LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN BELGIQUE

Manuel de base

politeia

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Colophon
La protection des données à caractère personnel en Belgique
Manuel de base

Cécile de Terwangne et Élise Degrave
Avec la collaboration d'Antoine Delforge et de Loïck Gérard

ISBN 978-2-509-03505-9
D/2019/8132/88
NUR 820

© Éditions Politeia s.a.
Boulevard de l'Empereur 34
1000 Bruxelles
Tél. (02) 289 26 10
Fax (02) 289 26 19
info@politeia.be
www.politeia.be

Aucun extrait de cette édition ne peut, même partiellement, être communiqué au public, reproduit ni traduit ou adapté sous quelque forme que ce soit moyennant photocopie, microfilm, enregistrement ou tout autre moyen sans l'autorisation écrite et préalable de l'éditeur.

LES AUTEURS

Élise Degrave

Élise Degrave est chargée de cours à la Faculté de droit de l'Université de Namur, chercheuse au CRIDS (Centre de recherches Information, Droit et Société) et co-directrice de la Chaire E-gouvernement de l'Université de Namur. Elle est l'auteure d'une thèse de doctorat consacrée à l'e-gouvernement et à la protection de la vie privée.
Aujourd'hui, elle enseigne notamment le cours de « Gouvernance de l'internet et E-gouvernement » ainsi que le cours de « Régulation des innovations technologiques ». Elle consacre ses recherches universitaires à ces différentes matières. Par ailleurs, elle est membre du Conseil wallon du numérique et est régulièrement auditionnée comme experte en protection de la vie privée par les pouvoirs publics, par les médias et lors de conférences.

Cécile de Terwangne

Cécile de Terwangne est professeur à la Faculté de Droit de l'Université de Namur. Elle dispense notamment les cours de « Vie privée et TIC », de « Droits de l'homme et société de l'information » et de « Numérique, droits fondamentaux et cybercriminalité ». Elle dirige le Master complémentaire en Droit des Technologies de l'Information et de la Communication (D.T.I.C.). Elle est également directrice de recherche au sein de l'Unité Libertés et Société de l'information du Centre de Recherches Information, Droit et Société (CRIDS) et co-directrice de la Chaire E.Gouvernement de l'Université de Namur. Elle est experte auprès du Conseil de l'Europe et de la Commission européenne. Elle est professeur invitée à l'Institut International des Droits de l'Homme, à Strasbourg.

Antoine Delforge

Antoine Delforge est assistant à la Faculté de Droit de l'Université de Namur et chercheur au Centre de Recherches Information, Droit et Société (CRIDS) ainsi qu'au Namur Digital Institute (NADI). Il oriente ses recherches en droit de la protection des données, notamment en matière d'archivage et de Big data. Il étudie également les liens qui existent entre droit de la protection des données et droit de la consommation.

Loïck Gérard

Loïck Gérard est assistant à la Faculté de Droit de l'Université de Namur et chercheur au sein du Centre de Recherche Information, Droit et Société (CRIDS). Ses recherches sont centrées sur l'application des nouvelles technologies aux autorités publiques et, plus particulièrement, sur les traitements et échanges de données à caractère personnel au sein des administrations.

TABLE DES MATIÈRES

Chapitre 6.
Quels contrôles ? 135

INTRODUCTION

À l'heure actuelle, l'entrée en application du Règlement européen général sur la protection des données[1] (ci-après RGPD) en Belgique a déjà mené à l'adoption de quatre lois importantes consacrées à la protection des données à caractère personnel des citoyens.

La loi du 3 décembre 2017 est consacrée à l'Autorité de protection des données, qui remplace la Commission de la protection de la vie privée.

La loi du 30 juillet 2018 précise les aspects du RGPD à propos desquels une marge de manœuvre était laissée aux législateurs nationaux.

La loi du 5 septembre 2018 institue le Comité de sécurité de l'information.

Enfin, la loi du 25 novembre 2018 opère une réforme importante de la loi sur le Registre national.

