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.

RÉSEAUX SOCIAUX

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.

Les réseaux sociaux à des fins de recherche : exigences éthiques et légales en matière de protection des données

Jose Antonio Castillo Parrilla et Iñigo de Miguel Beriain (UPV/EHU)

Les versions préliminaires de ce document ont été revues par le Dr Denise Amram, DPD, chercheur affilié au LIDER Lab - Institut DIRPOLIS, Scuola Superiore Sant'Anna (Italie) et DPD *de droit privé comparé à la Scuola Superiore Sant'Anna et le Prof. Giovanni Comandé, Dirpolis, Sant'Anna School of Advanced Studies, Pise, Italie.*

Cette partie des lignes directrices a été validée par Iñaki Pariente, ancien directeur de l'Agence basque de protection des données.

Les médias sociaux peuvent être décrits comme des plateformes en ligne qui permettent le développement de réseaux et de communautés d'utilisateurs, parmi lesquels des informations et du contenu sont partagés. Les fonctions supplémentaires des réseaux sociaux sont la personnalisation, l'analyse et la publication (principalement via des services de ciblage), ce qui permet soit des initiatives indépendantes, soit des offres de services plus larges. Les médias sociaux permettent aux individus de se créer des comptes afin d'interagir avec d'autres utilisateurs et de développer et élargir les connexions et les réseaux. Les utilisateurs partagent des données avec les administrateurs du réseau et avec d'autres utilisateurs à des fins totalement différentes. Le contenu partagé par les individus peut être créé par eux-mêmes (contenu généré par l'utilisateur) ou non. [723]

D'autre part, il est important de mentionner que l'objectif principal des données placées dans un réseau social est de permettre aux gens d'interagir, d'entrer en relation. En fait, les utilisateurs établissent deux types de relations : une relation verticale avec l'entreprise propriétaire du réseau, et une relation horizontale avec d'autres personnes avec lesquelles ils souhaitent interagir. Cette relation peut être générale (profils ouverts) ou particulière (profils à accès limité). Selon le type d'interaction en jeu, le statut juridique du traitement des données sera probablement différent.

En général, les réseaux sociaux sont optimaux pour les **pratiques d'extraction massive de données**. En effet, il existe des outils logiciels capables de collecter automatiquement les données des internautes à partir des espaces publics en ligne. En outre, la plupart des réseaux sociaux proposent des interfaces de programmation

[723] Lignes directrices EDPB 8/2020 sur le ciblage des utilisateurs de médias sociaux, p. 3.

d'applications, ou API[724] , qui simplifient le développement et l'innovation logiciels et permettent aux applications d'échanger des données et des fonctionnalités facilement et en toute sécurité. Ces circonstances rendent les réseaux sociaux particulièrement attrayants pour certains types de recherche, mais elles créent également des défis exigeants en termes de protection des données.

Cette partie des lignes directrices vise à aider les chercheurs ou les **innovateurs dans le** domaine des TIC **qui utilisent des données personnelles obtenues à partir de réseaux sociaux.** Il convient de mentionner que nous n'aborderons pas ici l'utilisation des réseaux sociaux pour collecter des données (comme, par exemple, en utilisant les enquêtes Google pour obtenir des données sur une série de questions précises auprès de personnes réelles). Cela est dû à une raison simple : dans ces cas, les données elles-mêmes ne proviennent pas d'un réseau social mais à travers un réseau social. En effet, les réseaux sociaux ne servent que d'outil pour recueillir ces données. Par conséquent, ces données ne sont pas si différentes des autres données collectées de manière plus traditionnelle (comme une enquête sur papier) et ne méritent donc pas une attention particulière ici.

Si les développeurs de TIC qui consultent ces lignes directrices prévoient d'utiliser des outils d'IA pour traiter les données obtenues à partir de ces réseaux, ils devraient consulter la partie des lignes directrices consacrée à l'intelligence artificielle (IA). S'ils prévoient de les utiliser à des fins liées à la biométrie, à l'internet des objets ou à la localisation géospatiale, ils doivent consulter les parties des présentes lignes directrices consacrées à ces questions. Afin d'éviter des répétitions inutiles, nous laissons ces questions en dehors de cette analyse.

CLAUSE DE NON-RESPONSABILITÉ

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

[724] Voir, sur les API : Oscar Borgogno & Giuseppe Colangelo, Data Sharing and Interoperability Through APIs : Insights from European Regulatory Strategy, Stanford-Vienna European Union Law Working Paper n° 38, http://ttlf.stanford.edu ; Russell, N. Cameron et Schaub, Florian et McDonald, Allison et Sierra-Pambley, William, APIs and Your Privacy (5 février 2019). Disponible à l'adresse SSRN : https://ssrn.com/abstract=3328825 ou http://dx.doi.org/10.2139/ssrn.3328825

1 Introduction aux réseaux sociaux et aux questions de protection des données

Quelques conseils préliminaires : il est absolument nécessaire de garder à l'esprit **que le fait qu'une grande partie des données contenues dans un réseau social soit facilement appréhendable ne légitime pas leur traitement.** Il s'agit d'un aspect crucial lorsqu'il s'agit du traitement de données obtenues à partir de réseaux sociaux : les chercheurs et les innovateurs en TIC doivent s'assurer avec soin qu'ils disposent d'une base juridique leur permettant d'accéder à ces données et de les stocker. Une fois qu'ils y ont accédé, ils devront s'assurer que la même base et/ou d'autres bases de légitimité leur permettent de poursuivre le traitement de ces données. En général, cela signifie qu'ils doivent avoir une connaissance approfondie des politiques de développement imposées par les réseaux sociaux (voir "Licéité, loyauté et transparence" dans la section "Principes" de la partie II des présentes lignes directrices pour de plus amples informations à ce sujet).

En outre, la transparence implique que les personnes visées par la recherche soient informées à un moment donné de la recherche en cours, du type de données personnelles que les responsables du traitement collectent et de la manière dont elles seront utilisées. Certains services précisent clairement que cela doit être fait avant de commencer la collecte. En l'absence d'une politique spécifique et lorsque les chercheurs/innovateurs mènent des recherches par observation auxquelles la nécessité d'obtenir un consentement préalable pourrait nuire, ils devraient en informer les personnes concernées dès que possible. Les chercheurs/innovateurs en TIC devraient toujours retirer de leur moissonnage les individus qui ne consentent pas à être inclus.

1.1 Concepts principaux

L'imprécision des données recueillies par les réseaux sociaux, ainsi que les règles juridiques en matière de protection des données personnelles, suggèrent aux gestionnaires des réseaux sociaux, et à ceux qui utilisent les données recueillies sur ces réseaux à des fins de recherche, de prendre en compte, plutôt que la catégorie du réseau social, à **la fois le type de données traitées et les principaux critères suivants :**

- la finalité pour laquelle ils utilisent les données ;

- la réglementation applicable, et notamment les conflits réglementaires pouvant résulter de leur activité et les finalités initiales de la collecte des données personnelles dans les réseaux sociaux.

Un réseau social est un **service de la société de l'information.** Le concept de service de la société de l'information est mentionné à l'article 2.a et aux considérants 17 et 18 de la directive CE 2000/31, ainsi qu'à l'article 4 (25) du RGPD. Ils font tous référence à l'article 1.1.b de la directive européenne 2015/1535. Un service de la société de l'information est tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

Les opérateurs d'un réseau social ont le double statut de fournisseur de services sociaux et de responsable du traitement des données, selon leur politique de confidentialité, qui les considère comme tels.[725] En tant que prestataires de services sociaux, ils sont soumis à la responsabilité des articles 12 à 15 de la directive 2000/31/CE. En tant que responsables du traitement des données, ils doivent à la fois s'assurer que les données sont traitées conformément à l'article 5 du RGPD et être en mesure de le démontrer (article 5.2 du RGPD). Ceux qui utilisent le réseau social à des fins qui dépassent le statut de simple utilisateur (par exemple, l'utilisation des réseaux sociaux à des fins de recherche) sont **également considérés comme responsables du traitement des données, et sont responsables en conséquence. Toutefois, il est également vrai qu'en cas de contrôle conjoint,** les responsables du traitement peuvent être impliqués à différentes étapes du traitement des données à caractère personnel et à différents degrés. Dans un tel scénario, le niveau de responsabilité de chacun d'eux doit être évalué au regard de toutes les circonstances pertinentes du cas particulier.[726]

1.2 Défis

L'utilisation des données recueillies par les réseaux sociaux soulève, en soi, certains **défis** liés au traitement des données qu'il convient de prendre en compte. Ces défis peuvent être encore plus particuliers lorsque la finalité du traitement est liée à la recherche. Les principaux enjeux liés à l'utilisation des données collectées par les réseaux sociaux à des fins de recherche sont les suivants :

- Les réseaux sociaux favorisent et renforcent la réutilisation constante des données, ce qui présente des risques liés à

- l'application de principes tels que la limitation de la finalité (art. 5.1.b), la limitation de la durée de conservation (art. 5.1.e), l'intégrité et la confidentialité (art. 5.1.f) ; etc.

- ou le statut juridique des profils personnels et autres données dérivées, en particulier s'ils restent des données personnelles et s'ils sont également des œuvres de propriété intellectuelle (PI) (la question de savoir si les données personnelles déduites sont des données personnelles ou simplement la PI de leurs producteurs).

- Le choix et l'utilisation correcte d'une base juridique pour la collecte de données auprès des réseaux sociaux, ce qui nécessite une compréhension adéquate et le respect des exigences de leurs politiques de développement.

- Le choix d'une base juridique pour la réutilisation des données obtenues par les réseaux sociaux et l'utilisation adéquate de ces données en fonction de la base choisie :

- Le consentement (et la possibilité d'obtenir un "consentement altruiste", notamment à la lumière de la proposition de loi sur la gouvernance des données).

---

[725] Afin de clarifier les rôles et responsabilités respectifs des fournisseurs et des cibleurs de médias sociaux, il est important de tenir compte des lignes directrices de l'EDPB (Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux Version 2.0 adoptée le 13 avril 2021, à l'adresse : https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11) et de la jurisprudence pertinente de la CJUE. Les arrêts rendus dans les affaires Wirtschaftsakademie (C-210/16), Témoins de Jéhovah (C-25/17) et Fashion ID (C-40/17) sont particulièrement pertinents ici.

[726] Voir : 4 Arrêt Wirtschaftsakademie, C-210/16, point 43 ; arrêt Témoins de Jéhovah, C-25/17, point 66 et arrêt Fashion ID, C-40/17, point 70.

- Intérêt légitime

- Intérêt public

- Exception de recherche

- L'identification des risques découlant de la recherche sur les données des médias sociaux, parmi lesquels on peut citer les suivants :

- atteinte à la vie privée des personnes par l'analyse massive de données personnelles ou non personnelles (vie privée collective), par exemple en raison de l'identification (ou de la ré-identification) des personnes concernées par le biais de profils personnels (il s'agit clairement d'un risque extrêmement élevé en raison de l'intention de promouvoir l'analyse massive de données qui pourrait conduire au profilage) ;

- ou l'atteinte à l'honneur, à la vie privée ou à l'image d'individus ou de groupes, par exemple en publiant des données brutes sans passer par un processus correct d'agrégation ou de pseudonymisation.

- La nature expansive des données à caractère personnel, qui fait qu'il est conseillé de supposer par défaut que des données à caractère personnel sont traitées, même si, à première vue, cela ne semble pas être le cas.[727]

- Bien qu'en de nombreuses occasions, et de plus en plus, la recherche à travers les réseaux sociaux naisse en tant que recherche, il est également fréquent que les profils de réseaux sociaux du chercheur n'aient pas cette finalité initiale et ne l'acquièrent qu'après un certain temps.

-L'hypothèse commune selon laquelle les données rendues publiques par les médias sociaux peuvent être utilisées librement. **Cette hypothèse est manifestement fausse, à moins que les données ne soient effectivement publiées dans des profils entièrement publics ("manifestement rendus publics par la personne concernée") et doit être soigneusement évitée.**

- Enfin, l'opacité des algorithmes de traitement des données peut avoir un impact négatif sur les utilisateurs et décourager la recherche (voir la partie III sur l'IA des présentes lignes directrices).

1.3 Types de données qui peuvent être collectées par les réseaux sociaux

Les réseaux sociaux peuvent fournir aux chercheurs trois types de données différents : les données fournies, les données observées et les données inférées/dérivées (ou une

[727] Le projet "Historic Graves" est un projet de patrimoine communautaire de base. Des groupes communautaires locaux sont formés à l'étude sur le terrain des cimetières historiques à l'aide de technologies de pointe peu coûteuses et à l'enregistrement de leur propre histoire orale. Ils constituent un dossier multimédia en ligne sur les tombes historiques de leur région et s'unissent pour former une ressource nationale. Puisqu'il s'agit d'un projet qui recueille des données sur les cimetières, on pourrait penser qu'il s'agit de données sur les personnes décédées et que le RGPD ne s'applique donc pas (considérant 27). Cependant, les données sur les cimetières et les tombes sont fournies par les proches des défunts, qui ne sont évidemment pas décédés, et en fournissant les données de leurs proches décédés, ils fournissent également leurs propres données personnelles.

combinaison de toutes ces données). Ces types de données pourraient être définis de la manière suivante :[728]

- "Les données fournies" font référence aux informations fournies activement par la personne concernée au fournisseur de médias sociaux et/ou au responsable du traitement. Par exemple : les utilisateurs de médias sociaux peuvent indiquer leur âge dans la description de leur profil. Dans les présentes lignes directrices, nous n'aborderons pas le traitement de ces données, car elles ne diffèrent pas des autres données recueillies par un fournisseur de services.
- "Les données observées" désignent les données fournies par la personne concernée en vertu de l'utilisation d'un service ou d'un dispositif. Il s'agit notamment de :
    - les données d'un utilisateur de médias sociaux particulier peuvent être recueillies sur la base de l'activité sur la plateforme de médias sociaux elle-même (par exemple le contenu que l'utilisateur a partagé, consulté ou aimé) ;
    - des données relatives à l'utilisation des appareils sur lesquels l'application du média social est exécutée (par exemple, coordonnées GPS, numéro de téléphone mobile) ;
    - les données obtenues par un développeur d'applications tiers en utilisant les interfaces de programmation d'applications (API) ou les kits de développement de logiciels (SDK) proposés par les fournisseurs de médias sociaux ;
    - les données collectées par l'intermédiaire de sites web de tiers qui ont incorporé des plugins sociaux ou des pixels ;
    - des données collectées par des tiers (par exemple, des parties avec lesquelles la personne concernée a interagi, acheté un produit, souscrit à des cartes de fidélité) ; ou
    - les données collectées par le biais de services proposés par des sociétés détenues ou exploitées par le fournisseur de médias sociaux.
- "Les données inférées" et "les données dérivées" sont celles créées par le responsable du traitement sur la base des données fournies par la personne concernée ou telles qu'observées par le responsable du traitement. Elles peuvent être dérivées par des calculs déterministes ou déduites de manière probabiliste. Par exemple, un fournisseur de médias sociaux pourrait déduire que des personnes sont susceptibles d'être intéressées par une certaine activité ou un certain produit sur la base de leur comportement de navigation sur le web et/ou de leurs connexions réseau.

