées concernant l'utilisateur. Toutefois, dans l'état actuel des choses, il ne semble pas couvrir les données déduites. Cela peut porter préjudice aux utilisateurs, car ils ont peu de possibilités de se faire une idée des données les plus sensées que le système traite à leur sujet.

En outre, le droit d'accès est actuellement étroitement lié au droit à la portabilité des données (voir le "Droit à la portabilité des données" ci-dessous, dans cette partie sur l'IdO).

6.2 Droit de rectification

Comme le prévoit l'article 16 du RGPD, les personnes concernées détiennent le droit de faire rectifier leurs données personnelles (voir la section "Droit de rectification" dans la partie "Droits" des présentes lignes directrices). Ce droit est particulièrement pertinent dans le cas de l'IdO, car toute inexactitude dans les données collectées pourrait avoir des conséquences dramatiques en termes de profilage (voir la section "Capacité d'action humaine" dans cette partie des lignes directrices). En effet, "les développeurs de l'IdO sont confrontés à un défi important pour conserver et mettre à jour leurs ensembles de

864 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

données afin de répondre à cette exigence. La vérification de l'identité de l'utilisateur est essentielle pour garantir la précision, en particulier lorsque plusieurs personnes peuvent potentiellement utiliser le même appareil."[865] Le principal problème ici est que les données sont souvent stockées dans différents serveurs et que les développeurs IdO ne sont pas toujours conscients de l'existence de certaines copies de sauvegarde concrètes. Ce point devrait être soigneusement examiné dans les contrats entre les responsables du traitement et les responsables du traitement conjoints ou les sous-traitants.

Les responsables du traitement sont tenus de communiquer les données rectifiées à chaque destinataire auquel les données à caractère personnel ont été communiquées, sauf si cela s'avère impossible ou implique des efforts disproportionnés. Les responsables du traitement pourraient difficilement faire valoir que le système de partage d'informations et de stockage est trop complexe pour garantir la rectification afin d'éviter cette obligation.

6.3 Droit à l'effacement

Les personnes concernées ont le droit de demander aux responsables du traitement l'effacement de leurs données à caractère personnel en vertu de l'article 17 du RGPD (voir la section "Droit à l'effacement" dans la section "Droits des personnes concernées", partie II des présentes lignes directrices). Toutefois, l'utilisation de l'informatique en nuage, l'existence de divers serveurs et référentiels, la possibilité que les données soient traitées par différents sous-traitants et responsables du traitement font qu'il est difficile de garantir que toutes les copies de sauvegarde et les données à caractère personnel -et pas seulement leurs clés de chiffrement- sont supprimées. Pour éviter de tels résultats, les développeurs IdO doivent surveiller attentivement les procédures.

Enfin, les responsables du traitement doivent garder à l'esprit que ce droit ne couvre pas les traitements nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement" ou lorsqu'ils "portent atteinte aux droits et libertés d'autrui". Si l'effacement de certaines données risque de porter gravement atteinte aux droits et libertés d'autrui, l'effacement ne doit pas être autorisé. Cela implique la nécessité de mettre en balance les différents intérêts en jeu.

865 Wachter, Sandra, (2018) Le RGPD et l'Internet des objets : un modèle de transparence en trois étapes, Law, Innovation and Technology, 10:2, 266-294, DOI : 10.1080/17579961.2018.1527479.

6.4 Droit de restreindre le traitement

Conformément à l'article 18 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'une des circonstances décrites dans cet article s'applique (à savoir : la précision de ses données est contestée ; le traitement est illicite et la personne concernée s'oppose à l'effacement de ses données à caractère personnel ; le responsable du traitement n'a plus besoin des données à caractère personnel, mais est tenu de les conserver ; ou la personne concernée s'oppose autrement au traitement.

Étant donné que différents responsables conjoints du traitement, sous-traitants ou sous-traitants secondaires peuvent être impliqués dans le traitement dans le cas de l'IdO, il peut être utile de garder à l'esprit que ce droit doit être exercé par l'un d'entre eux, qui doit informer les autres de cette exigence et agir en conséquence.

6.5 Droit d'opposition

Les personnes concernées ont le droit de s'opposer à tout moment, pour des raisons tenant à leur situation particulière, au traitement de données à caractère personnel. Ce droit ne s'applique que lorsque la base légale du traitement est l'intérêt légitime ou l'intérêt public. Lorsque la base légale du traitement est le consentement, les personnes concernées peuvent simplement retirer leur consentement.

