Les principes relatifs au traitement des données à caractère personnel et à sa licéité

De Terwangne, Cécile

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 3
Les principes relatifs au traitement des données à caractère personnel et à sa licéité

Cécile DE TERWANGNE[1]

Introduction : un chapitre de « principes » au sein du RGPD

1. Alors que la directive 95/46/CE[2] (ci-après « la Directive »), et avant elle déjà la Convention 108 du Conseil de l'Europe[3], rassemblait sous un seul chapitre les principes de base de la protection des données relatifs à la qualité des données et aux conditions de légitimation des traitements de données ordinaires et sensibles, mais aussi aux droits des personnes concernées et aux obligations des responsables du traitement, le règlement général sur la protection des données[4] (ci-après le « RGPD » ou « règlement ») met un peu d'ordre dans la présentation des choses. Désormais, les droits et obligations font l'objet de chapitres séparés. Quant aux conditions de licéité des traitements de données, elles sont présentées sous un chapitre sobrement intitulé « Principes ».

Comme auparavant, deux dispositions clés de ce dernier chapitre énoncent, l'une (l'article 5), les principes relatifs au traitement des données à caractère personnel (voy. le Chapitre 1 *infra*), et l'autre (l'article 6),

[1] Professeur à la Faculté de Droit Université de Namur et directrice de recherches au CRIDS.

[2] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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, *J.O.C.E.*, L 281/31 du 23 novembre 1995.

[3] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. STE, n° 108, 28 janvier 1981.

[4] 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.

les hypothèses dans lesquelles les traitements de données sont licites (voy. le Chapitre 2). Les articles 7 et 8 apportent des précisions nouvelles sur un élément qui a suscité de vifs débats lors du travail du législateur européen : le consentement de la personne concernée à ce que l'on traite ses données, et particulièrement le consentement des enfants (voy. le Chapitre 2, Section 2). Par ailleurs, les conditions de traitement des données sensibles sont également reprises dans ce chapitre de principes (les articles 9 et 10). Elles seront, quant à elles, analysées dans la contribution du présent ouvrage dédiée au régime des catégories particulières de données[5]. Enfin, une hypothèse spécifique fait son apparition, celle des traitements de données ne nécessitant pas l'identification des personnes concernées (l'article 11). Cette hypothèse est évoquée ci-après, sous la Section 3 du Chapitre 1, analysant le principe de minimisation, étant donné le lien que l'article 11 entretient avec ce principe.

[5] J.-M. Van Gyseghem, « Les catégories particulières de données à caractère personnel », dans le présent ouvrage.

CHAPITRE 1. Principes de base de la protection des données

2. L'article 5 du RGPD énonce l'ensemble des principes de base réalisant la protection des données : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité ; et responsabilité.

Ainsi donc, pour être admissibles aux yeux du RGPD, les traitements de données opérés doivent respecter ces principes de base qui tiennent, d'une part, aux traitements eux-mêmes et, d'autre part, aux données traitées. Un traitement de données à caractère personnel doit être licite, loyal et transparent, doit poursuivre une finalité déterminée, explicite et légitime et doit garantir la sécurité des données. En outre, seules les données pertinentes au regard de la finalité poursuivie, limitées à ce qui est nécessaire, présentant des qualités d'exactitude et de mise à jour, et conservées durant une période ne dépassant pas ce qui est nécessaire pour atteindre la finalité, peuvent faire l'objet du traitement.

Le non-respect de chacun des principes qui viennent d'être mentionnés et qui seront approfondis dans les pages qui suivent est punissable d'une

sanction pouvant s'élever jusqu'à 20.000.000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial[6].

Certains de ces principes sont repris et développés dans d'autres parties du texte du règlement. C'est le cas du principe de transparence qui prendra la forme d'obligations d'information des personnes concernées[7], ainsi que des règles de sécurité des données[8] et de responsabilité des différents acteurs[9].

3. Les principes fondamentaux de la protection des données ne sont pas modifiés dans le RGPD par rapport à ce qui régit cette matière depuis plusieurs décennies. Ces principes issus des Lignes directrices de 1980 de l'OCDE[10] et de la Convention 108 du Conseil de l'Europe ont fait leurs preuves et ont démontré leur capacité à résister à l'épreuve du temps et à être appliqués dans des contextes techniques, économiques et sociaux totalement mouvants. Certains affinements ou compléments ont toutefois été apportés, ainsi qu'on le verra ci-dessous.