La manière d'obtenir les données n'est pas pertinente pour les qualifier de données personnelles ou non personnelles, ni pour décider si elles appartiennent à des catégories particulières de données conformément à l'art. 9 du RGPD. Toutefois, **elle peut avoir des conséquences importantes à d'autres égards.** Par exemple, lorsqu'il s'agit de déterminer si les personnes concernées pouvaient prévoir, ou non, un traitement

[728] Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux Version 2.0 Adoptées le 13 avril 2021, à l'adresse : https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

particulier, ou lorsqu'il s'agit de déterminer les limites de leur droit à la portabilité ou les informations à leur fournir. Il faut garder à l'esprit que dans le cas de données observées, déduites ou dérivées, les utilisateurs ne sont généralement pas conscients que des données sont collectées ou générées.

Encadré 1 : Déduire des données. Exemples

Exemple 1

"La société X a développé une application qui, en analysant les données brutes des signaux d'électrocardiogramme générés par des capteurs commerciaux couramment disponibles pour les consommateurs, est capable de détecter des schémas de dépendance aux drogues. Le moteur de l'application peut extraire des caractéristiques spécifiques des données brutes de l'ECG qui, selon les résultats d'enquêtes précédentes, sont liées à la consommation de drogues. Le produit, compatible avec la plupart des capteurs du marché, peut être utilisé comme une application autonome ou par le biais d'une interface web nécessitant le téléchargement des données. Le consentement explicite de l'utilisateur doit être recueilli pour traiter les données à cette fin. Le respect de cette exigence de consentement peut être satisfait dans les mêmes conditions et au même moment que lorsque le consentement est recueilli auprès de la personne concernée en vertu de l'article 7, point a)."

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

Exemple 2

Les données Fitbit pourraient être utiles aux employeurs potentiels, qui pourraient en déduire que "l'impulsivité et l'incapacité à retarder la satisfaction - qui peuvent toutes deux être déduites des habitudes d'exercice d'une personne - sont liées à l'abus d'alcool et de drogues, aux troubles du comportement alimentaire, au tabagisme, à une dette de carte de crédit plus élevée et à des scores de crédit plus faibles. Le manque de sommeil - que le Fitbit permet de suivre - a été associé à un mauvais bien-être psychologique, à des problèmes de santé, à de mauvaises performances cognitives et à des émotions négatives telles que la colère, la dépression, la tristesse et la peur."

Source : Peppet, Scott R 'Regulating the Internet of Things : First Steps toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Tex. L. Rev. 85.

Il faut considérer que la déduction de données relatives à la santé est un traitement particulièrement sensible puisque ces données (qu'elles soient déduites ou non) sont des données de catégories spéciales.

1.4 Catégories de données collectées par les médias sociaux

En principe, il est parfaitement possible de recueillir **différents types de données par le biais des médias sociaux. En effet, il peut s'agir de données personnelles et non personnelles.** La compréhension des données comme étant non personnelles est d'une grande importance au niveau juridique et, évidemment, pour la préparation de ces lignes directrices, dans la mesure où le RGPD ne serait pas applicable, mais le règlement de l'UE 2018/1807 le serait. Dans la pratique, cette division entre ces deux types de données s'estompe en raison de l'utilisation croissante des technologies d'analyse des données, permettant une plus grande capacité de traitement des données et l'extrapolation des résultats (group privacy). Cette situation brouille la ligne de démarcation entre les données personnelles et non personnelles dans la mesure où, par exemple, les profils deviennent de plus en plus précis même s'ils ne sont pas liés à une personne spécifique et ne sont donc pas des données à caractère personnel.

La limite pour considérer une donnée comme étant une donnée à caractère personnel réside dans sa capacité à identifier directement ou indirectement une personne, et, en particulier, si les coûts et le temps nécessaires à cette identification ne sont pas excessifs[729] . Cependant, une telle classification n'est pas si facile à appliquer en pratique. Pour commencer, certaines données qui semblent anonymes à première vue peuvent être désanonymisées[730] (voir les sous-sections "Identification", "Pseudonymisation" et "Anonymisation" dans la section "Concepts principaux" de la partie II des présentes lignes directrices). En outre, les données à caractère personnel en tant que concept juridique jouissent d'une sorte de nature expansive dans la mesure où l'hyperproduction de données et la capacité de les traiter et de les analyser ne cessent de croître, réduisant ainsi les coûts et le temps nécessaires pour identifier une personne à partir d'un ensemble donné de données (personnelles ou non)[731] .

En gardant tout cela à l'esprit, on doit conclure que, **dans le cas des réseaux sociaux, le traitement des données personnelles est généralement la règle.** Cela est particulièrement vrai si l'on considère que, dans ce contexte, il est courant que les utilisateurs se connectent avec un ensemble de données personnelles. Il est tout à fait possible que (1) la plupart de ces données ne soient pas strictement nécessaires à la connexion et ne respectent donc pas le principe de minimisation des données (article 5.1.c du RGPD) ou que (2) les données soient utilisées à des fins qui vont au-delà de la simple connexion, violant dans ce cas le principe de limitation de la finalité

---

[729] Voir Consid. 26 du RGPD : " Pour déterminer si une personne physique est identifiable, il convient de tenir compte de tous les moyens raisonnablement susceptibles d'être utilisés ".

[730] Voir Consid. 26 du RGPD : " Les données à caractère personnel ayant fait l'objet d'une pseudonymisation, qui pourraient être attribuées à une personne physique par l'utilisation d'informations supplémentaires, devraient être considérées comme des informations sur une personne physique identifiable. "

[731] Voir : en général G. Comandé (Editor) Encyclopedia of Data Science and Law Edwards Eldgar, 2021 ; à paraître ; G. Comandé - G. Malgieri, *" Sensitive-by-distance : les données de quasi-santé à l'ère algorithmique " (2017)*, in *Information & Communications Technology Law*, Vol. 26, Iss. 3, p. 229-249 ; G. Comandé - G. Schneider, *" Les enjeux réglementaires des pratiques de data mining : Le cas des cycles de vie sans fin des 'données de santé' " (2018),* in *European Journal of Health Law*, volume 25, numéro 3, pages 284 - 307.

(article 5.1.b du RGPD). Enfin, le profilage personnel peut atteindre un haut niveau de précision, quel que soit le type de données utilisées pour la production de ces profils. **Cela nécessite de prendre en compte les précautions suivantes :**

- Les responsables du traitement **doivent supposer par défaut qu'ils traitent des données à caractère personnel** et agir en conséquence.

- Il est seulement conseillé d'éviter cette hypothèse si les données à utiliser et les données déduites par le responsable du traitement sont entièrement non personnelles (par exemple, les données météorologiques). Dans ces cas, les responsables du traitement doivent le documenter dans les registres de traitement.

- Si les données à traiter concernent des personnes décédées ou des personnes morales, des précautions doivent être prises pour éviter que ces données soient liées à des personnes physiques (par exemple, des parents de personnes décédées ou des personnes physiques liées à des personnes morales).

- Si les données à traiter concernent des personnes décédées, les règles nationales de traitement des données doivent également être prises en compte, car les données des personnes décédées ne sont pas des données à caractère personnel selon le RGPD.

- Il convient de définir un niveau de granularité dans le profilage afin de garantir suffisamment le respect de la vie privée des personnes qui peuvent potentiellement être liées à ce profilage.

- Des protocoles doivent être élaborés pour prévenir ou réduire la possibilité de ré-identification des utilisateurs dont les données ont été traitées à des fins de profilage. Ils doivent inclure un engagement juridiquement contraignant à ne pas chercher à obtenir une telle réidentification et l'adoption de mesures destinées à éviter une réidentification involontaire.

Outre la distinction initiale entre données personnelles et non personnelles, il convient de prendre en compte, au sein des données personnelles, **si des catégories spéciales de données personnelles sont concernées**. Cette distinction est importante dans la mesure où les conditions de traitement des données varient selon que des catégories particulières de données (article 9 du RGPD) sont concernées ou non.

Enfin, il convient de faire une remarque sur les **données dérivées ou déduites**. Il y a eu une certaine controverse quant à savoir si les données dérivées, et en particulier les profils personnels, devaient être considérés comme de la propriété intellectuelle. Indépendamment de cela, il convient de rappeler que, conformément à l'article 4, paragraphe 1, du RGPD, **ces données sont des données à caractère personnel dans la mesure où elles se rapportent à une personne identifiée ou identifiable.** Il convient d'ajouter qu'il est possible de tirer des conclusions sur ce que l'article 9 du RGPD considère comme des catégories spéciales de données à partir de données personnelles ordinaires ou même de données non personnelles combinées à d'autres données personnelles (confidentialité de groupe)[732] . Dans la mesure où ces déductions se rapportent à une personne identifiée ou identifiable, elles doivent être traitées comme

[732] Voir en général Taylor, L., Floridi, L., van der Sloot, B. eds. (2017) *Group Privacy : newchallenges of data technologies*, Dordrecht, Springer.

des catégories spéciales de données, indépendamment de leur compréhension (ou non) en tant qu'objets de propriété intellectuelle.

2 Étapes préliminaires : les questions cruciales à prendre en compte

Dans cette section, nous donnons quelques conseils généraux sur la manière d'aborder un projet de recherche aux **premiers stades de son cycle de production, c'**est-à-dire lorsqu'il n'est encore guère plus qu'une idée qui n'a pas encore été mise en œuvre. Il est important de les garder à l'esprit si l'on veut assurer la mise en œuvre des politiques de protection des données dès la conception (voir la section "Protection des données dès la conception et par défaut" dans les "Concepts principaux" de la partie II des présentes lignes directrices).

Les conseils essentiels sont les suivants :

1. Vérifier que votre projet est compatible avec le cadre de protection des données.
2. Mettre en œuvre un programme de formation sur les questions éthiques et juridiques à l'intention des développeurs de TIC et des autres parties prenantes concernées.
3. Définir les rôles joués par tous les agents impliqués dans le traitement.
4. Promouvoir l'engagement des utilisateurs finaux

2.1 Assurez-vous que votre projet est compatible avec les valeurs fondamentales de l'UE.

Avant d'envisager l'utilisation des données recueillies sur les réseaux sociaux pour le projet, les développeurs doivent avoir clairement à l'esprit leur objectif principal. Il se peut que cette utilisation ne soit pas compatible avec les normes éthiques et juridiques de l'UE incluses dans la Charte des droits fondamentaux de l'UE, par exemple. **Si tel était le cas, le projet ne devrait pas être approuvé.** D'autre part**, si une analyse montre que le traitement nécessaire ne sera pas acceptable sur la base de la politique des développeurs du réseau social, du RGPD et/ou du cadre juridique complémentaire, le projet ne doit pas non plus être approuvé.** Enfin, les développeurs doivent évaluer si le projet est acceptable selon les normes éthiques, même s'il est conforme aux obligations légales (voir "Vie privée dès la conception et par défaut" dans les "Principaux outils et actions" de la partie II des présentes lignes directrices).

En outre, **une idée claire de l'utilisation concrète des données recueillies par le biais des réseaux sociaux aidera les responsables du traitement à déterminer, dès les premières étapes du développement, certaines questions juridiques importantes concernant le traitement**, telles que le respect de la politique de développement du

réseau social, la nécessité éventuelle de transferts internationaux de données, l'existence de responsables conjoints du traitement ou de sous-traitants - qui doivent être soigneusement sélectionnés - ou les mesures de sécurité et d'organisation visant à minimiser les risques.

2.2 Mettre en œuvre un programme de formation sur les questions éthiques et juridiques à l'intention des développeurs TIC et des autres parties prenantes concernées.

La mise en œuvre de **programmes de formation de base** pour les chercheurs/innovateurs impliqués dans le traitement pourrait être extrêmement utile pour éviter les problèmes de protection des données lors du traitement des données obtenues à partir des médias sociaux. Certaines ressources utiles à cet effet sont, par exemple, disponibles auprès de l'Agence des droits fondamentaux[733] , de l'IEEE et de ses lignes directrices en matière d'éthique[734] , et de la Commission européenne[735] . **Cette formation devrait également inclure une compréhension approfondie de la politique du développeur du réseau social à partir duquel les données seront recueillies.**

Si la formation n'est pas possible, la mise en œuvre des conseils d'un **expert externe** dès le début du projet pourrait être une alternative acceptable. Si les chercheurs/innovateurs collectent des données à partir d'un réseau social concret, cette formation devrait inclure une analyse minutieuse de sa politique de développement particulière. Une implication précoce des DPD des institutions participantes est fortement conseillée.

Il est également fortement recommandé d'adopter des mesures appropriées pour garantir la confidentialité, l'intégrité et la disponibilité des données (voir la sous-section "Mesures en faveur de la confidentialité" dans la section "Intégrité et confidentialité" de la section "Principes" de la partie II des présentes lignes directrices).

2.3 Définir les rôles joués par tous les agents impliqués dans le traitement.

Les concepts de responsable du traitement, de responsable conjoint du traitement et de sous-traitant jouent un rôle crucial dans l'application du RGPD, car ils déterminent qui est responsable du respect des différentes règles de protection des données et comment les personnes concernées peuvent exercer leurs droits dans la pratique[736] (voir les "Principaux acteurs" dans la partie II des présentes lignes directrices, principalement les sections consacrées au "Responsable du traitement" ou au "Sous-traitant"). Dans le cas de l'utilisation des réseaux sociaux pour le traitement des données, il est tout aussi important de bien distinguer le responsable du traitement des données du sous-traitant, car les responsabilités de chacun sont différentes.