En cas d'exercice de ce droit, le responsable du traitement doit évaluer s'il existe une raison "impérieuse" de poursuivre le traitement. Cette notion doit être interprétée de manière stricte et étroite, et il ne peut s'agir des mêmes intérêts et raisons qui ont justifié le traitement en premier lieu. En effet, cette fois, le responsable du traitement doit réévaluer le traitement à la lumière des raisons personnelles invoquées par la personne concernée. Si un tel motif impérieux ne peut être trouvé et solidement argumenté, l'activité de traitement doit cesser. Dans ces cas, une évaluation erronée de ces raisons impérieuses de poursuivre le traitement pourrait être constatée, par exemple, par le nombre de fois où le responsable du traitement ne concède pas l'exercice du droit et poursuit le traitement. Lorsque le traitement consiste en un marketing direct, la personne concernée peut exercer un droit d'opposition de manière directe, et le responsable du traitement doit arrêter le traitement sans possibilité d'invoquer une raison impérieuse.

À cet égard, il convient de noter que ces données à caractère personnel peuvent toujours être traitées à d'autres fins, pour autant qu'il existe une base légale pour celles-ci.

6.6 Droit à la portabilité des données

Selon l'article 20 du RGPD, les personnes concernées ont un droit à la portabilité. Cela signifie un droit d'obtenir leurs données auprès d'un responsable du traitement dans un format structuré, couramment utilisé et lisible par machine, mais aussi un droit de

déplacer les données entre les responsables du traitement sans entrave, ou lorsque cela est techniquement possible. Toutefois, ce droit ne s'applique qu'aux données "concernant" la personne concernée et aux données qu'elle a "fournies" au responsable du traitement. Par conséquent, ni les données anonymes, ni les données inférées ou autrement "créées" ne sont incluses dans le droit à la portabilité (les données anonymes ne sont pas couvertes puisqu'elles ne concernent plus la personne concernée ; et les données inférées puisqu'elles n'ont pas été fournies par la personne concernée mais sont le résultat d'un processus technique développé par le responsable du traitement). Il semble donc que les personnes concernées n'aient pas le droit de faire transférer l'intégralité de leurs données profilées à un autre fournisseur. Le raisonnement qui sous-tend cette disposition est la protection du savoir-faire du responsable du traitement.

Les personnes concernées "devraient disposer d'outils leur permettant d'exporter facilement leurs données dans un format structuré et couramment utilisé. Par conséquent, l'interopérabilité des données est un élément technique essentiel pour déployer pleinement ce droit et les fabricants de dispositifs devraient fournir une interface conviviale aux utilisateurs qui souhaitent obtenir les données qu'ils stockent encore."[866]

Liste de contrôle : droits des personnes concernées

 Les responsables du traitement ont mis en place les procédures nécessaires pour garantir que les droits des personnes concernées sont adéquatement satisfaits, qu'il s'agisse des utilisateurs finaux ou de tiers.

 Les responsables de traitement ont mis en place les procédures nécessaires pour que les droits des personnes concernées soient satisfaits dans les délais (maximum un mois après la demande).

 Les responsables du traitement ont mis en place des outils efficaces pour garantir que les personnes concernées puissent exercer leurs droits de manière pratique, par exemple en introduisant des normes d'interopérabilité des données.

 Les personnes concernées sont en mesure d'avoir accès à toutes leurs données personnelles, y compris les données brutes qui sont enregistrées par les dispositifs IdO.

 Les développeurs de l'IdO ont mis en place des outils pour lire, éditer et modifier localement les données avant qu'elles ne soient transférées à un quelconque

866 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

responsable du traitement des données. En outre, les données personnelles traitées par un appareil sont stockées dans un format permettant la portabilité des données.

 Les responsables de traitement ont mis en place des outils capables de communiquer les données rectifiées à chaque destinataire auquel les données personnelles ont été divulguées, sauf si cela s'avère impossible ou implique des efforts disproportionnés.

 Les responsables de traitement ont mis en place des outils capables de garantir que toutes les données sont efficacement supprimées à la demande des personnes concernées s'il n'y a pas de raisons légitimes de s'opposer à cette demande.

 Les développeurs d'IdO ont mis en place une interface conviviale pour les utilisateurs qui souhaitent obtenir les données personnelles brutes et observées qu'ils stockent encore. Ces outils permettent aux personnes concernées d'exporter facilement leurs données dans un format structuré et couramment utilisé.

