

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



17/FR

WP251rev.01

**Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage
aux fins du règlement (UE) 2016/679**

Adoptées le 3 octobre 2017

Version révisée et adoptée le 6 février 2018

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

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

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

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

TABLE DES MATIERES

I. INTRODUCTION	5
II. DEFINITIONS.....	6
A. PROFILAGE	7
B. PRISE DE DECISION AUTOMATISEE	8
C. MANIERE DONT LE RGPD ABORDE LES CONCEPTS	9
III. DISPOSITIONS GENERALES SUR LE PROFILAGE ET LA PRISE DE DECISION AUTOMATISEE	10
A. PRINCIPES DE LA PROTECTION DES DONNEES	10
1. Article 5, paragraphe 1, point a) - Licéité, loyauté et transparence	10
2. Article 5, paragraphe 1, point b) – Traitement ultérieur et limitation des finalités.....	11
3. Article 5, paragraphe 1, point c) – Minimisation des données	12
4. Article 5, paragraphe 1, point d) – Exactitude	12
5. Article 5, paragraphe 1, point e) – Limitation de la conservation	13
B. BASES LEGALES DU TRAITEMENT	13
1. Article 6, paragraphe 1, point a) – Consentement.....	13
2. Article 6, paragraphe 1, point b – Nécessaire à l’exécution d’un contrat.....	14
3. Article 6, paragraphe 1, point c) – Nécessaire au respect d’une obligation légale.....	15
4. Article 6, paragraphe 1, point d) – Nécessaire à la sauvegarde des intérêts vitaux.....	15
5. Article 6, paragraphe 1, point e) – Nécessaire à l’exécution d’une mission d’intérêt public ou relevant de l’exercice de l’autorité publique.....	15
6. Article 6, paragraphe 1, point f) – Nécessaire aux fins des intérêts légitimespoursuivis par le responsable du traitement ou par un tiers	15
C. ARTICLE 9 – CATEGORIES PARTICULIERES DE DONNEES	16
D. DROITS DE LA PERSONNE CONCERNEE	17
1. Articles 13 et 14 – Droit d’être informé	18
2. Article 15 – Droit d’accès.....	18
3. Article 16 – Droit de rectification, article 17 – Droit à l’effacement et article 18 – Droit à la limitation du traitement	19
4. Article 21 – Droit d’opposition	20
IV. DISPOSITIONS SPECIFIQUES CONCERNANT LA PRISE DE DECISION EXCLUSIVEMENT AUTOMATISEE DEFINIE A L’ARTICLE 22	21
A. «DECISION FONDEE EXCLUSIVEMENT SUR UN TRAITEMENT AUTOMATISE»	22
B. «PRODUISANT DES EFFETS JURIDIQUES A L’EGARD D’UNE PERSONNE PHYSIQUE» OU «L’AFFECTANT DE MANIERE SIGNIFICATIVE DE FAÇON SIMILAIRE».....	23
C. EXCEPTIONS A L’INTERDICTION	25

1.	<i>Exécution d'un contrat</i>	25
2.	<i>Autorisée par le droit de l'Union ou le droit de l'État membre</i>	26
3.	<i>Consentement explicite</i>	26
D.	CATEGORIES PARTICULIERES DE DONNEES A CARACTERE PERSONNEL – ARTICLE 22, PARAGRAPHE 4.....	27
E.	DROITS DE LA PERSONNE CONCERNEE.....	27
1.	<i>Articles 13, paragraphe 2, point f), et article 14, paragraphe 2, point g) – Droit d'être informé</i>	27
2.	<i>Article 15, paragraphe 1, point h) – Droit d'accès</i>	30
F.	ÉTABLISSEMENT DE GARANTIES APPROPRIÉES.....	30
V.	ENFANTS ET PROFILAGE	31
VI.	ANALYSES D'IMPACT RELATIVES A LA PROTECTION DES DONNEES ET DELEGUE A LA PROTECTION DES DONNEES	33
	ANNEXE 1 – RECOMMANDATIONS DE BONNES PRATIQUES	35
	ANNEXE 2 – PRINCIPALES DISPOSITIONS DU RGPD	37
	PRINCIPALES DISPOSITIONS DU RGPD QUI FONT REFERENCE AU PROFILAGE ET A LA PRISE DE DECISION AUTOMATISEE EN GENERAL	38
	PRINCIPALES DISPOSITIONS DU RGPD QUI FONT REFERENCE A LA PRISE DE DECISION EXCLUSIVEMENT AUTOMATISEE DEFINIE A L'ARTICLE 22.....	39
	ANNEXE 3 - LECTURES COMPLEMENTAIRES	41

I. Introduction

Le règlement général sur la protection des données (RGPD) traite spécifiquement du profilage et de la prise de décision individuelle automatisée, y compris le profilage¹.

Le profilage et la prise de décision automatisée sont utilisés dans un nombre croissant de secteurs, tant privés que publics. La banque et la finance, la santé, la fiscalité, les assurances, la prospection et la publicité ne sont que quelques exemples de domaines où le profilage est régulièrement effectué pour faciliter la prise de décision.

Les progrès technologiques et les capacités en matière d'analyse de mégadonnées, d'intelligence artificielle et d'apprentissage automatique ont facilité la création de profils et la prise de décisions automatisées susceptibles d'avoir une incidence significative sur les droits et les libertés de chacun.

La disponibilité généralisée de données à caractère personnel sur internet et à partir de dispositifs IdO (internet des objets), et la capacité de trouver des corrélations et de créer des liens peuvent permettre de déterminer, d'analyser et de prédire des aspects de la personnalité, du comportement, des intérêts et des habitudes d'une personne.

Le profilage et la prise de décision automatisée peuvent être utiles pour les particuliers et les organisations, offrant des avantages tels que:

- une efficacité accrue; et
- des économies de ressources.

Ils présentent de nombreuses possibilités d'applications commerciales. Par exemple, ils peuvent être utilisés pour mieux segmenter les marchés et adapter les services et les produits aux besoins de chacun. La médecine, l'éducation, les soins de santé et les transports peuvent également tirer profit de ces processus.

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1–88). Le profilage et la prise de décision individuelle automatisée sont également couverts par la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. Bien que les présentes lignes directrices se concentrent sur le profilage et la prise de décision individuelle automatisée dans le cadre du RGPD, les orientations qu'elles fournissent sont également pertinentes en ce qui concerne les deux thèmes de la directive (UE) 2016/680, pour ce qui est des dispositions similaires au RGPD. L'analyse des caractéristiques spécifiques du profilage et de la prise de décision individuelle automatisée dans le cadre de la directive (UE) 2016/680 n'est pas incluse dans les présentes lignes directrices, puisque l'avis WP258 sur certaines questions clés de la directive (UE) 2016/680 (directive «police») [«Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)»], adopté par le groupe de travail «article 29» (GT29) le 29 novembre 2017, fournit des orientations à cet égard. Cet avis couvre la prise de décision individuelle automatisée et le profilage dans le contexte du traitement des données par les services répressifs aux pages 11 à 14 et est disponible à l'adresse suivante: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.

Cependant, le profilage et la prise de décision automatisée peuvent poser des risques importants pour les droits et libertés des personnes, qui nécessitent alors des garanties appropriées.

Ces processus peuvent être opaques. Il se peut que les particuliers ne sachent pas qu'ils font l'objet d'un profilage ou qu'ils ne comprennent pas ce que cela implique.

Le profilage peut perpétuer les stéréotypes existants et la ségrégation sociale. Il peut aussi enfermer des personnes dans une catégorie spécifique et les limiter aux préférences qui leur sont suggérées. Cela peut porter atteinte à leur liberté de choix en ce qui concerne, par exemple, certains produits ou services tels que des livres, de la musique ou des fils d'actualités. Dans certains cas, le profilage peut donner lieu à des prévisions inexactes. Dans d'autres cas, il peut conduire à un déni de services et de biens et à une discrimination injustifiée.

Le RGPD introduit de nouvelles dispositions qui permettent de faire face aux risques découlant du profilage et de la prise de décision automatisée, notamment, mais sans s'y limiter, en ce qui concerne la protection de la vie privée. Les présentes lignes directrices ont pour but de clarifier ces dispositions.

Le document couvre les aspects suivants:

- définitions du profilage et de la prise de décision automatisée, et de l'approche du RGPD dans ces domaines en général – [chapitre II](#)
- dispositions générales sur le profilage et la prise de décision automatisée – [chapitre III](#)
- dispositions spécifiques concernant la prise de décision exclusivement automatisée définie à l'article 22 – [chapitre IV](#)
- enfants et profilage – [chapitre V](#)
- analyses d'impact relatives à la protection des données et délégués à la protection des données – [chapitre VI](#)

Les annexes contiennent des recommandations sur les bonnes pratiques, en s'appuyant sur l'expérience acquise dans les États membres de l'Union européenne.

Le groupe de travail «article 29» sur la protection des données (GT29) contrôlera la mise en œuvre des présentes lignes directrices et pourra les compléter s'il y a lieu.

II. Définitions

Le RGPD introduit des dispositions visant à garantir que le profilage et la prise de décision individuelle automatisée (qu'il s'agisse ou non de profilage) ne sont pas utilisés de manière à avoir des répercussions injustifiées sur les droits des personnes; par exemple:

- des exigences particulières en matière de transparence et de loyauté;
- des obligations accrues en matière de responsabilité;
- des bases juridiques spécifiées pour le traitement;
- le droit pour les particuliers de s'opposer au profilage et plus particulièrement au profilage à des fins de prospection; et
- si certaines conditions sont remplies, la nécessité de réaliser une analyse d'impact relative à la protection des données.

Le RGPD ne se concentre pas seulement sur les décisions prises à la suite d'un traitement automatisé ou d'un profilage. Il s'applique à la collecte de données pour la création de profils, ainsi qu'à l'application de ces profils aux particuliers.

A. **Profilage**

Dans son article 4, paragraphe 4, le RGPD définit le profilage comme:

toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

Le profilage est composé de trois éléments:

- il doit s'agir d'une forme de traitement *automatisé*;
- il doit être effectué sur des *données à caractère personnel*; et
- l'objectif du profilage doit être d'*évaluer les aspects personnels* d'une personne physique.

L'article 4, paragraphe 4, fait référence à «toute forme de traitement automatisé» plutôt qu'à un traitement «exclusivement» automatisé (visé à l'article 22). Le profilage doit impliquer une certaine forme de traitement automatisé – bien que la participation humaine n'exclue pas nécessairement l'activité de la définition.

Le profilage est une procédure qui peut comporter une série de déductions statistiques. Il est souvent utilisé pour faire des prédictions au sujet des gens, en utilisant des données provenant de diverses sources pour déduire quelque chose sur une personne, en se fondant sur les qualités d'autres personnes qui semblent similaires sur le plan statistique.

Selon le RGPD, le profilage est un traitement automatisé de données à caractère personnel pour évaluer des aspects personnels, en particulier pour analyser *ou* faire des prédictions sur les particuliers. L'utilisation du mot «évaluer» suggère que le profilage implique une certaine forme d'appréciation ou de jugement à l'égard d'une personne.

Une simple classification des personnes en fonction de caractéristiques connues comme l'âge, le sexe et la taille ne conduit pas nécessairement au profilage. Cela dépendra de l'objectif de la classification. Par exemple, une entreprise peut souhaiter classer ses clients en fonction de leur âge ou de leur sexe à des fins statistiques et acquérir une vue d'ensemble de ses clients sans faire de prédictions ou tirer de conclusions au sujet d'une personne en particulier. Dans ce cas, le but n'est pas d'évaluer les caractéristiques individuelles et cela ne constitue donc pas du profilage.

Le RGPD s'inspire de la définition du profilage figurant dans la recommandation CM/Rec(2010)13² du Conseil de l'Europe (ci-après la «Recommandation»), mais n'est pas identique à celle-ci, étant donné que la Recommandation *exclut* les traitements qui ne comprennent pas d'inférence. Néanmoins, la Recommandation explique utilement que le profilage peut comporter trois étapes distinctes:

- une collecte de données;
- une analyse automatisée afin d'établir des corrélations;

² Conseil de l'Europe. La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Recommandation CM/Rec(2010)13 et exposé des motifs. Conseil de l'Europe, 23 novembre 2010.
[https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommandations/CMRec\(2010\)13E_Profiling.pdf](https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommandations/CMRec(2010)13E_Profiling.pdf).
Document consulté le 24 avril 2017.

- l'application de la corrélation à une personne pour déduire les caractéristiques du comportement actuel ou futur.