À la suite de ces lois successives et parcellaires, l'encadrement normatif de la protection des données à caractère personnel s'apparente à un puzzle éclaté. Chaque question régulée constitue pourtant un aspect important d'une même matière. On regrette vivement que le législateur ne les ait pas abordées simultanément, saisissant l'opportunité qu'offrait le RGPD de faire le point sur cette matière complexe et d'adopter une seule loi, construite de manière cohérente, qui aurait offert à chacun clarté et lisibilité.

En outre, pour chacune de ces lois, le Gouvernement demanda l'urgence, malgré la longueur de certaines d'entre elles. S'en suivit un délai insuffisant pour permettre à la Commission de la protection de la vie privée et à la Section de législation du Conseil d'État d'analyser le texte en profondeur. Le temps manqua également pour débattre sereinement des textes en Commission de la justice, avec l'aide d'experts. De tels échanges et analyses étaient pourtant nécessaires vu l'enjeu.

D'ores et déjà, des lacunes, des redites et des incohérences émergent des textes. Symptôme du malaise, la loi du 3 décembre 2017, par exemple, a déjà été modifiée deux fois, la première fois par une loi du 4 mars 2018, la seconde par une loi du 25 mai 2018.

On ne peut que regretter ces faiblesses législatives qui constituent autant de reculs dans la protection de la vie privée des citoyens, fondée notamment sur la transparence et la compréhension des règles qui s'imposent à chacun tout autant qu'elles les protègent.

Dans ce contexte, le présent ouvrage propose au lecteur une synthèse de la matière, agrégeant les règles de protection issues tant du RGPD que des quatre lois citées, et structurée selon un plan cohérent, pour l'aider à cheminer dans les méandres de la protection des données à caractère personnel.

Un premier chapitre présente les notions principales sur lesquelles est bâtie toute la protection mise en place : la donnée à caractère personnel et le traitement (section 1). Il s'arrête

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), *J.O.U.E.*, 4 mai 2016, L 119/1.

ensuite sur les acteurs intervenant dans ce paysage juridique : la personne concernée, le responsable du traitement et le sous-traitant (section 2). La première voit sa protection renforcée par le nouveau régime tandis que les deux autres voient peser sur eux des obligations alourdies ou inédites. Ce chapitre se conclut sur la définition des contours du champ d'application de la législation, tant matériel que personnel et territorial (section 3). Cet exercice révèle combien cette législation touche énormément d'aspects de la vie à la fois économique, sociale, politique, professionnelle, scientifique, relationnelle et de loisirs, et combien elle porte désormais loin au-delà de nos frontières. Au terme de cette section 3, l'exclusion générale du champ d'application réservée aux traitements à des fins exclusivement personnelles ou domestiques retient particulièrement l'attention.

Le chapitre 2 présente les principes de protection qu'il convient de respecter (section 1) et l'exigence de fonder tout traitement sur une des six bases de licéité prévues par le RGPD (section 2). Le régime de protection renforcée des données sensibles et judiciaires y est aussi exposé (section 3).

La longue liste des droits des personnes concernées est présentée au chapitre 3, avec les exemptions et dérogations que le législateur a accordées dans la loi-cadre, à l'invitation de l'article 23 du RGPD (section 1) tandis que les obligations des responsables de traitement et de leurs sous-traitants font l'objet d'une analyse à la section 2 de ce chapitre.

Dans le monde interconnecté d'aujourd'hui, on ne peut faire l'impasse sur les flux transfrontières de données. Les règles applicables à de tels transferts de données à caractère personnel sont décrites au chapitre 4.

Certains régimes largement dérogatoires ont été mis en place par le législateur belge. Les régimes spécifiques encadrant les traitements de données en matière pénale (titre 2 de la loi-cadre) et les traitements effectués par les services de renseignement, les forces armées ou d'autres autorités évoquées au titre 3 de la loi-cadre ne sont pas analysés dans le présent ouvrage qui se focalise sur deux régimes dérogatoires ; l'un concernant les traitements à des fins journalistiques ou d'expression universitaire, artistique ou littéraire (section 1), et l'autre réservé aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (section 2). Ces régimes d'exemptions et de dérogations sont l'objet du chapitre 5.