---

[733] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition et
[734] https://ethicsinaction.ieee.org/
[735] https://ec.europa.eu/justice/smedataprotect/index_en.htm
[736] Lignes directrices 07/2020 de l'EDPB sur les concepts de responsable du traitement et de sous-traitant dans le RGPD, p. 3, à l'adresse : https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en .

Certains doutes peuvent surgir quant à savoir laquelle des parties impliquées dans ce cadre joue le rôle de responsable du traitement, de sous-traitant ou, le cas échéant, s'il existe une situation de contrôle conjoint. **Pour dissiper ces doutes,** nous devons d'abord nous tourner vers la liste des définitions du RGPD, interprétées conformément aux lignes directrices de l'EDPB 7/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD et aux lignes directrices de l'EDPB 8/2020 sur le ciblage des utilisateurs de médias sociaux[737] et à la jurisprudence pertinente de la CJUE[738] .

En ce qui concerne l'utilisation des réseaux sociaux pour la recherche, et sans préjudice de la prudence casuistique susmentionnée, on peut affirmer qu'il **n'existe pas de situation de contrôle conjoint, dans la mesure où les moyens et les finalités de chaque traitement ne sont pas déterminés conjointement par le réseau social et l'institution chargée du développement des TIC, mais où le réseau social permet au développeur d'utiliser son environnement.** La relation entre les chercheurs et les réseaux sociaux repose généralement sur ce que l'on appelle les politiques des développeurs. La plupart des réseaux sociaux n'autorisent les chercheurs/innovateurs à collecter des données par le biais de leurs interfaces de programmation d'applications (API) que s'ils suivent les instructions définies dans ces politiques. Les chercheurs/innovateurs doivent donc s'assurer qu'ils procèdent effectivement à cette collecte s'ils veulent éviter d'être tenus pour responsables d'un traitement illégal des données. Bien entendu, il existe une exception possible à cette règle générale : si un développeur loue les services d'un réseau social pour traiter des données en son nom, cela peut impliquer un contrôle conjoint (cela dépendra des conditions concrètes du contrat et de la manière dont les responsabilités sur les données sont attribuées aux partenaires). Toutefois, si une telle exception ne s'applique pas :

- le réseau social est considéré comme le responsable du traitement des données qu'il effectue conformément aux finalités et aux objectifs qu'il poursuit, et le développeur TIC est le responsable du traitement des données pour les activités de traitement des données qu'il contrôle ;
- la relation entre le développeur et le réseau social est la suivante :
    - le réseau social joue le rôle de fournisseur de services de la société de l'information, et
    - l'institution de recherche le rôle de l'utilisateur des services de la société de l'information.
- les activités menées par l'institution de recherche à partir de son profil de recherche doivent être autorisées par le réseau social en tant que prestataire de services de la société de l'information, mais cela n'implique pas qu'il existe une situation de contrôle conjoint ni que la licence d'utilisation des données garantisse une base juridique pour le traitement des données à caractère personnel.

Ainsi, dans les scénarios les plus courants, les chercheurs et les innovateurs en TIC joueront le rôle d'un tiers par rapport aux réseaux sociaux et aux personnes concernées. Le réseau leur fournira des données qui appartiennent aux personnes concernées. Une

[737] Lignes directrices de l'EDPB (Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux Version 2.0 adoptée le 13 avril 2021, à l'adresse : https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11).

[738] Les arrêts Wirtschaftsakademie (C-210/16), Témoins de Jéhovah (C-25/17) et Fashion ID (C-40/17) sont particulièrement pertinents en l'espèce.

fois que ces données sont déjà sous le contrôle des chercheurs/innovateurs, ils deviennent les responsables du traitement de ces données et assument les responsabilités correspondantes.

Bien qu'une situation de contrôle conjoint n'existe généralement pas, il n'est pas impossible qu'une telle situation se produise. Il convient donc de rappeler **les garanties de l'article 26 du RGPD en cas de contrôle conjoint** (voir la section "Acteurs principaux" de la partie II des présentes lignes directrices) **entre le réseau social et l'institution de recherche :**

- Le développeur de TIC et le réseau social déterminent tous deux, de manière transparente, leurs responsabilités respectives en matière de respect des obligations prévues par le RGPD, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs devoirs respectifs de fournir les informations visées aux articles 13 et 14, au moyen d'un **arrangement entre eux.**
- L'arrangement
    - est mis à la disposition de la personne concernée ;
    - peut désigner un point de contact pour les personnes concernées ;
    - reflètent dûment les rôles et les relations respectifs des responsables conjoints du traitement vis-à-vis des personnes concernées.
- Enfin, tous les responsables du traitement, les responsables conjoints du traitement et les sous-traitants doivent se rappeler que les personnes concernées peuvent exercer leurs droits en vertu du RGPD (art. 26.3 du RGPD).

2.4 Préparer et documenter les contrats avec le réseau social et (le cas échéant) avec les responsables conjoints du traitement, les sous-traitants, etc.

La collecte de données auprès des réseaux sociaux implique souvent la conclusion d'une sorte d'accord avec leurs représentants. En effet, l'accès à leur API, ou à des outils similaires, ne sera probablement pas accordé si cet accord n'a pas été documenté. Parfois, l'adhésion aux politiques des développeurs ne fait même pas partie de cet accord, puisqu'il est parfaitement clair que quiconque reçoit des données du réseau doit les suivre. Le chercheur/innovateur doit cependant s'assurer que cette architecture juridique est fixée de manière adéquate dès le début.

D'autre part, il est évident qu'un responsable du traitement confiera souvent certaines des tâches techniques à un sous-traitant, qui pourrait même impliquer un sous-sous-traitant. En pratique, cependant, il y aura des moments où il sera difficile de s'assurer que le sous-traitant n'agit pas réellement comme un responsable du traitement ou un responsable du traitement conjoint.

Les chercheurs et les innovateurs doivent faire de leur mieux pour éviter ces problèmes, car le règlement sur la protection des données exige une réponse claire à la question "qui est responsable de ce traitement ?" afin de garantir une protection "effective et complète" des droits et libertés des personnes concernées.[739] Ainsi, une exigence clé

[739] Voir : Lignes directrices de l'EDPB (Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux Version 2.0 adoptée le 13 avril 2021, à l'adresse : https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11)

d'une politique adéquate de protection des données dès la conception est de **clarifier dès le début qui sont les responsables officiels du traitement des données et les sous-traitants, afin de s'assurer que la responsabilité légale est comprise.**

Afin d'atteindre cet objectif**, des accords écrits entre tous les agents impliqués dans le développement des outils devraient être conclus et documentés, dans la mesure du possible (voir l'article 28 du RGPD).** Ces accords devraient inclure des spécifications claires sur les responsabilités assumées par tous les participants. La promotion d'une interaction continue entre tous les DPD concernés pourrait être une excellente option. Des organes et des outils de contrôle ad hoc peuvent être adoptés pour garantir un contrôle sans faille du traitement effectué par les participants.

2.5 Promouvoir l'engagement des utilisateurs finaux

Étant donné que les TIC impliquent l'utilisation de données à caractère personnel provenant de différents types de personnes concernées, il est fortement recommandé d'entendre la voix des représentants des collectivités impliquées afin de s'assurer que les politiques de protection des données dès la conception (voir la sous-section "Protection des données dès la conception et par défaut" dans les "Concepts principaux" de la partie II des présentes lignes directrices) sont conformes à leurs intérêts, droits et libertés. L'organisation de **discussions préliminaires** avec ces représentants garantit la mise en œuvre d'un cadre ascendant qui pourrait être très utile à cette fin.

Liste de contrôle : Compréhension du projet

- L'utilisation des données recueillies par les réseaux sociaux ne favorise pas les scénarios incompatibles avec les valeurs fondamentales de l'UE.
- Le développement des TIC n'implique pas une utilisation disproportionnée des données personnelles recueillies par les réseaux sociaux.
- Le responsable du traitement s'est assuré que les membres de l'équipe traitant des données à caractère personnel ont été formés de manière adéquate à la politique du développeur correspondant au réseau social à partir duquel les données seront extraites, et aux concepts clés sur les questions de protection des données.
- Des outils d'évaluation adéquats sur la protection des données ont été mis en œuvre dès le début du projet.
- Les rôles joués par tous les différents agents impliqués dans le traitement des données ont été adéquatement clarifiés par les accords correspondants et le responsable du traitement peut fournir des preuves à ce sujet.
- Le développeur TIC est bien conscient des conditions d'utilisation des données recueillies auprès des réseaux sociaux.
- Les représentants des collectifs clés impliqués dans le traitement des données ont été consultés sur l'impact de l'utilisation des données collectées et du réseau social concret sélectionné.

3 Accéder aux données. Quelques conseils essentiels

Selon le RGPD, un traitement licite nécessite une base juridique (voir la sous-section "Licéité, loyauté et transparence" dans les "Principes" de la partie II des présentes lignes directrices). Si le traitement implique le type d'activités qui sont incluses dans le règlement "Vie privée et communications électroniques", les dispositions prises par ce nouvel outil s'appliqueront dès qu'il sera approuvé. À l'heure actuelle, l'article 6 du RGPD définit un total de six bases juridiques possibles. Dans le cas du traitement des données provenant des réseaux sociaux, il est essentiel de souligner que les **chercheurs ou les innovateurs en TIC doivent être conscients qu'ils auront certainement besoin de différentes bases juridiques pour le traitement des données au moment où ils accèdent aux données et au moment où ils effectuent leur recherche ou leur innovation sur la base de ces données.** Dans le premier cas, ce qui est nécessaire, c'est une base juridique pour obtenir les données du réseau social. Dans le second cas, il s'agit de trouver une base qui permette d'utiliser les données, déjà légitimement acquises, à des fins de recherche. **Il est essentiel de noter que le simple fait que les personnes concernées aient publié leurs données dans des espaces publics en ligne ne permet pas de les traiter.** Il s'agit toujours de données à caractère personnel, même si les données sont accessibles au public. La publication pourrait servir à éviter l'interdiction incluse dans l'article 9.1 du RGPD, si nous parlons de données de catégories spéciales, mais ne sert pas de base légale pour le traitement. **En tant que telles, les entreprises ne peuvent pas réutiliser librement les données, et ne peuvent pas les traiter ultérieurement à l'insu des personnes et sans une base adéquate pour un traitement licite.**

3.1 Domaine public ne signifie pas données publiques !

Le concept de "domaine public" doit être analysé de manière adéquate dans le contexte des réseaux sociaux. Si le chercheur ou l'innovateur en TIC a dû s'inscrire auprès d'une communauté d'utilisateurs afin d'avoir accès à des données spécifiques, ces données ne sont pas publiques : il s'agit de données que les personnes concernées ont souhaité partager exclusivement avec une communauté d'utilisateurs et selon les termes et conditions déterminés par le réseau social en question, qui sont acceptés au moment où les utilisateurs créent leur profil. Si les chercheurs sont en mesure d'accéder à un profil ou à d'autres types de données de médias sociaux sur un site simplement parce qu'ils sont des utilisateurs enregistrés, cela ne revient pas à dire que ces informations sont accessibles au public. Il est donc absolument essentiel pour le chercheur ou l'innovateur en TIC d'avoir une connaissance précise de ces conditions, qui peuvent différer sensiblement d'un réseau social à l'autre.

En outre, même si les données sont dans le domaine public, cela ne signifie pas du tout que vous pouvez les utiliser à des fins autres que celles pour lesquelles elles ont été

rendues publiques. C'est extrêmement important, car dans le cas contraire, vous pourriez encourir des responsabilités juridiques.

L'affaire Equifax : l'utilisation des données de l'espace public ne constitue pas nécessairement un traitement légitime

Equifax est une société qui a obtenu des données du portail d'information utilisé par les administrations publiques pour transmettre des informations aux citoyens. À partir de ces données, elle a créé un fichier qui transmettait soi-disant des informations sur la solvabilité des citoyens. Tout cela, sans informer les personnes concernées de ces traitements et en utilisant l'intérêt légitime de l'entreprise comme base de légitimité. Le 26 avril 2021, l'Agence espagnole de protection des données (AEPD) a condamné Equifax à une amende d'un million d'euros pour violation de la réglementation sur la protection des données, a interdit la poursuite de l'utilisation de ce fichier, a ordonné la suppression de toutes les données des personnes concernées et a ordonné à Equifax de notifier à toutes les entreprises qui ont consulté son fichier le contenu de cette résolution afin qu'elles fassent de même et cessent d'utiliser ces données.

Cet arrêt est d'une grande importance pour plusieurs raisons. La première est qu'il s'agit de la première sanction majeure découlant du changement de critères apporté par le RGPD et le règlement national (LOPDgdd) concernant l'utilisation des sources accessibles au public : le fait que les données soient accessibles au public ne signifie pas qu'elles peuvent être utilisées à n'importe quelle fin et sans autre explication. Dans la précédente loi espagnole, la LOPD de 1999, ce critère n'était pas aussi clair et semblait être le contraire.

Dans sa résolution, l'AEPD a rappelé que (1) toute utilisation secondaire des données doit être compatible avec la finalité initiale pour laquelle elles ont été collectées (principe de limitation de la finalité du traitement des données, article 5.1.b du RGPD), (2) elle doit avoir sa base de légitimation (il ne suffit pas d'alléguer que les données proviennent de sources accessibles au public), et que (3) la personne concernée doit être notifiée de l'utilisation secondaire de ses données. L'amende de 1 million d'euros était fondée sur la violation du principe de limitation de la finalité.

3.2 Accéder aux données d'un réseau social : quelques conseils essentiels

Voici quelques conseils essentiels fournis par l'association Ethics information for Linguistics and English Language[740] que vous devez suivre si vous envisagez d'accéder aux données d'un réseau social :

[740] https://resource.ppls.ed.ac.uk/lelethics/index.php/frequently-asked-questions/corpus-research/

- Si les données sont dans le domaine public, vous devez vous conformer à toutes les exigences énoncées par le fournisseur du corpus, y compris en ce qui concerne l'anonymat, ou à toute autre condition d'utilisation.
- Certains corpus peuvent nécessiter une approbation éthique, en particulier les corpus comprenant des données sur la santé physique ou mentale, ou les corpus contenant des données qui pourraient être utilisées pour anonymiser des personnes (par exemple, lorsque des réponses en texte libre sont autorisées).
- Si les données ne sont pas dans le domaine public, vous devez vous assurer que votre utilisation des données est conforme aux exigences énoncées par le fournisseur du corpus. Par exemple, les données ne doivent pas être partagées de manière non autorisée (par exemple, mises en ligne).
- Dans un cas comme dans l'autre, s'il y a des raisons de soupçonner que les personnes qui ont initialement fourni les données ne savaient pas qu'elles seraient utilisées à des fins de recherche, vous devez examiner attentivement les implications éthiques de votre recherche, et notamment la nécessité d'obtenir un consentement éclairé.