7 Responsabilité et contrôle

Le principe de responsabilité du RGPD est basé sur le risque : plus le risque du traitement des données pour les droits et libertés fondamentaux des personnes concernées est élevé, plus les mesures nécessaires pour atténuer ces risques sont importantes.[867] (Voir la section "Principe de responsabilité" dans les "Principes" de la partie II des présentes lignes directrices). Le principe de responsabilité est fondé sur toutes les obligations de conformité des responsables du traitement des données, notamment : les obligations de transparence (articles 12-14) ; la garantie de l'exercice des droits en matière de protection des données (articles 15-22) ; la tenue de registres des opérations de traitement des données (article 30) ; la notification des éventuelles violations de données à une autorité de contrôle nationale (article 33) et aux personnes concernées (article 34) ; et, en cas de risque plus élevé, le recrutement d'un DPD et la réalisation d'une AIPD (article 35).

Le traitement des données à caractère personnel dans les systèmes IdO pouvant souvent être considéré comme à haut risque,[868] les développeurs de l'IA devront souvent

867 Voir les articles 24, 25 et 32 du RGPD, qui exigent que les responsables du traitement prennent en compte les "risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques" lorsqu'ils adoptent des mesures spécifiques de protection des données.

868 Voir, en particulier, l'article 35, paragraphe 3, point a), selon lequel le traitement des données est considéré comme présentant un risque élevé dans les cas, entre autres, "d'une évaluation systématique et extensive d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé,

disposer d'un DPD et réaliser une AIPD. De même, les responsables du traitement devraient créer une politique de protection des données qui permet la **traçabilité des informations.** Enfin, s'il existe des codes de conduite approuvés, ceux-ci pourraient également être mis en œuvre (voir la sous-section "Économie d'échelle pour la conformité et sa démonstration" dans la section "Responsabilité" des "Principes" de la partie II des présentes lignes directrices).

Encadré 8 : La difficulté de la responsabilisation dans le développement IdO

La responsabilisation est une exigence essentielle compte tenu des risques inhérents à l'IdO, tels que "la nature opaque des flux de données distribués, les mécanismes de consentement inadéquats et l'absence d'interfaces permettant à l'utilisateur final de contrôler le comportement des appareils connectés à internet"[869] .

Une autre question particulièrement complexe est le fait que l'IdO permet de nombreux outils et technologies qui présentent leurs propres risques en matière de protection des données. En particulier, l'IA, l'apprentissage automatique, le big data, le cloud computing, "les données personnelles collectées par les dispositifs IdO étant généralement distribuées dans le cloud pour être traitées et analysées"[870] .

Des normes sont en cours d'élaboration par le CEN et le CENELEC.

Voir la liste ici :

https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5

7.1 Délégué à la protection des données

La nomination d'un DPD est l'une des meilleures mesures que peut prendre le responsable du traitement pour mettre correctement en œuvre les mesures qui garantissent le respect des droits des personnes concernées. La nomination d'un DPD n'est pas toujours une conséquence nécessaire du fonctionnement du déploiement de l'IdO. Il est toutefois indéniable que la désignation d'un DPD est obligatoire, du moins si les conditions fixées par l'article 37, paragraphe 1, s'appliquent. En effet, dans le cas de l'IdO, il arrivera souvent que les activités principales du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, en raison de leur nature, de

y compris le profilage, et sur laquelle sont fondées des décisions produisant des effets juridiques à l'égard de la personne physique ou l'affectant de manière significative de façon similaire".

869 Urquhartet L. *et* al, Demonstrably doing accountability in the Internet of Things, Journal international du droit et des technologies de l'information, 2019, 27, 1-27.

870 Ibid.

leur portée et/ou de leurs finalités, nécessitent un suivi régulier et systématique des personnes concernées à grande échelle. Néanmoins, même si ce n'est pas le cas, **il est toujours recommandé d'y procéder, au moins en termes de transparence** (voir la section "Transparence" dans les "Principes", partie II des présentes lignes directrices)**.**

7.2 Évaluation de l'impact sur la protection des données

Un AIPD n'est pas toujours obligatoire dans le cas du développement de l'IdO (voir la sous-section "Dans quels cas dois-je réaliser un AIPD" dans "Évaluation de l'impact sur la protection des données", "Principaux outils et actions", partie II des présentes lignes directrices). Cela dépend si les risques associés au traitement sont élevés ou non, conformément à l'article 35, paragraphe 3, du RGPD. Cependant, elle est fortement recommandée car elle soutient la responsabilisation. Par exemple, l'AIPD est obligatoire si le traitement implique une surveillance systématique d'une zone accessible au public à grande échelle, ou si elle est destinée à évaluer ou à noter les populations vulnérables. En tout état de cause, le WP29 a inclus certains critères fondamentaux dans ses lignes directrices sur l'analyse d'impact sur la protection des données (AIPD) et la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679[871] .