Le propos s'arrête ensuite, au chapitre 6, sur les multiples contrôles mis en place à l'occasion de l'entrée en application du RGPD. C'est principalement le contrôle effectué par l'Autorité de protection des données (section 1) et par les cours et tribunaux (section 2) qui retient l'attention, ainsi que certains contrôles particuliers (section 3) apparus à la suite de la disparition des comités sectoriels instaurés par le passé au sein de la Commission de la Vie privée, ou réservés aux données du Registre national ou encore aux données de sécurité sociale et de santé. Au titre des compétences de ces autorités de contrôle figure notamment le pouvoir d'imposer des sanctions en cas de non-respect des règles et obligations contenues dans le régime de protection, pouvoir qui a fait grand bruit au moment de l'adoption du RGPD au vu des montants astronomiques que peuvent atteindre les amendes.

La peur de la sanction instille sans doute chez beaucoup d'acteurs le souhait d'être en parfaite conformité avec les règles régissant la protection des données à caractère personnel. Le présent ouvrage axé sur une présentation cohérente de l'ensemble de ces règles applicables en Belgique devrait permettre à chacun de saisir pleinement la portée des principes, droits et obligations à respecter désormais.

Chapitre 1.

QUELLES NOTIONS ? QUELS ACTEURS ? QUEL CHAMP D'APPLICATION ?

QUELLES NOTIONS ? QUELS ACTEURS ? QUEL CHAMP D'APPLICATION ?[1]

Section 1. Les notions principales : la donnée à caractère personnel, le traitement

Les deux notions principales en la matière – la notion de « donnée à caractère personnel » et celle de « traitement » – sont définies à l'article 4 du RGPD. Ces définitions valent pour tous les traitements de données à caractère personnel qui sont couverts par le règlement européen. En Belgique, elles s'appliquent cependant au-delà du champ d'application du règlement étant donné que la loi du 30 juillet 2018[2] stipule que les définitions reprises dans le RGPD sont d'application. Dans un souci de cohérence, la loi a donc étendu l'application des définitions européennes aux domaines pour lesquels le législateur national est resté compétent, comme celui de la sécurité nationale.

Ces définitions sont quasiment inchangées par rapport à celles appliquées en Belgique depuis la loi du 8 décembre 1992[3]. Les éclaircissements apportés par le passé par la Commission de la protection de la vie privée[4], le Groupe de l'Article 29[5] et la jurisprudence sont dès lors toujours pertinents.

§ 1. Notion de donnée à caractère personnel

Par « donnée à caractère personnel », il faut entendre toute information qui concerne une personne physique identifiée ou identifiable (appelée la « personne concernée »)[6].

A. Toute information...

La notion de donnée à caractère personnel englobe n'importe quel type d'informations[7].

Ainsi, elle couvre les informations privées, partagées par un groupe restreint, voire totalement confidentielles, mais aussi les informations ayant fait l'objet d'une diffusion ou d'une publication. De la sorte, les données diffusées dans les médias, publiées sur un site Web[8] ou partagées sur les réseaux sociaux sont à considérer comme des données à caractère personnel et en conséquence, ne perdent pas leur protection du fait de leur caractère public.

1. Chapitre rédigé par Cécile de Terwangne.
2. Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
3. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
4. Devenue l'Autorité de protection des données, voy. *infra*.
5. Le Groupe de l'Article 29 mis en place par l'article 29 de la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est devenu le Comité européen de la protection des données, voy. *infra*. La directive 95/46 a été elle-même remplacée par le RGPD.
6. Article 4.1 du RGPD. Voy. les éclaircissements apportés sur cette notion cardinale par le Groupe de l'article 29, avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, *WP* 136. Ces éclaircissements apportés à propos de la définition de « donnée à caractère personnel », présente dans la directive 95/46, sont toujours pertinents sous le règne du RGPD qui a repris textuellement cette définition.
7. Pour de plus amples développements sur les différents types de données couvertes, voy. C. DE TERWANGNE, « Définitions clés et champ d'application du RGPD », in C. DE TERWANGNE et K. ROSIER, *Le Règlement général de protection des données (RGPD/GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 71 et s.
8. C.J.C.E., 16 décembre 2008 *Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy*, C-73/07, point 49.

