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.

GÉOLOCALISATION

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.

Données de localisation et de traçage

Iñigo de Miguel Beriain et Lorena Pérez Campillo (UPV/EHU)

La dernière section de ce document reproduit partiellement la partie de l'IA écrite à l'origine par Gianclaudio Malgieri et Andrés Chomczyk Penedo (VUB).

Mario Muñoz Organero et Julian Estévez ont apporté une aide précieuse pour les questions techniques.

Cette partie des lignes directrices a été révisée par Elena Gil González, avocate spécialisée en informatique et en protection des données, et finalement validée par Iñaki Pariente, ancien directeur de l'Agence basque de protection des données.

Introduction

"Dans le contexte des services de géolocalisation en ligne fournis par les services de la société de l'information, trois fonctionnalités différentes peuvent être discernées, avec des responsabilités différentes pour le traitement des données à caractère personnel. Il s'agit du responsable des données d'une infrastructure de géolocalisation, du fournisseur d'une application ou d'un service de géolocalisation spécifique et du développeur du système d'exploitation d'un appareil mobile intelligent. Dans la pratique, les entreprises remplissent souvent plusieurs rôles en même temps, par exemple lorsqu'elles combinent un système d'exploitation avec une base de données avec des points d'accès WiFi cartographiés et une plateforme publicitaire".[657] Dans cette section des lignes directrices, nous nous concentrons sur les deux derniers types de responsables du traitement : ceux qui sont disposés à fournir une application ou un service de géolocalisation spécifique ou à concevoir le système d'exploitation d'un appareil mobile intelligent.

De même, nous n'abordons pas les questions de protection des données liées au traitement effectué par des tiers en ligne qui permettent le traitement (ultérieur) des données de localisation, comme les navigateurs, les sites de réseaux sociaux ou les moyens de communication qui permettent par exemple la "géolocalisation". Nous ne considérons pas ici le développement d'un dispositif ou d'un système basé sur des données de localisation ou de proximité. Ces activités sont incluses dans les parties consacrées aux réseaux sociaux et aux services en ligne.

Il est également nécessaire de souligner que les développeurs du système d'exploitation du dispositif mobile intelligent pourraient être le responsable du traitement des données de proximité ou de localisation lorsqu'ils interagissent directement avec l'utilisateur et

657 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. 12, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

collectent des données à caractère personnel (par exemple en demandant l'enregistrement initial de l'utilisateur et/ou en collectant des informations de localisation à des fins d'amélioration des services). "Un développeur est également le responsable du traitement des données qu'il traite si l'appareil dispose d'une fonctionnalité de "call home" pour connaître sa localisation. Puisque les développeurs décident dans ce cas des moyens et des finalités d'un tel flux de données, ils sont les responsables du traitement de ces données. Un exemple courant d'une telle fonctionnalité de "call home" est la fourniture automatique de mises à jour du fuseau horaire en fonction de la localisation."[658]

Ce chapitre des lignes directrices suit la structure de la charte Locus.[659] Il s'agit d'une intention importante visant à créer certains principes internationaux communs pour aider les utilisateurs de données géospatiales à prendre des décisions mieux informées, et à fournir la base de la communication avec les personnes concernées par ces décisions. PANELFIT est heureux de coopérer à un tel effort de collaboration qui a été soutenu à l'origine par les initiatives Benchmark et EthicalGEO. Conformément à la Charte, nous considérons qu'il y a dix principes de base qui doivent être respectés lors de l'utilisation des données de position/proximité : réaliser des opportunités, comprendre les impacts, ne pas nuire, protéger les personnes vulnérables, traiter les biais, minimiser l'intrusion, minimiser les données, protéger la vie privée, empêcher l'identification des individus et assurer la responsabilité. Cette partie des lignes directrices vise à concrétiser ces principes éthiques en conseils juridiques tangibles.

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 adopté. Il se peut qu'au moment de l'utilisation de cet outil, le règlement soit en vigueur. Dans ce cas, il sera nécessaire de prendre en compte les éventuels changements que cela a pu engendrer dans le cadre réglementaire. Quoi qu'il en soit, ce document a tenté d'introduire certaines des principales dispositions incluses dans le projet de règlement "vie privée et communications électroniques". Ceci parce que, au minimum, nous devons comprendre qu'il s'agit d'exigences éthiques qu'une mise en œuvre correcte du RGPD exige. En ce sens, nous avons introduit dans cette partie des lignes directrices les principales instructions élaborées par l'EDPB à cet égard. [660]

Jusqu'à l'entrée en vigueur du règlement "vie privée et communications électroniques", une situation fragmentée existera. En effet, les autorités de contrôle sont maintenant confrontées à une situation où l'interaction 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

658 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. 12, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

659 https://ethicalgeo.org/locus-charter/

660 EDPB, Avis 5/2019 sur l'interaction entre la directive "vie privée et communications électroniques" et le RGPD, en particulier en ce qui concerne la compétence, les tâches et les pouvoirs des autorités chargées de la protection des données Adopté le 12 mars 2019, à l'adresse : https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

les domaines qui déclenchent l'application à la fois du RGPD et des lois nationales transposant la directive "vie privée et communications électroniques".[661]

1 Saisir les opportunités - compréhension de l'entreprise et plan de protection des données

1.1 Description

Les données géospatiales offrent de nombreux avantages sociaux et économiques, et ces possibilités doivent être exploitées de manière responsable. Les données géospatiales sont une vaste catégorie qui comprend, au moins, ces types de données :

- "**Données géospatiales**" pour un sens large. C'est le terme utilisé sur le site EthicalGEO. Il comprend à la fois les données de localisation et de proximité.
- " **Données de localisation** " : données géospatiales spécifiques ou très granulaires, qui permettent d'obtenir des informations très précises sur l'endroit où un sujet ou un dispositif est géopositionné.
- "**Données de proximité**" : données géospatiales moins précises, qui permettent de savoir de manière générale où un sujet ou un dispositif est géopositionné. Par exemple, en divisant une carte en plus grands quadrants, en utilisant des informations sur les codes postaux plutôt que des adresses spécifiques, etc. En général, les données de proximité informent l'utilisateur sur la proximité d'une personne concernée par rapport à une autre personne concernée ou à un lieu concret.

1.2 Définir l'objectif de votre projet et les enjeux de la protection des données

La phase initiale de compréhension de l'entreprise est essentielle en termes de protection des données, car elle se concentre sur la compréhension des objectifs du projet du point de vue de l'entreprise, la conversion de ces connaissances en une définition du problème de l'exploration de données, puis l'élaboration d'un plan préliminaire conçu pour atteindre les finalités. C'est un moment crucial puisque la protection des données dès la conception (voir la sous-section "Protection des données dès la conception et par défaut" dans la section "Concepts principaux" de la partie II des présentes lignes directrices) exige que les risques liés à la protection des données soient pris en compte lors de la rédaction de l'analyse de rentabilité et qu'ils soient suivis tout au long du

661 EDPB, Avis 5/2019 sur l'interaction entre la directive "vie privée et communications électroniques" et le RGPD, notamment en ce qui concerne la compétence, les tâches et les pouvoirs des autorités de protection des données Adopté le 12 mars 2019, à l'adresse : https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

projet. La protection des données dès la conception doit être un état d'esprit établi au sein d'une organisation et d'une équipe de projet.[662]

En pratique, cela signifie que toute personne désireuse de développer un outil TIC utilisant des données géospatiales devrait commencer par se demander quel est l'objectif de cet outil. Cette question est essentielle pour l'élaboration de leur politique de protection des données. Les développeurs de l'appareil doivent savoir dès le départ ce qu'ils attendent de lui. Si l'objectif du dispositif ne peut être atteint sans traiter une quantité disproportionnée de données à caractère personnel, si ces données doivent être conservées pendant des mois ou des années, s'il comporte des risques importants pour la vie privée des utilisateurs, si les garanties nécessaires ne peuvent être mises en place, etc. En outre, certains objectifs peuvent entrer en conflit avec les principes clés du RGPD ou de la Charte des droits fondamentaux de l'UE. Cela pourrait se produire, par exemple, lorsque les données de localisation/proximité sont utilisées pour recueillir par inadvertance des données sensibles, telles que les convictions religieuses de la personne concernée. Par exemple, en 2017, une "carte thermique mondiale" interactive montrant les mouvements des utilisateurs de l'application de fitness Strava a révélé par inadvertance l'emplacement du personnel militaire déployé dans des lieux classifiés[663] . Cet incident met en lumière certaines des questions juridiques et éthiques plus larges associées au partage de données ouvertes et au partage de données publiques par défaut. L'activation automatique de la géolocalisation sans intervention humaine doit être soigneusement évitée, car elle provoquerait un traitement illégal des données.

Encadré 1 : Exemples de différents dispositifs utilisant des données de localisation ou de proximité, et leurs conséquences en termes de traitement des données et de protection des données.

Ce n'est pas la même chose de concevoir un dispositif destiné à protéger une personne atteinte d'un certain niveau de démence et un dispositif destiné uniquement à permettre à une personne en bonne santé de savoir quels déplacements elle a effectués au cours des derniers mois. Les premières nécessiteront probablement l'utilisation d'outils capables de déterminer leur position très précisément, tandis que les secondes se contenteront d'une localisation moins précise. Les premiers utiliseront des données personnelles plus détaillées que les seconds. De même, certains produits nécessiteront des technologies qui n'auront pas besoin de préciser le temps que l'utilisateur passe dans tous les lieux concrets, alors que d'autres le feront (comme dans le cas de la personne atteinte de la maladie d'Alzheimer sévère). En outre, la conception de l'outil doit toujours prévoir des options permettant une utilisation proportionnelle des données. Même dans le cas d'une personne souffrant de la maladie d'Alzheimer, il devrait être possible de graduer l'utilisation des données géospatiales en fonction de ses besoins réels. Enfin, un développeur doit savoir dès le premier instant s'il est

662 Rapports techniques du JRC, Lignes directrices pour les administrations publiques sur la confidentialité de la localisation, à l'adresse suivante : https://publications.jrc.ec.europa.eu/repository/handle/JRC103110.

663 Voir : The Strava Heat Map and the End of Secrets, Wired, 2018, à l'adresse suivante : https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

nécessaire de conserver les données recueillies pendant des périodes plus ou moins longues. Un appareil qui veut seulement savoir si son utilisateur s'est rendu à un endroit où une prolifération de virus a été détectée n'aura probablement besoin de conserver les données de localisation que pendant quelques jours, tandis qu'un autre qui veut rendre compte des déplacements effectués au cours des derniers mois devra conserver les données beaucoup plus longtemps. Chacune de ces variantes aura des implications majeures en termes de protection des données à caractère personnel. Ce qui est indéniable, c'est que les développeurs peuvent difficilement définir leur politique de protection des données s'ils n'ont pas défini de manière adéquate l'objectif du dispositif à développer.

Les développeurs doivent être particulièrement conscients du fait que, parfois, toute augmentation marginale en termes de précision de la localisation ou de la recherche des contacts entraîne une augmentation significative de la quantité de données personnelles nécessaires.[664] Par exemple, la localisation basée sur le code postal est beaucoup moins précise et donc moins envahissante pour la vie privée que les systèmes de localisation exacte. Le premier peut suffire pour annoncer des restaurants locaux à des personnes de passage, tandis que le second sera nécessaire pour un service calculant le trajet le plus court en vélo entre deux points. Par conséquent, si les responsables du traitement des données envisagent une modification fondamentale du niveau de précision de la localisation ou du traçage requis, ils doivent examiner attentivement si cela est compatible avec le principe de minimisation des données (voir "Principe de minimisation des données" dans la partie II, section "Principes" des présentes lignes directrices. Vous trouverez plus de détails à ce sujet dans la section "Minimisation des données" ci-dessous dans la présente partie IV.

Enfin, les développeurs doivent décider si le produit mettra en œuvre une approche centralisée ou décentralisée. Les deux options doivent être considérées comme viables, à condition que des mesures de sécurité adéquates soient mises en place, chacune étant accompagnée d'un ensemble d'avantages et d'inconvénients. Toutefois, on considère généralement que les systèmes décentralisés respectent mieux la vie privée des utilisateurs. En effet, le point de départ du traitement des données devrait être les systèmes décentralisés qui cherchent à transférer le traitement sur les appareils des individus lorsque cela est possible. Des garanties et des mesures de sécurité doivent accompagner ces systèmes, ainsi que des informations et toutes les garanties supplémentaires nécessaires en cas de transferts internationaux de données.[665]

Ainsi, la phase conceptuelle du développement d'un dispositif ou d'un système devrait toujours inclure un examen approfondi de ces concepts alternatifs en pesant soigneusement les effets respectifs sur la protection des données/de la vie privée et les

664 Autorité norvégienne de protection des données (2018) Intelligence artificielle et vie privée. Autorité norvégienne de protection des données, Oslo, p.20. Disponible à l'adresse : https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf (consulté le 28 mai 2020).