Tous ces conseils peuvent être concrétisés dans les étapes suivantes :

- Premièrement, il faut toujours garder à l'esprit les **attentes raisonnables des personnes concernées quant à l'utilisation de leurs données (considérant 47 du RGPD).** Ce point est essentiel dans la plupart des politiques des développeurs des réseaux sociaux. Par exemple, la politique des développeurs de Twitter stipule que "nous interdisons l'utilisation des données de Twitter d'une manière qui serait incompatible avec les attentes raisonnables des personnes en matière de vie privée". En construisant sur l'API de Twitter ou en accédant au contenu de Twitter, vous avez un rôle particulier à jouer dans la sauvegarde de cet engagement, le plus important étant de respecter la vie privée des gens et de leur fournir la transparence et le contrôle sur la façon dont leurs données sont utilisées."[741]

- Deuxièmement, il ne suffit jamais d'obtenir l'autorisation d'accéder aux API et aux contenus d'un réseau social pour garantir un traitement licite des données. Il ne s'agit que d'une première étape. La plupart des réseaux sociaux ont élaboré des **lignes directrices** détaillées **sur l'utilisation des plateformes que les chercheurs doivent suivre à la lettre pour garantir le respect des politiques relatives à l'utilisation prévue des plateformes et la conformité aux exigences éthiques et juridiques en matière de protection des données.**

- Troisièmement, la plupart des réseaux sociaux ont développé des outils qui **offrent un soutien aux chercheurs** désireux d'utiliser leur interface de programmation d'applications (API). Il est toujours recommandé aux chercheurs d'utiliser ces services en cas de doute sur le traitement des données.

- Quatrièmement, cependant, les chercheurs et les innovateurs ne devraient jamais oublier qu'en tant que responsable du traitement, vous êtes chargé de veiller à ce que le cadre de protection des données soit correctement respecté. Ainsi, vous devez vérifier si les déclarations sur la légitimité du traitement des données effectué par les réseaux sociaux correspondent à la réalité. Passer en revue leurs

[741] https://developer.twitter.com/en/developer-terms/policy

politiques de collecte de données pour vérifier la solidité des consentements accordés du point de vue du RGPD semble une exigence nécessaire ou, du moins, prudente.

- Cinquièmement, les chercheurs/innovateurs doivent garder à l'esprit que les réseaux sociaux **peuvent modifier leurs politiques** de temps à autre sans préavis. Comme ils introduisent généralement cette mise en garde dans leurs propres politiques, les chercheurs ont la responsabilité de se tenir informés de ces éventuels changements. Il est donc fortement recommandé de revoir périodiquement ces politiques.
- Sixièmement, étant donné que les chercheurs traiteront des données qui n'ont pas été collectées auprès de la personne concernée, ils fourniront à cette dernière les informations requises par l'article 14, sauf si l'une des circonstances citées au point 5 s'applique.
- Enfin, en cas de doute, consultez toujours votre délégué à la protection des données et, si nécessaire, l'autorité de protection des données correspondante. .

Encadré : Prendre en compte les attentes et les préoccupations des personnes concernées. Le cas de Twitter

La plupart des chercheurs qui utilisent des ensembles de données de tweets n'obtiennent pas le consentement de chaque utilisateur de Twitter dont le tweet est collecté, et ces utilisateurs ne sont généralement pas avertis par le chercheur.

En 2017, Fiesler et Proferes ont élaboré une enquête exploratoire sur les perceptions des utilisateurs de Twitter concernant l'utilisation des tweets dans le cadre de la recherche. Au moment où cette recherche a été réalisée, la politique de confidentialité de Twitter mentionnait que les universitaires pouvaient utiliser les tweets dans le cadre de la recherche. Cependant, peu d'utilisateurs étaient auparavant au courant de ce fait, et la majorité d'entre eux estimaient que les chercheurs ne devraient pas pouvoir utiliser les tweets sans leur consentement. Toutefois, ces attitudes étaient très contextuelles et différaient en fonction de facteurs tels que la manière dont la recherche était menée ou diffusée, l'identité des chercheurs et le sujet de l'étude.

Source : Fiesler C. , Proferes N. "Participant" Perceptions of Twitter Research Ethics. Social Media + Society. Janvier 2018. doi:10.1177/2056305118763366.

Les chercheurs et les innovateurs qui utilisent des données obtenues à partir de réseaux sociaux sont tenus de se conformer à toutes les politiques établies par ces réseaux. Il est donc essentiel qu'ils examinent et comprennent ces politiques avant d'accéder aux API et aux contenus des réseaux sociaux. Le temps consacré à l'examen de ces politiques peut épargner aux chercheurs des heures de travail supplémentaires et peut même les aider à éviter des responsabilités juridiques.

Liste de contrôle. Accéder aux données

- Si les données sont dans le domaine public, les responsables du traitement ont respecté les exigences énoncées par le fournisseur du corpus, y compris en ce qui concerne l'anonymat, ou toute autre condition d'utilisation.
- Si les données ne sont pas dans le domaine public, les responsables du traitement se sont assurés que leur utilisation des données est conforme aux exigences éventuelles énoncées par le fournisseur du corpus.
- Les responsables du traitement connaissent les lignes directrices relatives à l'utilisation des plateformes qu'ils doivent suivre à la lettre afin de garantir la conformité aux politiques pour l'utilisation prévue des plateformes et le respect des exigences éthiques et juridiques en matière de protection des données.
- Les responsables du traitement ont pris en compte les attentes raisonnables des personnes concernées à propos de l'utilisation de leurs données.
- Les responsables de traitement ont vérifié si les déclarations sur la légitimité du traitement des données effectué par les réseaux sociaux correspondent à la réalité.
- Les chercheurs/responsables du traitement sont conscients qu'ils assument la responsabilité de se tenir informés des éventuels changements dans les politiques de la plateforme. Des révisions périodiques de ces politiques sont effectuées.
- Les responsables du traitement fournissent aux personnes concernées les informations demandées par l'article 14, sauf si l'une des circonstances citées au point 5 s'applique.

4 Choix d'une base juridique pour le traitement ultérieur

Une fois que les chercheurs/innovateurs deviennent les responsables du traitement des données recueillies sur les réseaux sociaux, ils doivent décider de la base juridique qui légitimera le traitement ultérieur de ces données dès que possible. Toutefois, et avant même de choisir la (ou les) base(s) juridique(s) du traitement, le responsable du traitement doit se demander si le traitement concerne des données à caractère personnel relevant de catégories spéciales. Dans ce cas, le responsable du traitement doit être conscient du fait que le traitement est soumis au veto de l'article 9.1 du RGPD, sauf si l'une des circonstances décrites à l'article 9.2 s'applique.

Après avoir conclu qu'aucune donnée d'une catégorie spéciale n'est concernée ou que le veto posé a été traité de manière adéquate, le responsable du traitement doit choisir la base juridique appropriée pour le traitement des données. Cela doit être fait très soigneusement, car la base juridique ne peut pas être modifiée pendant le traitement. Voici quelques critères qu'il convient de garder à l'esprit à cette fin :

- La nécessité ou l'utilité de l'utilisation des données obtenues à partir des réseaux sociaux pour la réalisation de la finalité ou de l'intérêt du traitement doit être suffisamment justifiée au regard de la base juridique retenue.
- Le responsable du traitement des données doit soigneusement peser (1) la base du droit utilisé, contre (2) les risques possibles découlant du traitement des données.
- En outre, le responsable du traitement doit envisager toutes les garanties adéquates afin de s'assurer que les intérêts, les droits et les libertés de la personne concernée sont correctement préservés. Cette mise en balance doit être particulièrement attentive si le consentement de la personne concernée sert de base juridique au traitement.

Les tableaux suivants donnent un bref aperçu des différentes bases alternatives de légitimation en vertu des articles 6 et des circonstances qui permettent de contourner le veto créé par l'article 9.1 du RGPD et de leur relation avec le traitement des données provenant des médias sociaux.

Le consentement est la base juridique la plus traditionnelle pour le traitement des données dans le contexte des réseaux sociaux. Toutefois, lorsqu'un responsable du traitement cherche à traiter des données à caractère personnel à des fins de recherche, l'intérêt public peut être une excellente option. Malheureusement, il exige que certaines conditions s'appliquent (voir la sous-section "Protection des données et recherche scientifique" dans les "Concepts principaux" de la partie II des présentes lignes directrices). L'intérêt légitime, quant à lui, est une autre base juridique appropriée pour le traitement dans ce contexte, mais on ne peut pas supposer qu'il sera toujours approprié[742] . Elle sera probablement la plus appropriée lorsque les responsables du traitement utilisent les données des personnes d'une manière à laquelle celles-ci s'attendent raisonnablement et qui a le moins d'impact possible sur la protection des données ou la vie privée, ou lorsqu'il existe une justification impérieuse pour le traitement.[743]

Bases juridiques possibles (Art. 6 du RGPD)

Bases juridiques du traitement	**Utilisation dans le contexte des réseaux sociaux**
6.1.a -consentement	Probablement, la base juridique la plus populaire pour le traitement des données,

[742] Par exemple, les autorités publiques ne peuvent se fonder sur des intérêts légitimes que si elles traitent des données pour une raison légitime autre que l'exécution de leurs tâches en tant qu'autorité publique, de sorte que la "tâche publique" est une meilleure base juridique dans ces situations (ICO : Legitimate interests, à l'adresse : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

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

	bien que son utilisation généralisée soit de plus en plus remise en question[744] (voir la section suivante).
6.1.e - le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.	Elle peut être applicable, mais les précautions suivantes doivent être observées : - L'objectif d'intérêt public doit être clairement identifié ainsi que le lien avec la recherche, - Il convient de motiver pourquoi l'utilisation des données issues des médias sociaux est nécessaire ou hautement souhaitable pour les finalités poursuivies. -La base du traitement a été établie par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis.
6.1.f - le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.	Elle peut être applicable, et constitue même la meilleure alternative au consentement comme base de légitimité. Les mises en garde suivantes doivent être observées : - le responsable du traitement doit procéder et motiver une mise en balance appropriée entre (1) l'intérêt légitime poursuivi et (2) l'impact sur les droits et libertés fondamentaux de la personne concernée ; cette mise en balance doit être effectuée avec un soin particulier si des données de mineurs sont concernées.

Catégories particulières de données à caractère personnel (art. 9 du RGPD)

Base de la légitimité	**Utilisation dans le contexte des réseaux sociaux**
9.1.a -consentement	Il est largement utilisé

[744] Voir, sur le traitement des données à des fins de santé dans le système américain de protection de la vie privée, Charlotte A. Tschider, " The consent myth : improving choice for patients of the future " (2019) 96 Washington University Law Review 1506.

9.2.e - le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée.	Elle peut être applicable, mais il convient d'être particulièrement prudent en ce qui concerne les garanties suivantes : - le respect du principe de limitation des finalités (art. 5.1.b du RGPD), en tenant compte des attentes de la personne concernée et du contexte (réseau social et impact du profil) dans lequel les données ont été publiées[745] ; - des mesures d'agrégation afin de réduire les possibilités de ré-identification.
9.2.g - le traitement est nécessaire pour des raisons d'intérêt public important, sur la base du droit de l'Union ou des États membres, qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.	Elle peut être applicable, à condition que le responsable du traitement des données respecte les précautions suivantes : - l'intérêt public poursuivi doit être clairement identifié, ainsi que la réglementation applicable ; - il doit être suffisamment justifié que la recherche via les réseaux sociaux est nécessaire ou hautement appropriée à cette fin ; - un soin particulier doit être apporté à l'élaboration de mesures de protection contre les impacts indus sur les droits fondamentaux des personnes concernées.
9.2.j - le traitement est nécessaire à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou des États membres qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de	Elle est pleinement applicable. Elle présente l'avantage que le principe de limitation de la finalité est moins strict (cf. art. 5.1.b du RGPD) et qu'elle permet le traitement des données indépendamment du consentement des personnes concernées, à condition que le responsable du traitement observe les garanties suivantes : - elle doit clairement identifier sa finalité (archivage, recherche scientifique, recherche historique ou objectifs statistiques) ; - elle doit justifier la proportionnalité du traitement des données par rapport à la finalité poursuivie ; - elle doit justifier l'utilité de l'utilisation des

[745] Récemment, le Conseil espagnol de la protection des données a infligé une amende à Equifax pour avoir utilisé des données de solvabilité publiées par des sources officielles afin d'alimenter ses propres fichiers, pour violation du principe de limitation de la finalité dans la mesure où il s'agit d'une utilisation incompatible des données bien qu'il s'agisse de données accessibles au public. Le critère de cette résolution peut également être applicable en cas d'utilisation de données publiées par la personne concernée elle-même, dans la mesure où les utilisations dérivées de ces données sont incompatibles.

la personne concernée.	réseaux sociaux dans la recherche ; - elle doit élaborer des mesures visant à éviter les impacts indus sur les droits fondamentaux des personnes concernées, en se concentrant sur (1) un niveau d'agrégation suffisant et (2) d'autres garanties pour éviter la ré-identification. - ell doit suivre strictement les prescriptions de l'art. 89 du RGPD

4.1 Consentement

Le consentement est le premier des six fondements de la licéité du traitement des données à caractère personnel énumérés à l'article 6. Selon l'article 6, paragraphe. 1(a)[746] , ce traitement est licite si les personnes concernées ont donné leur consentement au traitement de leurs données personnelles pour une ou plusieurs finalités spécifiques. Ainsi, si les données sont utilisées pour des finalités multiples, le consentement doit être donné pour chaque finalité séparément. Un consentement spécifique est essentiel pour éviter un consentement non valable. En effet, "si un traitement de données a des finalités multiples, alors le consentement doit être demandé pour chacune d'entre elles. La spécificité du consentement favorise la transparence dans la mesure où les personnes concernées connaissent chaque finalité du traitement des données, augmente leur contrôle sur ces finalités et les protège contre la dérive fonctionnelle." [747]

L'exigence de spécificité est particulièrement importante dans le cas de la réutilisation de données provenant de réseaux sociaux. Les utilisateurs finaux des réseaux sociaux ne sont souvent pas conscients du fait que leurs données sont utilisées à des fins autres que celles qu'ils poursuivent lorsqu'ils fournissent ces données. Toutefois, la plupart des réseaux sociaux veillent à ce que les personnes concernées donnent leur consentement à ce traitement ultérieur et leurs politiques en matière de développement couvriront certainement cette question. Les chercheurs et les développeurs désireux de traiter les données obtenues auprès des réseaux sociaux à des fins de recherche pourraient obtenir un nouveau consentement des personnes concernées. Bien entendu, cela est difficile et pas toujours nécessaire. Ils pourraient s'appuyer sur le consentement initial fourni par la personne concernée au réseau social. **Les chercheurs/innovateurs devraient** toutefois **s'assurer que le traitement qu'ils souhaitent effectuer est autorisé par le consentement initialement fourni par la personne concernée ou trouver une autre base juridique (en demandant un nouveau consentement ou en utilisant l'intérêt légitime ou l'intérêt public comme alternative, par exemple).** La consultation des conditions d'utilisation du réseau social

[746] EDPB : Lignes directrices 05/2020 sur le consentement au titre du règlement 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[747] Joyee De S., Imine A. (2019) On Consent in Online Social Networks : Impacts sur la vie privée et directions de recherche (article court). In : Zemmari A., Mosbah M., Cuppens-Boulahia N., Cuppens F. (eds) Risques et sécurité de l'internet et des systèmes. CRiSIS 2018. Notes de lecture en informatique, vol 11391. Springer, Cham. https://doi.org/10.1007/978-3-030-12143-3_11

et du consentement recueilli à l'origine est un excellent moyen de vérifier si l'utilisation secondaire des données peut être considérée comme compatible avec les finalités pour lesquelles les données ont été collectées à l'origine (voir la sous-section "Principe de limitation des finalités" dans les "Principes" de la partie II des présentes lignes directrices).