En cas de doute, la consultation de l'autorité de contrôle compétente avant le traitement est vivement recommandée (voir la section "Analyse d'impact sur la protection des données" des "Principaux outils et actions", partie II des présentes lignes directrices).

La CNIL a créé un excellent outil visant à fournir des conseils sur la façon de réaliser une évaluation des incidences sur la vie privée[872] , qui comprend des conseils pratiques et bien conçus. Sa consultation est vivement recommandée : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

Liste de contrôle

- Vérifiez si vous devez effectuer une analyse d'impact sur la protection des données pour votre activité de traitement.

[871] A29WP, Lignes directrices relatives à l'analyse d'impact sur la protection des données (AIPD) et à la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679, adoptées le 4 avril 2017 Telles que révisées et adoptées en dernier lieu le 4 octobre 2017, à l'adresse : https://ec.europa.eu/newsroom/article29/items/611236/en .

[872] CNIL, Évaluation de l'impact sur la vie privée. Application aux dispositifs de l'IdO. Février 2019. À : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

- Documentez cette vérification (qu'elle ait été positive ou non).

Si une AIPD est nécessaire :

- Commencez le plus tôt possible (en suivant le principe de la protection des données dès la conception).
- Obtenez une vue d'ensemble de ce qu'est une AIPD.
- Utilisez, dans la mesure du possible, les conseils et les modèles fournis par l'autorité de contrôle de la protection des données (APD) compétente.
- Si ce n'est pas le cas (votre APD ne fournit pas ce type de matériel ou vous devez répondre à de nombreux domaines de compétence de différentes APD), suivez les conseils fournis par le groupe de travail Article 29 dans le document wp248rev.01.
- Rassemblez l'équipe nécessaire pour mener l'analyse d'impact sur la protection des données.
- Réfléchissez aux moyens de faciliter votre travail.

7.3 Préparer la documentation du traitement

Les responsables du traitement doivent toujours garder à l'esprit que le développement de solutions IdO implique souvent l'utilisation de différents ensembles de données. La traçabilité du traitement, les informations sur l'éventuelle réutilisation des données et l'utilisation de données relatives à différents ensembles de données à différentes étapes ou aux mêmes étapes du cycle de vie doivent être assurées par les registres, puisque le responsable du traitement est responsable de la conformité à l'article 5 du RGPD et est en mesure de la démontrer (voir "Principe de responsabilité" dans la section "Principes" de la partie II des présentes lignes directrices). Quiconque traite des données à caractère personnel (y compris les responsables du traitement et les sous-traitants) doit documenter ses activités principalement à l'intention des autorités de contrôle qualifiées/pertinentes (voir la "Documentation du traitement" dans la section "Principaux outils et actions", partie II des présentes lignes directrices), mais aussi, le cas échéant, des personnes concernées et des autres parties prenantes.

Cela doit se faire, entre autres, par le biais de registres des activités de traitement qui sont conservés de manière centralisée par l'organisation pour l'ensemble de ses activités de traitement, et par une documentation supplémentaire relative à une activité individuelle de traitement des données (voir la section "Documentation du traitement" dans les "Principaux outils et actions", partie II des présentes lignes directrices).

Les premières étapes du développement du projet sont le moment idéal pour mettre en place une méthode systématique de collecte de la documentation nécessaire, puisque c'est à ce moment-là que l'organisation conçoit et planifie l'activité de traitement[873] .

Liste de contrôle. Documentation

- Contactez le bureau/personne qui tient les registres de traitement pour votre organisation.
  - Si nécessaire, votre délégué à la protection des données peut vous aider à établir le contact.
- Informez-les dès le début que vous avez l'intention de traiter des données à caractère personnel.
  - Votre activité de transformation doit être inscrite dans les registres avant le début de la transformation.
- Suivez leurs instructions concernant
  - les informations que vous devez fournir pour les registres de traitement,
  - le moment où vous devez envoyer des mises à jour de ces informations.

Documentation supplémentaire relative à une seule activité de traitement.

Les éléments suivants doivent être documentés :

- Une évaluation de l'activité de traitement et si elle est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques.
- Une analyse d'impact sur la protection des données lorsque l'évaluation ci-dessus donne un résultat positif.
- La consultation éventuelle de l'autorité de contrôle compétente avant le traitement.
- Les exigences et tests d'acceptation pour l'achat et/ou le développement du logiciel, du matériel et de l'infrastructure employés.