665 Denham, Elizabeth, Commissaire à l'information du Royaume-Uni, Combatting COVID-19 through data : some considerations for privacy, à l'adresse : https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/.

impacts possibles sur les droits des individus.[666] Si les développeurs optent pour le système centralisé, les données traitées par le serveur centralisé devraient en général être limitées au strict minimum.

Chaque fois que cela est possible et pertinent, les parties prenantes doivent être consultées sur les questions éthiques et juridiques qu'elles estiment être en jeu et sur la manière dont ces questions doivent être traitées. Les parties prenantes consultées doivent inclure des représentants des principaux groupes qui seront affectés par le système - directement ou indirectement. De cette façon, un éventail suffisamment diversifié d'idées et de préférences éclairera les choix de conception.

Liste de contrôle : [667]

Les développeurs ont fixé les principaux objectifs à atteindre par le dispositif et envisagé les problèmes de protection des données que leur développement et leur mise en œuvre pourraient entraîner.

Les développeurs ont soigneusement examiné si la quantité de données ou le type de traitement nécessaires au bon fonctionnement du service sont compatibles avec les considérations relatives à la protection des données.

Les développeurs peuvent assurer une mise en œuvre adéquate des politiques de vie privée dès la conception. Ils peuvent démontrer comment ils s'alignent sur le RGPD et le cadre réglementaire sur les données de localisation/proximité. Les actions mises en œuvre pour assurer cet alignement ont été soigneusement documentées.

Les développeurs ont examiné les avantages et les inconvénients d'un système centralisé/décentralisé et ont pris une décision éclairée qui peut être soumise à l'examen de l'opinion publique. À cette fin, des consultations avec les principales parties prenantes ont été menées et documentées.

Les développeurs ont consulté les parties prenantes sur les éventuelles questions éthiques et juridiques en jeu.

1.3 Mettre en place un programme de formation sur les questions de protection des données pour le personnel impliqué dans la conception du dispositif ou du système.

Cette action est l'un des conseils les plus importants à prendre en compte dès les premiers instants d'un développement commercial utilisant des données de localisation ou de proximité. Ses concepteurs (développeurs, programmeurs, codeurs, data

666 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

667 Cette liste de contrôle a été élaborée sur la base des documents suivants : http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/.

scientists, ingénieurs) sont susceptibles d'ignorer les implications éthiques et juridiques liées à l'utilisation de ces données. Cela pourrait entraîner des conséquences en termes de respect adéquat des normes de protection des données.

Il est primordial que ces travailleurs clés aient la plus grande conscience possible des implications éthiques et sociales de leur travail, et du fait que celles-ci peuvent même s'étendre à des choix de société.[668] Cela aidera le développeur à éviter un grand nombre de problèmes éthiques et juridiques inutiles. Ainsi, la mise en œuvre de programmes de formation de base incluant au moins les principes fondamentaux de la Charte des droits fondamentaux, les principes exposés à l'article 5 du RGPD, la nécessité d'une base légale pour le traitement (y compris les contrats entre les parties), les principes de vie privée dès la conception et par défaut, etc. constitue une excellente mesure en termes de conformité.

Cependant, il peut être difficile de former des personnes qui n'ont jamais été en contact avec les questions de protection des données. Une politique alternative/complémentaire consiste à impliquer un expert de la protection des données, des questions éthiques et juridiques dans l'équipe de développement, de manière à créer une équipe interdisciplinaire. Cela peut se faire en engageant un expert à cette fin (un travailleur interne ou un consultant externe) pour concevoir la stratégie et les décisions ultérieures sur les données personnelles requises par le développement des outils, avec la participation étroite du délégué à la protection des données.

L'adoption de mesures adéquates pour assurer la confidentialité, l'intégrité et la disponibilité des données est également fortement recommandée (voir la sous-section "Mesures en faveur de la confidentialité" dans la section "Intégrité et confidentialité" des "Principes" de la partie II des présentes lignes directrices).

Liste de contrôle :

Les développeurs ont vérifié que les concepteurs d'outils et tous ceux qui auront à traiter des données ont acquis une connaissance adéquate du cadre de protection des données, ou ils ont assuré une participation adéquate de professionnels formés aux questions de protection des données dans l'équipe de développement.

Les développeurs ont mis en place un programme de formation sur les questions de confidentialité, d'intégrité et de disponibilité des données.

Les développeurs ont fait appel à un expert des utilisations éthiques/juridiques dès les étapes préliminaires du projet de recherche.

668 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).

1.4 Examiner quelle base juridique permettra le traitement des données personnelles par le dispositif ou le système.

Les dernières versions du règlement "vie privée et communications électroniques" comprennent plusieurs bases juridiques qui pourraient servir à légitimer le traitement des données. En général, le consentement continuera probablement à jouer un rôle clé dans le traitement des données par le biais des communications électroniques. Cependant, l'article 8 de la version du règlement "vie privée et communications électroniques" du Conseil[669] inclut des bases alternatives pour l'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations à partir des équipements terminaux des utilisateurs finaux, concernant même leurs logiciels et matériels :

- A) il est nécessaire dans le seul but de fournir un service de communication électronique ;
- C) il est strictement nécessaire pour fournir un service spécifiquement demandé par l'utilisateur final ;
- D) elle est nécessaire aux seules fins de la mesure d'audience, à condition que cette mesure soit effectuée par le fournisseur du service demandé par l'utilisateur final, ou par un tiers, ou par des tiers conjointement pour le compte du fournisseur du service demandé ou conjointement avec lui, à condition que, le cas échéant, les conditions prévues aux articles 26 ou 28 du règlement (UE) 2016/679 soient remplies ;
- DA) il est nécessaire de maintenir ou de rétablir la sécurité des services de la société de l'information ou de l'équipement terminal de l'utilisateur final, d'empêcher la fraude ou de prévenir ou détecter les défaillances techniques pendant la durée nécessaire à cette fin ; ou
- E) il est nécessaire de procéder à une mise à jour du logiciel, sous réserve de certaines circonstances.

Si le traitement implique uniquement la collecte d'informations émises par l'équipement terminal de l'utilisateur final pour lui permettre de se connecter à un autre dispositif et, ou à un équipement de réseau, il est autorisé si des conditions telles que celles incluses dans l'article 8.2 du projet de règlement "vie privée et communications électroniques" s'appliquent (c'est-à-dire (a) qu'elle est effectuée exclusivement pour, et seulement pendant le temps nécessaire, établir ou maintenir une connexion ; ou (b) que l'utilisateur final a donné son consentement ; ou (c) qu'elle est nécessaire à des fins statistiques limitées dans le temps et l'espace à ce qui est nécessaire à cette fin et que les données sont rendues anonymes ou effacées dès qu'elles ne sont plus nécessaires à cette fin, (d) qu'elle est nécessaire pour fournir un service demandé par l'utilisateur final.) et que les garanties correspondantes ont été mises en œuvre avec succès (voir l'article 8, paragraphe 2, point d), du projet de règlement "vie privée et communications électroniques"[670] .

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

Encadré 2 : réutilisation des données personnelles

L'une des questions les plus controversées en termes de protection des données est la réutilisation des données personnelles et la possibilité de procéder à un traitement licite sur cette base. Cette question a fait l'objet d'une analyse approfondie dans des documents tels que l'avis conjoint EDPB-CEPD 03/2021 sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (Data Governance Act). En bref, l'EDPB et le CEPD réitèrent que tout traitement de données à caractère personnel tel que mentionné dans la proposition doit se faire en pleine conformité avec le RGPD, et donc accompagné de garanties appropriées en matière de protection des données. Cela signifie que la réutilisation des données à caractère personnel doit toujours respecter les principes de licéité, de loyauté et de transparence, ainsi que la limitation de la finalité, la minimisation des données, la précision, la limitation du stockage, l'intégrité et la confidentialité, conformément à l'article 5 du RGPD (73). Le projet de règlement ePrivacy du Conseil comprend une clause consacrée à cette question, l'article 8, (g) et (h).

Par ailleurs, il peut également arriver que les données soient finalement traitées sur une base juridique alternative, telle que l'intérêt public. Cela n'est pas du tout impossible si les circonstances le recommandent et si le traitement est fondé sur le 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. Toutefois, les développeurs doivent garder à l'esprit que ces bases alternatives ne sont applicables que si le responsable du traitement est une autorité publique. En outre, la réglementation de l'intérêt public peut être différente dans chaque État membre. Les responsables du traitement doivent être bien conscients de ces circonstances.

D'autre part, les données à caractère personnel **peuvent être réutilisées à des fins compatibles avec celles pour lesquelles elles ont été initialement collectées.** Ainsi, en principe, le développeur pourrait utiliser des données déjà disponibles pour développer l'appareil, sans collecter de nouvelles données. Toutefois, le responsable du traitement doit s'assurer et documenter soigneusement que cette finalité est bien compatible avec la finalité initiale (voir "Protection des données et recherche scientifique" dans la partie II, section "Concepts principaux" des présentes lignes directrices).[671]

Par ailleurs, les **données** personnelles **peuvent également être réutilisées après avoir été soumises à un processus d'anonymisation.** En d'autres termes, les données personnelles existant précédemment peuvent être transformées en données non personnelles. Le traitement n'entre donc pas dans le champ d'application du RGPD. Il peut encore relever du règlement relatif à la vie privée en ligne lorsqu'il entrera en vigueur. Dans ce cas, l'utilisation ultérieure de données anonymes sera autorisée. À cet égard, le responsable du traitement doit garder à l'esprit que le procédé technique consistant à soumettre les données personnelles à une technique d'anonymisation constitue en soi un traitement de données personnelles. Ce traitement peut être

671 EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 77.

considéré comme compatible avec la finalité initiale du traitement à condition que le procédé produise des informations véritablement anonymisées, au sens défini par l'ancien groupe de travail Article 29.[672] (Voir les sections "Anonymisation" et "Pseudonymisation" dans la partie "Concepts principaux" des présentes lignes directrices).

La base juridique qui constitue le fondement légal de l'utilisation des données de localisation/proximité devrait, en tout état de cause, comporter des **garanties** significatives. Une spécification claire de la finalité et des limitations explicites concernant l'utilisation ultérieure des données à caractère personnel doit être incluse, ainsi qu'une identification claire du ou des responsables du traitement concernés. Les catégories de données ainsi que les entités (et les finalités pour lesquelles les données personnelles peuvent être divulguées) doivent également être identifiées. Si les données sont utilisées à plusieurs fins, le responsable du traitement doit indiquer quelles catégories de données sont utilisées et à quelles fins. En plus de tout ce qui précède, il est important d'établir et de communiquer la période de temps pendant laquelle les données seront conservées. En outre, les informations ne doivent pas être utilisées pour déterminer la nature ou les caractéristiques d'un utilisateur final ou pour établir le profil d'un utilisateur final. En fonction du niveau d'ingérence, des garanties supplémentaires doivent être intégrées, en tenant compte de la nature, de la portée et des finalités du traitement. Voir, à ce sujet, l'article 8 du règlement "vie privée et communications électroniques".

Liste de contrôle : base juridique

Les développeurs ont vérifié qu'ils disposent d'une base juridique permettant un traitement licite des données.

Les responsables du traitement ont vérifié le cadre réglementaire européen ou national concernant l'utilisation des données personnelles.

Si les données personnelles sont utilisées à des fins compatibles, le responsable du traitement a effectué le test de compatibilité et s'est assuré que les utilisations sont compatibles.

Si les données sont utilisées dans un but autre que celui initialement recherché, l'outil est conçu pour informer l'utilisateur de cette utilisation.

Cet outil est conçu pour permettre la réutilisation des données à caractère personnel uniquement lorsqu'elle est fondée sur le droit de l'Union ou des États membres qui établit une liste de finalités compatibles claires pour lesquelles le traitement ultérieur peut être légalement autorisé ou constitue une mesure nécessaire et proportionnée dans une société démocratique.

672 Groupe de travail Article 29, Avis 5/2014 sur les techniques d'anonymisation. Adopté le 10 avril 2014, p-7-8., à l'adresse https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf.

1.5 Considération particulière du consentement comme base du traitement

Le consentement n'est pas toujours la base juridique qui légitime le traitement des données, comme exprimé précédemment. Toutefois, il ne s'agit pas des situations les plus courantes. Au contraire, le projet de règlement "vie privée et communications électroniques"[673] considère le consentement comme la principale base légale du traitement des données dans le contexte des communications électroniques. Toutefois, le consentement 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 leur dispositif inclut la nécessité d'obtenir le consentement des utilisateurs pour le traitement de manière informée et granulaire et la documentation de ce consentement. En outre, ce consentement doit être correctement accrédité.