SECTION 1. – Principe de licéité, loyauté et transparence

§ 1. Données traitées de manière licite

4. Les données à caractère personnel doivent être traitées de manière licite[11]. Cette exigence de licéité signifie que le traitement de données à caractère personnel doit se faire conformément à l'ensemble des règles légales applicables. Cela implique le respect des règles de protection des données, mais également de toute autre règle légale qui trouverait à s'appliquer à une situation de traitement de données, comme par exemple les obligations en matière de droit du travail, de droit des contrats ou de protection du consommateur, ou l'obligation de secret professionnel dans le cas où

---

[6] Voy. la contribution de L. Gerard, « Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? », dans le présent ouvrage.

[7] Voy. la contribution de Th. Tombal, « Les droits de la personne concernée dans le RGPD » dans le présent ouvrage.

[8] Voy. la contribution de Fr. Dumortier, « La sécurité des traitements de données à caractère personnel » dans le présent ouvrage.

[9] Voy. la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » dans le présent ouvrage.

[10] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (2013), C(80)58/FINAL, telles qu'amendées le 11 juillet 2013 par C(2013)79, http://www.oecd.org.

[11] Art. 5, § 1er, a), du RGPD.

celui-ci est applicable. Un médecin qui divulguerait dans une publication sur Internet le nom d'un de ses patients commettrait un traitement illicite.

L'article 6 du RGPD est intitulé « Licéité du traitement » plutôt que « Principes relatifs à la légitimation des traitements », comme dans la directive 95/46/CE. Cet article liste toutes les hypothèses dans lesquelles un traitement de données à caractère personnel est admis comme « licite ». Mais cela ne dispense pas du respect des autres aspects de l'exigence de licéité du traitement qui viennent d'être évoqués[12].

§ 2. Données traitées de manière loyale et transparente

5. Les données à caractère personnel doivent être traitées non seulement de manière licite mais également « de manière loyale et transparente »[13]. L'exigence de loyauté induit que les données ne soient pas obtenues ni traitées par des méthodes ou moyens déloyaux, par tromperie, comme ce fut le cas dans le scandale « Cambridge Analytica »[14] où les utilisateurs de Facebook qui ont répondu au test de personnalité en cause étaient amenés à croire qu'ils opéraient dans le cadre d'une étude universitaire et que le but poursuivi était donc académique, alors qu'en réalité le but de la récolte des données était commercial et de prospection politique. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données, d'une manière qui serait tout à fait inattendue ou imprévisible pour elles. Les personnes concernées doivent, en pleine connaissance de cause, pouvoir établir une relation de confiance avec ceux qui traitent leurs données à caractère personnel[15].

Le principe de loyauté est donc lié au droit à la transparence[16]. Ce droit à la transparence implique que certaines informations soient fournies spon-

---

[12] *Contra* : J. Ausloos, « Giving meaning to Lawfulness under the GDPR », *CiTiP Blog*, 2 mai 2017, https://www.law.kuleuven.be/citip/blog/2761-2/

[13] Art. 5, § 1er, a), du RGPD.

[14] C. Cadwalladr et E. Graham-Harrison, « Revealed : 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », *The Guardian*, 17 mars 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ; M. Rosenberg, N. Confessore et C. Cadwalladr, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17 mars 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook ; CNIL, « Affaire Cambridge Analytica/Facebook », 12 avril 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook.

[15] E. Degrave, « Le Règlement général sur la protection des données et le secteur public », *Rev. Droit communal*, 2018, pp. 4-5. Égal. Groupe 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260 rev.01, § 2 : « *Transparency […] is about engendering trust in the processes which affect the citizen by enabling them to understand, and in necessary, challenge those processes* ».

[16] Voy. considérant n° 60 du RGPD : « Le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement

tanément par le responsable du traitement aux personnes concernées[17]. L'idée est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données. C'est parce que sa collecte de données sur des internautes non-inscrits sur Facebook et navigant hors de ce réseau social fut jugée déloyale, que celui-ci a été sanctionné[18] tant par la CNIL[19] en France que par le Tribunal de première instance de Bruxelles[20] : « Concernant la collecte des données de navigation des internautes, via le cookie "datr", l'information dispensée via le bandeau d'information relatif aux cookies est imprécise. En effet, cette mention ne fait qu'indiquer que des informations sont collectées "[...] sur et en dehors de Facebook via les cookies", ce qui ne permet pas aux internautes d'être clairement informés et de comprendre que leurs données sont systématiquement collectées dès lors qu'ils naviguent sur un site tiers comportant un module social. Cette collecte massive de données effectuée via le cookie "datr" est déloyale en l'absence d'information claire et précise »[21].