873 L'article 25, paragraphe 1, du RGPD appelle cela "le moment de la détermination des moyens de traitement".

- La mise en œuvre de mesures techniques et organisationnelles.
- Les tests, évaluations et analyses régulières de l'efficacité des mesures techniques et organisationnelles.
- Les exigences et tests d'acceptation pour la sélection des sous-traitants.
- Les contrats stipulés avec les sous-traitants.
- Les inspections et audits éventuels du sous-traitant.
- La méthode de collecte du consentement.
- Les démonstrations de l'expression individuelle du consentement.
- Les informations fournies aux personnes concernées.
- La mise en œuvre des droits des personnes concernées.
- Le traitement effectif des droits des personnes concernées.
- Les notifications éventuelles de violation à l'autorité de contrôle compétente.
- La communication éventuelle des violations de données à la personne concernée.
- Toute autre communication avec l'autorité de contrôle compétente.

7.4 Concevoir votre politique de confidentialité

La politique de confidentialité est le document public qui explique comment votre projet traite les données personnelles et comment il applique les principes de protection des données, conformément aux articles 12-14 du RGPD. Toutes les personnes concernées doivent avoir accès à cette politique de confidentialité. Elle doit être documentée.

Un modèle non officiel, mais recommandable, se trouve ici : https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf.

Liste de contrôle. Politique de confidentialité

- Contactez le bureau/personne qui tient les registres de traitement pour votre organisation.
    - Si nécessaire, votre délégué à la protection des données peut vous

aider à établir le contact.

- Informez-les dès le début que vous avez l'intention de traiter des données à caractère personnel.
  - Votre activité de transformation doit être inscrite dans les registres avant le début de la transformation.
- Suivez leurs instructions concernant
  - les informations que vous devez fournir pour les registres de traitement,
  - le moment où vous devez envoyer des mises à jour de ces informations.

Documentation supplémentaire relative à une seule activité de traitement.

Les éléments suivants doivent être documentés :

- Une évaluation afin de déterminer si l'activité de traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques.
- Une analyse d'impact sur la protection des données lorsque l'évaluation ci-dessus donne un résultat positif.
- La consultation éventuelle de l'autorité de contrôle compétente avant le traitement.
- Les exigences et tests d'acceptation pour l'achat et/ou le développement du logiciel, du matériel et de l'infrastructure employés.
- La mise en œuvre de mesures techniques et organisationnelles.
- Les tests, évaluations et analyses régulières de l'efficacité des mesures techniques et organisationnelles.
- Les exigences et tests d'acceptation pour la sélection des sous-traitants.
- Les contrats stipulés avec les sous-traitants.
- Les inspections et audits éventuels du sous-traitant.
- Les méthodes de collecte du consentement.
- Les démonstrations de l'expression individuelle du consentement.
- Les informations fournies aux personnes concernées.
- La mise en œuvre des droits des personnes concernées.
- Le traitement effectif des droits des personnes concernées.
- Les notifications éventuelles de violation à l'autorité de contrôle compétente.
- La communication éventuelle des violations de données à la personne concernée.
- Toute autre communication avec l'autorité de contrôle compétente.

8 Intégrité et confidentialité

Selon le RGPD, les données à caractère personnel sont traitées d'une manière qui **garantit une sécurité appropriée** des données à caractère personnel, y compris la protection contre le **traitement non autorisé** ou **illégal** et contre la **perte, la destruction** ou les **dommages accidentels**, à l'aide de mesures techniques ou organisationnelles appropriées (principe "*d'intégrité et de confidentialité*"). (Voir la section "Intégrité et confidentialité" dans les "Principes", partie II des présentes lignes directrices).

En pratique, ce principe comporte trois aspects principaux : l'intégrité, la confidentialité et la disponibilité.

- L'intégrité fait référence à la protection des données personnelles "contre les dommages accidentels", par exemple en raison d'une erreur de transmission, d'une modification accidentelle ou non autorisée. Elle vise donc à prévenir tout type d'événement susceptible de "corrompre" les données d'une manière qui les rende impropres aux finalités du traitement.
- La confidentialité fait référence à la protection des données à caractère personnel "contre tout traitement non autorisé ou illicite".
- La disponibilité fait référence à la protection des données personnelles "contre la perte ou la destruction accidentelle", par exemple en raison de la défaillance d'un composant de stockage.