Il doit être parfaitement clair que le consentement de la personne concernée ne peut pas être obtenu librement par l'acceptation obligatoire de conditions générales ou par des possibilités d'exclusion.[674] **L'approche doit être granulaire.** D'autre part, les paramètres par défaut d'un système d'exploitation devraient garantir que les services de localisation sont désactivés (OFF), et les utilisateurs peuvent consentir explicitement à l'activation (ON) d'applications spécifiques. En outre, "il est important de faire la distinction entre le consentement à un service ponctuel et le consentement à un abonnement régulier. Par exemple, afin d'utiliser un service de géolocalisation particulier, il peut être nécessaire d'activer les services de géolocalisation dans l'appareil ou le navigateur. Si cette capacité de géolocalisation est activée, chaque site web peut lire les données de localisation de l'utilisateur de cet appareil mobile intelligent. Afin de prévenir les risques de surveillance secrète, l'ancien groupe de travail Article 29 considère qu'il est essentiel que le dispositif prévienne en permanence que la géolocalisation est activée, par exemple au moyen d'une icône visible en permanence.[675]

Enfin, et c'est important, l'ancien groupe de travail Article 29 a recommandé que les fournisseurs d'applications ou de services de localisation 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 ne serait pas valable de continuer à traiter des données de localisation 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 (ou plus souvent 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 électronique capable d'envoyer une demande à l'utilisateur afin de (re)gagner (ou non) son consentement pour poursuivre le traitement. Toutefois, il s'agit davantage d'une recommandation que d'une exigence légale.

---

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

674 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.

675 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.

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 les réglementations nationales ; 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.

Encadré 3 : Consentement général et garanties supplémentaires

L'autorité allemande de protection des données a récemment dressé une liste de garanties supplémentaires à mettre en œuvre en cas de consentement général.[676] Il s'agit de :

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 finalités de la recherche n'est pas possible.
    - Mettre en place des présences sur le web pour informer les participants à la recherche 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 s'opposer avant que les données ne soient utilisées pour de nouvelles questions de recherche.
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 ou la pseudonymisation.
    - Mise en œuvre de politiques spécifiques pour limiter l'accès aux données personnelles.

676 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/.

Encadré 4 : Exemple de bonnes pratiques pour les fournisseurs d'applications de géolocalisation selon l'ancien groupe de travail Article 29-[677] :

Une application qui souhaite utiliser des données de géolocalisation informe clairement l'utilisateur des finalités pour lesquelles elle veut utiliser les données, et demande un consentement sans ambiguïté pour chacune des finalités éventuellement différentes. L'utilisateur choisit activement le niveau de granularité de la géolocalisation (par exemple, au niveau du pays, de la ville, du code postal ou aussi précisément que possible). Une fois le service de localisation activé, une icône est visible en permanence sur chaque écran indiquant que les services de localisation sont "activés". Les utilisateurs peuvent retirer leur consentement en permanence, sans avoir à quitter l'application. Les utilisateurs peuvent également supprimer facilement et définitivement toutes les données de localisation stockées sur l'appareil.

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 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.

 Le consentement général utilisé pour le traitement de catégories spéciales de données est compatible avec les réglementations nationales.

 Lorsque le consentement général est utilisé, le responsable du traitement est particulièrement conscient que 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 du traitement ont une relation directe avec le sujet qui fournit les données.

 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 certains contextes tels que le cadre du travail.

 Les contrôleurs demandent aux personnes de s'inscrire activement.

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

 Les contrôleurs utilisent un langage clair et simple, facile à comprendre.

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

677 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. 15, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

- 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 données ou les catégories de données qui seront traitées 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 que cela ne porte atteinte à leur accès au service.
- Les contrôleurs évitent de faire du consentement une condition préalable à un service.

1.6 Connaître le niveau de protection des données concernées par le traitement.

Les développeurs doivent toujours garder à l'esprit que les dispositifs produits doivent minimiser l'intrusion dans la vie des personnes. En effet, ils devraient toujours se rappeler que les données sont protégées comme suit :

En tant que "données à caractère personnel", c'est-à-dire toute information relative à une personne physique identifiée ou identifiable (article 4, paragraphe 1, du RGPD), elles sont protégées par le RGPD. Les données de santé bénéficient d'une protection supplémentaire (article 9 du RGPD).

En tant que "données de localisation", c'est-à-dire les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques, indiquant la position géographique de l'équipement terminal de l'utilisateur, elles seront probablement protégées par le règlement "vie privée et communications électroniques".[678]

En outre, le futur règlement "Vie privée et communications électroniques" protégera les informations émises par les équipements terminaux des utilisateurs.

Cela pourrait changer dans les années à venir, mais pour le moment, cela donne un bon résumé de la situation actuelle.[679]

2 Comprendre les impacts

2.1 Description

Les utilisateurs de données de localisation ont la responsabilité de comprendre les effets potentiels de leurs utilisations des données, notamment en sachant qui (individus et

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

679 COMMUNICATION DE LA COMMISSION, Orientations sur les applications soutenant la lutte contre la pandémie de COVID 19 en relation avec la protection des données, Bruxelles, 16.4.2020 C(2020) 2523 final, p.6, à l'adresse : https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf.

groupes) et quoi pourrait être affecté, et comment. Cette compréhension doit être utilisée pour prendre des décisions éclairées et proportionnées, et pour minimiser les impacts négatifs.

2.2 Mesures éthiques générales à mettre en œuvre

Pour répondre à cette exigence éthique, deux perspectives doivent être gardées à l'esprit. D'une part, la nécessité de considérer l'impact du traitement des données en termes de protection des données en tant que tel. D'autre part, l'impact que ce traitement peut avoir sur l'environnement, la société ou les relations humaines. En ce qui concerne ce dernier point, il est essentiel de tenir compte des recommandations formulées par le groupe d'experts de haut niveau sur l'IA. Bien qu'elles aient été élaborées dans le contexte de l'IA, elles sont parfaitement applicables à l'utilisation des données géospatiales.[680] Les recommandations du groupe étaient les suivantes :

- Les dispositifs et systèmes utilisant des données géospatiales promettent d'aider à résoudre certains de nos problèmes sociétaux les plus urgents, mais cela doit se faire de la manière la plus respectueuse possible de l'environnement. Les processus de développement, de déploiement et d'utilisation du système, ainsi que l'ensemble de sa chaîne d'approvisionnement, doivent être évalués à cet égard. Cela comprend des mesures telles qu'un examen critique de l'utilisation des ressources et de la consommation d'énergie, en optant pour des choix moins dommageables pour l'environnement lorsqu'ils sont disponibles. Des mesures garantissant le respect de l'environnement dans l'ensemble de la chaîne d'approvisionnement des appareils et des systèmes ont été mises en œuvre.
- L'exposition omniprésente aux dispositifs et systèmes de localisation et de traçage dans tous les domaines de notre vie - qu'il s'agisse d'éducation, de travail, de soins ou de divertissement - peut modifier notre conception de l'action sociale ou avoir un impact sur nos relations sociales et notre attachement. Si ces dispositifs et systèmes peuvent être utilisés pour améliorer les compétences sociales, ils peuvent également contribuer à leur détérioration. Cela pourrait également affecter le bien-être physique et mental des personnes. Les effets de ces systèmes doivent donc être soigneusement surveillés et pris en compte.
- Au-delà de l'évaluation de l'impact du développement, du déploiement et de l'utilisation d'un dispositif ou d'un système sur les individus, cet impact doit également être évalué d'un point de vue sociétal, en tenant compte de son effet sur les institutions, la démocratie et la société dans son ensemble. Leur mise en œuvre doit toujours faire l'objet d'un examen attentif, notamment dans les situations de restriction des droits et libertés individuels.

680Groupe d'experts de haut niveau sur l'IA, Lignes directrices éthiques pour une intelligence artificielle digne de confiance (84 et suivants), à l'adresse : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Liste de contrôle :

Le dispositif ne comprend pas d'outils permettant une utilisation des données d'une manière peu compatible avec la préservation des espaces de confidentialité pertinents.

L'outil tient compte des principes de durabilité environnementale, tant en ce qui concerne le système lui-même que la chaîne d'approvisionnement à laquelle il est relié (le cas échéant).

La configuration par défaut de l'appareil ne permet pas une utilisation disproportionnée des données à des fins de surveillance.

Les responsables du traitement ont veillé à ce que l'outil tienne compte du bien-être de toutes les parties prenantes et une réduction générale de leur bien-être n'est pas du tout prévisible.

Le dispositif n'est pas conçu à des fins qui sont difficilement compatibles avec les principes éthiques propres à l'UE.

2.3 Questions juridiques : réalisation d'analyses de l'impact sur la protection des données

Une AIPD est un processus dans lequel le responsable du traitement, avant de lancer une procédure de traitement des données présentant un **risque élevé** pour les libertés et droits fondamentaux des personnes concernées, évalue l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel (article 35, paragraphe 1, du RGPD). Si les responsables du traitement sont confrontés à un risque élevé, alors une AIPD doit être menée conformément à l'article 35(7) du RGPD. Dans le cas des données de localisation et de proximité, l'EDPB a estimé "qu'une analyse d'impact sur la protection des données (AIPD) **doit être réalisée avant de mettre en œuvre un tel outil, car le traitement est considéré comme présentant probablement un risque élevé** (données relatives à la santé, adoption anticipée à grande échelle, surveillance systématique, utilisation d'une nouvelle solution technologique). L'EDPB recommande vivement la publication des AIPD".[681] .

Il est important de souligner qu'une AIPD doit être réalisée chaque fois que le responsable du traitement considère qu'un traitement concret comporte un risque élevé. La plupart des agences de protection des données imposent des analyses d'impact sur la protection des données lorsque le traitement implique une localisation systématique des personnes concernées.[682] Par conséquent, il peut parfaitement arriver qu'un développeur doive réaliser plusieurs AIPD au cours du processus de production. En effet, nous considérons que ces analyses doivent être revues et mises à jour lorsque cela est possible et surtout lorsque le responsable du traitement doit définir les politiques de conservation et d'élimination des données.

Dans certaines situations, si le résultat de l'analyse d'impact sur les données est que l'activité de traitement envisagée présente un risque élevé de porter atteinte aux libertés

681 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

682 Voir, par exemple, la position adoptée par l'Agence espagnole de protection des données dans : https://www.aepd.es/sites/default/files/2019-09/listas-DPIA-es-35-4.pdf.

et droits fondamentaux des personnes concernées, **le responsable du traitement doit demander l'avis de l'autorité de contrôle nationale**, comme le prescrit l'article 36 du RGPD. Certains États membres ont publié des listes qui contiennent des exemples d'activités de traitement des données qui déclencheraient cette AIPD obligatoire ; parmi ces exemples, nous pouvons identifier des situations qui correspondent à des techniques traitant des données de localisation et de proximité. Cela est particulièrement vrai si elles intègrent des techniques d'IA. Les autorités de contrôle peuvent exiger l'adoption de certaines mesures pour atténuer le risque, si possible, ou interdire l'utilisation du dispositif ou du système si cela n'est pas possible.

Liste de contrôle : une AIPD est-elle nécessaire ?

Le responsable du traitement a déterminé les juridictions où les activités de traitement des données auront lieu.

Le responsable du traitement a vérifié si ces juridictions ont adopté des listes indiquant les traitements qui requièrent une analyse obligatoire de l'impact sur la protection des données et a vérifié si le traitement des données prévu est couvert par ces dispositions.

Si le responsable du traitement n'est pas sûr de la nécessité d'effectuer une analyse de l'impact sur la protection des données, il doit consulter le DPD ou, à défaut, le service juridique du responsable du traitement.

Le cas échéant, le responsable du traitement a procédé à une analyse d'impact sur la protection des données.

Si nécessaire, le responsable du traitement a déposé une consultation préalable auprès de l'autorité de contrôle compétente.

Si des modifications étaient suggérées, le responsable du traitement suivait l'avis de l'autorité de contrôle.

3 Ne pas nuire

3.1 Description

La proximité physique amplifie les dommages potentiels que peuvent subir les personnes, la flore et la faune. Les utilisateurs de données doivent veiller à ce que les données de localisation individuelles ou collectives relatives à toutes les espèces ne soient pas utilisées à des fins de discrimination, d'exploitation ou de préjudice. Les droits établis dans le monde physique doivent être protégés dans les contextes et interactions numériques.