Si la recherche implique l'utilisation de **données recueillies auprès de différents réseaux sociaux**, les chercheurs doivent s'attacher à **concevoir des mécanismes d'évaluation du risque d'atteinte à la vie privée intra-fournisseur et éventuellement inter-fournisseur qui prennent en compte les données personnelles révélées pour toutes les activités de traitement des données pour un réseau social concret et pour tous les OSN qu'une personne concernée utilise, respectivement.**

Enfin, et surtout, étant donné que les chercheurs traiteront des données qui n'ont pas été collectées auprès de la personne concernée, ils fourniront à cette dernière les informations requises par l'article 14, à moins que l'une des circonstances citées au point 5 ne s'applique (voir la sous-section "Droit à l'information" de la section "Droits de la personne concernée" de la partie II des présentes lignes directrices).

Encadré : le cas des données effacées

Certains utilisateurs de réseaux sociaux publient des données sur leurs plateformes et les suppriment ensuite. Si ces données ont été récupérées par un chercheur avant leur suppression, il n'est pas certain que le consentement initial de l'utilisateur à l'utilisation de ses données reste intact. En fonction de la sensibilité des données et de l'analyse, les chercheurs doivent convenir dès le départ de la manière de gérer cette question. Par exemple, il n'est peut-être pas nécessaire de supprimer le nombre de messages d'une série chronologique, mais il peut être contraire à l'éthique de citer un message individuel qui a été supprimé depuis. Cependant, cette question n'est pas encore claire. Les chercheurs doivent donc rester prudents quant à l'utilisation de données supprimées.

Voir : Social Media Research Group, Using social media for social research : An introduction Mai 2016, p. 17 à l'adresse : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/524750/GSR_Social_Media_Research_Guidance_-_Using_social_media_for_social_research.pdf

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 se sont assurés que le consentement fourni par la personne concernée au réseau social couvre le type de traitement qu'ils sont prêts à effectuer.

☐ Si tel n'est pas le cas, les responsables du traitement doivent demander aux personnes concernées de renouveler leur consentement.

4.2 Intérêt légitime

L'intérêt légitime constitue une base alternative de traitement licite qui pourrait être applicable à l'utilisation des données recueillies sur les réseaux sociaux, même si les autorités publiques ***ne peuvent pas se fonder*** sur cette base pour agir. Pour ceux qui peuvent utiliser cette base légale, trois conditions cumulatives doivent être remplies[748] :

(i) la poursuite d'un intérêt légitime par le responsable du traitement des données ou par le ou les tiers auxquels les données sont communiquées,

(ii) la nécessité de traiter les données personnelles aux fins des intérêts légitimes poursuivis, et

(iii) à condition que les libertés et droits fondamentaux de la personne concernée dont les données doivent être protégées ne priment pas.

Ainsi, en principe, l'intérêt légitime pourrait être la base juridique parfaite pour le traitement dans ce contexte. Toutefois, il existe de bonnes raisons de considérer que cette base ne s'appliquera pas toujours à l'utilisation des données pour la recherche scientifique :

- Tout d'abord, l'intérêt légitime doit s'appliquer à tous les responsables du traitement conjoints, dans le cas où le contrôle conjoint s'applique au traitement. Dans l'affaire Fashion ID, la CJUE a précisé que, dans de telles circonstances, "il est nécessaire que chacun de ces responsables du traitement poursuive un intérêt légitime [...] à travers ces opérations de traitement pour que ces opérations soient justifiées à l'égard de chacun d'eux".
- Deuxièmement, les responsables du traitement doivent être en mesure de démontrer que le test de mise en balance a été correctement effectué (voir la section "Intérêt légitime et test de mise en balance" dans la section "Principaux outils et actions" de la partie II des présentes lignes directrices). Cela signifie que les responsables du traitement conjoints sont en mesure d'établir que le traitement est nécessaire à la réalisation de ces intérêts légitimes. Cet objectif est difficile à atteindre, car le terme "nécessaire" exige un lien entre le traitement et les intérêts poursuivis. Cela signifie qu'il convient d'examiner si d'autres moyens moins invasifs sont disponibles pour servir le même objectif. De même, les sous-traitants doivent être en mesure de démontrer que les intérêts légitimes en jeu ne sont pas supplantés par les intérêts ou les libertés et droits fondamentaux de la personne concernée. Tout cela est difficile à démontrer, surtout si des mineurs sont impliqués dans le traitement. [749]
- Troisièmement, l'intérêt légitime pourrait difficilement s'appliquer comme base juridique d'un traitement licite si ce traitement implique des pratiques intrusives

[748] 9 CJUE, arrêt dans l'affaire Fashion ID, 29 juillet 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629.

[749] Voir l'avis 06/2014 du groupe de travail Article 29 sur la notion d'intérêts légitimes du responsable du traitement des données en vertu de l'article 7 de la directive 95/46/CE, WP217, 9 avril 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

de profilage et de suivi, par exemple celles qui consistent à suivre des individus sur plusieurs sites web, emplacements, dispositifs, services ou trocs de données.[750]

- Quatrièmement, si nous considérons les données relatives aux personnes concernées qui ont déjà eu une relation antérieure avec le chercheur et l'innovateur en TIC par le biais du réseau social, l'utilisation de l'intérêt légitime comme base juridique semble plutôt raisonnable. Toutefois, les responsables du traitement doivent prendre en considération si la relation antérieure était similaire à celle qui est sur le point d'être établie.

Si l'intérêt légitime est finalement choisi comme base juridique du traitement, les responsables du traitement doivent garder à l'esprit que les obligations de transparence et le **droit d'opposition** doivent être examinés attentivement. **Les personnes concernées doivent avoir la possibilité de s'opposer au traitement de leurs données à des fins ciblées avant que le traitement ne soit lancé.** Les utilisateurs de médias sociaux devraient non seulement avoir la possibilité de s'opposer au traitement lorsqu'ils accèdent à la plateforme, mais aussi disposer de contrôles garantissant que le traitement sous-jacent à des fins spécifiques de leurs données personnelles n'a plus lieu après qu'ils se sont opposés au traitement.[751]

Liste de contrôle : intérêt légitime

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

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

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

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

 Si les responsables du traitement prévoient le traitement de données relatives aux enfants, ils ont pris des précautions supplémentaires pour s'assurer que l'intérêt légitime

[750] Groupe de travail Article 29, Avis sur le profilage et la prise de décision automatisée, WP 251, rév. 01, p. 15, voir également Article 29 WP, Avis sur l'intérêt légitime, p. 32 et 48 : "Dans l'ensemble, il existe un déséquilibre entre l'intérêt légitime de l'entreprise et la protection des droits fondamentaux des utilisateurs et l'article 7, point f), ne devrait pas être invoqué comme fondement juridique du traitement. L'article 7, point a), serait un motif plus approprié à utiliser, pour autant que les conditions d'un consentement valable soient remplies".

[751] Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux Version 2.0 Adoptées le 13 avril 2021, à l'adresse : https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11)

est une base de données appropriée.

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

 Les responsables de traitement ont mis en place des outils adéquats pour que le droit d'opposition soit facile à mettre en œuvre par les personnes concernées.

 Si les responsables du traitement ont identifié un impact significatif sur la protection des données personnelles, ils ont examiné s'ils devaient également mener une AIPD.

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

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

Selon l'article 6, point e), du RGPD, le traitement est licite s'il est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public. Ici, il faut garder à l'esprit que la "recherche scientifique" est un terme trop large qui fait généralement référence à la recherche de connaissances, par le biais d'une certaine méthodologie, dans tout domaine de la connaissance humaine. Ainsi, il est tout à fait probable que si les responsables du traitement utilisent une méthodologie scientifique et, d'une manière ou d'une autre, recherchent des connaissances en pensant à l'utilisation des données, ce traitement pourrait être licite sur la base du motif juridique d'intérêt public.

En outre, l'intérêt public pourrait servir à ignorer le veto prévu à l'article 9.1 du RGPD s'ils utilisent des catégories spéciales de données lorsque d'autres bases juridiques (comme la recherche par exemple) ne sont pas applicables en l'espèce. Toutefois, dans ce cas, le traitement doit être fondé sur la législation de l'UE ou d'un État membre et doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour sauvegarder les droits fondamentaux et les intérêts de la personne concernée[752] (voir la sous-section "Protection des données et recherche scientifique" de la section "Concepts principaux" de la partie II des présentes lignes directrices**).**

D'autre part, il faut se rappeler que l'article 5 (b) du RGPD établit le principe de limitation de la finalité, selon lequel les données ne peuvent pas être traitées pour des finalités autres que celles spécifiques initiales. Il est intéressant de noter que cet article prévoit que certaines finalités, dont la recherche scientifique, sont considérées comme compatibles avec la finalité initiale, ce qui rend leur traitement ultérieur présumé licite. Par conséquent, lorsque le responsable du traitement peut faire valoir, documents à l'appui, que la finalité du traitement est la recherche scientifique, les **utilisations secondaires des données à caractère personnel sont en principe considérées comme**

[752] Voir les lignes directrices du pilier de l'OCSE " D4.1 : Legal and Policy Framework and Federation Blueprint' (2021), p. 76-77. À l'adresse : https://repository.eosc-pillar.eu/index.php/s/tbqe6B7rDycdFCJ#pdfviewer

compatibles avec la finalité initiale du traitement des données à caractère personnel (voir la sous-section "Principe de limitation de la finalité" dans la section "Principes" de la partie II des présentes lignes directrices).

En outre, il est tout à fait probable que le réseau social qui a initialement recueilli les données ait inclus dans le consentement de la personne concernée une clause autorisant, à lui ou à un tiers, un traitement ultérieur à des fins de recherche ou, du moins, ait informé la personne concernée que ce traitement serait considéré comme compatible avec son consentement initial. Si tel était le cas, le traitement à des fins de recherche serait légitime sur la même base licite qui a permis au réseau social de collecter les données.

Cette évaluation, toutefois, doit être effectuée avant le traitement ultérieur à des fins secondaires et doit être fondée sur des critères objectifs. Le cadre juridique sur cette question peut varier considérablement entre les États membres de l'UE. Les responsables du traitement doivent donc être conscients du cadre normatif concret applicable. La consultation de leurs DPD est fortement recommandée à cette fin[753] ainsi que l'inclusion d'un conseiller/unité éthico-juridique dans le projet donné.

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

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

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

 Les responsables du traitement ont mis en œuvre les garanties et les mesures organisationnelles consacrées pour s'aligner sur l'article 89 du RGPD et la réglementation nationale correspondante.
 Les responsables de traitement ont documenté toutes les informations concernant cette question dans l'AIPD.

5 Loyauté et Questions de transparence

La loyauté est un principe essentiel du RGPD. On peut dire que l'ensemble de la protection des données, et donc le RGPD, concerne la loyauté envers les personnes concernées. Le RGPD peut être considéré comme précisant ce que signifie réellement la *loyauté*. Dans le cas des données recueillies par l'utilisation des réseaux sociaux, il est particulièrement important d'éviter les biais liés au sexe, à la race, à l'âge, à l'orientation sexuelle, à l'origine nationale, à la religion, à la santé et au handicap, etc. Cela peut être problématique car il est possible que certaines des données recueillies via les réseaux

[753] Vous trouverez des questions pratiques et des réponses à ce sujet sur le site https://www.ru.nl/rdm/gdpr-research/faq-gdpr-research/.

sociaux ne correspondent pas à des utilisateurs réels, ou que leurs données sensibles ne soient pas du tout exactes. Cela pourrait créer des biais cachés (voir la sous-section "Licéité, loyauté et transparence" de la section "Concepts principaux" de la partie II des présentes lignes directrices).

La transparence, en revanche, est une stratégie essentielle pour équilibrer le pouvoir entre le responsable du traitement et la personne concernée. Elle fonctionne en mettant tout en lumière et en l'ouvrant ainsi à un examen minutieux. L'objectif principal de la transparence est d'informer d'emblée les **personnes concernées** de l'existence du traitement et de ses principales caractéristiques. D'autres informations (telles que les données concernant la personne concernée) sont disponibles sur demande. Les personnes concernées doivent également être informées de certains événements, notamment des violations de données (dans le cas où la personne concernée est exposée à un risque élevé). De toute évidence, la transparence est une condition préalable à la détection et à l'intervention en cas de non-conformité (voir la sous-section "Licéité, loyauté et transparence" de la section "Concepts principaux" de la partie II des présentes lignes directrices).