Les responsables du traitement qui effectuent le profilage devront s'assurer qu'ils satisfont aux exigences du RGPD lors de toutes les étapes susmentionnées.

D'une manière générale, le profilage consiste à recueillir des informations sur une personne (ou un groupe de personnes) et à évaluer leurs caractéristiques ou leurs comportements afin de les placer dans une certaine catégorie ou un certain groupe, notamment pour analyser et/ou faire des prédictions sur, par exemple:

- leur capacité à effectuer une tâche;
- leurs intérêts; ou
- leur comportement probable.

Exemple

Un courtier de données recueille des données auprès de différentes sources publiques et privées, soit pour le compte de ses clients, soit pour ses propres besoins. Il compile les données pour établir des profils sur les personnes concernées et les place dans des segments. Il vend ces informations aux entreprises qui souhaitent améliorer le ciblage de leurs biens et services. Le courtier de données effectue un profilage en plaçant une personne dans une certaine catégorie en fonction de ses intérêts.

L'existence ou non d'une décision individuelle automatisée, telle que définie à l'article 22, paragraphe 1, dépendra des circonstances.

B. Prise de décision automatisée

La prise de décision automatisée a une portée différente et peut partiellement chevaucher le profilage ou en résulter. La prise de décision exclusivement automatisée est la capacité de prendre des décisions par des moyens technologiques sans intervention humaine. Les décisions automatisées peuvent être fondées sur n'importe quel type de données, par exemple:

- les données fournies directement par les personnes concernées (comme les réponses à un questionnaire);
- les données observées au sujet des personnes (comme les données de localisation recueillies par l'intermédiaire d'une application);
- des données dérivées ou inférées, comme un profil de la personne qui a déjà été créé (p. ex. une cote de solvabilité).

Les décisions automatisées peuvent être prises avec ou sans profilage; le profilage peut se faire sans prendre de décisions automatisées. Toutefois, le profilage et la prise de décision automatisée ne sont pas nécessairement des activités distinctes. Quelque chose qui commence comme un simple processus décisionnel automatisé pourrait devenir un processus fondé sur le profilage, selon la façon dont les données sont utilisées.

Exemple

Imposer des amendes pour excès de vitesse sur la seule base des preuves fournies par les radars est un processus décisionnel automatisé qui n'implique pas nécessairement un profilage.

Toutefois, la décision serait fondée sur le profilage si les habitudes de la personne concernée au volant étaient surveillées au fil du temps. Par exemple, si le montant de l'amende infligée est le résultat d'une évaluation faisant intervenir d'autres facteurs, comme le fait de savoir si l'excès de vitesse est une récidive ou si le conducteur a commis récemment d'autres infractions au code de la route.

Les décisions qui ne sont pas exclusivement automatisées peuvent également inclure un profilage. Par exemple, avant d'accorder une hypothèque, une banque peut tenir compte de la cote de solvabilité de l'emprunteur, avec une intervention significative supplémentaire effectuée par des humains avant que toute décision ne soit appliquée à un individu.

C. **Manière dont le RGPD aborde les concepts**

Le profilage peut être utilisé de trois façons différentes:

- i) un profilage général;
- ii) une prise de décision fondée sur le profilage; et
- iii) une prise de décision *exclusivement* automatisée, y compris le profilage, qui produit des effets juridiques ou affecte de manière significative de façon similaire la personne concernée (article 22, paragraphe 1).

La différence entre les points ii) et iii) est mieux illustrée par les deux exemples suivants présentant le cas d'une personne qui fait une demande de prêt en ligne:

- un être humain décide s'il accorde ou non le prêt sur la base d'un profil produit par des moyens purement automatisés (ii);
- un algorithme décide si le prêt est accordé et la décision est automatiquement transmise à la personne concernée, sans évaluation préalable et significative par un être humain (iii).

Les responsables du traitement peuvent effectuer un profilage et recourir à une prise de décision automatisée à condition de respecter tous les principes et de disposer d'une base légale pour le traitement. Des garanties et restrictions supplémentaires s'appliquent dans le cas d'une prise de décision exclusivement automatisée, y compris le profilage, visée à l'article 22, paragraphe 1.

Le chapitre III des présentes lignes directrices explique les dispositions du RGPD pour *tous* les profilages et *toutes* les prises de décisions individuelles automatisées. Cela comprend les processus décisionnels qui ne sont *pas* exclusivement automatisés.

Le chapitre IV des présentes lignes directrices explique les dispositions spécifiques qui *ne s'appliquent qu'*à la prise de décision individuelle automatisée, y compris le profilage³. Il existe une interdiction générale de ce type de traitement afin de tenir compte des risques potentiels pour les droits et les libertés des personnes.

³ Telle que définie à l'article 22, paragraphe 1, du RGPD.

III. Dispositions générales sur le profilage et la prise de décision automatisée

Cet aperçu des dispositions s'applique à tous les profilages et à toutes les prises de décisions automatisées. Les dispositions spécifiques supplémentaires énoncées au chapitre IV s'appliquent si le traitement correspond à la définition de l'article 22, paragraphe 1.

A. Principes de la protection des données

Ces principes s'appliquent à tous les profilages et toutes les décisions automatisées concernant des données à caractère personnel⁴. Afin de garantir la conformité, les responsables du traitement doivent prendre en considération les éléments clés suivants:

1. Article 5, paragraphe 1, point a) - Licéité, loyauté et transparence

La transparence du traitement⁵ est une exigence fondamentale du RGPD.

Le processus de profilage est souvent invisible pour la personne concernée. Il fonctionne en créant des données dérivées ou déduites sur les individus, c'est-à-dire de «nouvelles» données à caractère personnel qui n'ont pas été fournies directement par les personnes concernées elles-mêmes. Chacun possède un niveau de compréhension différent et pour certains, il peut être difficile de comprendre les techniques complexes intervenant dans le profilage et les processus décisionnels automatisés.

En vertu de l'article 12, paragraphe 1, le responsable du traitement doit fournir toute information concernant le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible⁶.

Pour les données collectées directement auprès de la personne concernée, ces informations doivent être fournies au moment de la collecte (article 13); pour les données obtenues indirectement, les informations doivent être fournies dans les délais prévus à l'article 14, paragraphe 3.

Exemple

Certains assureurs proposent des tarifs et des services fondés sur le comportement au volant d'une personne. Les éléments pris en considération dans ces cas pourraient inclure la distance parcourue, le

⁴ RGPD – Considérant 72 «Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnel, par exemple le fondement juridique du traitement ou les principes en matière de protection des données.»

⁵ Les lignes directrices du groupe de travail «article 29» sur la transparence couvrent de manière plus détaillée la transparence en général; voir les lignes directrices sur la transparence au titre du règlement (UE) 2016/679 (Guidelines on transparency under Regulation 2016/679) (wp260rev.01), 11 avril 2018 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

⁶ Bureau du Commissaire à l'information de l'Australie. Projet de consultation: le guide des mégadonnées et des principes australiens de protection de la vie privée (Guide to big data and the Australian Privacy Principles, 05/2016) dispose ce qui suit: «Les déclarations de confidentialité doivent communiquer les pratiques de traitement de l'information de façon claire et simple, mais aussi de façon exhaustive et suffisamment précise pour être bien comprises. *La technologie même qui permet une plus grande collecte de renseignements personnels offre également la possibilité de formuler des déclarations de confidentialité plus dynamiques, à plusieurs niveaux et axés sur l'utilisateur*». <https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles>. Document consulté le 24 avril 2017.

temps de conduite et le trajet suivi, ainsi que des prédictions fondées sur d'autres données recueillies par les capteurs dans une voiture (intelligente). Les données recueillies sont utilisées pour le profilage afin d'identifier les mauvais comportements au volant (accélération rapide, freinage brusque et excès de vitesse). Ces informations peuvent être recoupées avec d'autres sources (par exemple la météo, la circulation, le type de route) pour mieux comprendre le comportement du conducteur.

Le responsable du traitement doit s'assurer qu'il dispose d'une base légale pour ce type de traitement. Il doit également fournir à la personne concernée des informations sur les données collectées et, s'il y a lieu, sur l'existence d'une prise de décision automatisée visée à l'article 22, paragraphes 1 et 4, sur la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Les exigences spécifiques relatives à l'information et à l'accès aux données à caractère personnel sont examinées aux chapitres III (section D) et IV (section E).

Le traitement doit également être loyal et transparent.

Le profilage peut être déloyal et créer de la discrimination, par exemple en refusant aux personnes l'accès à un emploi, à un crédit ou à une assurance, ou en les ciblant avec des produits financiers excessivement risqués ou coûteux. L'exemple suivant, qui ne satisferait pas aux exigences de l'article 5, paragraphe 1, point a), illustre comment le profilage déloyal peut conduire à ce que certains consommateurs se voient proposer des offres moins attractives que d'autres.

Exemple

Un courtier de données vend à des sociétés financières des profils de consommateurs sans le consentement de ceux-ci ou sans connaître les données sous-jacentes. Les profils classent les consommateurs en catégories (avec des qualificatifs tels que «profil rural ayant du mal à joindre les deux bouts», «difficultés en milieu urbain-profil ethnique de deuxième génération», «débutants difficiles: jeunes parents célibataires») ou une «note», en mettant l'accent sur la vulnérabilité financière des consommateurs. Les sociétés financières proposent à ces consommateurs des prêts sur salaire et d'autres services financiers «non traditionnels» (prêts à taux élevé et autres produits financièrement risqués)⁷.

2. Article 5, paragraphe 1, point b) – Traitement ultérieur et limitation des finalités

Le profilage peut impliquer l'utilisation de données à caractère personnel qui ont été collectées à l'origine à d'autres fins.

⁷ Cet exemple est tiré de: Sénat des États-Unis, Comité du commerce, des sciences et des transports. Examen du secteur des courtiers de données: collecte, utilisation et vente de données sur les consommateurs à des fins de marketing (A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes), rapport du personnel pour le président Rockefeller, 18 décembre 2013. <https://www.commerce.senate.gov/public/cache/files/Od2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf>. Voir page ii du résumé et page 12 du corps du document en particulier. Document consulté le 21 juillet 2017.

Exemple

Certaines applications mobiles fournissent des services de localisation permettant à l'utilisateur de trouver des restaurants offrant des rabais à proximité de sa position. Toutefois, les données recueillies sont également utilisées pour établir un profil de la personne concernée à des fins de prospection – pour déterminer ses préférences alimentaires ou son mode de vie en général. La personne concernée s'attend à ce que ses données soient utilisées pour trouver des restaurants, mais pas pour recevoir des publicités pour la livraison de pizzas simplement parce que l'application a déterminé qu'elle rentre tard à la maison. Cette utilisation ultérieure des données de localisation peut ne pas être compatible avec les finalités pour lesquelles elles ont été collectées initialement et peut donc nécessiter le consentement de la personne concernée⁸.

La compatibilité de ce traitement supplémentaire avec les finalités initiales pour lesquelles les données ont été collectées dépendra d'une série de facteurs⁹, y compris les informations que le responsable du traitement a initialement fournies à la personne concernée. Ces facteurs sont reflétés dans le RGPD¹⁰ et résumés ci-dessous:

- le lien entre les finalités pour lesquelles les données ont été collectées et les finalités du traitement ultérieur;
- le contexte dans lequel les données à caractère personnel ont été collectées et les attentes raisonnables des personnes concernées quant à leur utilisation ultérieure;
- la nature des données;
- l'impact du traitement ultérieur sur les personnes concernées; et
- les garanties appliquées par le responsable du traitement afin d'assurer un traitement loyal et d'éviter tout impact indu sur les personnes concernées.

3. Article 5, paragraphe 1, point c) – Minimisation des données

Les possibilités commerciales engendrées par le profilage, les coûts de stockage moins élevés et la capacité de traiter de grandes quantités d'informations peuvent encourager les organisations à collecter plus de données à caractère personnel qu'elles n'en ont réellement besoin, au cas où cela s'avérerait utile pour l'avenir. Les responsables du traitement doivent s'assurer qu'ils respectent le principe de minimisation des données, ainsi que les exigences des principes de limitation des finalités et de limitation de la durée de conservation.

Ils devraient être en mesure d'expliquer et de justifier clairement la nécessité de collecter et de conserver des données à caractère personnel, ou d'envisager d'utiliser des données agrégées, anonymisées ou (lorsque cela garantit une protection suffisante) pseudonymisées pour le profilage.

4. Article 5, paragraphe 1, point d) – Exactitude

⁸ Il convient de noter que les dispositions du futur règlement «vie privée et communications électroniques» peuvent également s'appliquer.