La disponibilité et l'intégrité sont en quelque sorte liées dans le cas de l'IdO, puisque seules les données correctement préservées peuvent être mises à la disposition de la personne concernée. La confidentialité, en revanche, est une question plus complexe qui mérite des mesures complexes en raison de la nature pure des processus concernés et des risques inhérents à ces processus.

8.1 Disponibilité et intégrité

L'IdO implique généralement la collecte d'une quantité impressionnante de données. Le traitement ou l'analyse de ces données a généralement lieu dans des endroits très éloignés dans le cloud et, pour pouvoir les atteindre, il est nécessaire d'utiliser des réseaux partagés, des réseaux publics, etc. Certaines de ces données sont des données brutes et d'autres des données agrégées, qui sont créées par l'interaction de différents systèmes IdO.

Dans ces circonstances, il est généralement difficile de mettre toutes les données à la disposition des personnes concernées. En effet, ce ne serait pas une bonne idée dans le cas de données brutes. La plupart des systèmes complexes de l'IdO, intégrant plusieurs outils, n'ont besoin que de données agrégées et n'ont pas besoin des données brutes collectées par les dispositifs de l'IdO. Par conséquent, les responsables du traitement suppriment généralement les données brutes dès qu'ils ont extrait les données nécessaires à leur traitement. Cependant, les dispositifs devraient toujours inclure une fonctionnalité permettant aux personnes concernées de contrôler ce processus et de contrôler le processus de suppression de toutes leurs données personnelles. En principe, la suppression devrait avoir lieu au point le plus proche de la collecte des données brutes (par exemple, sur le même appareil après le traitement).[874] Ces données ne seraient donc pas disponibles pour les personnes concernées ou un intrus. Cela n'est pas particulièrement important, car ils ne pourraient guère tirer profit de l'accès à ces données. En revanche, le stockage de toutes les données irait à l'encontre des principes de minimisation, de limitation de la finalité et de limitation du stockage, sans compter que cela augmenterait probablement les coûts des services.

D'autre part, il convient de noter que l'intégrité des données pourrait être compromise par la manière dont les données IdO sont partagées et stockées. Il peut arriver que l'un des responsables du traitement ou des responsables du traitement conjoints supprime ou endommage les données à un moment donné. Afin d'éviter de tels scénarios, les copies de sauvegarde constituent une mesure de sécurité obligatoire. Leur création doit être prévue dès les premières étapes du fonctionnement du système IdO.

8.2 Effectuer une analyse des risques de sécurité

Selon le principe de confidentialité, les responsables du traitement doivent minimiser les risques pour les droits, intérêts et libertés des personnes concernées. À cette fin, ils doivent travailler selon une approche fondée sur le risque (voir la section "Intégrité et confidentialité" dans les "Principes", partie II des présentes lignes directrices). L'approche fondée sur le risque de la législation sur la protection des données exige des responsables du traitement qu'ils se conforment à leurs obligations et mettent en œuvre des mesures appropriées dans le cadre de leur situation particulière - la nature, la portée, le contexte et les finalités du traitement qu'ils ont l'intention de faire, et les risques que cela présente pour les droits et libertés des personnes. Leurs considérations de conformité impliquent donc d'évaluer les risques pour les droits et libertés des personnes et de juger de ce qui est approprié dans ces circonstances. Dans tous les cas, les responsables du traitement doivent s'assurer qu'ils respectent les exigences en matière de protection des données et qu'ils sont en mesure de montrer comment ils s'y

874 Avis 8/2014 du groupe de travail Art 29 sur la protection des données sur les développements récents de l'Internet des objets (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

conforment, par exemple au moyen d'une documentation (voir "Responsabilité" dans la partie "Principes" de la partie II des présentes lignes directrices).

Pour gérer les risques pour les personnes qui découlent du traitement des données à caractère personnel dans les systèmes IdO, il est important que les responsables du traitement acquièrent une bonne compréhension et une bonne articulation des droits fondamentaux, des risques et de la manière d'équilibrer ces droits et d'autres intérêts. En définitive, il est nécessaire que les responsables du traitement évaluent les risques que l'utilisation de l'IdO fait peser sur les droits des personnes, qu'ils déterminent la manière dont ils doivent y faire face et qu'ils établissent l'impact que cela a sur leur utilisation de l'IdO.[875] À cette fin, deux facteurs clés doivent être pris en considération : [876]

- Les risques découlant du traitement lui-même, tels que l'apparition de biais associés au profilage ou aux systèmes automatisés de prise de décision.
- Les risques découlant du traitement par rapport au contexte social et les effets secondaires indirectement liés à l'objet du traitement qui peuvent survenir.