L'obligation de fournir des informations est à géométrie variable, liée précisément à l'exigence de loyauté : les articles 13 et 14 du RGPD prévoient qu'au-delà de certains renseignements à donner en toutes

et de ses finalités ». Égal. : European Union Agency for Fundamental Rights (FRA), European Court of human rights, Council of Europe, *Handbook on European data protection law*, 2014, p. 76, https://rm.coe.int/16806b294a : « *Fair processing means transparency of processing, especially vis-à-vis data subjects* » ; Groupe 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260 rev.01, § 2 : « *Transparency is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the EU* ».

[17] Voy. les articles 13 et 14 du RGPD qui imposent un devoir d'information des personnes concernées, soit lors d'une collecte directe des données, soit lors d'une collecte indirecte.

[18] La condamnation prononcée se base sur les lois française et belge mettant en œuvre l'article 6, § 1er, a), de la directive 95/46/CE. Cette disposition étant reprise à l'article 5, § 1er, a) du RGPD, on peut estimer que le raisonnement serait identique sous l'empire du RGPD. D'autres irrégularités au regard de la législation de protection des données étaient également reprochées à Facebook et ont été sanctionnées dans les deux décisions évoquées ici.

[19] CNIL, « Délibération de la formation restreinte de la CNIL SAN-2017-006 du 27 Avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland », 27 avril 2017, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2. La sanction prononcée s'élève à 150.000 €.

[20] Civ. Bruxelles, 16 février 2018, n° 2016/153/A, https://www.privacycommission.be/sites/privacycommission/files/documents/jugement_facebook_16022018.pdf. Voy. égal. le communiqué de presse de la CPVP, https://www.privacycommission.be/fr/news/victoire-de-la-commission-vie-privee-dans-la-procedure-facebook ; E. Degrave, « Facebook, les cookies et la justice belge : le retour », *Justice en ligne*, 22 mars 2018, http://www.justice-en-ligne.be/article 1044.html.

[21] CNIL, « Facebook sanctionné pour de nombreux manquements à la loi Informatique et Libertés », 16 mai 2017, https://www.cnil.fr/fr/facebook-sanctionne-pour-de-nombreux-manquements-la-loi-informatique-et-libertes.

circonstances, d'autres informations ne sont à transmettre que si cela est nécessaire pour garantir la loyauté du traitement des données[22]. Ces informations supplémentaires portent sur la durée de conservation des données traitées, l'existence de divers droits pour la personne concernée, etc[23]. Ce dernier point de l'information à donner sur les droits est jugé particulièrement important car cet aspect de la transparence affecte directement l'exercice de leurs droits par les individus[24] et permet à ceux-ci de demander des comptes aux responsables de traitement et aux sous-traitants[25]. Au titre des renseignements à donner systématiquement figure l'information sur les destinataires des données. La Cour de justice avait déjà signalé que cette information devait être fournie pour assurer la loyauté du traitement : « Il s'ensuit que l'exigence de traitement loyal des données personnelles prévue à l'article 6 de la directive 95/46 oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données »[26].

Dans un souci de clarté, les auteurs du règlement ont souhaité faire figurer explicitement le principe de transparence aux côtés de l'exigence de traitement licite et loyal. Ce principe de transparence est explicité dans un long considérant[27] qui commence par préciser que le traitement des données doit être transparent à l'égard des personnes concernées, de même que « la mesure dans laquelle ces données sont ou seront traitées », expression dont on ne perçoit pas vraiment la portée réelle. Le considérant évoque en outre la qualité de l'information à fournir aux personnes concernées et son contenu, éléments qui font l'objet des articles 12 à 14 du règlement. Certaines précisions se rattachent plus particulièrement à la notion de loyauté et à l'idée de ne pas prendre les individus en traitre lorsqu'on s'apprête à traiter leurs données. C'est le cas de l'indication que

[22] Art. 13, § 2 et 14, § 2, du RGPD. Ces deux dispositions exigent que des informations additionnelles soient fournies lorsqu'elles sont nécessaires « pour garantir un traitement équitable et transparent ». Le terme « équitable » est une traduction malheureuse du terme « *fair* » présent dans la version anglaise du RGPD et repris de la directive 95/46 qui avait été traduit dans la version française de l'époque par « loyal », ce qui correspond mieux au sens voulu par les auteurs du texte et indique de façon plus explicite le lien entre les obligations de transparence et l'obligation de loyauté du traitement.

[23] Pour une présentation détaillée du devoir d'information, voy. la contribution de Th. Tombal, « Les droits de la personne concernée dans le RGPD » dans le présent ouvrage.