⁹ Comme souligné par le groupe de travail «article 29» sur la protection des données. Avis 03/2013 sur la limitation des finalités, 2 avril 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Document consulté le 24 avril 2017.

¹⁰ Article 6, paragraphe 4, du RGPD.

Les responsables du traitement devraient tenir compte de l'exactitude à toutes les étapes du processus de profilage, en particulier lors de:

- la collecte de données;
- l'analyse des données;
- l'établissement du profil d'une personne; ou
- l'application d'un profil pour prendre une décision affectant la personne.

Si les données utilisées dans un processus automatisé de prise de décision ou de profilage sont inexacts, toute décision ou tout profil qui en résulte sera erroné. Les décisions peuvent être prises sur la base de données dépassées ou d'une interprétation incorrecte de données externes. Des inexactitudes peuvent conduire à des prédictions ou des déclarations inappropriées concernant, par exemple, le risque de santé, de crédit ou d'assurance d'une personne.

Même si les données brutes sont enregistrées avec exactitude, l'ensemble de données peut ne pas être entièrement représentatif ou les analyses peuvent contenir des biais cachés.

Les responsables du traitement doivent mettre en place des mesures solides pour vérifier et s'assurer en permanence que les données réutilisées ou obtenues indirectement sont exactes et à jour. Cela renforce l'importance de fournir des informations claires sur les données à caractère personnel traitées, afin que la personne concernée puisse corriger toute inexactitude et améliorer la qualité des données.

5. Article 5, paragraphe 1, point e) – Limitation de la conservation

Les algorithmes d'apprentissage automatique sont conçus pour traiter de grands volumes d'informations et établir des corrélations qui permettent aux organisations de produire des profils très complets et intimes des individus. Bien qu'il puisse y avoir des avantages à conserver les données dans le cas du profilage, puisqu'il y aura plus de données dont l'algorithme pourra s'inspirer, les responsables du traitement doivent respecter le principe de minimisation des données lorsqu'ils collectent des données à caractère personnel et veiller à ce qu'ils ne conservent ces données à caractère personnel que le temps nécessaire et proportionné aux finalités pour lesquelles ces données sont traitées.

La politique de conservation du responsable du traitement devrait tenir compte des droits et libertés des personnes concernées, conformément aux exigences de l'article 5, paragraphe 1, point e).

Le responsable du traitement doit également s'assurer que les données restent à jour tout au long de la période de conservation afin de réduire le risque d'inexactitudes¹¹.

B. Bases légales du traitement

La prise de décision automatisée visée à l'article 22, paragraphe 1, n'est autorisée que si l'une des exceptions décrites au chapitre IV (sections C et D) s'applique. Les bases légales suivantes applicables au traitement sont pertinentes pour tous les autres profilages et décisions individuelles automatisées.

1. Article 6, paragraphe 1, point a) – Consentement

¹¹ Autorité norvégienne de protection des données. La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée (The Great Data Race - How commercial use of personal data challenges privacy), rapport, novembre 2015. Datatilsynet <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/> Document consulté le 24 avril 2017.

Le consentement comme base du traitement est traité de manière générale dans les lignes directrices du GT29 sur le consentement¹². Le consentement explicite est l'une des exceptions à l'interdiction de la prise de décision et du profilage automatisés définis à l'article 22, paragraphe 1.

Le profilage peut être opaque. Il s'appuie souvent sur des données dérivées ou déduites d'autres données, plutôt que sur des données fournies directement par la personne concernée.

Les responsables du traitement qui cherchent à se fonder sur le consentement pour procéder à un profilage devront démontrer que les personnes concernées comprennent exactement ce à quoi elles consentent, et se rappeler que le consentement n'est pas toujours une base appropriée pour le traitement¹³. Dans tous les cas, les personnes concernées devraient disposer de suffisamment d'informations pertinentes sur l'utilisation envisagée et les conséquences du traitement pour garantir que leur consentement représente un choix éclairé.

2. Article 6, paragraphe 1, point b – Nécessaire à l'exécution d'un contrat

Les responsables du traitement peuvent souhaiter utiliser le profilage et les processus décisionnels automatisés parce qu'ils :

- permettent une plus grande cohérence ou loyauté dans le processus de prise de décision (p. ex. en réduisant le risque d'erreur humaine, de discrimination et d'abus de pouvoir);
- réduisent le risque que les clients ne règlent pas les paiements pour des biens ou des services (par exemple en utilisant le référencement du crédit); ou
- leur permettent de prendre des décisions dans des délais plus courts et d'améliorer leur efficacité.

Indépendamment de ce qui précède, ces seules considérations ne suffisent pas à démontrer que ce type de traitement est *nécessaire* à l'exécution d'un contrat, en vertu de l'article 6, paragraphe 1, point b). Comme décrit dans l'avis du GT29 sur l'intérêt légitime¹⁴, la nécessité doit être interprétée de manière restrictive.

Voici un exemple de profilage qui ne répondrait pas à la base de l'article 6, paragraphe 1, point b) pour le traitement.

Exemple

Un utilisateur achète des articles auprès d'un détaillant en ligne. Afin d'exécuter le contrat, le détaillant doit traiter les informations relatives à la carte de crédit de l'utilisateur à des fins de

¹² Groupe de travail «article 29» sur la protection des données. Lignes directrices sur le consentement au titre du règlement (UE) 2016/679 (Guidelines on Consent under Regulation 2016/679), WP259, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Document consulté le 18 décembre 2017.

¹³ Ibid.

¹⁴ Avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE. Commission européenne, 9 avril 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf. Document consulté le 24 avril 2017.

paiement et l'adresse de l'utilisateur pour livrer les marchandises. L'exécution du contrat ne dépend pas de l'établissement d'un profil des goûts et des choix de style de vie de l'utilisateur en fonction de ses visites sur le site web. Même si le profilage est spécifiquement mentionné dans les petits caractères du contrat, ce seul fait ne le rend pas «nécessaire» à l'exécution du contrat.

3. Article 6, paragraphe 1, point c) – Nécessaire au respect d'une obligation légale

Il peut se produire des cas où il y aura une obligation légale d'effectuer un profilage¹⁵ – par exemple dans le cadre de la prévention de la fraude ou du blanchiment d'argent. L'avis du GT29 sur les intérêts légitimes¹⁶ fournit des informations utiles sur cette base de traitement, y compris les garanties à appliquer.

4. Article 6, paragraphe 1, point d) – Nécessaire à la sauvegarde des intérêts vitaux

Cela couvre les situations dans lesquelles le traitement est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique.

Certains types de traitement peuvent servir des raisons importantes d'intérêt public ainsi que les intérêts vitaux de la personne concernée. Il peut s'agir, par exemple, du profilage nécessaire pour mettre au point des modèles permettant de prédire la propagation de maladies potentiellement mortelles ou dans des situations d'urgence humanitaire. Dans ces cas, toutefois, et en principe, le responsable du traitement ne peut se fonder sur des raisons d'intérêt vital que si aucune autre base juridique n'est disponible pour le traitement¹⁷. Si le traitement concerne des données à caractère personnel d'une catégorie particulière, le responsable du traitement devrait également s'assurer qu'elles satisfont aux exigences de l'article 9, paragraphe 2, point c).

5. Article 6, paragraphe 1, point e) – Nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

L'article 6, paragraphe 1, point e), pourrait constituer une base appropriée pour le profilage du secteur public dans certaines circonstances. La tâche ou la fonction doit avoir une base juridique claire.

6. Article 6, paragraphe 1, point f) – Nécessaire aux fins des intérêts légitimes¹⁸ poursuivis par le responsable du traitement ou par un tiers

Le profilage est autorisé s'il est nécessaire aux fins des intérêts légitimes¹⁹ poursuivis par le responsable du traitement ou par un tiers. Toutefois, l'article 6, paragraphe 1, point f), ne s'applique pas automatiquement au seul motif que le responsable du traitement ou un tiers a un intérêt légitime.

¹⁵ Considérants 41 et 45 du RGPD.

¹⁶ Page 19 de l'avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, groupe de travail «article 29» sur la protection des données. Commission européenne, 9 avril 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf. Document consulté le 24 avril 2017.

¹⁷ Considérant 46 du RGPD.

¹⁸ Les intérêts légitimes énumérés au considérant 47 du RGPD comprennent le traitement à des fins de prospection et le traitement strictement nécessaire à des fins de prévention de la fraude.

¹⁹ L'«intérêt légitime» du responsable du traitement ne peut pas rendre le profilage licite si le traitement relève de la définition de l'article 22, paragraphe 1.

Le responsable du traitement doit procéder à une mise en balance afin de déterminer si les intérêts ou les droits et libertés fondamentaux de la personne concernée prévalent sur ses propres intérêts.

Les éléments suivants sont particulièrement importants:

- le niveau de détail du profil (une personne concernée faisant l'objet d'un profil au sein d'une cohorte au sens large, comme les «personnes ayant un intérêt pour la littérature anglaise», ou segmentée et ciblée à un niveau granulaire);
- l'exhaustivité du profil (que le profil ne décrive qu'un petit aspect de la personne concernée ou qu'il brosse un tableau plus complet);
- l'impact du profilage (les effets sur la personne concernée); et
- les garanties visant à assurer la loyauté, la non-discrimination et l'exactitude du processus de profilage.

Bien que l'avis du GT29 sur les intérêts légitimes²⁰ se fonde sur l'article 7 de la directive 95/46/CE relative à la protection des données (ci-après la «directive»), il contient des exemples qui restent utiles et pertinents pour les responsables du traitement qui effectuent le profilage. Il suggère également qu'il serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes comme base légale pour des pratiques intrusives de profilage et de suivi à des fins de marketing ou de publicité, par exemple celles qui impliquent le suivi d'individus sur plusieurs sites web, emplacements, dispositifs, services ou courtage de données.

Le responsable du traitement devrait également tenir compte de l'utilisation future ou de la combinaison de profils lors de l'évaluation de la validité du traitement en vertu de l'article 6, paragraphe 1, point f).

C. Article 9 – Catégories particulières de données

Les responsables du traitement ne peuvent traiter des données à caractère personnel d'une catégorie particulière que s'ils peuvent satisfaire à l'une des conditions énoncées à l'article 9, paragraphe 2, ainsi qu'à une condition de l'article 6. Cela comprend les données d'une catégorie particulière dérivées ou déduites de l'activité de profilage.

Le profilage peut engendrer des données d'une catégorie particulière par inférence à partir de données qui n'appartiennent pas à une catégorie particulière en soi, mais qui le deviennent lorsqu'elles sont combinées avec d'autres données. Par exemple, il peut être possible de déduire l'état de santé d'une personne à partir des historiques de ses achats d'aliments combinés à des données sur la qualité et la teneur énergétique des aliments.

Il est alors possible de découvrir des corrélations qui donnent des indications au sujet de la santé, des convictions politiques, des croyances religieuses ou de l'orientation sexuelle des individus, comme le démontre l'exemple suivant:

Exemple

²⁰ Groupe de travail «article 29» sur la protection des données. Avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE. Commission européenne, 9 avril 2014, page 47, exemples aux pages 59 et 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Document consulté le 24 avril 2017.

Une étude²¹ a combiné les «J'aime» de Facebook avec des données d'enquête limitées et a constaté que les chercheurs ont prédit avec précision l'orientation sexuelle d'un utilisateur masculin dans 88 % des cas, l'origine ethnique de l'utilisateur dans 95 % des cas et si un utilisateur était chrétien ou musulman dans 82 % des cas.

Si des préférences et des caractéristiques sensibles sont déduites du profilage, le responsable du traitement doit s'assurer:

- que le traitement n'est pas incompatible avec la finalité initiale;
- qu'il a identifié une base légale pour le traitement des données d'une catégorie particulière; et
- qu'il informe la personne concernée du traitement.

La prise de décision automatisée telle que définie à l'article 22, paragraphe 1, qui est fondée sur des catégories particulières de données est couverte au chapitre IV (section D).

D. Droits de la personne concernée²²

Le RGPD introduit des droits renforcés pour les personnes concernées et crée de nouvelles obligations pour les responsables du traitement.

Dans le contexte du profilage, ces droits sont opposables au responsable du traitement qui crée le profil et au responsable du traitement qui prend une décision automatisée au sujet d'une personne concernée (avec ou sans intervention humaine), si ces entités ne sont pas les mêmes.

Exemple

Un courtier de données entreprend le profilage de données à caractère personnel. Conformément à ses obligations en vertu des articles 13 et 14, il devrait informer la personne concernée du traitement, notamment de son intention de partager son profil avec d'autres organisations. Il devrait également présenter séparément les détails du droit d'opposition en vertu de l'article 21, paragraphe 1.