Dans le cas de l'utilisation de données provenant de réseaux sociaux, la transparence signifie, selon nous, que "les sujets de recherche prévus doivent être informés à un moment donné de la recherche en cours, du type de données personnelles que les responsables du traitement collectent et de la manière dont elles seront utilisées. Certains services précisent clairement que cela doit être fait avant de commencer la collecte. Pour d'autres qui n'ont pas de politique spécifique et lorsque les chercheurs/innovateurs mènent des recherches par observation auxquelles l'obtention d'un consentement préalable pourrait nuire, ils doivent informer les personnes concernées dès que possible. Les chercheurs/innovateurs en TIC devraient toujours retirer de leur moissonnage les personnes qui ne consentent pas à être incluses." [754]

Dans le cas de l'utilisation de données provenant de réseaux sociaux, il est nécessaire de souligner qu'en général, l'article 14 du RGPD sera applicable à un moment donné. Ainsi, les personnes concernées doivent être pleinement conscientes que leurs données sont partagées avec des tiers (voir la sous-section "Droit à l'information" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). Cela peut se faire de différentes manières. Par exemple, la CNIL a conseillé aux responsables de traitement d'inclure tous les tiers dans une notice de confidentialité exhaustive, mais mise à jour périodiquement, ou d'insérer un lien dans cette notice et de rediriger les personnes vers la liste des tiers et de leurs propres politiques de confidentialité. [755]

Les responsables du traitement doivent garantir la transparence non seulement en fournissant des informations adéquates, mais aussi en utilisant un certain nombre d'**outils complémentaires.** La désignation d'un DPD, qui sert alors de point de contact unique pour les questions des personnes concernées, est une excellente option. La préparation de registres adéquats du traitement à l'intention des autorités de contrôle ou la réalisation d'analyses d'impact sur la protection des données sont également des mesures hautement recommandées pour promouvoir la transparence. De même, la

[754] https://info.lse.ac.uk/staff/divisions/Secretarys-Division/Assets/Documents/Information-Records-Management/Social-media-personal-data-and-research-guidance-v.1.pdf

[755] https://www.cnil.fr/fr/transmission-des-donnees-des-partenaires-des-fins-de-prospection-electronique-quels-sont-les

réalisation d'analyses visant à évaluer l'efficacité et l'accessibilité des informations fournies aux personnes concernées contribue à garantir la mise en œuvre efficace de ce principe[756] .

Enfin, la mise en œuvre de ce que l'on appelle les outils d'amélioration de la transparence (TET)[757] pourrait être une excellente option pour garantir le respect du principe de transparence, en particulier lorsqu'un traitement massif ou automatisé des données est prévu.

5.1 Biais

Les biais créent des préjudices et des discriminations à l'encontre de certains groupes ou personnes. Des préjudices peuvent également résulter de l'exploitation intentionnelle des biais (des consommateurs) ou de l'exercice d'une concurrence déloyale, telle que l'homogénéisation des prix par le biais de la collusion ou d'un marché non transparent. L'utilisation des données recueillies par les réseaux sociaux pourrait contribuer à exacerber une telle situation, principalement en constituant des ensembles de données biaisées. Cela pourrait se produire, par exemple, en raison d'une collecte inadéquate des données produites par les personnes concernées. "Les données issues des médias sociaux peuvent être difficiles à vérifier - les utilisateurs peuvent mentir sur leur âge, leur localisation, leur emploi ou tout autre caractéristique. **Les chercheurs doivent être conscients de ce problème et aborder cette difficulté le cas échéant.** Il n'est pas conseillé de comprendre les utilisateurs comme le "grand public", en raison des inégalités d'accès à internet, et les chercheurs devraient envisager comment favoriser la diversité (le cas échéant) dans leur échantillon."[758] Il peut également arriver que des données déduites ou dérivées créent de tels biais en raison de leurs propres problèmes techniques. Si ces données biaisées alimentent le profilage ou la prise de décision automatisée, cela pourrait avoir des conséquences sociales inacceptables. Bien entendu, si la recherche implique l'utilisation de l'IA, cela augmentera probablement le risque lié aux biais (voir la sous-section "Licéité, loyauté et transparence" de la section "Concepts principaux" de la partie II des présentes lignes directrices).

Afin d'éviter un tel scénario, une **évaluation critique de la provenance des données est nécessaire**. À cette fin, des mesures organisationnelles doivent être mises en œuvre pour garantir la précision et la fiabilité des données collectées, tout en s'en remettant en fin de compte au droit des utilisateurs de ne pas divulguer des informations privées (par exemple, en confirmant si un enregistrement est exact ou non). En outre, la réalisation d'un audit consacré à la détection des biais dans les données brutes ou dans les

---

[756] Voir les lignes directrices du pilier de l'OCSE " D4.1 : Legal and Policy Framework and Federation Blueprint " (2021), p. 44 et suivantes. À l'adresse : https://repository.eosc-pillar.eu/index.php/s/tbqe6B7rDycdFCJ#pdfviewer

[757] Les TET peuvent être subdivisés en TET "ex ante" et TET "ex post". Les TET ex ante guident le processus décisionnel de l'utilisateur avant qu'il ne fasse son choix quant à la divulgation de données à caractère personnel à un responsable du traitement. Inversement, les TET ex post visualisent les données personnelles divulguées de manière à rendre transparents les processus qui ont eu lieu depuis que l'utilisateur a divulgué ses données (voir P. Murmann ; S. Fischer-Hübner, `Usable Transparency Enhancing Tools - A Literature Review' (2017), document de travail. À l'adresse : http://www.diva-portal.org/smash/get/diva2:1119515/FULLTEXT02.pdf).

[758] Université de York, **Guidelines for the Use of Social Media Data in Research**, à l'adresse : https://www.york.ac.uk/staff/research/governance/research-policies/social-media-data-use-research/.

ensembles de données déduites ou dérivées est nécessaire, en particulier lorsque les responsables du traitement utilisent des ensembles de données produits via les réseaux sociaux.

5.2 Transparence

Les bases de recherche sur les données recueillies via les réseaux sociaux impliquent souvent le traitement d'un grand nombre de données personnelles. Cela crée un scénario complexe. Les responsables du traitement doivent être conscients que, même si cela peut être difficile à réaliser, les personnes concernées doivent être en mesure de comprendre comment, et dans quel but, leurs données personnelles sont utilisées. En général, cela signifie que **les chercheurs doivent utiliser des outils capables de fournir ces connaissances de la manière la plus simple possible.** L'explicabilité est particulièrement importante dans le cas du traitement automatique des données ou du profilage. "Les méthodes permettant de donner des informations, d'offrir un droit de refus ou de demander un consentement **doivent être aussi conviviales que possible.** Par conséquent, les politiques d'information doivent se concentrer sur les informations compréhensibles par l'utilisateur et ne doivent pas se limiter à une politique générale de confidentialité sur le site web des responsables du traitement". [759]

Si le responsable du traitement "prévoit" d'effectuer un traitement à des fins autres que celles pour lesquelles les données ont été collectées à partir du réseau social, il doit informer au préalable les utilisateurs ou les personnes concernées de ce nouveau traitement, en fournissant des informations et en se conformant à toutes les autres exigences, telles que l'existence d'une base juridique pour cette nouvelle finalité ou la réalisation d'une évaluation de la compatibilité (voir la sous-section "Principe de limitation de la finalité" de la section "Concepts principaux" de la partie II des présentes lignes directrices). Bien entendu, les exigences de transparence sont clairement liées au principe de loyauté, puisque plus il est difficile pour l'utilisateur de comprendre le traitement des données, plus la différence entre les différents types d'utilisateurs est grande. En général, "plus la quantité de données est importante, plus il est difficile d'en avoir un aperçu clair et intelligible sous forme de texte. Les symboles offrent un moyen de représenter les catégories de données personnelles d'une manière allégée et reconnaissable. Pour cela, il faut des représentations graphiques significatives et auto-explicatives des données. "[760]

Selon le RGPD, les informations qu'un responsable de traitement doit fournir aux personnes concernées varient selon que ces informations ont été obtenues auprès d'elles ou non. Si les données personnelles ne sont pas obtenues auprès de l'utilisateur (art. 14 du RGPD), comme dans le cas de la réception des données d'un réseau social, le responsable du traitement doit être particulièrement attentif à fournir à la personne concernée une information adéquate, d'autant plus qu'une collecte massive de données

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

[760] Bier C., Kühne K., Beyerer J. (2016) PrivacyInsight : Le tableau de bord de la vie privée de nouvelle génération. In : Schiffner S., Serna J., Ikonomou D., Rannenberg K. (eds) Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science, vol 9857. Springer, Cham. https://doi.org/10.1007/978-3-319-44760-5_9

est effectuée. Ainsi, les responsables du traitement doivent informer l'utilisateur des dispositions de l'art. 14 du RGPD[761] .

Il est toutefois nécessaire de mentionner que, parfois, il peut être extrêmement difficile pour les responsables du traitement qui ont recueilli les données à partir d'un réseau social d'informer les personnes concernées du traitement. Si tel est le cas, ils peuvent rappeler l'article 14.5 (b), qui stipule que "la fourniture de cette information s'avère impossible ou impliquerait un effort disproportionné, notamment pour les traitements à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, sous réserve des conditions et garanties visées à l'article 89, paragraphe 1, ou dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de nuire gravement à la réalisation des finalités de ce traitement " (voir la sous-section "Protection des données et recherche scientifique" de la section "Concepts principaux " de la partie II des présentes lignes directrices).

Dans ce cas, le responsable du traitement doit prendre les mesures appropriées pour protéger les droits et libertés et les intérêts légitimes de la personne concernée, y compris en rendant l'information accessible au public (voir la sous-section "Droit à l'information" de la section "Droits de la personne concernée" de la partie II des présentes lignes directrices). Ainsi, en principe, les responsables du traitement pourraient éviter de fournir des informations sur le traitement aux personnes concernées si cela est rendu impossible, mais seulement s'ils *prennent des mesures appropriées pour protéger les droits et libertés et les intérêts légitimes de la personne concernée, y compris en rendant les informations accessibles au public.*

Notez toutefois avec prudence que l'effort disproportionné peut, dans certaines juridictions, être interprété de manière étroite. Par exemple, une décision récente (mars 2019) de l'autorité polonaise de protection des données (APD polonaise) a condamné une entreprise d'extraction de données à une amende de 220 000 € pour avoir omis de fournir des avis de confidentialité à 5,7 millions de personnes dont les données avaient été extraites d'un registre public. L'APD polonaise a rejeté l'argument selon lequel le placement d'un avis de confidentialité sur le site web de l'entreprise d'extraction de données était suffisant pour informer les individus, en particulier lorsque les individus ne savaient pas que leurs données avaient été extraites et étaient traitées.[762]

Liste de contrôle : loyauté et transparence
Loyauté
- Les responsables du traitement réalisent des audits visant à détecter des biais dans les jeux de données construits et/ou les conclusions de l'analyse.
- Les responsables du traitement ont mis en place des mesures adéquates pour éviter les biais provoqués par l'utilisation d'outils d'IA.

[761] Voir : CNIL, La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial, à l'adresse : https://www.cnil.fr/fr/la-reutilisation-des-donnees-publiquement-accessibles-en-ligne-des-fins-de-demarchage-commercial.
[762] Campbell, Fiona, Data Scraping - Considering the Privacy Issues, à l'adresse : https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues.

Transparence

 Le responsable du traitement fournit

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

 Les données à caractère personnel n'ayant pas été fournies par la personne concernée, les responsables du traitement ont fourni toutes les informations énumérées à l'article 14.1 du RGPD ;

 Les données personnelles n'étant pas fournies par la personne concernée, les informations sont fournies :

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

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

 Si la fourniture des informations est rendue impossible, les responsables du traitement prennent des mesures appropriées pour protéger les droits et libertés et les intérêts légitimes de la personne concernée, y compris en rendant les informations accessibles au public.

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

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

Le principe de minimisation (voir la sous-section "Principe de minimisation" de la section "Concepts principaux" au sein de la partie II des présentes lignes directrices) stipule que les données à caractère personnel doivent être **adéquates**, **pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées. D'autre part, selon l'article 5, paragraphe 1, point e), du RGPD, les données à caractère personnel doivent être "conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées". Enfin, la limitation de la finalité signifie que les données à caractère personnel ne peuvent pas être traitées à des

fins autres que celles stipulées dans la politique de confidentialité au moment de la collecte des données, à moins que ces autres finalités soient compatibles avec les finalités initiales et en vertu de garanties appropriées (art. 6.4 du RGPD). Par exemple, le traitement ultérieur correspond à des activités d'archivage d'intérêt public, à des fins de recherche scientifique et historique ou à des fins statistiques (voir la sous-section "Traitement des données et recherche scientifique" des "Concepts principaux" au sein de la partie II des présentes lignes directrices).

La combinaison de ces trois principes crée un outil normatif combiné qui doit être strictement suivi par les responsables du traitement utilisant des données recueillies par le biais des réseaux sociaux. En général, les responsables du traitement[763] doivent rendre explicites les finalités du traitement : "divulguées, expliquées ou exprimées sous une forme intelligible". Conformément au principe de minimisation des données, ils doivent également identifier la quantité minimale de données à caractère personnel nécessaire pour atteindre leurs objectifs. En outre, en ce qui concerne le principe de responsabilité, les responsables du traitement doivent être en mesure de démontrer qu'ils ne collectent et ne conservent que les données à caractère personnel nécessaires, et qu'elles ne sont utilisées que pour les finalités spécifiques qui ont été informées en vertu d'une base juridique adéquate.

En résumé, la fixation d'objectifs clairs pour le traitement permettra de s'assurer que les données personnelles à traiter sont :

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

6.1 Principe de minimisation

Le principe de minimisation stipule que les données à caractère personnel doivent être **adéquates**, **pertinentes et limitées à ce qui est nécessaire au regard des finalités** pour lesquelles elles sont traitées. (Voir la section "Minimisation des données" dans la section "Principes" de la partie II des présentes lignes directrices). Selon ce principe, les responsables du traitement doivent être conscients de l'objectif à atteindre par le biais du traitement, afin d'éviter d'utiliser plus de données que nécessaire. En outre, les responsables du traitement doivent également essayer d'éviter d'utiliser des catégories spéciales de données à caractère personnel si elles ne sont pas strictement nécessaires.