Boîte 9 :

Par exemple, si une application IdO ne garantit pas la sécurité des informations au moyen de mesures de sécurité telles que le cryptage des données dans les différents états par lesquels les informations passent, nous mettrons la sécurité en danger. De plus, les techniques de cryptage doivent utiliser des algorithmes reconnus au niveau international, considérés comme sûrs et avec une clé suffisamment longue.

Afin de minimiser ces risques, les responsables du traitement doivent s'assurer que des mesures techniques et organisationnelles appropriées sont mises en œuvre pour éliminer, ou au moins atténuer le risque de sécurité, en réduisant la probabilité que les menaces identifiées se concrétisent, ou en réduisant leur impact. Il est nécessaire de prendre en compte les normes de sécurité qui existent déjà sur le marché, ainsi que les normes de conformité en matière de protection des données qui s'appliqueront à la solution IdO, telles que le RGPD pour la protection des données ou PCI-DSS pour les

875 ICO (2020) IoT auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.13-14. Disponible à l'adresse : https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf (consulté le 15 mai 2020).

876 AEPD (2020) Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Espanola Proteccion Datos, Madrid, p.30. Disponible sur : www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (consulté le 15 mai 2020).

transactions utilisant des cartes de paiement. En outre, les développeurs IdO doivent toujours se rappeler que l'article 32, paragraphe 4, du RGPD précise qu'un élément important de la sécurité consiste à s'assurer que les employés accédant aux données n'agissent que sur instruction et selon les instructions du responsable du traitement (voir la section "Intégrité et confidentialité" des "Principes" de la partie II des présentes lignes directrices).

Boîte 10 :

Par exemple, si l'application comprend un module de gestion des données bancaires ou de paiement par carte de crédit/débit, il est nécessaire de prendre en compte la norme PCI DSS. De plus, si elle doit gérer et traiter des données personnelles, elle doit être adaptée au cadre réglementaire opérant sur le territoire, comme le RGPD dans l'Union européenne.

Quelques mythes d'évaluation des risques déjà disponibles :

- CNIL : https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
- ISO : ISO/IEC 29134

La description générale des mesures de sécurité techniques et organisationnelles doit faire partie des registres du traitement, dans la mesure du possible (article 30, paragraphe 1, point g), pour les responsables du traitement, et article 30, paragraphe 2, point d), pour les sous-traitants) et toutes les mesures mises en œuvre font partie de l'AIPD, en tant que mesures correctives pour limiter le risque. Enfin, une fois les mesures sélectionnées mises en œuvre, les risques résiduels restants doivent être évalués et maintenus sous contrôle. L'analyse des risques et l'AIPD sont les outils qui s'appliquent.

Comme indiqué dans les exigences et les tests d'acceptation pour l'achat et/ou le développement des logiciels, du matériel et de l'infrastructure employés, l'évaluation des risques et les décisions prises "doivent être documentées afin de respecter l'exigence de protection des données dès la conception" (de l'article 25 du RGPD) (voir la section "Protection des données dès la conception et par défaut" dans la section "Concepts principaux", partie II des présentes lignes directrices).

Enfin, les responsables du traitement doivent toujours être conscients que, conformément à l'article 32, paragraphe 1, point d), du RGPD, la protection des données est un processus. Par conséquent, **ils doivent tester, apprécier et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles**. Les procédures qui permettent aux responsables du traitement d'identifier les changements

qui déclencheraient le réexamen de l'analyse de l'impact sur la protection des données doivent être créées à ce moment-là. Dans la mesure du possible, les responsables du traitement doivent essayer d'imposer un modèle dynamique de suivi des mesures en jeu (voir la section "Intégrité et confidentialité" dans la partie II "Principes" des présentes lignes directrices).

8.3 Être conscient des risques qui sont intrinsèquement liés à la plupart des systèmes IdO.