Le courtier de données partage le profil avec une autre société. Cette société utilise le profil pour envoyer des messages de prospection à la personne concernée.

La société doit informer l'individu [article 14, paragraphe 1, point c)] des raisons d'utiliser ce profil, et de la source d'où proviennent ces informations [article 14, paragraphe 2, point f)]. La société doit également informer la personne concernée de son droit de s'opposer au traitement, y compris au profilage, à des fins de prospection (article 21, paragraphe 2).

²¹

Michael Kosinski, David Stilwell et Thore Graepel. Les traits et attributs privés sont prévisibles à partir des enregistrements numériques du comportement humain (Private traits and attributes are predictable from digital records of human behaviour). Actes de l'Académie nationale des sciences des États-Unis d'Amérique, <http://www.pnas.org/content/110/15/5802.full.pdf>. Document consulté le 29 mars 2017.

²² Cette section est pertinente tant pour le profilage que pour la prise de décision automatisée. Pour la prise de décision automatisée en vertu de l'article 22, veuillez noter qu'il existe également des exigences supplémentaires telles que décrites au chapitre IV.

Le courtier de données et la société devraient permettre à la personne concernée d'accéder aux informations utilisées (article 15) pour rectifier toute information erronée (article 16) et, dans certaines circonstances, effacer le profil ou les données à caractère personnel utilisées pour la créer (article 17). La personne concernée devrait également être informée de son profil, par exemple dans quels «segments» ou «catégories» elle est placée.²³

Si la société utilise le profil dans le cadre d'un processus décisionnel exclusivement automatisé ayant des effets juridiques sur la personne concernée ou l'affectant de manière significative de façon similaire, la société est le responsable du traitement soumis aux dispositions de l'article 22. (Cela n'exclut pas le courtier de données de l'article 22 si le traitement atteint le niveau requis.)

1. Articles 13 et 14 – Droit d'être informé

Compte tenu du principe fondamental de transparence qui sous-tend le RGPD, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé.

En particulier, lorsque le traitement implique une prise de décision fondée sur le profilage (indépendamment du fait qu'il relève ou non des dispositions de l'article 22), le fait que le traitement vise à la fois a) le profilage et b) la prise de décision fondée sur le profil généré doit être clairement indiqué à la personne concernée²⁴.

Le considérant 60 indique que la fourniture d'informations sur le profilage fait partie des obligations de transparence du responsable du traitement en vertu de l'article 5, paragraphe 1, point a). La personne concernée a le droit d'être informée par le responsable du traitement et, dans certaines circonstances, de s'opposer au «profilage», indépendamment du fait qu'il s'agisse ou non d'une prise de décision individuelle exclusivement automatisée fondée sur le profilage.

D'autres orientations sur la transparence en général sont disponibles dans les lignes directrices du GT29 sur la transparence dans le cadre du RGPD²⁵.

2. Article 15 — Droit d'accès

L'article 15 donne à la personne concernée le droit d'obtenir des précisions sur toutes les données à caractère personnel utilisées pour le profilage, y compris les catégories de données utilisées pour l'élaboration d'un profil.

²³ Autorité norvégienne de protection des données. La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée (The Great Data Race - How commercial use of personal data challenges privacy), rapport, novembre 2015. <https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/> Document consulté le 24 avril 2017.

²⁴ RGPD – Article 13, paragraphe 1, point c), et article 14, paragraphe 1, point c). L'article 13, paragraphe 2, point f), et l'article 14, paragraphe 2, point g), exigent que le responsable du traitement informe la personne concernée de l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4. Cela est expliqué plus en détail au chapitre IV.

²⁵ Groupe de travail «article 29» sur la protection des données. Lignes directrices sur la transparence au titre du règlement (UE) 2016/679 (Guidelines on transparency under Regulation 2016/679), WP260, 28 novembre 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, consultées le 18 décembre 2017.

Outre les informations générales sur le traitement, le responsable du traitement est tenu, conformément à l'article 15, paragraphe 3, de mettre à disposition les données utilisées pour créer le profil, et de donner accès aux informations sur le profil et les segments dans lesquels la personne concernée a été placée.

Cela diffère du droit à la portabilité des données en vertu de l'article 20, en vertu duquel le responsable du traitement ne doit communiquer que les données fournies par la personne concernée ou observées par le responsable du traitement, et non le profil lui-même²⁶.

Le considérant 63 prévoit une certaine protection pour les responsables du traitement qui s'inquiètent de révéler des secrets d'affaires ou liés à la propriété intellectuelle, ce qui peut être particulièrement pertinent en ce qui concerne le profilage. Il indique que ce droit d'accès ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Toutefois, les responsables du traitement ne peuvent pas invoquer la protection de leurs secrets d'affaires comme excuse pour refuser l'accès ou refuser de fournir des informations à la personne concernée.

Le considérant 63 dispose que lorsque c'est possible, le responsable du traitement devrait pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant.

3. Article 16 – Droit de rectification, article 17 – Droit à l'effacement et article 18 – Droit à la limitation du traitement

Le profilage peut comporter un élément de prédiction, ce qui augmente le risque d'inexactitude. Les données saisies peuvent être inexactes ou non pertinentes, ou sorties de leur contexte. Il peut y avoir un problème avec l'algorithme utilisé pour établir les corrélations.

Le droit de rectification de l'article 16 pourrait s'appliquer lorsque, par exemple, une personne est placée dans une catégorie qui donne des indications sur sa capacité à accomplir une tâche, et que ce profil est fondé sur des informations incorrectes. Les personnes peuvent contester l'exactitude des données utilisées et tout groupement ou catégorie qui leur a été appliqué.

Les droits de rectification et à l'effacement²⁷ s'appliquent à la fois aux «données à caractère personnel saisies» (les données à caractère personnel utilisées pour créer le profil) et aux «données de sortie» (le profil lui-même ou la «note» attribuée à la personne).

L'article 16 prévoit également que la personne concernée a le droit de compléter les données à caractère personnel par des informations complémentaires.

Exemple

²⁶Page 9, Lignes directrices du GT29 sur le droit à la portabilité des données (WP29 Guidelines on the Right to data portability), WP242 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Consultées le 8 janvier 2018.

²⁷ RGPD– Article 17.

Le système informatique d'un cabinet médical local de chirurgie place une personne dans un groupe qui est le plus susceptible de contracter une maladie cardiaque. Ce «profil» n'est pas nécessairement inexact, même si elle ne souffre jamais d'une maladie cardiaque. Le profil indique simplement qu'elle est *plus susceptible* de la contracter. C'est peut-être exact d'un point de vue statistique.

Néanmoins, la personne concernée a le droit, compte tenu de la finalité du traitement, de fournir une déclaration supplémentaire. Dans le scénario ci-dessus, cela pourrait se fonder, par exemple, sur un système informatique médical plus avancé (et un modèle statistique) tenant compte de données supplémentaires et effectuant des examens plus détaillés que celui du cabinet médical local avec des capacités plus limitées.

Le droit à la limitation du traitement (article 18) s'appliquera à n'importe quelle étape du processus de profilage.

4. Article 21 — Droit d'opposition

Le responsable du traitement doit porter *explicitement* à l'attention de la personne concernée les détails du droit d'opposition prévu à l'article 21, paragraphes 1 et 2, et les présenter clairement et séparément des autres informations (article 21, paragraphe 4).

En vertu de l'article 21, paragraphe 1, la personne concernée peut s'opposer au traitement (y compris au profilage) pour des raisons tenant à sa situation particulière. Les responsables du traitement sont spécifiquement tenus de prévoir ce droit dans tous les cas où le traitement est fondé sur l'article 6, paragraphe 1, point e) ou f).

Une fois que la personne concernée exerce ce droit, le responsable du traitement doit interrompre²⁸ (ou éviter de commencer) le processus de profilage, à moins qu'il puisse démontrer qu'il existe des motifs légitimes impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée. Le responsable du traitement peut également être amené à effacer les données à caractère personnel pertinentes²⁹.

Le RGPD ne fournit aucune explication de ce qui serait considéré comme des motifs légitimes et impérieux³⁰. Il se peut, par exemple, que le profilage soit bénéfique pour la société dans son ensemble (ou pour l'ensemble de la communauté) et pas seulement pour les intérêts commerciaux du responsable du traitement, comme le profilage destiné à prédire la propagation de maladies contagieuses.

Le responsable du traitement devrait:

- tenir compte de l'importance du profilage par rapport à son objectif particulier;

²⁸ RGPD – Article 18, paragraphe 1, point d).

²⁹ RGPD – Article 17, paragraphe 1, point c).

³⁰ Voir l'explication sur la légitimité, avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, groupe de travail «article 29» sur la protection des données. 9 avril 2014. Pages 24 à 26, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Document consulté le 24 avril 2017.

- examiner l'impact du profilage sur les intérêts, les droits et les libertés de la personne concernée – lequel devrait être limité au minimum nécessaire pour atteindre l'objectif; et
- effectuer une mise en balance.

Il doit toujours y avoir une mise en balance entre les intérêts concurrents du responsable du traitement et le fondement de l'opposition de la personne concernée (que ce soit pour des raisons personnelles, sociales ou professionnelles). Contrairement à la directive 95/46/CE, c'est au responsable du traitement plutôt qu'à la personne concernée qu'il incombe de prouver l'existence de motifs légitimes et impérieux.

Il ressort clairement du libellé de l'article 21 que le critère de mise en balance est différent de celui de l'article 6, paragraphe 1, point f). En d'autres termes, il ne suffit pas qu'un responsable du traitement démontre simplement que l'analyse de son intérêt légitime antérieur était correcte. Ce critère de mise en balance exige que l'intérêt légitime soit *impérieux*, ce qui implique un seuil plus élevé pour les objections majeures.

L'article 21, paragraphe 2 accorde un droit *inconditionnel* à la personne concernée de s'opposer au traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection³¹. Cela signifie qu'il n'est pas nécessaire de procéder à une mise en balance des intérêts; le responsable du traitement doit respecter les souhaits de la personne sans remettre en cause les motifs de l'objection. Le considérant 70 fournit un contexte supplémentaire à ce droit et indique qu'il peut être exercé à tout moment et sans frais.

IV. Dispositions spécifiques concernant la prise de décision exclusivement automatisée définie à l'article 22

L'article 22, paragraphe 1, dispose ce qui suit:

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée *exclusivement* sur un traitement automatisé, y compris le profilage, produisant des *effets juridiques* la concernant ou *l'affectant de manière significative de façon similaire*.

Le terme «droit» dans la disposition ne signifie pas que l'article 22, paragraphe 1, ne s'applique que lorsqu'il est activement invoqué par la personne concernée. L'article 22, paragraphe 1, établit une interdiction générale de prendre des décisions fondées exclusivement sur un traitement automatisé. Cette interdiction s'applique que la personne concernée prenne ou non une mesure concernant le traitement de ses données à caractère personnel.

En résumé, l'article 22 prévoit ce qui suit:

- i) en principe, il existe une interdiction générale de prendre des décisions individuelles entièrement automatisées, y compris le profilage qui a un effet juridique ou un effet d'une importance similaire;
- ii) toutefois, cette règle admet des exceptions;

³¹ Conformément à l'article 12, paragraphe 2, les responsables du traitement qui collectent des données à caractère personnel auprès de personnes dans le but de les utiliser à des fins de prospection devraient, au moment de la collecte, envisager de proposer aux personnes concernées un moyen facile d'indiquer qu'elles ne souhaitent pas que leurs données à caractère personnel soient utilisées à des fins de prospection, plutôt que de leur demander d'exercer leur droit d'opposition à une occasion ultérieure.

iii) lorsque l'une de ces exceptions s'applique, des mesures doivent être mises en place pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes³².

Cette interprétation renforce l'idée que la personne concernée a le contrôle de ses données à caractère personnel, ce qui est conforme aux principes fondamentaux du RGPD. Interpréter l'article 22 comme une interdiction plutôt que comme un droit à invoquer signifie que les personnes sont automatiquement protégées contre les effets potentiels de ce type de traitement. Le libellé de l'article suggère que telle en est l'intention et il est étayé par le considérant 71 qui indique ce qui suit:

Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, **devrait être permise** lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre [...] ou nécessaire à la conclusion ou à l'exécution d'un contrat [...], ou si la personne concernée a donné son consentement explicite.

Cela implique que le traitement au titre de l'article 22, paragraphe 1, n'est généralement pas autorisé³³.