Lorsque les chercheurs/innovateurs recueillent des données sur les réseaux sociaux, ils peuvent finir par traiter beaucoup plus de données personnelles et sensibles qu'ils n'en ont réellement besoin pour les finalités spécifiques de la recherche. Il existe plusieurs moyens d'éviter un tel scénario. En principe, les responsables du traitement **devraient promouvoir l'utilisation de données anonymes** (voir la section "Identification, pseudonymisation et anonymisation" de la partie II, section "Concepts

[763] Il est important d'identifier qui est le "responsable du traitement des données" ; les développeurs sont rarement les "responsables du traitement des données", car ils ne sont pas chargés de s'occuper de l'objectif commercial, cette tâche revenant à la direction de l'entreprise.

principaux" des présentes lignes directrices). En effet, éviter l'identification d'individus spécifiques à partir de l'analyse des big data, ou la ré-identification d'utilisateurs de données dont les données ont été pseudonymisées, est une garantie fondamentale pour prévenir l'impact indu sur les personnes concernées par le traitement des données[764] . S'ils n'ont pas besoin de données personnelles, ils pourraient demander au réseau social de leur fournir des données anonymisées. Bien entendu, ils peuvent également rendre anonymes les données une fois qu'elles ont été collectées, mais, dans ce cas, ils ne doivent pas oublier **que l'anonymisation implique un traitement des données et qu'ils doivent donc disposer d'une base juridique qui la légitime** (voir la sous-section "Identification, pseudonymisation et anonymisation" dans la section "Concepts principaux" de la partie II des présentes lignes directrices).

En outre, les chercheurs/innovateurs doivent garder à l'esprit que l'anonymat peut être difficile à atteindre. Très souvent, l'agrégation et la déduction des pratiques en matière de données peuvent facilement désanonymiser les ensembles de données. Ainsi, les **responsables du traitement ne doivent pas présumer que leurs processus d'anonymisation permettront de préserver la vie privée des personnes concernées. En effet, ils doivent effectuer des AIPD et des évaluations des risques pour s'en assurer** (voir Responsabilité dans cette partie des lignes directrices).

Une alternative à l'anonymisation en tant que telle est l'utilisation de **données agrégées**. Dans le contexte de la protection des données, il convient de distinguer deux types d'agrégation (voir la section "Minimisation des données" dans la section "Principes" de la partie II des présentes lignes directrices) :

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

Lorsque la finalité du traitement peut être atteinte en utilisant des données agrégées, cela est recommandé (voir la sous-section "Principe de minimisation des données" de la section "Principes" de la partie II des présentes lignes directrices). Dans ces circonstances, personne d'autre que la personne concernée ne devrait accéder aux données brutes (données obtenues ou observées), à moins qu'une raison extrêmement pertinente ne s'applique (par exemple, les questions de sécurité nationale interprétées de manière restrictive). En effet, il arrive qu'une recherche spécifique n'ait besoin que de données agrégées et n'ait pas besoin des données brutes collectées dans les réseaux sociaux. Par conséquent, les **responsables du traitement doivent supprimer les données brutes dès qu'ils ont extrait les données nécessaires à leur traitement**. En

[764] Les lignes directrices 3/2013 du WP29 sur la limitation de la finalité (p. 3) soulignent que l'adoption de garanties visant à prévenir les impacts indus sur les personnes concernées est un facteur clé à prendre en compte lors de l'évaluation des utilisations ultérieures compatibles des données.

principe, la suppression doit avoir lieu au point le plus proche de la collecte des données brutes (par exemple, sur le même appareil après le traitement).

6.2 Limitation de la finalité

Le principe de limitation de la finalité (voir la section "Principes" de la sous-section "Limitation de la finalité" de la partie II des présentes lignes directrices) exige que les données personnelles collectées soient traitées uniquement dans le but pour lequel elles ont été recueillies. La limitation de la finalité est un concept clé lors du traitement des données obtenues à partir des réseaux sociaux et la plupart des plateformes l'incluent dans leurs politiques de développement. Les chercheurs et les innovateurs doivent suivre strictement ces politiques. D'autre part, il est souvent vrai que les personnes concernées ne sont pas vraiment conscientes des autorisations qu'elles fournissent aux réseaux sociaux pour le traitement. C'est une raison particulièrement importante pour laquelle les responsables du traitement utilisant ces données ne doivent pas les traiter à des fins qui pourraient être considérées comme incompatibles avec le consentement initial.

Ainsi, les **responsables du traitement doivent mettre en œuvre des outils permettant de garantir que le traitement n'a pas lieu si les personnes concernées ne donnent pas leur consentement, à moins qu'une autre base juridique ne permette le traitement (**voir la sous-section "Licéité, loyauté et transparence" des "Principes" de la partie II des présentes Lignes directrices). L'utilité des données stockées pour la finalité de la recherche devra être périodiquement réévaluée afin d'éviter tout traitement illégal des données.

Il convient de noter que lorsque les données sont utilisées pour des raisons d'intérêt public ou à des fins de recherche, d'archivage ou de statistiques, ces utilisations dérivées ne seront pas considérées comme incompatibles avec les finalités initiales, à condition qu'elles soient correctement pseudonymisées, chaque fois que le traitement ultérieur de ces données ne permet pas de ré-identifier les personnes concernées (art. 5.1.b & 89.1 RGPD) (voir la section "Examiner si le cadre réglementaire concernant la recherche scientifique s'applique à l'activité" dans cette partie des Lignes directrices).

6.3 Limitation du stockage

Le principe de limitation de la conservation oblige les responsables du traitement des données à ne pas conserver les données à caractère personnel "pendant une durée supérieure à celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées" et à introduire des mesures de pseudonymisation et d'anonymisation qui réduisent/suppriment l'identifiabilité des personnes concernées dès que possible à ces fins. Le problème ici est qu'habituellement les réseaux sociaux peuvent utiliser les données stockées à des fins différentes. En outre, il arrive que les données soient collectées et stockées "juste au cas où" elles pourraient servir à une utilisation future. Les responsables du traitement doivent être conscients du fait que, même si le RGPD autorise le stockage pendant des périodes plus longues, il **doit y avoir une bonne et réelle raison d'opter pour une telle période prolongée (**voir la sous-section "Principe de limitation du stockage" dans la section "Principes" de la partie II des présentes lignes directrices). En d'autres termes, un responsable du traitement ne doit pas être tenté de

conserver les données plus longtemps que ce qui est strictement nécessaire, dans le but de les avoir à disposition au cas où des finalités ou des projets nouveaux se présenteraient à l'avenir, différents de ceux qui sont légalement autorisés.

Afin d'éviter un stockage illicite, un test de nécessité doit être effectué par chacune des parties prenantes à la fourniture d'un service spécifique dans le réseau social, les finalités de leurs traitements respectifs pouvant en effet être différentes. Par exemple, les données personnelles communiquées par les utilisateurs lorsqu'ils s'abonnent à un service spécifique du réseau social doivent être supprimées dès qu'ils mettent fin à l'abonnement. De même, les informations supprimées de leur compte par les utilisateurs ne doivent pas être conservées. Lorsque les utilisateurs n'utilisent pas le réseau social pendant une période définie, le profil de l'utilisateur doit être considéré comme inactif. Après une autre période, les données doivent être supprimées. Les utilisateurs doivent être informés avant que ces mesures ne soient prises, par tous les moyens dont dispose la partie prenante concernée.[765]

En résumé, si les responsables du traitement n'ont pas besoin des données et qu'aucune raison juridique obligatoire ne les oblige à les conserver, ils doivent les rendre totalement anonymes ou les supprimer. Les chercheurs doivent consulter leur DPD s'ils souhaitent conserver les données pendant une période plus longue et connaître la réglementation nationale applicable.

Ce pourrait également être un excellent moment pour **envisager des délais d'effacement des différentes catégories de données, et documenter clairement ces décisions** (voir la sous-section "Principe de responsabilité" dans la section "Principes" de la partie II des présentes lignes directrices). À cet égard, il convient de préserver l'équilibre approprié entre la durabilité de la recherche, la reproductibilité, l'ouverture des données, la science ouverte et le principe de minimisation prévu par le RGPD, en considérant également que le traitement d'ensembles de données pseudo/anonymisées pourrait générer des ensembles de données pseudo/identifiables. À cette fin, il convient de suivre les critères énoncés dans la recommandation 156 du RGPD:

(1) le traitement des données à caractère personnel à des fins de recherche scientifique doit être soumis à des garanties appropriées pour les droits et libertés de la personne concernée lorsqu'il est assuré, en particulier que des mesures techniques et organisationnelles sont mises en œuvre pour respecter le principe de minimisation des données ;

(2) le traitement ultérieur des données à caractère personnel devrait avoir lieu lorsque le responsable du traitement a évalué la possibilité de réaliser ces finalités au moyen d'un traitement des données qui ne permet pas l'identification des personnes concernées ou qui offre des garanties suffisantes de pseudonymisation ;

(3) les conditions et garanties en question peuvent inclure des procédures spécifiques permettant aux personnes concernées d'exercer leurs droits, ainsi que des mesures techniques et organisationnelles visant à minimiser le traitement des données à caractère personnel conformément aux principes de proportionnalité et de nécessité.

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

Liste de contrôle : gouvernance des données
Minimisation

 Le responsable du traitement ne traite que des données anonymisées ou pseudonymisées dans la mesure du possible.

 Le responsable du traitement traite la quantité minimale de données nécessaires pour atteindre les objectifs poursuivis.

 Le responsable du traitement ne traite les données des catégories spéciales que si cela est strictement nécessaire.

Limitation de l'objet

 Les responsables du traitement n'utilisent les données que pour les finalités pour lesquelles elles ont été collectées, sauf si une base légale permet leur traitement licite.

Limitation du stockage

 Les responsables du traitement ne conservent pas les données à caractère personnel "plus longtemps que nécessaire pour les finalités pour lesquelles les données à caractère personnel sont traitées".

 Les contrôleurs vérifient l'utilité des données stockées pour l'objectif prévu de la recherche.

 Les données sont stockées d'une manière qui entrave autant que possible le traitement des données personnelles.
 Les responsables du traitement ont documenté toutes les informations concernant ces questions.

7 Responsabilité et contrôle

Le principe de responsabilité du RGPD est fondé sur le risque : plus le traitement des données présente un risque élevé pour les droits et libertés fondamentaux des personnes concernées, plus les mesures nécessaires pour atténuer ces risques sont importantes (voir la sous-section "Principe de responsabilité" dans la section "Principes" de la partie II des présentes lignes directrices)[766] . Étant donné que le traitement des données à caractère personnel recueillies sur les réseaux sociaux peut être considéré comme présentant un risque élevé,[767] , les chercheurs/innovateurs doivent également désigner

[766] 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.

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

un DPD et réaliser une AIPD. En outre, les responsables du traitement doivent élaborer une politique de protection des données qui permette la **traçabilité des informations** (voir la sous-section "Principe de responsabilité" dans la section "Principes" de la partie II des présentes lignes directrices).

7.1 Délégué à la protection des données

Dans la plupart des cas, la recherche en matière de TIC s'appuyant sur des données provenant de réseaux sociaux implique des opérations 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. Par conséquent, la désignation d'un DPD est obligatoire dans les conditions prévues par l'article 37, paragraphe 1, du règlement. Même si ce n'est pas le cas, **il est toujours recommandé de procéder à cette nomination, au moins en termes de transparence** (voir la sous-section "Principe de licéité, de loyauté et de transparence" dans la section "Principes" de la partie II des présentes lignes directrices)**.**

7.2 Analyse d'impact sur la protection des données

La réalisation d'une AIPD est souvent obligatoire dans le cas des réseaux sociaux, car elle implique une surveillance systématique d'un espace accessible au public à grande échelle (article 35, paragraphe 3, du RGPD). Même si ce n'était pas le cas, certaines autres circonstances pourraient la rendre obligatoire ou, au moins, fortement recommandée (voir la sous-section "Analyse de l'impact sur la protection des données" de la section "Principaux outils et actions" au sein de la partie II des présentes lignes directrices).

Liste de contrôle

- Le responsable du traitement a réalisé une AIPD pour l'activité de traitement. Le responsable du traitement s'est assuré qu'il :
  - A commencé le plus tôt possible (selon le principe de la protection des données dès la conception).
  - A fourni un aperçu clair de ce qu'est une AIPD.
  - A utilisé, dans la mesure du possible, les orientations et les modèles fournis par l'autorité de contrôle de la protection des données (APD) compétente. Si ce n'est pas le cas (par exemple, si l'autorité de contrôle de la protection des données ne fournit pas ce type de matériel ou si elle doit s'occuper de plusieurs domaines de compétence de différentes autorités de contrôle de la protection des données), l'autorité de contrôle de la protection des données a suivi les orientations fournies par le groupe de travail Article 29 dans le document wp248rev.01.
  - A réuni l'équipe nécessaire à la réalisation de l'analyse de l'impact sur la

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

protection des données.

- A réfléchi aux moyens de faciliter votre travail.

7.3 Concevoir votre politique de protection de la vie privée et préparer la documentation du traitement

La politique de confidentialité est le document public qui explique comment un projet de recherche traite les données personnelles et comment il applique les principes de protection des données, conformément aux articles 12-14 du RGPD. Toutes les personnes concernées doivent avoir accès à cette politique de confidentialité. Elle doit être documentée. Un modèle non officiel, mais recommandable, se trouve ici : https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf.

Les responsables du traitement doivent toujours garder à l'esprit que, dans le cas de données recueillies sur les réseaux sociaux, ils peuvent finir par mélanger différents ensembles de données ou créer des données déduites ou dérivées. La traçabilité du traitement, les informations sur l'éventuelle réutilisation des données et l'utilisation des données relatives à différents ensembles de données dans les mêmes ou différentes étapes du cycle de vie, doivent être assurées par les registres. Quiconque traite des données à caractère personnel (y compris les responsables du traitement et les sous-traitants) doit documenter ses activités, principalement à l'intention des autorités de contrôle qualifiées/pertinentes. Cela doit se faire par le biais de registres des activités de traitement qui sont conservés de manière centralisée par l'organisation pour l'ensemble de ses activités de traitement, et de documents supplémentaires qui se rapportent à une activité individuelle de traitement des données (voir la sous-section "Documentation du traitement" dans la section "Principaux outils et actions" de la partie II des présentes lignes directrices).

Les premières étapes du développement du projet sont le moment idéal pour mettre en place une méthode systématique de collecte de la documentation nécessaire, puisque c'est à ce moment-là que l'organisation conçoit et planifie l'activité de traitement[768] .