Entrent également dans la définition les informations professionnelles ou commerciales, dès l'instant où elles peuvent être rattachées à un individu[1].

Enfin, la notion englobe tant les informations objectives, vérifiables et contestables que les informations subjectives : les avis, appréciations et évaluations des personnes relèvent aussi de la notion de données à caractère personnel. Il faudra en tenir compte notamment lorsque, par exemple, un employé, un candidat à un poste ou un étudiant voudra exercer son droit d'accès à l'égard de son évaluation par le (futur) employeur ou de ses résultats d'examen[2].

Si tous les types d'information sont couverts, toutes les formes que peut prendre l'information entrent également dans la notion de donnée à caractère personnel. Les données peuvent ainsi prendre la forme d'écrits, d'images (photos, vidéos)[3], de sons… Il peut s'agir de données de localisation, de données de comportement en ligne, de données biométriques, etc.[4]

B. ...concernant une personne physique

Par ailleurs, il faut bien sûr qu'un lien soit établi entre une donnée et une personne physique vivante : la donnée doit « concerner » la personne en cause. « S'agissant de cette dernière condition, celle-ci est satisfaite lorsque, en raison de son contenu, sa finalité ou son effet, l'information est liée à une personne déterminée. »[5]

Cela peut conduire à ce que des données matérielles portant sur des choses, mais pouvant être reliées à des individus particuliers, sont aussi à considérer comme des données à caractère personnel. C'est ce qu'ont indiqué les avis de la Commission de la protection de la vie privée portant sur les données cadastrales[6] et sur les images satellites[7].

La personne concernée par l'information doit être identifiée, ou à tout le moins identifiable, pour qu'on puisse parler de « données à caractère personnel ». Cette exigence est développée dans le premier paragraphe de la section 2 du présent chapitre.

1. Le Tribunal de première instance de Bruxelles a spécifié que « par données à caractère personnel, il faut comprendre toutes les informations qui concernent une personne physique quel que soit le secteur plus spécialisé dans lequel elles s'inscrivent ». Ce qui a amené le tribunal à considérer comme telles les informations relatives à la solvabilité d'une des parties au litige, indépendamment du fait que ces informations ont aussi une nature commerciale et professionnelle (Civ. Bruxelles, 12 avril 1995, n° rôle 9553A, http://jure.juridat.just.fgov.be).
2. C.J.U.E., 20 décembre 2017, *Novak*, C434/16, point 34.
3. Pour de nombreux cas où des images d'individus sous forme de photographies ou de films vidéo ont été considérées comme des données à caractère personnel, voy. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A.M*, 2002, pp. 198 et s. ; Gand, 28 mars 2002, *T. Strafr.*, 2002, liv. 6, p. 329 ; Liège (6e ch.), 27 juin 2003, *R.D.T.I.,* 2004, no 18, pp. 105 et s. ; Mons (1re ch.), 2 mai 2005, *J.L.M.B.*, 2005, p. 1057.
4. Le Conseil d'État a estimé qu'« un test d'haleine entraîne la collecte d'une donnée à caractère personnel » (C.E., 27 octobre 2005, no 150.861, J.-L. France, http ://www.raadvst-consetat.be).
5. C.J.U.E., 20 décembre 2017, *Novak*, C434/16, point 35. Pour de plus amples développements sur ces critères, voy. Groupe Article 29, avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, WP 136, pp. 10-13 ; É. Degrave, « Copies d'examen et protection des données à caractère personnel, observations sous C.J.U.E. (2e ch.), 20 décembre 2017 », *J.T.*, 2018, pp. 481-482.
6. Comité sectoriel pour l'Autorité fédérale, délibération AF n° 02/2012 du 9 février 2012 concernant la demande du SPF Intérieur, Direction générale Sécurité civile, d'accéder à certaines données cadastrales (Documentation patrimoniale – SPF Finances) dans le cadre de la réforme des services de secours.
7. Commission de la protection de la Vie privée (CPVP), avis 26/2006 du 12 juillet 2006 concernant l'utilisation d'images satellites afin de dépister et de constater des infractions aux normes urbanistiques.