Toutefois, l'interdiction prévue à l'article 22, paragraphe 1, *ne s'applique que* dans des circonstances spécifiques lorsqu'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, a un effet juridique sur une personne ou l'affecte de manière significative de façon similaire, comme expliqué plus en détail dans les lignes directrices. Même dans ces cas, il existe des exceptions définies qui permettent un tel traitement.

Les mesures de protection requises, examinées plus en détail ci-après, comprennent le droit d'être informé (abordé aux articles 13 et 14 – informations particulièrement utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues du traitement pour la personne concernée), et les garanties, telles que le droit d'obtenir une intervention humaine et le droit de contester la décision (abordés à l'article 22, paragraphe 3).

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les personnes concernées, le responsable du traitement effectue une [analyse d'impact relative à la protection des données](#).³⁴ Outre les autres risques liés au traitement, une analyse d'impact relative à la protection des données peut s'avérer particulièrement utile pour les responsables du traitement qui ne sont pas certains que les activités proposées relèvent de la définition de l'article 22, paragraphe 1, et, si une exception identifiée le permet, des mesures de sauvegarde qui doivent être appliquées.

A. **«Décision fondée exclusivement sur un traitement automatisé»**

³² Le considérant 71 indique qu'en tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

³³ D'autres commentaires sur l'interprétation de l'article 22 en tant qu'interdiction figurent à l'annexe 2.

³⁴ Groupe de travail «article 29» sur la protection des données, lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679. 4 avril 2017. Commission européenne. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Document consulté le 24 avril 2017.

L'article 22, paragraphe 1, fait référence aux décisions «fondées exclusivement» sur un traitement automatisé. Cela signifie qu'il n'y a pas d'intervention humaine dans le processus de décision.

Exemple

Un processus automatisé produit ce qui est en fait une recommandation au sujet d'une personne concernée. Si un être humain examine et tient compte d'autres facteurs dans la prise de décision finale, cette décision ne serait pas «fondée exclusivement» sur un traitement automatisé.

Le responsable du traitement ne peut pas contourner les dispositions de l'article 22 en créant une intervention humaine de toutes pièces. Par exemple, si quelqu'un applique systématiquement des profils générés automatiquement à des individus sans aucune influence réelle sur le résultat, il s'agirait quand même d'une décision fondée exclusivement sur un traitement automatisé.

Pour qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique. Le contrôle devrait être effectué par une personne qui a l'autorité et la compétence pour modifier la décision. Dans le cadre de l'analyse, il convient de tenir compte de toutes les données pertinentes.

Dans le cadre de son analyse d'impact relative à la protection des données, le responsable du traitement devrait identifier et consigner le degré d'intervention humaine dans le processus de prise de décision et le stade auquel cela se produit.

B. «Produisant des effets juridiques à l'égard d'une personne physique» ou «l'affectant de manière significative de façon similaire»

Le RGPD reconnaît que la prise de décision automatisée, y compris le profilage, peut avoir de graves conséquences pour les personnes concernées. Le RGPD ne définit pas le terme «effets juridiques» ni l'expression «de manière significative de façon similaire», mais la formulation utilisée indique clairement que seuls les effets ayant une incidence grave seront couverts par l'article 22.

Décision «produisant des effets juridiques»

Un effet juridique exige que la décision, qui est fondée exclusivement sur un traitement automatisé, affecte les droits juridiques d'une personne, comme la liberté de s'associer avec d'autres personnes, de voter lors d'élections ou d'intenter une action en justice. Un effet juridique peut également affecter le statut juridique d'une personne ou ses droits en vertu d'un contrat. Parmi les exemples de ce type d'effet, il convient de mentionner les décisions automatisées au sujet d'une personne qui se traduisent par:

- l'annulation d'un contrat;
- le droit ou le refus d'un avantage social particulier accordé par la loi, comme l'allocation familiale ou l'allocation de logement;
- le refus d'admission dans un pays ou le refus de citoyenneté.

«l'affectant de manière significative de façon similaire»

Même si un processus décisionnel n'a pas d'effet sur les droits juridiques des personnes, il pourrait quand même relever du champ d'application de l'article 22 s'il produit un effet équivalent ou qui affecte la personne concernée de manière significative de façon similaire.

En d'autres termes, même s'il n'y a pas de changement dans ses droits ou obligations juridiques, la personne concernée pourrait quand même être suffisamment affectée pour exiger les protections prévues par cette disposition. Le RGPD ajoute l'expression «de façon similaire» (absente de l'article 15 de la directive 95/46/CE) à l'expression «l'affectant de manière significative». Par conséquent, le niveau d'*importance* doit être similaire à celui d'une décision produisant un effet juridique.

Le considérant 71 fournit les exemples typiques suivants: «le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine».

Pour que le traitement des données affecte une personne de manière significative, les effets du traitement doivent être suffisamment conséquents ou importants pour être pris en considération. En d'autres termes, la décision doit être de nature à:

- affecter de manière significative la situation, le comportement ou les choix des personnes concernées;
- avoir un impact prolongé ou permanent sur la personne concernée; ou
- à l'extrême, entraîner l'exclusion ou la discrimination des personnes.

Même s'il est difficile d'être précis sur ce qui serait considéré comme suffisamment *significatif* pour atteindre le niveau requis, les décisions suivantes pourraient entrer dans cette catégorie:

- les décisions qui ont une incidence sur la situation financière d'une personne, comme son admissibilité à un crédit;
- les décisions qui affectent l'accès d'une personne aux services de santé;
- les décisions qui privent une personne d'une possibilité d'emploi ou qui la désavantagent gravement;
- les décisions qui affectent l'accès d'une personne à l'éducation, par exemple les admissions à l'université.

Cela nous amène également à la question de la publicité en ligne, qui s'appuie de plus en plus sur des outils automatisés et qui implique uniquement la prise de décision individuelle automatisée. Outre le respect des dispositions générales du RGPD, couvertes au chapitre III, les dispositions de la proposition de règlement «vie privée et communications électroniques» peuvent également être pertinentes. En outre, les enfants ont besoin d'une protection renforcée, comme nous le verrons plus loin au chapitre V.

Dans de nombreux cas typiques, la décision de présenter une publicité ciblée fondée sur le profilage, telle qu'une publicité pour un magasin de mode en ligne grand public basée sur un simple profil démographique, n'affectera pas les personnes concernées de façon similaire de manière significative : «les femmes de la région bruxelloise âgées de 25 à 35 ans qui sont susceptibles de s'intéresser à la mode et à certains articles d'habillement».

Toutefois, il se peut que ce soit le cas, selon les caractéristiques particulières de la situation, y compris en ce qui concerne:

- le caractère intrusif du processus de profilage, y compris le suivi des personnes sur différents sites web, appareils et services;
- les attentes et les souhaits des personnes concernées;
- la façon dont l'annonce est diffusée; ou
- le recours aux vulnérabilités connues des personnes concernées visées.

Un traitement qui pourrait avoir peu d'incidences sur les personnes en général peut en fait avoir un effet significatif à l'égard de certains groupes de la société, tels que les groupes minoritaires ou les

adultes vulnérables. Par exemple, une personne dont il est connu qu'elle éprouve des difficultés financières ou qui est susceptible d'éprouver de telles difficultés, et qui est régulièrement ciblée par des publicités pour des prêts à taux d'intérêt élevé, peut s'inscrire à ces offres et s'endetter davantage.

La prise de décision automatisée qui se traduit par des prix différentiels fondés sur des données à caractère personnel ou des caractéristiques personnelles pourrait également avoir un effet significatif si, par exemple, des prix prohibitifs empêchent effectivement une personne d'accéder à certains biens ou services.

La personne concernée pourrait également subir des effets l'affectant de manière significative de façon similaire, qui seraient déclenchés par les actions d'individus autres que celui auquel se rapporte la décision automatisée. Une illustration en est donnée ci-dessous.

Exemple

Hypothétiquement, une société émettrice de cartes de crédit pourrait réduire la limite de crédit d'un client, non pas en fonction de ses propres antécédents de remboursement, mais en fonction de critères de crédit non traditionnels, comme une analyse d'autres clients vivant dans la même région qui font leurs courses dans les mêmes magasins.

Cela pourrait signifier qu'une personne est privée d'opportunités en raison des actions de tiers.

Dans un contexte différent, l'utilisation de ces types de caractéristiques pourrait avoir l'avantage d'accorder du crédit à ceux qui n'ont pas d'antécédents de crédit conventionnels et qui, autrement, se seraient vu refuser cette possibilité.

C. Exceptions à l'interdiction

L'article 22, paragraphe 1, interdit de manière générale la prise de décision individuelle fondée exclusivement sur un traitement automatisé et produisant des effets juridiques ou affectant la personne concernée de manière significative de façon similaire, comme décrit ci-dessus.

Cela signifie que le responsable du traitement ne devrait pas entreprendre le traitement décrit à l'article 22, paragraphe 1, sauf si l'une des exceptions suivantes prévues à l'article 22, paragraphe 2, s'applique, lorsque la décision est:

- a) nécessaire à la conclusion ou à l'exécution d'un contrat;
- b) autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou
- c) fondée sur le consentement explicite de la personne concernée.

Lorsque la prise de décision concerne des catégories particulières de données définies à l'article 9, paragraphe 1, le responsable du traitement doit également s'assurer qu'elles peuvent satisfaire aux exigences de l'article 22, paragraphe 4.

1. Exécution d'un contrat

Les responsables du traitement peuvent souhaiter utiliser des processus décisionnels exclusivement automatisés à des fins contractuelles parce qu'ils estiment que c'est la façon la plus appropriée

d'atteindre l'objectif. Il se peut que l'intervention humaine de routine soit parfois irréaliste sur le plan pratique ou impossible en raison de la quantité de données traitées.

Le responsable du traitement doit être en mesure de démontrer que ce type de traitement est nécessaire, en tenant compte du fait qu'une méthode plus respectueuse de la vie privée pourrait être adoptée.³⁵ S'il existe d'autres moyens efficaces et moins intrusifs pour atteindre le même but, alors le traitement ne serait pas «nécessaire».

La prise de décision automatisée décrite à l'article 22, paragraphe 1, peut également être nécessaire pour le traitement précontractuel.

Exemple

Une entreprise annonce un poste vacant. Dans la mesure où les postes au sein de l'entreprise en question sont très convoités, celle-ci reçoit des dizaines de milliers de candidatures. En raison du nombre exceptionnellement élevé de candidatures, l'entreprise peut considérer qu'il n'est pas possible d'identifier les candidats appropriés sans utiliser d'abord des moyens entièrement automatisés pour éliminer les candidatures non pertinentes. Dans ce cas, une prise de décision automatisée peut s'avérer nécessaire pour établir une liste restreinte de candidats possibles, avec l'intention de conclure un contrat avec une personne concernée.

Le chapitre III (section B) fournit davantage d'informations sur les contrats en tant que base légale pour le traitement.

2. Autorisée par le droit de l'Union ou le droit de l'État membre

La prise de décision automatisée, y compris le profilage, pourrait avoir lieu en vertu de l'article 22, paragraphe 2, point b), si le droit de l'Union ou de l'État membre en autorisait l'utilisation. La législation pertinente doit également prévoir des mesures appropriées pour sauvegarder les droits et libertés et les intérêts légitimes de la personne concernée.

Le considérant 71 indique que cela pourrait inclure l'utilisation de la prise de décision automatisée définie à l'article 22, paragraphe 1, aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale, ou d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement.

3. Consentement explicite

L'article 22 exige un consentement *explicite*. Le traitement qui relève de la définition de l'article 22, paragraphe 1, présente des risques importants en matière de protection des données, et un niveau élevé de contrôle individuel sur les données à caractère personnel est donc jugé approprié.

³⁵ Buttarelli, Giovanni. Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, Contrôleur européen de la protection des données, 11 avril 2017, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf Consulté le 24 avril 2017.

Le «consentement explicite» n'est pas défini dans le RGPD. Les lignes directrices du GT29 sur le consentement³⁶ fournissent des orientations sur la façon dont cela doit être interprété.

Le chapitre III (section B) fournit davantage d'informations sur le consentement en général.

D. Catégories particulières de données à caractère personnel – Article 22, paragraphe 4

La prise de décision automatisée (décrite à l'article 22, paragraphe 1) qui implique des catégories particulières de données à caractère personnel n'est autorisée que dans les conditions cumulatives suivantes (article 22, paragraphe 4):

- il existe une exception applicable en vertu de l'article 22, paragraphe 2; et
- l'article 9, paragraphe 2, point a) ou g), s'applique.