3.2 Assurer la sécurité

L'un des principaux problèmes que peut poser le traitement massif de données est l'exposition de données personnelles à des tiers non autorisés. Une violation des données pourrait causer des dommages considérables à des milliers ou des millions d'utilisateurs, dont la vie privée pourrait être compromise. Par exemple, au Qatar, une faille de sécurité dans l'application nationale de recherche des contacts a exposé les données personnelles sensibles de plus d'un million de personnes en mai 2020. [683]

Ces risques doivent être atténués par la mise en œuvre de contrôles de sécurité techniques et/ou organisationnels. Les mesures techniques comprennent, sans s'y limiter, l'utilisation de techniques cryptographiques de pointe, capables de sécuriser les données stockées dans les serveurs et les applications, les échanges entre les applications et le serveur distant. Une authentification mutuelle entre l'application et le serveur doit également être effectuée. Si l'application signale des utilisateurs, cela doit faire l'objet d'une autorisation appropriée, par exemple au moyen d'un code à usage unique lié à une identité pseudonyme de l'utilisateur. Si la confirmation ne peut être obtenue de manière sécurisée, aucun traitement de données ne doit avoir lieu qui présume de la validité du statut de l'utilisateur.[684]

Les mesures organisationnelles doivent garantir une mise en œuvre adéquate de principes de sécurité bien établis tels que le "besoin de savoir" (c'est-à-dire autoriser l'accès à des informations ou à des connaissances si cela est nécessaire pour accomplir une tâche donnée), la création de rôles avec différentes autorisations d'accès aux données, ou la "sécurité par couches" (c'est-à-dire une stratégie de sécurité défensive comportant plusieurs couches conçues pour ralentir une attaque de sécurité). Il est important de savoir que le niveau global de sécurité d'une solution est aussi fort que le maillon le plus faible. Ainsi, "chaque composant d'une solution, qu'il s'agisse de systèmes centraux ou de dispositifs distants, doit être sécurisé de manière adéquate".[685] Or, bien souvent, ce maillon faible peut être dû à une erreur humaine. Prenons, par exemple, le cas de mots de passe faibles faisant l'objet d'attaques de phishing ou la perte d'un appareil stockant des données. C'est pourquoi les mesures de sécurité doivent inclure des programmes de formation et de sensibilisation du personnel concerné.

Avant de déployer l'outil dans le monde réel, il est conseillé d'effectuer des tests de sécurité (tests de données aléatoires, également appelés "fuzzing", analyse de vulnérabilité, etc.) Ceux-ci serviront à vérifier que le produit continue à fonctionner de manière acceptable lorsque son utilisation normale est abandonnée et qu'il ne présente aucune vulnérabilité qui pourrait permettre à des tiers de compromettre sa sécurité. Ces deux types de tests sont importants pour le bon fonctionnement de l'outil. Par exemple, un système d'intégration continue devrait être configuré pour exécuter des tests automatiquement après chaque modification du code source.

---

683 https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

684 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

685 Rapports techniques du JRC, Lignes directrices pour les administrations publiques sur la confidentialité de la localisation, à l'adresse suivante : https://publications.jrc.ec.europa.eu/repository/handle/JRC103110.

Encadré 5 : Vérification et contrôle des identifiants et des participants dans l'outil

Lorsqu'une application crée ou utilise un identifiant unique, des mesures doivent être prises pour garantir que l'identifiant est lié à l'utilisateur légitime de l'application et que cette information est tenue à jour. Chaque partie utilisant des identifiants est responsable de prendre des mesures pour :

- mettre en œuvre des mesures destinées à garantir que tout identifiant unique ne s'applique qu'à un seul utilisateur unique. Si cela est trop complexe, introduisez des mesures visant à prévenir ou à atténuer les conséquences indésirables et informez-en les personnes concernées.

- veiller à ce que les identifiants uniques soient tenus à jour et ne soient conservés que le temps nécessaire à la réalisation de l'objectif de l'application et des raisons notifiées aux utilisateurs.

- empêcher qu'un identifiant unique soit associé à un autre utilisateur, sauf si un besoin justifié du PROJET l'exige.

L'utilisation d'un identifiant permanent (tel qu'un numéro IMEI ou un identifiant publicitaire) crée généralement plus de risques que l'utilisation d'un identifiant aléatoire ou rotatif.

En outre, la gestion des profils des utilisateurs finaux/participants doit être réfléchie avant le développement. Authentifier les utilisateurs lorsque cela est possible en utilisant des méthodes d'authentification adaptées au risque. Lorsque l'affirmation d'une identité réelle est une composante importante d'un service, une authentification plus forte, telle qu'une authentification à deux facteurs utilisant un téléphone portable et un UICC, devrait être appliquée.

Liste de contrôle : [686]

 Le responsable du traitement a évalué les formes potentielles d'attaques auxquelles l'outil pourrait être vulnérable, a introduit des mesures d'atténuation et les a documentées.

 Le responsable du traitement a examiné différents types et natures de vulnérabilités, comme la pollution des données, les infrastructures physiques et les cyberattaques.

 Le responsable du traitement a mis en place des mesures ou des systèmes pour garantir l'intégrité et la résilience du système contre les attaques potentielles.

 Le responsable du traitement a vérifié comment le système se comporte dans des situations et des environnements inattendus.

 Le responsable du traitement examine dans quelle mesure le système pourrait être à

686 Cette liste de contrôle a été construite sur la base de ces documents : EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie COVID-19 Adoptées le 21 avril 2020 ; Groupe d'experts de haut niveau sur l'intelligence artificielle (2019) Lignes directrices éthiques pour une IA digne de confiance. Commission européenne, Bruxelles. Disponible à l'adresse : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

double usage. Si c'est le cas, le responsable du traitement a pris des mesures préventives appropriées contre cela.

 Le responsable du traitement s'est assuré que le système dispose d'un plan de repli suffisant s'il est confronté à des attaques adverses ou à d'autres situations inattendues (par exemple, procédures de commutation technique ou demande d'un opérateur humain avant de poursuivre).

Les données envoyées au serveur central sont transmises par un canal sécurisé. L'utilisation des services de notification fournis par les fournisseurs de plateformes OS est soigneusement évaluée et ne conduit pas à la divulgation de données à des tiers.

Les demandes ne sont pas vulnérables à la falsification par un utilisateur malveillant.

Des techniques cryptographiques de pointe sont mises en œuvre pour sécuriser les échanges entre l'application et le serveur et entre les applications et, en règle générale, pour protéger les informations stockées dans les applications et sur le serveur.

Le serveur central ne conserve pas les identifiants de connexion réseau (par exemple, les adresses IP) des utilisateurs.

Afin d'éviter l'usurpation d'identité ou la création de faux utilisateurs, le serveur authentifie l'application.

L'application authentifie le serveur central.

Les fonctionnalités du serveur sont protégées contre les attaques par rejeu.

Les informations transmises par le serveur central sont signées afin d'authentifier leur origine et leur intégrité.

L'accès à toutes les données stockées dans le serveur central et non accessibles au public est limité aux seules personnes autorisées.

Le gestionnaire d'autorisations de l'appareil au niveau du système d'exploitation ne demande que les autorisations nécessaires pour accéder aux modules de communication et les utiliser, pour stocker les données dans le terminal et pour échanger des informations avec le serveur central.

 Le personnel et autre personne physique du projet a été informé et sensibilisé aux mesures de sécurité.

3.3 Mettre en place des mécanismes visant à notifier les violations de données dès que possible

Les violations de données représentent un danger sérieux pour les droits et libertés des personnes concernées. Les responsables du traitement sont censés les notifier aux autorités de contrôle et aux personnes concernées dans les meilleurs délais. En outre, si la violation des données est susceptible d'entraîner un risque élevé, les personnes concernées doivent être informées personnellement et sans délai excessif. La notification doit décrire les détails de la violation des données, les mesures de contrôle déjà prises et les recommandations pour les personnes concernées afin de limiter les dommages. Dans la pratique, il peut être impossible de contacter tous les utilisateurs.

Par conséquent, une communication publique - si elle est efficace - peut être considérée comme suffisante. Toute communication avec les personnes concernées doit être transparente et rédigée dans un langage clair et simple.[687]

Liste de contrôle :

Les responsables du traitement ont mis en œuvre des politiques adéquates pour notifier les violations de données dès que possible et tous les participants au processus de développement en sont bien conscients.

Des modèles concernant les informations à inclure dans les notifications ont été conçus.

Des politiques et des outils de communication, visant à faciliter la communication avec les personnes concernées en cas de violation des données, ont été créés.

4 Protéger les personnes vulnérables

4.1 Description

Les personnes et les lieux vulnérables peuvent subir un préjudice disproportionné du fait de l'utilisation abusive des données de localisation, et peuvent ne pas avoir la capacité de se protéger. Dans ces contextes, les utilisateurs de données doivent faire preuve d'une prudence accrue, agir de manière proportionnée et éviter positivement de causer du tort.

4.2 Questions éthiques et juridiques

L'une des questions fondamentales dans le développement d'une technologie TIC est qu'elle doit éviter d'aboutir à des résultats d'exclusion pour une partie de la population. Cela est particulièrement vrai lorsque nous parlons de populations vulnérables, telles que les personnes handicapées, les personnes à faible pouvoir d'achat ou les personnes ayant des difficultés à interagir avec les appareils électroniques. Dans le cas des dispositifs conçus à des fins de traçabilité ou de localisation, cela implique, entre autres, ce qui suit :

- Développer des produits qui peuvent être utilisés par le biais de différents types d'appareils, smartphones, jetons, etc., afin que ceux qui ne possèdent pas l'un de ces appareils puissent en acquérir un autre.
- Introduire des options de fonctionnement adaptées aux personnes handicapées, afin que celles-ci ne les empêchent pas d'utiliser les outils conçus.

687 Rapports techniques du JRC, Lignes directrices pour les administrations publiques sur la confidentialité de la localisation, à l'adresse suivante : https://publications.jrc.ec.europa.eu/repository/handle/JRC103110.

- Simplifier autant que possible le fonctionnement de leurs opérations de base, afin que toute personne puisse les utiliser sans fournir un effort excessif par rapport à ses capacités.
- Les politiques de confidentialité doivent être rédigées dans un style convivial, afin que chacun puisse les comprendre.
- Si le dispositif est spécifiquement destiné aux personnes vulnérables (par exemple, un dispositif de localisation pour éviter que les malvoyants ne se perdent) ou aux utilisateurs mineurs, les politiques de confidentialité doivent être adaptées à ce groupe cible spécifique. Cela peut signifier qu'elles doivent être accessibles par la voix plutôt qu'uniquement par le texte, par des images plutôt que par de longs textes, ou que le langage est adapté, par exemple, à la compréhension d'un adolescent moyen.

Le cas des enfants est particulièrement important. Selon le considérant 38 du RGPD, "les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel, car ils peuvent être moins conscients des risques, des conséquences et des garanties concernées, ainsi que de leurs droits par rapport au traitement". L'ICO a élaboré des recommandations extrêmement utiles à cet effet[688] .

Liste de contrôle :

Les responsables du traitement ont mis en place des contrôles supplémentaires pour leurs systèmes de profilage/décision automatisée afin de protéger tout groupe vulnérable (y compris les enfants).

Les informations et les politiques de confidentialité doivent être accessibles par différents moyens (voix, images, vidéo ou dans un langage facile à comprendre). Cela est particulièrement important si le dispositif de localisation est destiné à un groupe d'utilisateurs spécifique.

Le consentement est adapté aux populations vulnérables et aux besoins des enfants.

Des options d'utilisation facilitant l'utilisation du dispositif par les populations vulnérables ont été envisagées.

Si le responsable du traitement est disposé à utiliser les données pour une finalité autre que celle initialement demandée, l'outil est conçu pour demander l'autorisation aux utilisateurs vulnérables d'une manière qui soit compatible avec leurs conditions personnelles.

5 Biais d'adresse

5.1 Description

Les biais dans la collecte, l'utilisation et la combinaison des ensembles de données de localisation peuvent soit exclure les groupes affectés de la cartographie qui transmet les

688 https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/.

droits ou les services, soit amplifier les impacts négatifs de l'inclusion dans un ensemble de données. Il faut donc veiller à comprendre les biais dans les ensembles de données et à éviter les résultats discriminatoires.

5.2 Questions juridiques

Les biais sont l'un des principaux problèmes liés à l'utilisation des dispositifs et systèmes TIC, un problème qui va à l'encontre du principe de loyauté (voir "Principe de licéité, de loyauté et de transparence" dans la partie II, section "Principes" des présentes lignes directrices). Dans le cas des dispositifs basés sur des données de localisation et/ou de proximité, les biais peuvent provenir d'au moins deux situations différentes :

- Biais créés par un système d'IA interagissant avec les dispositifs ou systèmes de localisation. Parfois, les dispositifs ou systèmes de localisation intègrent des outils d'IA ou interagissent avec eux (voir la partie III des présentes lignes directrices consacrée aux systèmes d'IA). Si tel est le cas, les développeurs doivent veiller tout particulièrement à ce qu'ils n'introduisent pas de biais dans le fonctionnement du dispositif ou du système de localisation. À cette fin, ils doivent adopter un certain nombre de mesures, telles que décrites dans la partie III des présentes lignes directrices consacrée aux systèmes d'IA
- Biais créés par les données recueillies. Ce type de biais est particulièrement probable si l'outil TIC vise à fournir des informations basées sur des données recueillies auprès d'une population entière. Il faut garder à l'esprit que, selon l'origine des données agrégées, il est très probable que leur degré de représentation sociale soit inexact. En effet, comme l'a montré la recherche sur les médias locatifs, le contexte et la marginalisation importent avec les données de localisation.[689] Cela peut créer des problèmes d'iniquité, car certaines classes sociales (notamment celles qui n'utilisent pas les appareils ou qui souffrent d'un manque de capacités spécifiques permettant d'obtenir les données) sont sous-représentées dans l'analyse et la prise de décision ultérieure.[690] Cela pourrait laisser de côté des populations entières et en déformer d'autres, et conduire à un déploiement de ressources non seulement biaisé et injuste - en faveur des quartiers les plus riches, par exemple - mais aussi inefficace du point de vue des politiques publiques.[691] Bien entendu, la mauvaise représentation peut également introduire des biais dans les interventions de police et de l'ordre public, produisant des résultats préjudiciables aux communautés à faibles revenus, par exemple. Les développeurs de dispositifs ou de systèmes de localisation doivent s'efforcer d'éviter ce type de biais, soit en fournissant des dispositifs à ceux qui seraient autrement marginalisés, soit en intégrant des informations complémentaires

689 Graham, M., Zook, M. (2013). Réalités augmentées et géographies inégales : Exploration des contours géolinguistiques du web. Environment and Planning A, 45, 77-99.