§ 2. Notion de traitement

Aux termes de l'article 4.2 du RGPD, on entend par « traitement » « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Les opérations entrant dans la notion de traitement sont donc particulièrement variées et vont de la collecte à la destruction des données. En fait, tout ce qui peut être fait avec des données à caractère personnel, tout type d'actions ou d'utilisations des données entre dans la définition de « traitement ».

À titre d'illustration, la Cour d'appel de Liège a considéré dans un arrêt du 19 novembre 2009 que le fait, pour un gestionnaire de site Internet, d'enregistrer et de conserver des données pour lui permettre d'envoyer des courriels non sollicités constitue un traitement de données à caractère personnel[1]. Il a aussi été affirmé que la consultation et l'utilisation de données du répertoire d'immatriculation des véhicules (D.I.V.) étaient constitutives d'un traitement de données. De même, le transfert de données de la D.I.V. à des entreprises privées par les services communaux, via un détour par la commune (le bourgmestre, la police ou le receveur communal), constitue un traitement de données au regard de la législation[2].

On notera encore que ce qui permet de lier plusieurs opérations pour les considérer comme formant un seul traitement est la finalité qui est poursuivie par cet ensemble d'opérations[3]. La finalité est l'élément unificateur du traitement[4]. On aura par exemple les traitements suivants, impliquant chacun des opérations variées : les traitements « administration du personnel », « contrôle sur le lieu de travail », « lutte contre la fraude et les infractions de la clientèle », « collecte de dons », « relations publiques », « gestion du contentieux », « gestion des emprunts de bibliothèque », « octroi de crédit », « gestion du parcours scolaire », etc.

Il se peut par ailleurs qu'un traitement ne soit constitué que d'une seule opération. La seule collecte de données réalise déjà un traitement, même si on ne s'en tient qu'à cette opération.

La consultation de données, cependant, ne doit pas, la plupart du temps, être prise isolément, mais doit être considérée comme faisant partie du traitement initié par la personne qui diffuse, publie ou rend les données accessibles. En effet, quiconque ne faisant rien d'autre que consulter un site Internet dans lequel apparaissent des données à caractère personnel (nom des membres d'un cabinet d'avocats, liste de résultats sportifs, nom de l'auteur d'un billet posté sur le Net…) ne doit pas être considéré comme étant en train d'effectuer un traitement de données. En accédant à l'information, il s'inscrit comme le dernier maillon du traitement dont le responsable sera la personne qui a décidé de rendre les données accessibles et de les diffuser via Internet (la diffusion peut aussi se faire par un annuaire, un dictionnaire

1. Liège (7e ch.), 19 novembre 2009, *D.A.O.R.*, 2010/96, p. 453.
2. J.P. Mol, 11 janvier 2005, *R.W.*, 2007-2008, liv. 11, pp. 448 et 449.
3. C. de Terwangne et J.-M. Van Gyseghem, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », in C. de Terwangne (ed.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013.
4. Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 379.

ou autre). Le lecteur n'initie pas un nouveau traitement tant qu'il ne fait que prendre connaissance des données. Par contre, s'il utilise les données pour une finalité différente de celle ayant présidé à la diffusion, il démarrera un nouveau traitement, différent du premier, et deviendra à ce moment responsable de ce nouveau traitement. Ce sera le cas, par exemple, s'il utilise le numéro de téléphone consulté pour faire du démarchage commercial à l'égard de l'abonné. La mise à disposition des numéros de téléphone dans l'annuaire poursuit la finalité de permettre la mise en communication de deux personnes, mais non l'utilisation des informations diffusées à des fins de marketing direct. Il y a donc ici un traitement qui poursuit une finalité différente. On verra ci-après qu'en principe, seules les réutilisations compatibles avec la première finalité sont admissibles (voy. *infra*, Chapitre 2, Section 1, § 5.).