Article 9, paragraphe 2, point a) – le consentement explicite de la personne concernée; ou
--

Article 9, paragraphe 2, point g) – traitement nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre 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.

Dans les deux cas susmentionnés, le responsable du traitement doit mettre en place des mesures appropriées pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes.

E. Droits de la personne concernée³⁷

1. Articles 13, paragraphe 2, point f), et article 14, paragraphe 2, point g) – Droit d'être informé

Compte tenu des risques et atteintes potentiels que le profilage visé à l'article 22 fait peser sur les droits des personnes concernées, les responsables du traitement devraient être particulièrement attentifs à leurs obligations en matière de transparence.

L'article 13, paragraphe 2, point f), et l'article 14, paragraphe 2, point g), exigent des responsables du traitement qu'ils fournissent des informations spécifiques et facilement accessibles sur la prise de décision automatisée fondée exclusivement sur un traitement automatisé, y compris le profilage, qui

³⁶ Groupe de travail «article 29» sur la protection des données. Lignes directrices sur le consentement au titre du règlement (UE) 2016/679 (Guidelines on Consent under Regulation 2016/679), WP259. 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Consultées le 18 décembre 2017.

³⁷ L'article 12 du RGPD prévoit les modalités applicables à l'exercice des droits de la personne concernée.

produit des effets juridiques ou affecte la personne concernée de manière significative de façon similaire³⁸.

Si le responsable du traitement prend des décisions automatisées au sens de l'article 22, paragraphe 1, il doit:

- dire à la personne concernée qu'il pratique ce type d'activité;
- fournir des informations utiles concernant la logique sous-jacente; et
- expliquer l'importance et les conséquences prévues du traitement.

La communication de ces informations aidera également les responsables du traitement à s'assurer qu'ils respectent certaines des garanties requises visées à l'article 22, paragraphe 3, et au considérant 71.

Si la prise de décision et le profilage automatisés ne satisfont pas à la définition de l'article 22, paragraphe 1, il est néanmoins de bonne pratique de fournir les informations ci-dessus. En tout état de cause, le responsable du traitement doit fournir à la personne concernée des informations suffisantes pour rendre le traitement loyal³⁹ et satisfaire à toutes les autres exigences en matière d'information prévues aux articles 13 et 14.

Informations utiles concernant la «logique sous-jacente»

En raison de la croissance et de la complexité de l'apprentissage automatique, il peut s'avérer difficile de comprendre le fonctionnement d'un processus décisionnel ou d'un profilage automatisé.

Le responsable du traitement devrait trouver des moyens simples d'informer la personne concernée de la raison d'être de la décision ou des critères sur lesquels elle est fondée. Le RGPD exige que le responsable du traitement fournisse des informations utiles sur la logique sous-jacente, mais pas nécessairement une explication complexe des algorithmes utilisés ou la divulgation de l'algorithme complet⁴⁰. Les informations fournies doivent toutefois être suffisamment complètes pour que la personne concernée comprenne les raisons de la décision.

Exemple

Un responsable du traitement utilise la note de solvabilité pour évaluer et rejeter la demande de prêt d'une personne. La note peut avoir été fournie par une agence de référence de crédit ou calculée directement sur la base des informations détenues par le responsable du traitement.

Quelle que soit la source [et les informations sur la source doivent être fournies à la personne concernée en vertu de l'article 14, paragraphe 2, point f), lorsque les données à caractère personnel

³⁸ Voir l'article 22, paragraphes 1 et 4. Les lignes directrices du groupe de travail sur la transparence couvrent les exigences générales en matière d'information énoncées aux articles 13 et 14.

³⁹ Le considérant 60 du RGPD dispose que «le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci.»

⁴⁰ La complexité ne peut excuser l'absence de fourniture d'informations à la personne concernée. Le considérant 58 dispose que le principe de transparence «vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne.»

n'ont pas été collectées auprès de la personne concernée], si le responsable du traitement se fonde sur cette note, il doit être en mesure de l'expliquer et d'en expliquer la raison à la personne concernée.

Le responsable du traitement explique que ce processus l'aide à prendre des décisions de prêt loyales et responsables. Il fournit des détails sur les principales caractéristiques prises en considération pour parvenir à la décision, la source de ces informations et leur pertinence. Cela peut inclure, par exemple:

- les informations fournies par la personne concernée dans le formulaire de demande;
- des informations sur la situation antérieure du compte, y compris tout arriéré de paiement; et
- les registres publics officiels tels que les registres de fraude et les registres d'insolvabilité.

Le responsable du traitement inclut également des informations pour informer la personne concernée que les méthodes de notation de la solvabilité utilisées sont régulièrement testées pour s'assurer qu'elles restent loyales, efficaces et impartiales.

Le responsable du traitement fournit des coordonnées de contact à la personne concernée afin que celle-ci puisse demander le réexamen de toute décision refusée, conformément aux dispositions de l'article 22, paragraphe 3.

«Importance» et «conséquences prévues»

Ces termes suggèrent que des informations doivent être fournies sur les traitements prévus ou futurs et sur la manière dont la prise de décision automatisée pourrait affecter la personne concernée⁴¹. Afin de rendre ces informations utiles et compréhensibles, des exemples réels et tangibles du type d'effets possibles devraient être donnés.

Dans un contexte numérique, les responsables du traitement pourraient être en mesure d'utiliser des outils supplémentaires pour illustrer ces effets.

Exemple

Une compagnie d'assurance utilise un processus décisionnel automatisé pour fixer les primes d'assurance-automobile en fonction du comportement des clients au volant. Pour illustrer l'importance et les conséquences prévues du traitement, elle explique que la conduite dangereuse peut entraîner une augmentation des primes d'assurance et fournit une application comparant les comportements de conducteurs fictifs, y compris ceux qui ont des habitudes dangereuses au volant comme l'accélération rapide et le freinage de dernière minute.

Elle utilise des graphiques pour donner des conseils sur la façon d'améliorer ces habitudes et, par conséquent, de réduire les primes d'assurance.

⁴¹ Conseil de l'Europe. Projet de rapport explicatif sur la version modernisée de la Convention 108 du Conseil de l'Europe, paragraphe 75: «Les personnes concernées ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données, y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage. Par exemple, dans le cas d'un système d'évaluation de leur solvabilité par notation, les emprunteurs ont le droit d'obtenir connaissance de la logique sur laquelle repose le traitement de leurs données et qui aboutit à la décision d'octroi ou de refus du crédit, au lieu d'être simplement informés de la décision elle-même. La compréhension de ces éléments contribue à l'exercice effectif d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente.» <https://rm.coe.int/convention-pour-la-protection-des-personnes-a-l-egard-du-traitement-au/16806b6ec3>. Consultée le 24 avril 2017.

Les responsables du traitement peuvent utiliser des techniques visuelles similaires pour expliquer la manière dont une décision antérieure a été prise.

2. Article 15, paragraphe 1, point h) — Droit d'accès

L'article 15, paragraphe 1, point h), autorise les personnes concernées à disposer des mêmes informations concernant une prise de décision exclusivement automatisée, y compris un profilage, que celles requises en vertu de l'article 13, paragraphe 2, point f), et de l'article 14, paragraphe 2, point g), à savoir:

- l'existence d'une prise de décision automatisée, y compris un profilage;
- des informations utiles concernant la logique sous-jacente; et
- l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le responsable du traitement devrait déjà avoir fourni ces informations à la personne concernée, conformément à ses obligations au titre de l'article 13⁴².

L'article 15, paragraphe 1, point h), dispose que le responsable du traitement devrait fournir à la personne concernée des informations sur les *conséquences prévues* du traitement, plutôt qu'une explication d'une décision *particulière*. Le considérant 63 clarifie ce point en précisant que toute personne concernée devrait avoir le droit de se faire «communiquer» des informations sur le traitement automatique des données, y compris la logique sous-jacente et, *au moins* en cas de profilage, les conséquences d'un tel traitement.

En exerçant ses droits en vertu de l'article 15, la personne concernée peut prendre connaissance d'une décision prise à son égard, y compris une décision fondée sur un profilage.

Le responsable du traitement devrait fournir à la personne concernée des informations générales (notamment sur les facteurs pris en considération pour le processus décisionnel et sur leur «importance» respective à un niveau agrégé) qui lui sont également utiles pour contester la décision.

F. Établissement de garanties appropriées

Si la base applicable au traitement est l'article 22, paragraphe 2, point a) ou l'article 22, paragraphe 2, point c), l'article 22, paragraphe 3 exige que les responsables du traitement mettent en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes des personnes concernées. En vertu de l'article 22, paragraphe 2, point b), le droit de l'État membre ou de l'Union qui autorise le traitement doit également prévoir des mesures de sauvegarde appropriées.

Ces mesures devraient inclure au minimum un moyen permettant à la personne concernée d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision.

L'intervention humaine est un élément clé. Tout examen doit être effectué par une personne qui a l'autorité et la compétence appropriées pour modifier la décision. L'examineur devrait procéder à une évaluation approfondie de toutes les données pertinentes, y compris toute information supplémentaire fournie par la personne concernée.

⁴² L'article 12, paragraphe 3, du RGPD précise les délais de fourniture de ces informations.

Le considérant 71 souligne qu'*en tout état de cause*, les garanties appropriées devraient également comprendre:

«[...] une information spécifique de la personne concernée ainsi que le droit [...] d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.»

Le responsable du traitement doit fournir à la personne concernée un moyen simple d'exercer ces droits.

Cela souligne la nécessité d'assurer la transparence du traitement. La personne concernée ne pourra contester une décision ou exprimer son point de vue que si elle comprend parfaitement la manière dont la décision a été prise et sur quelle base. Les exigences de transparence sont examinées au chapitre IV (section E).

Des erreurs ou des biais dans les données recueillies ou partagées ou une erreur ou un biais dans le processus décisionnel automatisé peuvent avoir comme conséquences:

- des classifications incorrectes; et
- des évaluations fondées sur des projections imprécises; qui
- ont une incidence négative sur les individus.

Les responsables du traitement devraient procéder à des évaluations fréquentes des ensembles de données qu'ils traitent afin de vérifier s'il n'y a pas de biais, et élaborer des moyens de traiter tout élément préjudiciable, y compris toute dépendance excessive à l'égard des corrélations. Les systèmes qui vérifient les algorithmes et les examens réguliers de l'exactitude et de la pertinence de la prise de décision automatisée, y compris le profilage, sont d'autres mesures utiles.

Les responsables du traitement devraient mettre en place des procédures et des mesures appropriées pour prévenir les erreurs, les inexactitudes⁴³ ou la discrimination sur la base de données de catégories particulières. Ces mesures devraient être utilisées sur une base cyclique; non seulement au stade de la conception, mais aussi en permanence, car le profilage est appliqué aux individus. Les résultats de ces mesures devraient être pris en considération dans la conception du système.

D'autres exemples de mesures de sauvegarde appropriées sont disponibles dans la section [Recommandations](#)

V. Enfants et profilage

Le RGPD instaure des obligations supplémentaires pour les responsables du traitement des données lorsqu'ils traitent des données à caractère personnel relatives aux enfants.

L'article 22 lui-même ne fait aucune distinction selon que le traitement concerne des adultes ou des enfants. Toutefois, le considérant 71 indique que les décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques ou affectant la personne concernée de manière

⁴³ Le considérant 71 du RGPD indique ce qui suit:

«Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, [...]»

significative de façon similaire, ne devraient pas s'appliquer aux enfants⁴⁴. Étant donné que cette formulation n'est pas reflétée dans l'article lui-même, le GT29 estime qu'il ne s'agit pas d'une interdiction absolue de ce type de traitement à l'égard des enfants. Toutefois, à la lumière de ce considérant, le GT29 recommande aux responsables du traitement de ne pas invoquer, en principe, les exceptions prévues à l'article 22, paragraphe 2, pour le justifier.

Il peut néanmoins y avoir des circonstances dans lesquelles il est nécessaire que les responsables du traitement prennent des décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques ou affectant les enfants de manière significative de façon similaire, par exemple pour protéger leur bien-être. Dans un tel cas, le traitement peut être effectué sur la base des exceptions visées à l'article 22, paragraphe 2, points a), b) ou c), selon le cas.

Dans ces cas, des garanties appropriées doivent être en place, comme l'exigent l'article 22, paragraphe 2, point b), et l'article 22, paragraphe 3, et elles doivent donc être adaptées aux enfants. Le responsable du traitement doit veiller à ce que ces garanties soient efficaces pour protéger les droits, les libertés et les intérêts légitimes des enfants dont les données sont traitées.

La nécessité d'une protection spécifique pour les enfants est reflétée dans le considérant 38, qui dispose ce qui suit:

«Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant.»