690 Frith J, Saker M. It Is All About Location : Smartphones and Tracking the Spreading of COVID-19. Social Media + Society. Juillet 2020. doi:10.1177/2056305120948257

691 Jay Stanley et Jennifer Stisa Granick The Limits of Location Tracking in an Epidemic, ACLU Whitepaper, 8 avril 2020, à l'adresse : https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic.

qui corrigent l'erreur. S'il est impossible de l'éviter, ils devraient consigner l'existence du biais, afin que ceux qui auraient à prendre des décisions grâce au mécanisme développé en soient conscients.

Liste de contrôle : [692]
Le responsable du traitement a mis en place des moyens de mesurer si l'outil fait un nombre inacceptable de prédictions biaisées.
Le responsable du traitement a mis en place une série de mesures pour accroître la précision de l'outil.
Le responsable du traitement a mis en place des mesures pour évaluer s'il est nécessaire de disposer de données supplémentaires, par exemple pour éliminer les biais.
Le responsable du traitement a vérifié le préjudice qui serait causé si l'outil faisait des prédictions biaisées.

6 Minimiser les intrusions

6.1 Description

Étant donné la nature intime et personnelle des données de localisation, les utilisateurs devraient éviter d'examiner inutilement et de manière intrusive la vie des gens et les lieux où ils vivent, ce qui pourrait porter atteinte à la dignité humaine.

6.2 Questions juridiques : utilisation de données anonymes au lieu de données personnelles

Les développeurs doivent garder à l'esprit que les responsables du traitement des données en charge de leurs appareils ou systèmes devront être en mesure de démontrer que le traitement est **nécessaire à l'objectif poursuivi** et qu'il est **moins intrusif que d'autres options** permettant d'atteindre le même but ; et non qu'il s'agit d'une partie nécessaire des méthodes qu'ils ont choisies.[693] S'il existe des alternatives réalistes et

692 Cette liste de contrôle a été adaptée de celle élaborée par le Groupe d'experts de haut niveau sur l'intelligence artificielle (2019) Lignes directrices en matière d'éthique pour une IA digne de confiance. Commission européenne, Bruxelles. Disponible à l'adresse : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (consulté le 20 mai 2020).

693 CEPD (2017) Necessity toolkit : assessing the necessity of measures that limit the fundamental right to the protection of personal data, p.5. Contrôleur européen de la protection des données, Bruxelles. Disponible à l'adresse : https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en (consulté le 15 mai 2020) ; ICO (sans date) Lawful basis for processing. Bureau du commissaire à l'information, Wilmslow. Disponible 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/ (consulté le 15 mai 2020).

moins intrusives, le traitement des données personnelles n'est pas jugé nécessaire.[694] Ainsi, les développeurs doivent fournir aux appareils et aux systèmes des options qui leur permettent de réduire l'utilisation des données à ce qui est strictement nécessaire (voir "Principe de minimisation" dans "Concepts principaux", partie II des présentes lignes directrices). Le concept de nécessité est toutefois complexe et a une signification indépendante dans le droit de l'Union européenne.[695] En général, il exige que le traitement soit un moyen ciblé et proportionné d'atteindre une finalité spécifique. Bien qu'elle ne doive pas être interprétée de manière stricte au point de signifier que seules les données absolument essentielles sont traitées, il ne suffit pas de faire valoir que le traitement est nécessaire parce que les responsables du traitement ont choisi d'exploiter leur entreprise d'une manière particulière. Par exemple, l'outil ne doit pas permettre d'identifier directement les utilisateurs lors de l'utilisation de l'application.

Le principe de minimisation des données stipule que les données personnelles doivent être "adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées".[696] Ce principe éthique signifie que, lorsqu'il s'agit d'utiliser des données de localisation ou de proximité, il faut toujours privilégier le traitement de données anonymisées plutôt que de données personnelles[697] (voir les sections "Licéité et loyauté" et "Anonymisation" de la partie II des présentes lignes directrices). En effet, si des données personnelles peuvent être remplacées par des données non personnelles sans que cela n'affecte les finalités du traitement, l'utilisation de données anonymisées doit être clairement privilégiée, conformément au RGPD.

Liste de contrôle[698] :

L'outil est basé sur une architecture reposant autant que possible sur les appareils des utilisateurs.

Les demandes faites par les applications au serveur central ne révèlent pas d'informations inutiles pour les besoins du service au système.

Afin d'éviter la réidentification par le serveur central, des serveurs proxy sont mis en œuvre. Le but de ces serveurs non collaboratifs est de mélanger les identifiants de plusieurs utilisateurs avant de les partager avec le serveur central, afin d'empêcher ce dernier de connaître les identifiants (tels que les adresses IP) des utilisateurs.

L'application et le serveur sont soigneusement développés et configurés afin de ne pas collecter de données inutiles (par exemple, aucun identifiant ne doit être inclus dans

694 Voir CJUE, Affaires jointes C92/09 -et C93/09-, Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, 9. novembre 2010.

695 Voir CJUE, affaire C524/06-, Heinz Huber c. Bundesrepublik Deutschland, 18 décembre 2008, para. 52.

696 Article 5(1)(c) du RGPD.

697 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

698 Cette liste de contrôle a été élaborée sur la base de celle qui figure dans les lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020, à l'adresse suivante : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

les journaux du serveur, etc.

6.3 Si l'utilisation de données anonymes n'est pas possible, utiliser le minimum de données personnelles et les pseudonymiser

Si l'anonymisation n'était pas possible, les responsables du traitement devraient au moins essayer de travailler avec des données pseudonymisées (voir la sous-section "Pseudonymisation" dans "Concepts principaux" de la partie II des présentes lignes directrices). En fin de compte, chaque responsable du traitement doit définir quelles données à caractère personnel sont réellement nécessaires (et lesquelles ne le sont pas) aux fins du traitement, y compris les périodes de conservation des données pertinentes. En effet, les responsables du traitement doivent garder à l'esprit que la nécessité du traitement doit être prouvée avant d'utiliser une quelconque base juridique issue de l'article 6 ou 9, paragraphe 2, du RGPD. Bien que le consentement puisse sembler être le seul fondement juridique qui n'exige pas de nécessité, il implique en fait la nécessité dans une certaine mesure, car un consentement valide aux fins du RGPD est donné pour une finalité spécifique, et le traitement doit être nécessaire par rapport à cette finalité, conformément à l'article 5, paragraphe 1, point c). En d'autres termes, les principes de minimisation des données, de limitation de la finalité et de licéité exigent des responsables du traitement qu'ils veillent à ce que les finalités recherchées par le dispositif ou le système ne puissent être atteintes sans utiliser des données moins personnelles de localisation ou de proximité, ou ces catégories de données avec un degré de détail moindre.

Dans la pratique, l'EDPB a considéré que ce principe signifie que "l'application ne doit pas collecter d'informations non liées ou non nécessaires, qui peuvent inclure l'état civil, les identifiants de communication, les éléments du répertoire de l'équipement, les messages, les journaux d'appels, les données de localisation, les identifiants des appareils, etc. Les données diffusées par les applications ne doivent comporter que des identifiants uniques et pseudonymes, générés par l'application et spécifiques à celle-ci. Ces identifiants doivent être renouvelés régulièrement, à une fréquence compatible avec l'objectif de contenir la propagation du virus, et suffisante pour limiter le risque d'identification et de suivi physique des personnes."[699]

En général, pour offrir des services de géolocalisation, la collecte et le traitement des identificateurs d'ensembles de services (SSID) ne sont pas nécessaires. Par conséquent, la collecte et le traitement des SSID sont excessifs aux fins de l'offre de services de géolocalisation basés sur la cartographie de l'emplacement des points d'accès WiFi.[700]

Encadré 6 : Application de recherche des contacts en cas de pandémie

Ce type d'application nous fournit quelques bons exemples de politiques de données qui respectent les règlements sur la protection des données. Voici quelques conseils utiles élaborés par l'ICO :

699 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

700 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. 16, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

- l'échange d'informations entre les appareils ne comprend pas de données personnelles telles que les informations sur les comptes ou les noms d'utilisateur ;
- les processus de correspondance ont lieu sur l'appareil et ne sont pas entrepris par l'hôte de l'application ou avec l'intervention d'un autre tiers ; et
- les informations requises pour la fonctionnalité de base des applications de recherche des contacts créées à l'aide de la FTC n'utilisent pas de données de localisation, que ce soit lors de l'échange entre les appareils, du téléchargement vers l'hôte de l'application ou des notifications ultérieures aux autres utilisateurs à partir de l'hôte de l'application.

Liste de contrôle[701] **:**

Conformément au principe de minimisation des données, l'application ne collecte pas de données autres que celles qui sont strictement nécessaires à ses finalités.

Lorsque cela est possible compte tenu de la finalité du traitement, les responsables du traitement donneront la préférence à l'utilisation de données anonymes. Si des données personnelles doivent être utilisées, les données pseudonymes prévaudront sur les données personnelles directes.

L'outil ne collecte que les données transmises par les instances de l'application ou des applications équivalentes interopérables. Aucune donnée relative à d'autres applications et/ou dispositifs de communication de proximité n'est collectée.

Les demandes faites par les applications au serveur central ne révèlent pas d'informations inutiles pour les besoins du service au système.

Les demandes faites par l'outil au serveur central ne révèlent pas d'informations inutiles sur l'utilisateur, à l'exception, éventuellement, et seulement si nécessaire, de ses identifiants pseudonymes et de sa liste de contacts.

L'utilisation de l'application ne permet pas aux utilisateurs d'apprendre quoi que ce soit sur les autres utilisateurs, si cela n'est pas strictement nécessaire.

Le serveur central ne tient pas à jour ni ne fait circuler une liste des identifiants pseudonymes des utilisateurs.

701 Cette liste de contrôle a été élaborée sur la base de celle qui figure dans les lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020, à l'adresse suivante : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

6.4 Questions juridiques : N'utiliser que le type de données strictement nécessaire

En général, les dispositifs ne doivent pas entrer en conflit avec la position de la personne concernée en tant que titulaire du droit à la vie privée. Cela signifie qu'en général, les utilisateurs doivent être protégés contre une privation inutile de leur vie privée. Ainsi, un utilisateur ne devrait pas avoir à prendre de mesures pour empêcher le suivi, car l'appareil devrait le fournir par défaut. Si l'outil peut fonctionner sans identification directe des personnes, des mesures appropriées doivent être mises en place pour empêcher la réidentification. En outre, les informations collectées doivent résider sur l'équipement terminal de l'utilisateur et seules les informations pertinentes doivent être collectées en cas d'absolue nécessité.[702] En général, les données ne doivent être traitées que si elles sont strictement nécessaires.

En outre, un développeur ne doit utiliser que le type de données strictement nécessaire à la finalité du traitement, et afin d'éviter l'utilisation de tout kit de développement logiciel (SDK) tiers collectant des données à d'autres fins. Par défaut, les développeurs doivent s'assurer que l'appareil n'envoie pas de données à des tiers sans en informer la personne concernée. Par exemple, aucun identifiant ne doit figurer dans les journaux du serveur. De même, les informations sur la proximité entre les utilisateurs de l'application doivent pouvoir être obtenues sans les localiser. Ce type d'application ne nécessite pas, et ne devrait donc pas impliquer, l'utilisation de données de localisation (directement ou par combinaison de données), mais uniquement de données de proximité. En revanche, si l'on souhaite connaître la géolocalisation concrète d'un individu, on ne devrait pas avoir accès aux données de proximité en combinant différents ensembles de données. Ainsi, le dispositif devrait être conçu pour éviter un tel scénario par défaut. De manière générale, l'outil ne devrait pas collecter de données supplémentaires qui ne sont pas strictement nécessaires à ses finalités, sauf à titre facultatif et dans le seul but d'aider à la prise de décision d'informer l'utilisateur. Par exemple, si certaines fonctionnalités de l'outil peuvent améliorer l'expérience de l'utilisateur, mais ne sont pas strictement nécessaires au bon fonctionnement de l'outil, par exemple la géolocalisation pour simplifier une recherche géographique, le participant doit pouvoir choisir d'utiliser ou non la géolocalisation pour simplifier la recherche géographique. Dans ces cas, le suivi plus invasif doit être désactivé par défaut, laissant à l'utilisateur la décision d'y adhérer.