Il est nécessaire de prendre en compte les aspects clés de l'application IdO lors de la définition de ses fonctionnalités et de l'impact potentiel sur la protection des données, tels que :

- Généralement, il y a une partie pour la collecte de données ou pour fournir des informations pour l'application ou les services IdO, donc la sécurité des données collectées doit être gérée.
- Le traitement ou l'analyse de ces données a généralement lieu dans des endroits très éloignés dans le nuage et, pour pouvoir les atteindre, il est nécessaire d'utiliser des réseaux partagés, des réseaux publics, etc. Cet aspect a un impact sur la protection des données stockées et en mouvement gérées en personne par l'équipe de développement ou par un tiers.
- Il est de plus en plus courant que les applications IdO soient hyper connectées à d'autres, provenant soit du même fabricant ou développeur, soit d'un autre, créant ainsi de vastes réseaux de dispositifs IdO. Il est donc nécessaire de prendre en compte la sécurité des données partagées ou accessibles par des tiers.
- L'intégration avec des tiers assure la compatibilité avec d'autres produits et confère à l'application une plus grande polyvalence et fonctionnalité, mais d'un autre côté elle rend nécessaire la définition d'une procédure pour évaluer la sécurité des composants fournis par des fournisseurs externes.
- L'interaction entre l'"utilisateur" humain et la "machine-produit" est présente et une attention particulière doit être accordée pour garantir une expérience utilisateur satisfaisante sans compromettre la sécurité.
- L'évaluation de la sécurité de l'application IdO doit comprendre des tests techniques tels que l'examen du code et les tests de pénétration. Les tests de pénétration permettent de vérifier le niveau de sécurité du système, de le détecter rapidement et, en cas d'échec, de corriger les éventuelles erreurs susceptibles d'affecter la sécurité des données pendant la mise en œuvre, afin d'atténuer ou de minimiser les risques avant de passer à la production. Le test de pénétration est un test très efficace pendant la phase d'évaluation, car il soumet les solutions aux mêmes menaces, auxquelles elles pourraient être confrontées pendant le fonctionnement normal d'une application IdO. Dans le cadre de ce qu'on appelle

le piratage éthique, ces tests visent à découvrir les faiblesses du système qui pourraient être exploitées à l'avenir par un pirate.

Boîte 11 :

Une application IdO qui permet de contrôler des ampoules à distance depuis un dispositif mobile, supportée par des communications sans fil au moyen du protocole ou de la spécification Zigbee, et qui utilise en même temps une passerelle pour se connecter à Internet, peut être un exemple utile des aspects clés à prendre en compte pour la fonctionnalité mentionnée ci-dessus.

Liste de contrôle : droits des personnes concernées

 Les responsables du traitement ont mis en place les procédures nécessaires pour garantir que les droits des personnes concernées sont adéquatement satisfaits, qu'il s'agisse des utilisateurs finaux ou de tiers.

 Les responsables de traitement ont mis en place les procédures nécessaires pour que les droits des personnes concernées soient satisfaits dans les délais (maximum un mois après la demande).

 Les responsables du traitement ont mis en place des outils efficaces pour garantir que les personnes concernées puissent exercer leurs droits de manière pratique, par exemple en introduisant des normes d'interopérabilité des données.

 Les personnes concernées sont en mesure d'avoir accès à toutes leurs données personnelles, y compris les données brutes qui sont enregistrées par les dispositifs IdO.

 Les développeurs de l'IdO ont mis en place des outils pour lire, éditer et modifier localement les données avant qu'elles ne soient transférées à tout responsable de traitement. En outre, les données personnelles traitées par un appareil sont stockées dans un format permettant la portabilité des données.

 Les responsables de traitement ont mis en place des outils capables de communiquer les données rectifiées à chaque destinataire auquel les données personnelles ont été divulguées, sauf si cela s'avère impossible ou implique des efforts disproportionnés.

 Les responsables de traitement ont mis en place des outils capables de garantir que toutes les données sont efficacement supprimées à la demande des personnes

concernées s'il n'y a pas de raisons légitimes de s'opposer à cette demande.

 Les responsables du traitement ont veillé à ce que les schémas de retrait soient fins et couvrent :

(1) toute donnée collectée par un objet spécifique ;

(2) un type spécifique de données collectées par quelque chose ;

(3) un traitement de données spécifique.

 Les personnes concernées se voient offrir la possibilité de désactiver la fonctionnalité "connectée" de l'objet et de lui permettre de fonctionner comme l'objet original, non connecté (c'est-à-dire désactiver la fonctionnalité connectée de la montre ou des lunettes intelligentes).

 Les développeurs d'IdO ont mis en place une interface conviviale pour les utilisateurs qui souhaitent obtenir à la fois des données agrégées et/ou des données brutes qu'ils stockent encore. Ces outils permettent aux personnes concernées d'exporter facilement leurs données dans un format structuré et couramment utilisé.

 Les responsables du traitement ont documenté toutes les informations concernant ces problèmes.