Section 2. Les acteurs principaux : la personne concernée, le responsable du traitement et le sous-traitant

Les trois principaux acteurs intervenant en présence de traitements de données à caractère personnel et à qui la législation accorde, selon le cas, des droits ou des obligations, sont la personne concernée (§ 1.), le responsable du traitement (§ 2.) et le sous-traitant (§ 3.).

§ 1. La personne concernée

A. Un individu vivant

Les règles de protection des données visent en fait à protéger les *individus* à travers la protection accordée aux *données* qui les concernent.

Ces individus sont protégés « indépendamment de leur nationalité ou de leur lieu de résidence »[1]. Le seul élément qui importe pour que la protection s'applique à une donnée est que celle-ci se rapporte à une personne physique. Les données concernant les personnes morales telles les sociétés, les associations, les fondations, les ministères, les communes, etc. ne sont donc pas protégées au titre de la législation objet de l'analyse. Toutefois, des données d'individus ayant une fonction au sein d'une personne morale sont bien des données à caractère personnel[2].

La protection ne s'applique que du vivant des individus concernés. Elle ne couvre pas les données se rapportant aux personnes décédées[3].

B. Un individu identifié ou identifiable

La personne à laquelle se rapporte l'information doit être identifiée ou à tout le moins identifiable pour que l'information puisse être qualifiée de « donnée à caractère personnel ». La personne peut être identifiée directement ou indirectement. Elle peut l'être par référence à un simple identifiant, tel qu'un nom, un numéro d'identification, des données de localisation ou

1. Considérant 14 du RGPD.
2. Voy. l'affaire soumise au Tribunal de commerce de Courtrai dans laquelle la donnée en cause était l'information selon laquelle une personne physique avait été administratrice d'une personne morale : Comm. Courtrai (1re ch.), 19 juin 2003.
3. Voy. considérant 27 du RGPD.

un identifiant en ligne (adresse IP, par exemple[1]), ou en faisant intervenir, voire en cumulant un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[2].

On sera attentif à ce qu'il ne faut donc pas nécessairement disposer du nom d'une personne ou de sa photographie pour qu'elle soit qualifiée d'identifiable. Un numéro renvoyant à un individu précis (comme le numéro du registre national, le numéro matricule d'un étudiant, le numéro de TVA d'un indépendant) ou à un bien (numéro de carte de crédit, plaque d'immatriculation[3], par exemple) ou un appareil associé à un individu (un téléphone portable, une montre connectée…) permet de rendre cet individu identifiable. Cela peut être la conjonction d'éléments qui rende une personne identifiable. Le recueil de données sur la santé mentale en Belgique, portant sur l'âge, le sexe, le code postal, la profession et le type de pathologie, a conduit à ce qu'on ne puisse pas considérer les données recueillies comme anonymes car la conjonction de ces données permettait, dans certaines communes et selon le type de profession concerné, de conduire à des individus déterminés. À l'heure des *Big data*, le brassage de données statistiques initialement anonymes conduit dans bien des cas à rendre identifiables les personnes concernées par ces données.

L'identification dont il est question doit se comprendre non comme l'établissement de l'identité civile d'un individu, mais comme *l'individualisation* de cette personne, la capacité de la traiter différemment des autres[4].

La Cour de Justice a également précisé que pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel », il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne[5].