Encadré 7. La question de la précision

En principe, les données à caractère personnel doivent être exactes. Toutefois, dans le cas des données de localisation ou de proximité, une précision excessive peut menacer la vie privée de la personne concernée ou de tiers. Par conséquent, le développeur de l'outil doit tenter de réduire la précision ou l'exactitude en ce qui concerne les données de localisation au niveau minimum nécessaire pour garantir qu'elles remplissent l'objectif pour lequel elles ont été conçues. Les données de localisation peuvent être très précises (comme la localisation d'un appareil à un coin

702 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adoptées le 21 avril 2020, p. 7. À l'adresse : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

de rue spécifique) ou plus imprécises (codes postaux, quadrants, une ville ou même un pays). Plus les données sont précises et exactes, plus elles ont tendance à être révélatrices, et plus le risque de ré-identification est grand.

Il est particulièrement important d'éviter, dans la mesure du possible, les lieux connus qui sont liés à l'identité d'une personne, tels que son domicile ou son lieu de travail. La raison en est que ces données contribuent souvent à l'identification du sujet.

En outre, certains lieux sont particulièrement sensibles en raison de ce qu'ils peuvent révéler sur le propriétaire de l'appareil, comme les hôpitaux, les écoles, les boîtes de nuit, les cliniques d'avortement, les dispensaires ou les organisations et événements politiques. Bien que ces lieux n'augmentent pas toujours les risques de réidentification, ils comportent des risques plus importants d'abus ou d'utilisations inattendues. Par conséquent, il est idéal d'éviter autant que possible l'exactitude dans l'utilisation des données faisant référence à ces lieux.

Liste de contrôle[703] **:**

L'outil ne collecte pas de données autres que celles strictement nécessaires à ses finalités, sauf à titre facultatif et dans le seul but d'aider à la prise de décision d'informer l'utilisateur.

Si l'outil est destiné à la recherche de contacts, il ne permet pas aux utilisateurs d'identifier les mouvements des autres utilisateurs.

En général, aucune donnée ne quitte l'équipement des utilisateurs si elle n'est pas strictement nécessaire.

La conception des dispositifs ou de l'outil tient compte des principes de protection de la vie privée dès la conception et vise à ne pas collecter plus de données que nécessaire.

Si la conception de l'appareil ou des outils permet plusieurs options concernant la collecte et le traitement ultérieur des données, la plus protectrice sera définie par défaut.

7 Minimiser les données

7.1 Description

La plupart des applications commerciales et de mission n'ont pas besoin de l'échelle la plus invasive de localisation disponible afin de fournir le niveau de service prévu. Les utilisateurs doivent se conformer aux pratiques qui respectent le principe de minimisation des données, à savoir n'utiliser que les données personnelles nécessaires,

703 Cette liste de contrôle a été élaborée sur la base de celle qui figure dans les lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020, à l'adresse suivante : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

adéquates, pertinentes et limitées à la finalité, y compris l'abstraction des données de localisation à l'échelle la moins invasive possible pour l'application.

7.2 Questions juridiques : Limitation de la finalité

Afin de minimiser l'intrusion dans la vie de la personne concernée, il est essentiel que le dispositif soit conçu de manière à bien préserver le principe de limitation de la finalité. Lorsqu'ils traitent des données de localisation ou de proximité, les destinataires ne doivent utiliser ces informations que pour la tâche pour laquelle elles leur ont été fournies. Ils doivent garder à l'esprit que les données qui ont été collectées à des fins "initiales" spécifiques ne doivent être traitées qu'à ces fins initiales, ou à des fins compatibles. Le traitement ultérieur des données est autorisé dans certaines circonstances en vertu du RGPD. Premièrement, lorsque le responsable du traitement recherche une autre base légale, et sous réserve du respect de toutes les autres exigences légales, telles qu'une information transparente et l'octroi des droits des utilisateurs. Deuxièmement, à certaines fins autorisées au préalable, comme la recherche scientifique ou l'archivage. Troisièmement, lorsque le traitement ultérieur a des finalités compatibles. Pour le cas général, le RGPD donne des critères pour déterminer la compatibilité des finalités, ce qui inclut le lien entre le traitement initial et le traitement ultérieur, la nature des données, les attentes de la personne concernée ou l'existence de garanties appropriées (voir art. 6(4) et voir la sous-section "Limitation des finalités" dans la section "Principes", dans la partie II des présentes lignes directrices).

Si vous envisagez d'offrir une plate-forme publicitaire et/ou un environnement de type boutique en ligne pour des applications qui seront en mesure de traiter les données personnelles résultant de (l'installation et de l'utilisation de) l'application de données géospatiales, indépendamment des fournisseurs d'applications, cela doit être soigneusement expliqué aux utilisateurs. Ceux-ci devraient donner leur consentement explicite à ces fins. Le refus d'un traitement inutile ne doit pas entraîner l'impossibilité d'utiliser l'appareil ou le système. En général, les murs de traçage, c'est-à-dire le type de système qui lie le service au consentement à l'utilisation des données, et qui ne sont pas nécessaires au fonctionnement de l'outil, doivent être soigneusement évités.

Si l'outil a été conçu pour travailler sur des données de proximité, il ne doit pas permettre au développeur ou à un tiers d'utiliser ces données pour tirer des conclusions sur la localisation des utilisateurs en fonction de leur interaction et/ou de tout autre moyen. Si l'outil a été conçu pour fonctionner sur des données de localisation, il ne doit pas permettre au développeur ou à un tiers de tirer des conclusions sur l'interaction des utilisateurs avec d'autres personnes.

Le responsable du traitement doit accorder une attention particulière aux finalités auxquelles la personne concernée ne s'attend pas, comme par exemple le profilage et/ou le ciblage comportemental. Si les finalités du traitement changent de manière significative au point d'être incompatibles avec le traitement initial, le responsable du traitement **doit rechercher** une nouvelle base légale valable, comme un **nouveau consentement spécifique.** Par exemple, si une entreprise a déclaré à l'origine qu'elle ne partagerait pas de données personnelles avec un tiers, mais qu'elle souhaite maintenant le faire, ce traitement ne passera probablement pas le test de compatibilité. Par conséquent, considérant que la meilleure base légale dans ce cas est le consentement des utilisateurs, le responsable du traitement doit demander le consentement préalable actif

de chaque client pour cette activité de traitement supplémentaire. L'absence de réponse (ou tout autre type de scénario d'exclusion) ne suffit pas. En outre, le responsable du traitement doit offrir une véritable possibilité de retirer le consentement à tout moment, ainsi que la possibilité d'exercer les droits des utilisateurs, tels que l'effacement des données ou la limitation du traitement.

Il est également important de faire la distinction entre le consentement à un service ponctuel et le consentement à un abonnement régulier. Par exemple, afin d'utiliser un service de géolocalisation particulier, il peut être nécessaire d'activer les services de géolocalisation dans l'appareil ou le navigateur. Si cette capacité de géolocalisation est activée, chaque site web peut lire les données de localisation de l'utilisateur de cet appareil mobile intelligent. **Afin de prévenir les risques de surveillance secrète, le groupe de travail Article 29 a estimé qu'il était essentiel que le dispositif prévienne en permanence que la géolocalisation est "activée", par exemple au moyen d'une icône visible en permanence.**[704] **Cela peut difficilement être considéré comme une exigence obligatoire pour le responsable du traitement, mais c'est certainement une bonne pratique qui doit être recommandée.**

Liste de contrôle[705] **:**

 Les responsables du traitement ont clairement identifié leur(s) finalité(s) de traitement, qui doivent être "spécifiques".

 Les responsables du traitement ont documenté ces finalités.

 Les responsables du traitement incluent les détails de leurs finalités dans les informations sur la vie privée des personnes, en veillant à ce que la personne concernée soit correctement informée, conformément à l'art. 12-14 du RGPD.

L'outil ne peut pas être détourné par inadvertance de son usage principal.

L'outil n'utilise pas de murs pour collecter des données inutiles

Si le responsable du traitement entreprend un traitement ultérieur de données à caractère personnel, un test de compatibilité a été effectué et documenté afin de respecter le principe de responsabilité. Ce test doit prendre en compte, au minimum, les facteurs énumérés à l'art. 6(4) du RGPD.

Si le responsable du traitement souhaite traiter ultérieurement les données pour une finalité autre que celle initialement obtenue et incompatible avec la finalité initiale, et dans le cas où le consentement est la base légale la plus adéquate, l'outil est conçu pour demander la permission aux utilisateurs. Dans tout autre cas, le responsable du traitement doit trouver la base légale la plus adéquate.

704 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.

705 Cette liste de contrôle a été construite sur la base de ces documents : EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopté le 21 avril 2020 ; ICO (no date) Principle (b) : purpose limitation. Bureau du commissaire à l'information, Wilmslow. Disponible à l'adresse suivante : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (consulté le 17 mai 2020).

Si l'outil a été conçu pour fonctionner sur des données de proximité, il ne peut pas être utilisé pour tirer des conclusions sur la localisation précise des utilisateurs en fonction de leur interaction et/ou de tout autre moyen.

Si l'outil a été conçu pour travailler sur des données de localisation, il ne peut pas être utilisé pour tirer des conclusions sur l'interaction des utilisateurs avec d'autres personnes ou pour faire des déductions sur d'autres catégories de données en fonction des lieux visités par la personne ou par tout autre moyen.

7.3 Ne pas conserver les données plus longtemps que nécessaire (limitation du stockage)

Les dispositifs doivent être programmés de manière à minimiser la durée de stockage des données : ils ne doivent conserver les données que pendant le temps strictement nécessaire pour atteindre leur objectif (voir "Limitation du stockage" dans "Principes", partie II des présentes lignes directrices). Bien entendu, cela dépendra probablement de l'objectif requis par l'application. Le stockage n'est acceptable que s'il est nécessaire pour atteindre l'objectif de l'outil. Par exemple, si une application est destinée à suivre une personne souffrant de la maladie d'Alzheimer, au cas où elle s'égarerait en raison des effets de la maladie, les données devront probablement être supprimées très souvent. Si l'on pense à un dispositif visant à aider les utilisateurs à savoir s'ils ont été proches d'une personne souffrant d'une maladie infectieuse, les données devront être conservées pendant des jours ou des semaines.

N'oubliez pas qu'un identifiant unique de dispositif (UDID) attribué de manière aléatoire, tel qu'un numéro unique, ne devrait être stocké qu'à des fins opérationnelles, pendant la durée nécessaire aux fins du traitement. "Après cette période, cet UDID devrait être anonymisé davantage, tout en tenant compte du fait qu'une véritable anonymisation est de plus en plus difficile à réaliser et que les données de localisation combinées peuvent encore conduire à une identification. Cet UDID ne devrait pas pouvoir être lié à des UDID antérieurs ou futurs attribués à l'appareil, ni à un quelconque identifiant fixe de l'utilisateur ou du téléphone (comme une adresse MAC, un numéro IMEI ou IMSI ou tout autre numéro de compte)."[706]

Liste de contrôle :

L'historique des contacts ou les données de localisation stockées sur le serveur central sont supprimés dès qu'ils ne sont plus nécessaires aux fins du traitement.

La procédure d'effacement des données est conçue de manière adéquate et le responsable du traitement et les utilisateurs en sont bien conscients.

Tout identifiant inclus dans l'historique local est supprimé après X jours de sa collecte (la valeur X étant définie par la finalité du traitement).

---

706 Avis 13/2011 du WP29 sur les services de géolocalisation sur les appareils mobiles intelligents, à l'adresse : https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf.

Les données contenues dans les journaux des serveurs sont réduites au minimum et sont conformes aux exigences en matière de protection des données.

S'il existe un serveur central et qu'il doit stocker des identifiants de données, ceux-ci doivent être supprimés une fois qu'ils sont distribués aux autres applications, sauf si une raison juridique/technique recommande le contraire.

8 Protéger la vie privée

8.1 Description

Le suivi des déplacements des personnes dans l'espace et dans le temps permet d'appréhender les aspects les plus intimes de leur vie. Dans les rares cas où les données de localisation agrégées et anonymisées ne répondent pas aux besoins spécifiques de l'entreprise ou de la mission, les données de localisation qui identifient les individus doivent être protégées et utilisées uniquement sur la base d'une raison légale qui autorise le traitement des données.

8.2 Introduire une politique de confidentialité adéquate

Le développeur doit toujours s'assurer que l'appareil/le système intègre une politique de confidentialité adéquate, conformément aux articles 12 et 13 du RGPD et aux exigences introduites par le règlement ePrivacy et le cadre juridique national. Celle-ci doit décrire comment l'outil collecte, utilise, conserve et divulgue les données personnelles. En outre, le dispositif doit inclure des informations sur les droits des personnes concernées de manière accessible[707] .