L'article 22 n'empêche pas les responsables du traitement de prendre des décisions exclusivement automatisées concernant les enfants, si la décision ne produit pas d'effet juridique ou n'affecte pas l'enfant de manière significative de façon similaire. Cependant, une prise de décision exclusivement automatisée qui influence les choix et le comportement d'un enfant pourrait potentiellement produire un effet juridique ou l'affecter de manière significative de façon similaire, selon la nature des choix et des comportements en question.

Dans la mesure où les enfants représentent un groupe plus vulnérable de la société, les organisations devraient, en général, s'abstenir de les profiler à des fins de marketing⁴⁵. Les enfants peuvent être particulièrement vulnérables dans l'environnement en ligne et plus facilement influencés par la publicité comportementale. Par exemple, dans les jeux en ligne, le profilage peut être utilisé pour cibler les joueurs qui, selon l'algorithme, sont plus susceptibles de dépenser de l'argent dans le jeu et pour fournir des publicités plus personnalisées. L'âge et la maturité de l'enfant peuvent affecter sa

⁴⁴ Considérant 71 – «Cette mesure ne devrait pas concerner un enfant.»

⁴⁵ L'avis 02/2013 du GT29 sur les applications destinées aux dispositifs intelligents (WP202), adopté le 27 février 2013, dans sa section 3.10 consacrée aux enfants, précise à la page 26 que les responsables du traitement des données ne doivent pas traiter les données des enfants à des fins de publicité comportementale, ni directement ni indirectement, car l'enfant n'est pas en mesure d'en comprendre la finalité et cela dépasse donc les limites du traitement licite.

capacité à comprendre la motivation qui sous-tend ce type de marketing ou les conséquences qui en découlent⁴⁶.

L'article 40, paragraphe 2, point g, fait explicitement référence à l'élaboration de codes de conduite prévoyant des garanties pour les enfants; il est également possible de compléter des codes existants⁴⁷.

VI. Analyses d'impact relatives à la protection des données et délégué à la protection des données

La responsabilité est un domaine important et une exigence explicite dans le cadre du RGPD.⁴⁸

En tant qu'outil clé de responsabilisation, une analyse d'impact relative à la protection des données permet au responsable du traitement d'évaluer les risques associés à la prise de décision automatisée, y compris le profilage. Il s'agit d'une façon de montrer que des mesures appropriées ont été mises en place pour faire face à ces risques et démontrer la conformité avec le RGPD.

L'article 35, paragraphe 3, point a), souligne la nécessité pour le responsable du traitement d'effectuer une analyse d'impact relative à la protection des données dans les cas suivants:

l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est *fondée sur* un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

L'article 35, paragraphe 3, point a), fait référence aux évaluations, y compris le profilage et les décisions qui sont «fondées» sur un traitement automatisé, plutôt que sur un traitement «exclusivement» automatisé. Cela signifie que l'article 35, paragraphe 3, point a), s'appliquera dans le cas d'une prise de décision, y compris un profilage, produisant des effets juridiques ou affectant les personnes concernées de manière significative de façon similaire, qui *n'est pas* entièrement automatisée, ainsi que d'une prise de décision exclusivement automatisée définie à l'article 22, paragraphe 1.

Si le responsable du traitement envisage un «modèle» dans lequel il prend des décisions *exclusivement* automatisées ayant une *forte incidence* sur les personnes concernées sur la base de profils établis à leur sujet et qu'il *ne peut* se fonder sur le consentement de ces personnes, sur un contrat conclu avec elles ou sur une loi l'autorisant, le responsable du traitement ne devrait pas poursuivre la procédure.

Le responsable du traitement peut toujours envisager un «modèle» de prise de décision fondé sur le profilage, en augmentant sensiblement le niveau d'intervention humaine, de sorte que le modèle *n'est plus un processus décisionnel entièrement automatisé*, bien que le traitement puisse encore présenter

⁴⁶ Une étude de l'UE sur [l'impact du marketing par l'intermédiaire des médias sociaux, des jeux en ligne et des applications mobiles sur le comportement des enfants](#) a montré que les pratiques de marketing ont une incidence manifeste sur le comportement des enfants. Cette étude s'est fondée sur des enfants âgés de 6 à 12 ans.

⁴⁷ Un exemple de code de conduite en matière de marketing auprès des enfants est celui produit par la FEDMA, memorandum explicatif, disponible à l'adresse: <http://www.oecd.org/sti/ieconomy/2091875.pdf> Consulté le 15 mai 2017. Voir en particulier: «6.2 Les agents de marketing ciblant les enfants, ou pour lesquels les enfants sont susceptibles de constituer une partie de leur public, ne devraient pas exploiter la crédulité, la loyauté, la vulnérabilité ou le manque d'expérience des enfants; 6.8.5 Les agents de marketing ne devraient pas subordonner l'accès d'un enfant à un site web à la collecte de renseignements personnels détaillés. En particulier, des mesures incitatives spéciales telles que des offres de prix et des jeux ne devraient pas être utilisées pour inciter les enfants à divulguer des informations personnelles détaillées» (traduction libre).

⁴⁸ Comme l'exige l'article 5, paragraphe 2, du RGPD.

des risques pour les droits et libertés fondamentaux des personnes concernées. Si tel est le cas, le responsable du traitement doit s'assurer qu'il peut faire face à ces risques et satisfaire aux exigences décrites au chapitre III des présentes lignes directrices.

Une analyse d'impact relative à la protection des données peut également s'avérer utile pour permettre au responsable du traitement de définir les mesures qu'il introduira pour faire face aux risques liés à la protection des données concernées par le traitement. Ces mesures⁴⁹ pourraient notamment consister à:

- informer la personne concernée de l'existence et de la logique sous-jacente du processus décisionnel automatisé;
- expliquer l'importance et les conséquences prévues du traitement pour la personne concernée;
- fournir à la personne concernée les moyens de s'opposer à la décision; et à
- permettre à la personne concernée d'exprimer son point de vue.

D'autres activités de profilage peuvent justifier une analyse d'impact relative à la protection des données, selon les particularités du cas. Les responsables du traitement peuvent consulter les lignes directrices du GT29 sur les analyses d'impact relatives à la protection des données⁵⁰ pour de plus amples renseignements et pour déterminer la nécessité d'effectuer une analyse d'impact relative à la protection des données.

Une exigence supplémentaire en matière de responsabilité est la désignation d'un délégué à la protection des données (DPD), lorsque le profilage et/ou la prise de décision automatisée constituent une activité de base du responsable du traitement et exigent un suivi régulier et systématique à grande échelle des personnes concernées [article 37, paragraphe 1, point b)]⁵¹.

Commented [W11]: SENS

⁴⁹ Reflétant les exigences de l'article 13, paragraphe 2, point f), de l'article 14, paragraphe 2, point g), et de l'article 22, paragraphe 3.

⁵⁰ Groupe de travail «article 29» sur la protection des données. Groupe de travail «article 29», lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679. 4 avril 2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Consultées le 24 avril 2017.

⁵¹ Groupe de travail «article 29» sur la protection des données. Lignes directrices concernant les délégués à la protection des données (DPD). 5 avril 2017; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 Consultées le 22 janvier 2018.

ANNEXE 1 – Recommandations de bonnes pratiques

Les recommandations de bonnes pratiques suivantes aideront les responsables du traitement des données à satisfaire aux exigences des dispositions du RGPD sur le profilage et la prise de décision automatisée⁵².

Article	Objet	Recommandation
5, paragraphe 1, point a), 12, 13, 14	Droit à l'information	<p>Les responsables du traitement devraient consulter les lignes directrices du GT29 sur la transparence (WP260) pour les exigences générales en matière de transparence.</p> <p>Outre les exigences générales, lorsque le responsable du traitement traite des données au sens de l'article 22, il doit fournir des informations utiles concernant la logique sous-jacente.</p> <p>Au lieu de fournir une explication mathématique complexe sur le fonctionnement des algorithmes ou de l'apprentissage automatique, le responsable du traitement devrait envisager d'utiliser des moyens clairs et complets pour fournir les informations à la personne concernée, par exemple:</p> <ul style="list-style-type: none"> • les catégories de données qui ont été ou seront utilisées dans le processus de profilage ou de prise de décision; • les raisons pour lesquelles ces catégories sont jugées pertinentes; • la façon dont tout profil utilisé dans le processus décisionnel automatisé est établi, y compris les statistiques utilisées dans l'analyse; • les raisons pour lesquelles ce profil est pertinent pour le processus décisionnel automatisé; et • la manière dont il est utilisé aux fins d'une décision au sujet de la personne concernée. <p>Ces informations seront généralement plus pertinentes pour la personne concernée et contribueront à la transparence du traitement.</p> <p>Les responsables du traitement peuvent envisager des techniques de visualisation et des techniques interactives pour faciliter la transparence algorithmique⁵³.</p>

⁵² Les responsables du traitement doivent également s'assurer qu'ils ont mis en place des procédures solides pour garantir qu'ils peuvent remplir les obligations qui leur incombent en vertu des articles 15 à 22 dans les délais prévus par le RGPD.

⁵³ Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0 (Commissariat à l'information - Mégadonnées, intelligence artificielle, apprentissage automatique et protection des données version 2.0), mars 2017. Page 87, paragraphe 194, mars 2017.

<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

Document consulté le 24 avril 2017.

article 6, paragraphe 1, point a)	Consentement comme base du traitement	Si les responsables du traitement se fondent sur le consentement comme base du traitement, ils devraient consulter les lignes directrices du GT29 sur le consentement (WP259).
15	Droit d'accès	Les responsables du traitement peuvent envisager de mettre en place un mécanisme permettant aux personnes concernées de vérifier leur profil, y compris les détails des informations et des sources utilisées pour l'établir.
16	Droit de rectification	Les responsables du traitement qui donnent aux personnes concernées l'accès à leur profil dans le cadre de leurs droits au titre de l'article 15 devraient leur donner la possibilité de mettre à jour ou de corriger toute inexactitude concernant leurs données ou leur profil. Cela peut également aider les responsables du traitement à remplir leurs obligations au titre de l'article 5, paragraphe 1, point d). Les responsables du traitement pourraient envisager d'introduire des outils de gestion des préférences en ligne tels qu'un tableau de bord sur la protection de la vie privée. Cela donnerait aux personnes concernées la possibilité de gérer l'utilisation de leurs informations dans un certain nombre de services différents – ce qui leur permettrait de modifier les paramètres, de mettre à jour leurs données à caractère personnel et d'examiner ou de modifier leur profil pour corriger toute inexactitude.
21, paragraphes 1 et 2	Droit d'opposition	Le droit d'opposition visé à l'article 21, paragraphes 1 et 2, doit être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information (article 21, paragraphe 4). Les responsables du traitement doivent s'assurer que ce droit est affiché clairement sur leur site web ou dans toute documentation pertinente et qu'il n'est pas dissimulé dans d'autres modalités et conditions.
22 et considérant 71	Garanties appropriées	La liste suivante, bien que non exhaustive, fournit quelques suggestions de bonnes pratiques dont les responsables du traitement doivent tenir compte lorsqu'ils prennent une décision fondée exclusivement sur un traitement automatisé, y compris le profilage (visée à l'article 22, paragraphe 1): <ul style="list-style-type: none"> • des contrôles réguliers d'assurance qualité de leurs systèmes pour veiller à ce que les personnes soient traitées équitablement et ne fassent pas l'objet de discriminations, que ce soit sur la base de catégories particulières de données à caractère personnel ou autrement; • l'audit algorithmique, qui consiste à tester les algorithmes utilisés et développés par les systèmes d'apprentissage automatique pour prouver qu'ils

		<p>fonctionnent réellement comme prévu et qu'ils ne produisent pas de résultats discriminatoires, erronés ou injustifiés;</p> <ul style="list-style-type: none"> • pour les audits effectués par un «tiers» indépendant (lorsque la prise de décision fondée sur le profilage a une forte incidence sur les personnes concernées), fournir à l'auditeur toute information nécessaire sur le fonctionnement de l'algorithme ou du système d'apprentissage automatique; • obtenir des garanties contractuelles pour les algorithmes de tiers que l'audit et les tests ont été effectués et que l'algorithme est conforme aux normes convenues; • des mesures spécifiques de minimisation des données afin de prévoir des périodes de conservation clairement définies pour les profils et pour toutes les données à caractère personnel utilisées lors de la création ou de l'application des profils; • l'utilisation de techniques d'anonymisation ou de pseudonymisation dans le contexte du profilage; • les moyens de permettre à la personne concernée d'exprimer son point de vue et de contester la décision; et • un mécanisme d'intervention humaine dans des cas précis, par exemple en fournissant un lien vers une procédure de recours au moment où la décision automatisée est transmise à la personne concernée, avec des délais convenus pour l'examen du dossier et un point de contact désigné pour toute question. <p>Les responsables du traitement peuvent également envisager des possibilités telles que:</p> <ul style="list-style-type: none"> • des mécanismes de certification des opérations de traitement; • des codes de conduite pour les processus d'audit recourant à un apprentissage automatique; • des comités d'examen éthique pour évaluer les inconvénients et les avantages potentiels pour la société liés à des applications particulières dans le domaine du profilage.
--	--	--