Enfin et surtout, les responsables du traitement doivent garder à l'esprit que les comités d'éthique joueront probablement un rôle clé dans le traitement des données personnelles. Toutefois, cela pourrait changer considérablement selon les secteurs et les pays. Les responsables du traitement doivent interroger leur DPD à ce sujet.

Enfin, les responsables du traitement ne doivent pas oublier qu'il peut y avoir des implications éthiques au-delà de la conformité légale. La consultation d'un expert en éthique des réseaux sociaux est toujours recommandée.

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

Liste de contrôle. Politique de confidentialité

- Le responsable du traitement a contacté le bureau/personne qui tient les registres de traitement pour l'organisation.
  - Si nécessaire, le délégué à la protection des données peut aider à établir ce contact.
- Le responsable du traitement a informé très tôt le bureau/personne susmentionné de son intention de traiter des données à caractère personnel.
  - Cette activité de traitement doit être inscrite dans les registres avant le début du traitement.
- Le responsable du traitement a suivi les instructions sur :
  - les informations nécessaires pour fournir les registres de traitement,
  - le moment où le responsable du traitement doit envoyer des mises à jour de ces informations.

Documentation supplémentaire relative à une seule activité de traitement.

Les éléments suivants doivent être documentés :

- Évaluation du fait que l'activité de traitement entraîne un risque élevé pour les droits et les libertés de personnes physiques.
- Analyse d'impact sur la protection des données lorsque l'évaluation ci-dessus donne un résultat positif.
- Potentielle consultation de l'autorité de contrôle compétente avant le traitement.
- Requêtes et tests d'acceptation pour l'achat et/ou le développement des logiciels, du matériel et de l'infrastructure employés.
- Implémentation des mesures techniques et organisationnelles.
- Tests réguliers, évaluation et enregistrement de l'efficacité des mesures techniques et organisationnelles.
- Requêtes et tests d'acceptation pour la sélection des sous-traitants.
- Contrats stipulés avec les sous-traitants.
- Possibles inspections et audits du sous-traitant.
- Méthode de collecte du consentement.
- Démonstrations de l'expression individuelle du consentement.
- Informations fournies aux personnes concernées.
- Mise en œuvre des droits des personnes concernées.
- Traitement effectif des droits des personnes concernées.
- Possible notification des violations à l'autorité de contrôle compétente.
- Possible communication des violations de données à la personne concernée.

Toute autre communication avec l'autorité de contrôle compétente.

8 Intégrité et confidentialité

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

Ce principe comporte trois aspects principaux : l'intégrité, la confidentialité et la disponibilité. La disponibilité et l'intégrité sont en quelque sorte liées, puisque seules les données correctement préservées peuvent être mises à la disposition de la personne concernée. La confidentialité, en revanche, est une question plus complexe qui mérite des mesures complexes en raison du type de processus concernés et des risques inhérents à ces processus.

8.1 Disponibilité et intégrité

La recherche alimentée par l'utilisation des données des réseaux sociaux implique parfois la collecte d'une quantité impressionnante de données. Le traitement de ces données a généralement lieu dans des endroits éloignés dans le nuage et, pour pouvoir les atteindre, il est nécessaire d'utiliser des réseaux partagés, des réseaux publics, etc. Dans ces circonstances, il **est généralement extrêmement difficile de mettre toutes les données à la disposition des personnes concernées.** Par ailleurs, il convient de noter que l'intégrité des données peut être compromise par la manière dont elles sont partagées et stockées. Il se peut que l'un des sous-traitants ou des responsables du traitement conjoints supprime ou endommage les données à un moment donné. Afin d'éviter de tels scénarios, il est fortement recommandé de réaliser des copies de sauvegarde. Leur création doit être prévue dès les premières étapes de la recherche.

8.2 Effectuer une analyse des risques de sécurité

Selon le principe de confidentialité, les responsables du traitement doivent minimiser les risques pour les droits, intérêts et libertés des personnes concernées. À cette fin, ils doivent adopter une approche fondée sur le risque (voir la sous-section "Intégrité et confidentialité" dans la section "Principes" de la partie II des présentes lignes directrices). Dans tous les cas, les responsables du traitement doivent s'assurer qu'ils respectent les exigences en matière de protection des données et qu'ils sont en mesure de montrer comment ils s'y conforment, par exemple au moyen de documents (voir la sous-section "Responsabilité" dans la section "Principes" de la partie II des présentes lignes directrices).

Pour gérer les risques pour les personnes qui découlent du traitement des données à caractère personnel recueillies sur les réseaux sociaux, il est important que les responsables du traitement acquièrent une compréhension et une articulation mûres des

droits fondamentaux, des risques et de la manière de mettre en balance ces intérêts et d'autres. En définitive, il est nécessaire que les responsables du traitement évaluent les risques que l'utilisation des données fait peser sur les droits des personnes, qu'ils déterminent la manière dont ils doivent y faire face et qu'ils établissent l'impact que cela a sur leur utilisation à des fins de recherche. À cette fin, deux facteurs clés doivent être pris en considération : . [769]

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

Afin de minimiser ces risques, les responsables du traitement doivent s'assurer que des mesures techniques et organisationnelles appropriées sont mises en œuvre pour éliminer, ou au moins atténuer, le risque pour la sécurité, en réduisant la probabilité que les menaces identifiées se concrétisent, ou en réduisant leur impact. Il est nécessaire de prendre en compte les normes de sécurité qui existent déjà sur le marché, ainsi que les normes de conformité en matière de protection des données qui s'appliqueront au traitement. En outre, les développeurs doivent toujours se rappeler que l'article 32, paragraphe 4, du RGPD précise qu'un élément important de la sécurité consiste à s'assurer que "toute personne physique agissant sous l'autorité du responsable du traitement ou du sous-traitant qui a accès à des données à caractère personnel ne les traite que sur instruction du responsable du traitement, à moins que le droit de l'Union ou des États membres ne l'exige" (voir la sous-section "Intégrité et confidentialité" dans la section "Principes" de la partie II des présentes lignes directrices).

La description générale des mesures de sécurité techniques et organisationnelles doit faire partie des registres de traitement, si possible (article 30, paragraphe 1, point g), pour les responsables du traitement, et article 30, paragraphe 2, point d), pour les sous-traitants) et toutes les mesures mises en œuvre doivent faire partie de l'AIPD, en tant que mesures correctives pour limiter le risque. Enfin, une fois les mesures sélectionnées mises en œuvre, le risque résiduel restant doit être évalué et maintenu sous contrôle. L'analyse des risques et l'AIPD sont les outils qui s'appliquent. L'évaluation des risques et les décisions prises "doivent être documentées afin de se conformer à l'exigence de protection des données dès la conception" (de l'article 25 du RGPD) (voir la sous-section "Protection des données dès la conception et par défaut (**DPbDD**)" dans la section "Concepts principaux" de la partie II de ces lignes directrices).

Enfin, les responsables du traitement doivent toujours être conscients que, conformément à l'article 32, paragraphe 1, point d), du RGPD, la protection des données est un processus. Par conséquent, **ils doivent tester, apprécier et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles**. Les procédures qui aident les responsables du traitement à identifier les changements qui déclencheraient un réexamen de l'AIPD doivent être créées à ce moment-là. Dans la mesure du possible, les responsables du traitement doivent essayer d'imposer un modèle

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

dynamique de suivi des mesures en jeu (voir la sous-section "Intégrité et confidentialité" dans la section "Principes" de la partie II des présentes lignes directrices).

Liste de contrôle : intégrité et confidentialité

 Les responsables du traitement ont mis en place les procédures nécessaires pour garantir que les droits des personnes concernées sont adéquatement satisfaits, que les personnes concernées soient les utilisateurs finaux ou des tiers.

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

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

 Les personnes concernées sont en mesure d'avoir accès à toutes leurs données personnelles, y compris les données brutes qui sont collectées sur les réseaux sociaux.

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

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

 Les responsables de traitement ont mis en place des outils capables de garantir que toutes les données sont efficacement effacées à la demande des personnes concernées si aucune raison légitime ne s'oppose à cette demande.

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

(1) toute donnée collectée par un moyen spécifique ;

(2) un type spécifique de données collectées par tout moyen ;

(3) un traitement de données spécifique.

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

9 Droits des personnes concernées

Le chapitre III du RGPD prévoit un ensemble de droits que les personnes concernées peuvent exercer pour protéger leurs données personnelles. Bien que chaque droit

comporte des détails et des questions spécifiques susceptibles d'affecter et d'être affectés par la recherche et le développement dans le domaine des TIC (voir la sous-section "Protection des données et recherche scientifique" dans la section "Concepts principaux" de la partie II des présentes lignes directrices), ils partagent tous certaines caractéristiques générales concernant la transparence de leur information, de leur communication et de leurs modalités d'exercice (article 12 du RGPD). Dans cette section, nous analysons chaque droit spécifique à la lumière d'un traitement qui utilise des données recueillies sur les réseaux sociaux. Cependant, étant donné que nous avons déjà analysé le droit à l'information (voir la section "Transparence" de cette partie des Lignes directrices), et que le droit de ne pas faire l'objet d'une prise de décision automatisée a été largement abordé dans la section "Capacité d'action humaine" de cette partie des Lignes directrices, nous allons maintenant nous concentrer sur les droits restants.

9.1 Droit d'accès

L'article 12, point a), prévoit que les personnes concernées ont le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel les concernant sont ou ne sont pas traitées et, si tel est le cas, d'accéder à ces données (voir la sous-section "Droit d'accès" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). En bref, la personne concernée a le droit d'obtenir du responsable du traitement des informations sur (1) les données à caractère personnel stockées ainsi que leurs catégories, (2) la source et les destinataires des données à caractère personnel auxquels les données sont communiquées, (3) la connaissance de la logique impliquée dans le traitement automatique des données concernant la personne concernée, et (4) la finalité du traitement des données à caractère personnel. L'ensemble de ces exigences figure à l'article 15 du RGPD. **Ce droit est particulièrement important dans le cas des données recueillies sur les réseaux sociaux, car les personnes concernées ne sont généralement pas conscientes de l'existence de ces données. En outre, des données déduites peuvent être créées par le responsable du traitement et ces données peuvent présenter un intérêt particulier pour la personne concernée.** Ainsi, les responsables du traitement doivent s'assurer qu'ils ont mis en place des outils adéquats pour satisfaire les exigences des personnes concernées conformément aux précisions incluses dans le RGPD.

9.2 Droit de rectification

Comme le prévoit l'article 16 du RGPD, les personnes concernées ont le droit de faire rectifier leurs données personnelles (voir la sous-section "Droit de rectification" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). Cela est particulièrement pertinent dans le cas des données recueillies sur les réseaux sociaux, car les personnes concernées peuvent fournir des informations fausses ou inexactes en raison d'un manque de compréhension des implications qu'elles pourraient avoir. Les responsables du traitement sont tenus de communiquer les données rectifiées à chaque destinataire auquel les données à caractère personnel ont été divulguées, sauf si cela s'avère impossible ou implique des efforts disproportionnés. Les responsables du traitement ne peuvent pas faire valoir que la gestion de grands

ensembles de données est trop complexe pour garantir la rectification afin d'éviter cette exigence.

9.3 Droit à l'effacement

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

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

9.4 Droit de limitation le traitement

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

Étant donné qu'un responsable du traitement autre que le réseau social qui a recueilli les données à l'origine est impliqué dans le traitement, il serait bon de garder à l'esprit que ce droit peut être exercé par n'importe lequel des acteurs impliqués, qui devrait informer les autres de cette exigence et procéder en conséquence. Dans ce contexte, il peut être très utile de développer des accords de partage des données qui aident à clarifier les responsabilités attribuées à chacun de ces rôles dans l'exécution des activités spécifiques de traitement des données à réaliser, si les politiques de développement ne clarifient pas cette question.

9.5 Droit d'opposition

Les personnes concernées doivent avoir la possibilité de révoquer tout consentement préalable donné à un traitement de données spécifique et de s'opposer au traitement des données les concernant (voir la sous-section "Droit d'opposition" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). L'exercice de ce droit doit être possible sans aucune contrainte technique ou organisationnelle et les

outils fournis pour enregistrer ce retrait doivent être accessibles, visibles et efficaces. Ainsi, les chercheurs/innovateurs devraient mettre cette option à la disposition des personnes concernées dès qu'ils commencent à traiter les données recueillies sur les réseaux sociaux.

9.6 Droit à la portabilité des données

Conformément au RGPD, les personnes concernées ont un droit à la portabilité (voir la sous-section "Droit à la portabilité" dans la section "Droits des personnes concernées" de la partie II des présentes lignes directrices). Pour satisfaire à cette exigence, les responsables du traitement doivent stocker les données dans des formats normalisés qui permettent aux personnes concernées de transmettre les données qu'elles ont fournies d'une application automatisée, telle qu'un réseau social, à une autre. [770]

Quoi qu'il en soit, il est nécessaire de souligner que le droit à la portabilité des données ne s'applique qu'aux données "concernant" la personne concernée et aux données qu'elle a "fournies" au responsable du traitement. Par conséquent, les données anonymes et les données inférées ou dérivées ne sont pas incluses dans le droit à la portabilité, puisque les données anonymes ne concernent pas la personne concernée et que les données inférées ou dérivées n'ont pas été fournies par la personne concernée.

Liste de contrôle : droits des personnes concernées

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

- Les responsables de traitement ont mis en place les procédures nécessaires pour que les droits des personnes concernées soient satisfaits dans les délais (maximum un mois après la demande, prolongeable de deux mois supplémentaires au regard de la complexité de la tâche et du nombre de demandes).

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

- Les personnes concernées sont en mesure d'avoir accès à toutes leurs données personnelles, y compris les données observées, obtenues, dérivées et déduites.

- Les responsables du traitement ont fourni aux personnes concernées un accès à distance à leurs données personnelles. En particulier, les responsables du traitement qui fournissent des services en ligne basés sur des données à caractère personnel ont fourni un outil en ligne à cette fin.

- Les responsables de traitement ont mis en place des outils capables de

[770] Voir I. GRAEF, Mandating Portability and Interoperability in Online Social Networks : Enjeux réglementaires et de droit de la concurrence dans l'Union européenne (22 juillet 2013). Politique des télécommunications 2015, vol. 39, n° 6, p. 502-514.

communiquer les données rectifiées à chaque destinataire auquel les données personnelles ont été divulguées, sauf si cela s'avère impossible ou implique des efforts disproportionnés.

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

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

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