Les informations incluses doivent être expliquées dans un langage compréhensible, qui peut être compris par des personnes qui ne connaissent pratiquement rien aux systèmes TIC. Cet avis doit inclure, au minimum, tous les sujets énumérés aux art. 13-14 du RGPD, à savoir : des informations relatives (1) à la finalité du traitement, (2) aux données personnelles collectées, (3) à la manière dont les données collectées sont utilisées, (4) aux personnes avec lesquelles les données de localisation personnelles sont partagées, (5) à la manière dont les personnes concernées peuvent retirer leur consentement et accéder à leurs données de localisation personnelles ou les rectifier, (6) des informations sur les droits liés à la prise de décision automatisée, (7) les coordonnées du DPD correspondant, au cas où il devrait être contacté, (8) des informations sur les périodes de conservation, etc.[708] En outre, il est important de tenir les personnes concernées informées de toute modification du traitement de leurs données personnelles, qui doit être reflétée dans la politique de confidentialité. En outre,

707 Rapports techniques du JRC, Lignes directrices pour les administrations publiques sur la confidentialité de la localisation, à l'adresse suivante : https://publications.jrc.ec.europa.eu/repository/handle/JRC103110.

708 Rapports techniques du JRC, Lignes directrices pour les administrations publiques sur la confidentialité de la localisation, à l'adresse suivante : https://publications.jrc.ec.europa.eu/repository/handle/JRC103110.

le système doit être conçu de manière à ce que la personne concernée soit informée des changements (par des messages, des icônes, des alertes, etc.).

Outre les exigences d'information obligatoires mentionnées, les responsables du traitement sont encouragés à suivre les bonnes pratiques suivantes concernant la fourniture d'informations transparentes dans les projets qui impliquent le traitement de données de localisation ou de proximité. Ces pratiques ne sont pas obligatoires, bien sûr, mais elles sont fortement recommandées :[709]

- Quelles sont les utilisations concrètes qui seront faites des données recueillies ?
- Indiquez la fréquence et le détail de la collecte des données géospatiales ;
- Indiquez la nature et le type de données collectées ;
- Le cas échéant, rappelez aux personnes concernées qu'elles peuvent oublier qu'elles sont suivies et que le dispositif peut enregistrer leurs visites dans des lieux privés ou leur proximité avec des personnes concrètes (ce n'est pas obligatoire, mais cela peut être considéré comme une bonne pratique) ;
- Le cas échéant, rappelez aux participants que des preuves suggérant des activités illégales peuvent être mises au jour par les données géospatiales. Si c'est le cas, la divulgation peut ne pas être protégée par la politique de confidentialité de l'institution de recherche et pourrait être potentiellement découverte par les forces de l'ordre (voir l'article 10 du RGPD) ;
- Prévoir un moyen facile de rappeler aux personnes concernées qu'elles font l'objet d'un suivi. Par exemple, en activant une icône lorsque des données de localisation ou de proximité sont collectées et en désactivant cette icône lorsque les données ne sont pas collectées ;
- Fournir une déclaration expliquant que les personnes ne seront pas identifiées dans une publication ou une présentation de la recherche sans le consentement explicite du participant (à moins qu'une autre base juridique pour le traitement soit applicable) ;
- Fournir une déclaration expliquant que les données identifiables ne seront pas partagées avec des tiers sans le consentement du sujet, mais que les données dépersonnalisées peuvent être partagées ;
- Le cas échéant, rappelez et montrez aux personnes concernées comment elles peuvent désactiver ou interrompre temporairement la localisation ou la collecte de données de proximité quand elles le souhaitent ;
- Dresser une liste des destinataires qui auront accès aux données ;
- Évaluer le risque que les participants soient ré-identifiés à partir des données fournies ;
- Évaluer le risque de préjudice éventuel si les données étaient réidentifiées par inadvertance, y compris, le cas échéant, la perte financière, le préjudice psychologique et/ou le préjudice physique ;
- Informer les personnes concernées de leurs droits et de la manière de les faire valoir ;
- Fournir aux personnes concernées les coordonnées du DPD correspondant.

709 Goldenholz DM, Goldenholz SR, Krishnamurthy KB, et al. Using mobile location data in biomedical research while preserving privacy. *Journal of the American Medical Informatics Association*, ocy071, https://doi.org/10.1093/jamia/ocy071.

Il est recommandé d'opter pour des options de conception juridique qui peuvent rendre les politiques de confidentialité plus visuelles et plus faciles à comprendre. Par exemple, vous pouvez opter pour l'iconographie afin de respecter le devoir d'information du responsable du traitement des données, les vidéos, le storytelling, ou même un formatage simple comme l'utilisation de graphiques. Il est nécessaire de proposer aux participants un modèle d'"autogestion de la vie privée" où les participants ont facilement accès (via un lien ou un élément de menu) aux brèves coordonnées de l'entité. La page d'accueil de l'application est un excellent endroit pour afficher des informations pertinentes sur la vie privée, des informations de contact et fournir un hyperlien vers une "deuxième couche" d'informations plus détaillées sur la vie privée, conformément à l'article 12.7 du RGPD.

Si le traitement implique des tiers, une clause contractuelle avec les destinataires des données, qu'ils soient responsables du traitement ou sous-traitants, doit être signée. Cette clause peut stipuler que le destinataire s'abstient de tenter de ré-identifier les personnes concernées et que, en cas de ré-identification, ces données doivent être supprimées et le fait doit être notifié.

Liste de contrôle : [710]

Les responsables du traitement revoient régulièrement leurs traitements et, le cas échéant, mettent à jour leur documentation et les informations relatives à la vie privée des personnes.

Les utilisateurs sont informés de toutes les données personnelles qui seront collectées. Ces données ne sont collectées que si une base légale pour le traitement s'applique.

Les responsables du traitement expliquent comment les gens peuvent accéder aux détails des informations qui sont utilisées pour les services offerts par l'outil.

8.3 Protéger les droits des utilisateurs

Les personnes concernées peuvent invoquer de nombreux droits liés à leurs données, qui sont décrits en détail dans la section correspondante (voir "Droits des personnes concernées" dans la partie II des présentes lignes directrices). En général, les développeurs doivent faire de leur mieux pour concevoir le dispositif ou l'outil de manière à respecter les droits des utilisateurs et à les aider à les exercer. Cela peut se faire, par exemple, en mettant en place un moyen simple d'accéder aux données ou en développant des mesures techniques pour faciliter les droits de portabilité. Toutefois, des restrictions aux droits et obligations prévus dans la proposition de règlement sur la vie privée en ligne et/ou dans le RGPD sont possibles, lorsqu'elles constituent une mesure nécessaire, appropriée et proportionnée dans une société démocratique pour certaines finalités.[711] En général, les dispositifs utilisant des données de localisation et

710 Cette liste de contrôle a été construite sur la base de ces documents : EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopté le 21 avril 2020 ; ICO (no date) Principle (b) : purpose limitation. Bureau du commissaire à l'information, Wilmslow. Disponible à l'adresse suivante : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (consulté le 17 mai 2020).

711 Voir l'article 15 de la directive "vie privée et communications électroniques" et l'article 23 du RGPD.

de proximité devraient permettre à leurs utilisateurs d'obtenir un accès à leurs données dans un format lisible par l'homme et permettre la rectification et l'effacement sans collecter de données personnelles excessives.

Quelques conseils concrets pour faciliter la mise en œuvre des droits		
Droits	**Numéro**	**Conseil**
Droit d'accès	Les données sont souvent stockées sous une forme très diversifiée, ce qui rend leur accès difficile, surtout pour une personne concernée non qualifiée.	Fournir une fonctionnalité permettant d'afficher toutes les données relatives à une personne concernée. Si les données sont nombreuses, elles peuvent être réparties sur plusieurs écrans. Si les données sont trop volumineuses, offrez à la personne la possibilité de télécharger un fichier contenant toutes ses données. En ce qui concerne les données de localisation ou de proximité, les responsables du traitement peuvent permettre aux personnes concernées d'accéder aux informations dans des formats utilisables tels que des visualisations de cartes, dans le cas où elles utilisent déjà de tels formats.
Droit de rectification	Dans certains cas, les données collectées par le dispositif ne seront pas exactes. Les personnes concernées doivent pouvoir rectifier ces données.	Permettre la modification directe des données dans le compte de l'utilisateur (si applicable et/ou possible). Fournir des conseils sur les raisons pour lesquelles cela pourrait ne pas être conseillé dans certaines circonstances.
Droit à l'effacement	Les personnes concernées ont le droit de faire supprimer leurs données personnelles. Toutefois, ce droit peut être limité dans certaines circonstances spécifiques. En outre, les utilisateurs doivent être conscients des implications techniques d'un effacement général des données. Ainsi, les responsables du traitement doivent permettre aux personnes concernées d'effacer uniquement les données auxquelles le droit s'applique et présenter	Fournir une fonctionnalité permettant d'effacer toutes les données relatives à un individu auxquelles le droit à l'effacement s'applique (et uniquement ces données). En outre, prévoir une notification automatique aux responsables du traitement des données pour qu'ils effacent également ces données. Prévoir l'effacement de ces données dans les copies de sauvegarde, ou fournir une solution alternative qui ne restaure pas les données effacées relatives à cette personne. Introduire une fonctionnalité qui alerte toujours l'utilisateur sur les conséquences de l'effacement.

	certaines informations avant de les autoriser à procéder.	
Droit à la limitation du traitement	Il est souvent dans l'intérêt des personnes concernées que les données d'un type particulier ne soient pas traitées. L'outil doit être adapté à leurs préférences si les conditions de l'article 18 du RGPD s'appliquent.	Fournir une fonctionnalité qui permet à la personne concernée de s'opposer au traitement de données personnelles spécifiques. Lorsque les personnes concernées exercent leur droit d'opposition de cette manière, l'outil doit supprimer les données déjà collectées et ne doit plus collecter ultérieurement de telles données.
Droit à la portabilité des données	Les utilisateurs doivent être en mesure de recevoir les données à caractère personnel qu'ils ont fournies au responsable du traitement à partir de l'appareil sans avoir besoin de compétences techniques avancées. Ils ont également le droit de faire transférer leurs données à un autre responsable du traitement (c'est-à-dire au fournisseur d'un autre service). Remarque : cela n'inclut pas les données recueillies par d'autres moyens, comme des sources externes ou des processus d'analyse ou d'inférence.	Fournir une fonction permettant à la personne concernée de télécharger ses données dans un format standard lisible par une machine (CSV, XML, JSON, etc.).

Il est nécessaire de mentionner que le règlement "vie privée et communications électroniques" comprend des droits supplémentaires tels que la confidentialité des communications, l'identification de la ligne appelante, ou des droits visant spécifiquement les données de localisation autres que les données relatives au trafic (voir le chapitre III de la proposition). Les responsables du traitement doivent s'assurer que l'outil ne permet pas une violation de ces droits en introduisant des mesures destinées à limiter l'utilisation des données géospatiales si cela n'est pas essentiel pour le service. Par exemple, "que l'utilisateur final ait ou non empêché l'accès aux capacités GNSS (Global Navigation Satellite Systems) de l'équipement terminal ou à d'autres types de données de localisation basées sur l'équipement terminal par le biais des paramètres de l'équipement terminal, lorsqu'un appel est passé aux services d'urgence, ces paramètres ne peuvent pas empêcher l'accès à ces données de localisation GNSS pour déterminer et fournir la localisation de l'appelant de l'utilisateur final aux services d'urgence une organisation s'occupant des communications d'urgence, y compris les

centres de réception des appels de sécurité publique, dans le but de répondre à cet appel" (règlement "vie privée et communications électroniques", article 13.3). [712]

Liste de contrôle[713] **:**

Les utilisateurs peuvent exercer leurs droits via l'application.

Si l'outil a été conçu pour fonctionner sur des données de proximité, il ne peut pas être utilisé pour tirer des conclusions sur la localisation des utilisateurs en fonction de leur interaction et/ou de tout autre moyen.

Si l'outil a été conçu pour travailler sur des données de localisation, il ne peut pas être utilisé pour tirer des conclusions sur l'interaction des utilisateurs avec d'autres personnes.

Si les données sont utilisées à des fins compatibles, le responsable du traitement a effectué le test de compatibilité.

Si le responsable du traitement souhaite utiliser les données dans un but autre que celui initialement recherché, l'outil est conçu pour demander la permission aux utilisateurs.

9 Empêcher l'identification des personnes

9.1 Description

À mesure que les données de localisation mobile d'un individu sont situées dans un contexte géospatial de plus en plus large, leur anonymat s'effrite. Par conséquent, des mesures doivent être mises en place pour éviter que l'utilisation ultérieure des données ne permette d'identifier les personnes ou leur localisation.

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

713 Cette liste de contrôle a été élaborée sur la base des lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020.

9.2 Questions juridiques : utilisation de données anonymes au lieu de données personnelles

Voir la section "Questions juridiques : utilisation de données anonymes au lieu de données personnelles" dans cette partie IV.

9.3 Questions juridiques : Si l'utilisation de données anonymes n'est pas possible, utiliser la quantité minimale de données personnelles et les pseudonymiser.

Voir la section 7 "Si l'utilisation de données anonymes n'est pas possible, utiliser le minimum de données personnelles et les pseudonymiser" dans cette partie IV.