ANNEXE 2 – Principales dispositions du RGPD

Principales dispositions du RGPD qui font référence au profilage et à la prise de décision automatisée en général

Article	Considérant	Remarques
3, paragraphe 2, point b)	24	Le suivi du comportement des personnes concernées, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. Considérant 24 «[...] suivies sur internet, [...] l'utilisation [...] de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.»
4, paragraphe 4	30	Définition du profilage à l'article 4, paragraphe 4 Considérant 30 «des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence [...] peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.»
5 et 6	72	Considérant 72: «Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnel, par exemple le fondement juridique du traitement (article 6) ou les principes en matière de protection des données (article 5).»
8	38	Utilisation des données à caractère personnel d'enfants à des fins de profilage. Considérant 38: « Les enfants méritent une protection spécifique [...] notamment, [...] à l'utilisation de données à caractère personnel relatives aux enfants à des fins de [...] création de profils de personnalité ou d'utilisateur.»
13 et 14	60	Droit d'être informé Considérant 60: «En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci.»
15	63	Droits d'accès Considérant 63: «le droit de connaître et de se faire communiquer [...] les finalités du traitement des données à caractère personnel, [...] et les conséquences que ce traitement pourrait avoir, au moins en cas de profilage.»
21, paragraphes 1, 2 et 3	70	Droit de s'opposer au profilage Considérant 70 «[...] le droit [...] de s'opposer à ce traitement, y compris le profilage dans la mesure où il est lié à une telle prospection.»
23	73	Considérant 73: «Des limitations à certains principes spécifiques [...] au droit d'opposition, aux décisions fondées sur le profilage [...] peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique [...]» afin de sauvegarder des objectifs spécifiques d'intérêt public général.

35, paragraphe 3, point a)	91	Une analyse d'impact relative à la protection des données est requise dans le cas de «l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est <i>fondée</i> sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;» Cette disposition couvre la prise de décision, y compris le profilage, qui n'est pas exclusivement automatisée.
----------------------------	----	---

Principales dispositions du RGPD qui font référence à la prise de décision exclusivement automatisée définie à l'article 22

Article	Considérant	Remarques
13, paragraphe 2, point f), et 14, paragraphe 2, point g)	61	Droit d'être informé au sujet: <ul style="list-style-type: none"> • de l'existence d'un processus décisionnel automatisé en vertu de l'article 22, paragraphes 1 et 4; • des informations utiles concernant la logique sous-jacente; • de l'importance et des conséquences prévues de ce traitement.
15, point h)		Droits d'accès spécifiques aux informations concernant l'existence d'une prise de décision automatisée, y compris un profilage.
22, paragraphe 1	71	Interdiction de prendre des décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, qui produisent des effets juridiques ou affectent la personne concernée de manière significative de façon similaire. En plus de l'explication fournie dans le corps des lignes directrices, les points suivants développent la raison d'être de l'article 22 en tant qu'interdiction: <ul style="list-style-type: none"> • Bien que le chapitre III traite des droits de la personne concernée, les dispositions des articles 12 à 22 ne concernent pas exclusivement l'exercice <i>actif</i> des droits. Certains droits sont <i>passifs</i>; ils ne portent pas tous sur des situations dans lesquelles la personne concernée prend une mesure, c'est-à-dire qu'elle formule une demande, une plainte ou une exigence quelconque. Les articles 15 à 18 et 20 et 21 concernent l'exercice actif des droits de la personne concernée, mais les articles 13 et 14 concernent les devoirs que le responsable du traitement doit remplir, sans aucune intervention active de la personne concernée. Ainsi, l'inclusion de l'article 22 dans ce chapitre ne signifie pas en soi qu'il s'agit d'un droit d'opposition; • L'article 12, paragraphe 2, mentionne «l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22»; mais cela ne signifie pas que l'article 22, paragraphe 1, lui-même doit être interprété comme un droit. Il <i>existe</i> un droit actif au titre de l'article 22, mais il fait partie des garanties qui doivent être appliquées dans les cas où la prise de décision automatisée est autorisée [article 22,

		<p>paragraphe 2, points a) à c)] - le droit d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision. Il ne s'applique que dans ces cas, car il est interdit d'effectuer le traitement décrit à l'article 22, paragraphe 1, sur d'autres bases;</p> <ul style="list-style-type: none"> • L'article 22 se trouve dans une section du RGPD appelée «Droit d'opposition et prise de décision individuelle automatisée», ce qui implique que l'article 22 n'est <i>pas</i> un droit d'opposition comme l'article 21. Cela est encore renforcé par l'absence, à l'article 22, d'une obligation d'information explicite équivalente à celle qui figure à l'article 21, paragraphe 4; • Si l'article 22 devait être interprété comme un droit d'opposition, l'exception prévue à l'article 22, paragraphe 2, point c), n'aurait pas beaucoup de sens. L'exception prévoit que la prise de décision automatisée peut encore avoir lieu si la personne concernée a donné son consentement explicite (voir ci-dessous). Cela serait contradictoire, car une personne concernée ne peut pas s'opposer et consentir au même traitement; • Une objection signifierait qu'une intervention humaine doit avoir lieu. Les exceptions visées à l'article 22, paragraphe 2, points a) et c), prévalent sur la règle principale de l'article 22, paragraphe 1, mais uniquement tant qu'une intervention humaine est à la disposition de la personne concernée, conformément à l'article 22, paragraphe 3. Étant donné que la personne concernée a déjà demandé une intervention humaine (par son opposition), l'article 22, paragraphe 2, points a) et c), serait automatiquement contourné dans tous les cas, le rendant ainsi dénué de sens dans les faits. <p>Considérant 71: «Ce type de traitement inclut le “profilage” qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements [...]» <i>«Cette mesure ne devrait pas concerner un enfant.»</i></p>
<p>22, paragraphe 2, points a) à c)</p>	<p>71</p>	<p>L'article 22, paragraphe 2, lève l'interdiction de traitement sur la base de a) l'exécution ou la conclusion d'un contrat, b) du droit de l'Union ou de l'État membre, ou c) du consentement explicite. Le considérant 71 fournit un complément d'information sur l'article 22, paragraphe 2, point b), et indique que le traitement visé à l'article 22, paragraphe 1: «[...] devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des</p>

		institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement [...].»
22, paragraphe 3	71	L'article 22, paragraphe 3, et le considérant 71 précisent également que même dans les cas visés à l' article 22, paragraphe 2, points a) et c) , le traitement devrait faire l'objet de garanties appropriées. Considérant 71: «qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant.»
23	73	Considérant 73: «Des limitations à certains principes spécifiques [...] au droit d'opposition, aux décisions fondées sur le profilage [...] peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique [...]» afin de sauvegarder des objectifs spécifiques d'intérêt public général.
35, paragraphe 3, point a)	91	Exigences concernant la réalisation d'une analyse d'impact relative à la protection des données
47, paragraphe 2, point e)		Les règles d'entreprise contraignantes visées à l' article 47, paragraphe 1 , devraient préciser au moins «le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l' article 22 ».

ANNEXE 3 - Lectures complémentaires

Les présentes lignes directrices tiennent compte des documents suivants:

- [GT29, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation \(Document d'orientation sur les éléments essentiels d'une définition et d'une disposition sur le profilage dans le règlement général de l'UE sur la protection des données\), adopté le 13 mai 2013;](#)
- [GT29, avis 2/2010 sur la publicité comportementale en ligne, WP171;](#)
- [GT29, avis 03/2013 sur la limitation des finalités, WP 203;](#)
- [GT29, avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP217](#)
- [GT29, Statement on the role of a risk-based approach to data protection legal frameworks \(Déclaration sur le rôle d'une approche fondée sur les risques dans les cadres juridiques de protection des données\), WP218;](#)
- [GT29, avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, WP223;](#)
- [GT29, Lignes directrices concernant les délégués à la protection des données \(DPD\), WP243;](#)

- [GT29, Lignes directrices sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, WP244;](#)
- [GT29, Lignes directrices sur le consentement, WP259](#)
- [GT29, Lignes directrices sur la transparence, WP260](#)
- [Conseil de l'Europe. Recommandation CM/Rec\(2010\)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage;](#)
- [Conseil de l'Europe. Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, janvier 2017](#)
- [Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0 \(Commissariat à l'information - Mégadonnées, intelligence artificielle, apprentissage automatique et protection des données version 2.0\), mars 2017](#)
- [Bureau du Commissaire à l'information de l'Australie - Consultation draft: Guide to big data and the Australian Privacy Principles \(Projet de consultation: le guide des mégadonnées et des principes australiens de protection de la vie privée\), mai 2016](#)
- [Contrôleur européen de la protection des données \(EDPS\), avis 7/2015 – Relever les défis des données massives, 19 novembre 2015](#)
- [Datatilsynet – Big Data – privacy principles under pressure \(Mégadonnées - les principes de protection de la vie privée sous pression\), septembre 2013](#)
- [Conseil de l'Europe. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel - Projet de rapport explicatif sur la version modernisée de la Convention 108 du Conseil de l'Europe, août 2016](#)
- [Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy \(La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée\). Rapport, novembre 2015.](#)
- [Contrôleur européen de la protection des données – Évaluer la nécessité de mesures qui limitent le droit fondamental à la protection des données à caractère personnel: une boîte à outils \(Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit\).](#)
- [Comité mixte des autorités européennes de surveillance. Joint Committee Discussion Paper on the use of Big Data by financial institutions \(Document de discussion du Comité mixte sur l'utilisation des mégadonnées par les institutions financières\), 2016-86. \[https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf\]\(https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf\).](#)
- [Commission de la protection de la vie privée. Rapport Big Data <https://www.autoriteprotectiondonnees.be/rapport-big-data>.](#)
- [Sénat des États-Unis, Comité du commerce, des sciences et des transports. Examen du secteur des courtiers de données: collecte, utilisation et vente de données sur les consommateurs à des fins de marketing \(A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes\), rapport du personnel pour le président Rockefeller, 18 décembre 2013. \[https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf\]\(https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf\)](#)
- [Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for \(Esclave de l'algorithme? Pourquoi un «droit à une explication» n'est probablement pas le remède que vous recherchez\). Document de recherche, publié le 24 mai 2017. \[https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855\]\(https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855\)](#)
- [NYTimes.com. Showing the Algorithms behind New York City Services \(Présentation des algorithmes qui sous-tendent les services de la ville de New York\). <https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1>. Document consulté le 24 août 2017.](#)
- [Conseil de l'Europe. Recommandation CM/Rec\(2018\)x du Comité des Ministres aux États membres sur des lignes directrices à l'intention des États membres en vue de respecter, protéger et](#)

assurer les droits de l'enfant dans l'environnement numérique (projet révisé, 25 juillet 2017). <https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren> . Document consulté le 31 août 2017.

- Unicef. Privacy, protection of personal information and reputation rights (Protection de la vie privée, protection des renseignements personnels et droit à la réputation). Discussion paper series: Children's Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Document consulté le 31 août 2017.
- Chambre des Lords. Growing up with the internet (Grandir avec internet.). Comité spécial des communications, 2^e rapport des sessions 2016-2017. <https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm>. Consulté le 31 août 2017.
- Sandra Wachter, Brent Mittelstadt et Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation (Pourquoi le règlement général sur la protection des données ne prévoit pas de droit à l'explication de la prise de décision automatisée.), 28 décembre 2016. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/ . Document consulté le 13 décembre 2017.
- Sandra Wachter, Brent Mittelstadt et Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR (Raisonnements contrefactuels sans ouvrir la boîte noire: décisions automatisées et RGPD), 6 octobre 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Document consulté le 13 décembre 2017.
- Gouvernement australien. Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7 (Guide des bonnes pratiques, Aide automatisée à la prise de décisions administratives. Méthodologie en six étapes et résumé des points de la liste de contrôle - Partie 7), février 2007. <https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf>. Document consulté le 9 janvier 2018.