§ 2. Le responsable du traitement

A. Critères

D'après l'article 4.7 du Règlement qui reprend les termes de la directive 95/46 (et donc de la loi du 8 décembre 1992), le responsable du traitement est celui « qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». Il peut s'agir d'une personne physique ou morale d'une autorité publique, d'un service ou d'un autre organisme[6]. Le responsable du traitement est donc la personne ou l'entité « responsable des choix qui président à la définition et à la mise en œuvre des traitements »[7]. Le Groupe de l'article 29 a

1. Considérant 30 du RGPD. Voy. F. Zuiderveen Borgesius, « The Breyer Case of the Court of Justice of the European Union : IP Addresses and the Personal Data Definition », *EDPL*, 2017/1, pp. 130-137 ; J.-Ph. Moiny, « Are Internet protocol addresses personal data ? The fight against online copyright infringement », *C.L.S.R.,* 27, 2011, pp. 348 à 361.
2. Art. 4, 1°, du RGPD.
3. La Commission de la protection de la vie privée a spécifié que le numéro de châssis et autres données d'identification d'un véhicule constituent des données à caractère personnel dès lors qu'ils peuvent être rattachés au propriétaire du véhicule (avis *Car Pass,* 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules).
4. Voy. le considérant 36 du RGPD, qui reprend le contenu du considérant 36 de la directive 95/46 avec l'ajout mis en évidence ci-après : « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, *tels que le ciblage*. »
5. C.J.U..E, arrêt du 19 octobre 2016, *Breyer*, C582/14, EU :C :2016 :779, point 43 ; C.J.U.E., arrêt du 20 décembre 2017, *Novak*, C434/16, point 31.
6. Art. 4.7 du RGPD.
7. M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreaux et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 126.

considéré qu'« *être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres* »[1].

Étant donné que la qualité de responsable du traitement dépend des deux critères énoncés ci-dessus, la désignation concrète des responsables de traitement sera affaire de cas par cas. Le Groupe de l'article 29 ne dit rien d'autre en considérant que la capacité de déterminer les finalités et les moyens du traitement « se déduira généralement d'une analyse des éléments factuels ou des circonstances de l'espèce : il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions "pourquoi ce traitement a-t-il lieu ?" et "qui l'a entrepris ?"[2] »

Pour effectuer cette analyse, il faut donc s'attarder sur le rôle de chaque acteur pour comprendre qui a *effectivement* un pouvoir de décision sur les finalités du traitement (le « pourquoi »[3] du traitement) et sur les « éléments essentiels des moyens »[4] (le « comment »[5])[6].

Précisons que le fait de ne pas avoir techniquement accès aux données n'est pas *en soi* un critère suffisant pour échapper à la qualité de responsable de traitement[7].

Une désignation erronée du responsable du traitement, c'est-à-dire qui est contredite par la situation de fait, ne lie pas le juge ni l'autorité de contrôle qui, dans une telle hypothèse, seront amenés à qualifier de responsable du traitement la personne répondant aux critères légaux.

Par ailleurs, comme auparavant, le RGPD précise que « lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre »[8].

B. Co-responsabilité

La qualité de responsable du traitement peut être partagée et il se peut que l'on désigne plusieurs co-responsables d'un traitement selon que plusieurs intervenants définissent les finalités ou les moyens de celui-ci[9]. On parle alors de responsables conjoints[10]. Dans ce cas, ils se doivent de rédiger un accord entre eux fixant les obligations de chacun[11].

1. Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http ://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.
2. Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.
3. *Ibid*, p. 14.
4. *Idem.* Est notamment considérée comme un élément essentiel la localisation des données.
5. *Idem.*
6. A. Delforge, « Les obligations générales du responsable du traitement et la place du sous-traitant », in C. de Terwangne et K. Rosier (dir.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 381 et s.
7. C.J.U.E, 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, aff. C-210/16, EU :C :2018 :388. Pour un commentaire de cet arrêt voy. S. Xefteri, « La responsabilité conjointe de l'exploitant du réseau social et de l'administrateur d'une page fan », *Rev. Aff. Eur.*, 2018/2, pp. 391-401.
8. Art. 4.7 du RGPD.
9. Art. 4.7 du RGPD. Voy. A. Delforge, *op. cit.*
10. Art. 26 du RGPD. La C.J.U.E. a par exemple considéré que l'administrateur d'une *Fan page* était responsable-conjoint de certains traitements de données avec *Facebook*. Voy. C.J.U.E, 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, précitée.
11. Sur ce point, voy. *infra.*