10 Assurer la responsabilité

10.1 Description

Les personnes représentées dans les données de localisation collectées, combinées et utilisées par les organisations, doivent pouvoir s'interroger sur la manière dont elles sont collectées et utilisées par rapport à elles et à leurs intérêts, et faire appel à ces utilisations proportionnellement aux niveaux de détail et au potentiel de nuisance.

10.2 Questions juridiques

Conformément à l'article 5, paragraphe 2, du RGPD, le responsable du traitement est responsable du respect de tous les principes du RGPD mentionnés à l'article 5, paragraphe 1, et doit être en mesure de le démontrer. Cela inclut le principe de responsabilité (voir "Principe de responsabilité" dans la partie II, section "Principes" des présentes lignes directrices).

Le principe de responsabilité du RGPD est fondé 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.[714] Le principe de responsabilité repose sur plusieurs obligations de conformité pour les responsables du traitement des données, notamment : des 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).

---

714 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.

Liste de contrôle[715] **:**

Le responsable du traitement a documenté la manière dont les effets indésirables du système ou de l'outil sont détectés, arrêtés et empêchés de se reproduire.

Le responsable du traitement a documenté toutes les mesures prises par l'organisation, ainsi que les garanties mises en œuvre, pour assurer la conformité avec le règlement sur la protection des données.

Si les données sont utilisées à des fins compatibles, le responsable du traitement a documenté de manière adéquate la réalisation du test de compatibilité.

Le responsable du traitement a documenté toutes les AIPD réalisées, les activités réalisées par le DPD correspondant et ses interactions avec les APD correspondantes (le cas échéant).

10.3 Assurer la transparence

La transparence est la clé de la responsabilité. On ne peut garantir la responsabilité que si les informations sur le fonctionnement du système ou du dispositif sont disponibles de manière transparente et appropriée. L'outil doit être conçu de manière à ce que la transparence et le contrôle par l'utilisateur puissent devenir une réalité[716] .

En outre, comme l'a déclaré l'EDPB, "afin de garantir leur loyauté, leur responsabilité et, plus largement, leur conformité à la loi, les outils TIC doivent être auditables et devraient être régulièrement examinés par des experts indépendants. Le code source de l'application doit être mis à la disposition du public pour permettre un examen aussi large que possible".[717] Cependant, cela pourrait entrer en conflit avec des considérations de propriété intellectuelle. En tout état de cause, les développeurs doivent veiller à ce que leurs appareils intègrent des fonctions permettant aux utilisateurs finaux d'être pleinement conscients du traitement qui sera réservé à leurs données.

Il faut veiller à ce que l'outil informe correctement les personnes concernées des informations dont il a besoin et des raisons pour lesquelles il en a besoin. La mise en place d'un "espace données personnelles" où elles peuvent être informées des données personnelles traitées, voire les modifier, les corriger ou les mettre à jour si nécessaire et le cas échéant, est fortement recommandée. Il est également conseillé d'établir une stratégie d'information appropriée. Il est conseillé dans tous les cas que l'information soit écrite en caractères qui ne sont pas excessivement petits afin que le participant puisse visualiser facilement l'information via l'écran d'un smartphone. Il faut essayer

715 Cette liste de contrôle a été élaborée sur la base des lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020.

716 CEPD. Avis 7/2015. Relever les défis du big data. Un appel à la transparence, au contrôle des utilisateurs, aux données,
la protection par la conception et la responsabilité. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

717 EDPB, Lignes directrices 04/2020 sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19 Adopté le 21 avril 2020

d'éviter que le participant ne commence à utiliser l'outil sans avoir lu et compris ce qui sera fait avec ses données. Enfin, il est recommandé d'opter pour des options de conception juridique qui peuvent rendre la politique de confidentialité plus visuelle et plus facile à comprendre. (Voir la section "Transparence" dans "Principe de licéité, de loyauté et de transparence" dans la partie II, section "Principes" des présentes lignes directrices).

Liste de contrôle[718] **:**

Le code source de l'application et de son backend est ouvert, et les spécifications techniques ont été rendues publiques, afin que toute partie concernée puisse auditer le code et, le cas échéant, contribuer à l'améliorer, à corriger les éventuels bugs et à assurer la transparence du traitement des données personnelles.

10.4 Évaluation des risques et AIPD

Voir la sous-section "Intégrité et confidentialité" de la section "Principes" de la partie II des présentes lignes directrices du présent document.

10.5 Diligence raisonnable du sous-traitant

Le principe de responsabilité (voir "Principe de responsabilité" dans la partie II section "Principes" des présentes lignes directrices) est également présent lorsqu'un responsable du traitement choisit de faire appel aux services d'un sous-traitant. À cet égard, l'article 28, paragraphe 1, du RGPD[719] exige que les responsables du traitement prennent certaines mesures de diligence raisonnable, avant de donner aux sous-traitants l'accès à des données à caractère personnel pour l'exécution d'activités de traitement des données. Comme pour les autres dispositions du RGPD, il n'est pas précisé quelles actions spécifiques un responsable du traitement doit mener lors de l'évaluation des sous-traitants. Le seul critère fourni par le RGPD est que les **responsables du traitement doivent juger les sous-traitants sur la base de leur capacité à démontrer qu'ils peuvent effectuer des activités de traitement en conformité avec le RGPD.**

Les responsables du traitement doivent toujours garder à l'esprit que le développement d'outils de localisation implique souvent l'utilisation de différents ensembles de données. Les registres doivent garantir la traçabilité du traitement, les informations sur la réutilisation éventuelle des données et l'utilisation de données appartenant à des ensembles de données différents dans les mêmes, ou différentes, étapes du cycle de vie.

718 Cette liste de contrôle a été élaborée sur la base des lignes directrices 04/2020 de l'EDPB sur l'utilisation des données de localisation et des outils de recherche des contacts dans le contexte de l'épidémie de COVID-19, adoptées le 21 avril 2020.

719 "Article 28 Sous-traitant 1. "Lorsque le traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci ne fait appel qu'à des sous-traitants présentant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de telle sorte que le traitement réponde aux exigences du présent règlement et assure la protection des droits de la personne concernée."

Si les responsables du traitement mènent un développement qui nécessite de compter sur un tiers pour certaines activités de traitement, ils doivent se poser deux questions : (1) quel type de comportement est attendu pour démontrer le respect de cette obligation ; et (2), si une certaine forme d'action positive est attendue, comment les responsables du traitement doivent-ils procéder pour mener à bien cette diligence raisonnable ?

Pour la première question, le RGPD indique que si les responsables du traitement entendent rester en conformité avec le RGPD, ils ne peuvent retenir qu'un sous-traitant capable de démontrer sa conformité avec le RGPD. Par conséquent, les responsables du traitement doivent demander des informations pour l'évaluer. En d'autres termes, le RGPD attend des responsables du traitement qu'ils interrogent activement leur sous-traitant potentiel à ce sujet ; il ne suffit pas de s'appuyer sur une clause de déclaration et de garantie dans l'accord de traitement des données (voir "Intégrité et confidentialité" dans la section "Principes" de la partie II des présentes lignes directrices). Pour s'en assurer, les responsables du traitement peuvent envoyer des questionnaires à tous les sous-traitants ou demander à ces derniers de prouver qu'ils ont passé un audit externe. En outre, les responsables du traitement peuvent ajouter une clause contractuelle d'audit permettant au responsable du traitement de procéder lui-même à un audit d'un sous-traitant si des preuves supplémentaires sont nécessaires.

Quant à la manière dont les responsables du traitement doivent effectuer cette diligence raisonnable, là encore le RGPD ne fournit pas de points concrets à analyser. Néanmoins, certaines autorités de contrôle nationales ont proposé des sujets à prendre en compte, comme le fait de savoir si le sous-traitant suit les normes du secteur, de demander la fourniture d'informations tant juridiques que techniques sur la manière dont le sous-traitant traite les données à caractère personnel, s'il adhère à un code de conduite ou s'il a suivi un programme de certification. [720]

Outre ces considérations générales, et selon la manière dont le traitement demandé par ce tiers s'intègre dans le cadre de l'outil développé, d'autres questions doivent être posées. A cet égard, **toute question que les responsables du traitement se poseraient lors du développement de l'outil devrait être posée au sous-traitant.** Nous nous en remettons aux questions posées dans la liste de contrôle incluse dans l'encadré ci-dessous pour plus d'indications.

Liste de contrôle : diligence raisonnable du sous-traitant

Si le traitement implique un transfert international de données, les responsables du traitement ont obtenu des informations concernant le lieu où les activités de traitement des données auront lieu et (1) ont procédé à l'examen de la jurisprudence suggéré au point ci-dessous ; et (2) ont évalué si les juridictions, dans le cas de pays non membres de l'UE, sont considérées comme adéquates par la Commission européenne.

720 ICO (aucune date) Guide du Règlement général sur la protection des données (RGPD), Quelles sont les responsabilités et les obligations des responsables du traitement lorsqu'ils font appel à un sous-traitant ? Information Commissioner's Office, Wilmslow. Disponible à l'adresse : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/ (consulté le 20 mai 2020).

Les responsables du traitement ont examiné la jurisprudence des autorités de contrôle nationales où le sous-traitant opère afin de vérifier les sanctions potentielles.

Les responsables du traitement ont exigé la preuve de l'adhésion à un code de conduite ou à une certification (ceci n'est pas strictement nécessaire mais peut être considéré comme une bonne pratique).

Les responsables du traitement ont exigé la preuve d'une certification ISO pertinente (ceci n'est pas strictement nécessaire mais peut être considéré comme une bonne pratique).

Si un sous-traitant est impliqué, les responsables du traitement doivent obtenir une copie des registres des activités de traitement.

Les responsables du traitement se sont enquis du processus de développement de l'outil, en particulier du type de données utilisées pour la formation de l'outil et des données dont il a besoin pour fonctionner et fournir un résultat utile.

10.6 **Délégués à la protection des données (DPD)**

Les DPD jouent un rôle crucial lors de la conception et de la mise en œuvre des activités de traitement des données dans le respect du RGPD. Ils constituent une autre garantie que le RGPD rend obligatoire à certaines occasions et, en général, il est recommandé de nommer une telle personnalité. Le groupe de travail Article 29 considère qu'il s'agit "d'une pierre angulaire de la responsabilité et que la nomination d'un DPD peut faciliter la conformité".[721]

L'article 37, paragraphe 1, du RGPD [722] indique quand les responsables du traitement et les sous-traitants doivent désigner un DPD. Dans le cas des dispositifs et systèmes de localisation et de proximité**, la désignation d'un DPD sera très probablement nécessaire, car la plupart d'entre eux traitent des données à caractère personnel d'une manière qui peut nécessiter un suivi régulier des personnes concernées à grande échelle, ou qui peut être effectué par les autorités publiques**.

Il serait utile que la réglementation de chaque État membre relative à la nécessité de désigner un DPD élargisse la liste des activités qui exigent la désignation d'un DPD ou, au moins, fournisse des exemples clairs qui pourraient aider à interpréter quelles activités de traitement des données effectuées par les responsables du traitement et les sous-traitants exigent une telle désignation.

---

721 Groupe de travail Article 29 (2017) Lignes directrices sur les délégués à la protection des données ("DPD"), p.4. Commission européenne, Bruxelles.

722 Article 37. Désignation du délégué à la protection des données. 1. Le responsable du traitement et le sous-traitant désignent un délégué à la protection des données dans tous les cas où : (a) le traitement est effectué par une autorité ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leurs fonctions juridictionnelles ; b) les activités principales du responsable du traitement ou du sous-traitant consistent en des traitements 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 ; ou c) les activités principales du responsable du traitement ou du sous-traitant consistent en des traitements à grande échelle de catégories particulières de données conformément à l'article 9 et de données à caractère personnel relatives aux condamnations pénales et aux infractions visées à l'article 10.

Si un DPD doit être désigné, pour l'une des raisons mentionnées ci-dessus, il est nécessaire d'avoir sa participation dès le début du projet, comme la rédaction d'une AIPD (requise par l'article 39, paragraphe 1, point c)) ainsi que toute autre question liée à la protection des données au sein de l'entité (comme prescrit par l'article 39, paragraphe 1, point a)). Cela peut inclure l'examen d'un sous-traitant potentiel, comme décrit dans le point précédent.

Liste de contrôle : DPD

Les responsables du traitement ont vérifié si l'institution a déjà nommé un DPD.

Si ce n'est pas le cas, ils ont vérifié auprès du service juridique si les activités de traitement des données envisagées nécessitent la désignation d'un DPD, en examinant les interprétations européennes faisant autorité, les réglementations locales, les interprétations locales faisant autorité et la jurisprudence nationale et européenne pertinente.

Les responsables du traitement ont exigé la nomination d'un DPD si nécessaire, et son implication dans le processus de développement de l'outil si nécessaire.

En règle générale, le DPD doit être informé de chaque démarche entreprise afin de pouvoir intervenir s'il le juge utile.