[24] C.J.U.E., 1er octobre 2015, arrêt *Smaranda Bara*, C-201/14, § 33.

[25] Groupe 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260 rev.01, § 4.

[26] C.J.U.E., 1er octobre 2015, arrêt *Smaranda Bara*, C-201/14, § 34.

[27] Considérant n° 39 du règlement.

les personnes doivent être informées des risques liés au traitement de leurs données. On ne retrouve pas pareille exigence dans le devoir d'information des articles 13 et 14 et il faut avouer qu'il ne sera pas toujours évident de mettre cette exigence en pratique…

La loyauté du traitement de données à caractère personnel ne se limite pas à la collecte, mais doit être garantie à toutes les étapes de celui-ci[28]. Par ailleurs, la question du moment où l'on informe les personnes concernées du traitement de leurs données est intrinsèquement liée à l'exigence de loyauté[29].

6. Dans certaines circonstances, le devoir de loyauté implique que préférence soit donnée à la collecte de données directement auprès des personnes concernées, et non pas de manière indirecte auprès de sources tierces[30]. C'est le cas dans un contexte d'emploi, notamment lors des procédures de recrutement des employés[31]. En présence de données médicales, également, le principe édicté par la Recommandation n° R(97)5 du Comité des ministres du Conseil de l'Europe relative aux données médicales[32] consiste en ce que « les données médicales doivent en principe être collectées *auprès de la personne concernée*. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 4, 6 et 7 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données »[33].

7. Enfin, le Groupe de l'article 29 a insisté[34] sur le fait que « l'obligation de traiter les données à caractère personnel conformément au principe de loyauté doit être interprétée strictement lorsqu'un enfant est concerné. Dans la mesure où un enfant n'est pas encore complètement

---

[28] Groupe 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260 rev.01, § 5.

[29] Groupe 29, Guidelines on transparency under Regulation 2016/679, précitées, § 48.

[30] V. Verbruggen, *Les Codes commentés. La protection des données*, Bruxelles, Larcier, 2011, pp. 55 et 56.

[31] Recommandation n° CM/Rec(2015)5 du 1er avril 2015 du Comité des ministres du Conseil de l'Europe sur le traitement des données à caractère personnel dans le cadre de l'emploi, pt 5.1.

[32] Point 4.2 de la recommandation.

[33] V. Verbruggen, *Les Codes commentés. La protection des données*, *op. cit.*, p. 55.

[34] Groupe 29, Avis 2/2009 du 11 février 2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), WP 160. Voy. égal. Groupe 29, Document de travail 1/2008 du 18 février 2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), WP 147.

mûr, les responsables du traitement doivent en avoir conscience et agir en toute bonne foi lors du traitement de ses données »[35].

SECTION 2. – Principe de limitation des finalités

8. Présenté depuis 37 ans comme la véritable pierre angulaire de la protection des données, le principe de limitation des finalités ou « principe de finalité », tel qu'il est couramment nommé, exige que les données soient collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. Les finalités du traitement des données doivent donc être fixées et claires dès le début (*the « purpose specification » dimension*)[36] (§ 1). On peut effectuer sur ces données toutes les opérations qui seront considérées comme compatibles avec ces finalités d'origine (*the « compatible use » dimension*)[37] (§ 2).

§ 1. Finalité du traitement déterminée, explicite et légitime

a) Finalité déterminée

9. Tout traitement de données doit poursuivre une ou des finalité(s) déterminée(s). Il s'agit de savoir, dès le démarrage[38] d'un traitement de données, quel(s) objectif(s) ce traitement est appelé à servir. La finalité ne peut être inexistante (« on ne sait pas encore à quoi vont servir ces données mais comme on a l'occasion de les collecter, collectons-les toujours ») ni floue.

La spécification de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel (le traitement « gestion de clientèle », « gestion du contentieux », « contrôle sur le lieu de travail », « lutte contre la fraude », « relations publiques », « sécurité des biens et des personnes », …) et permettre à la personne concernée de contrôler le sort réservé aux données la concernant[39].

---

[35] V. Verbruggen, *Les Codes commentés. La protection des données*, *op. cit.*, p. 56.

[36] Groupe 29, Opinion 03/2013 on purpose limitation, WP 203, 2 avril 2013, pp. 11-12.

[37] *Ibid.*, pp. 12-13.

[38] Le Groupe 29 (Opinion 03/2013 on purpose limitation, WP 203, 2 avril 2013, p. 15) précise : « *prior to, and in any event, no later than the time when the collection of personal data occurs* ».

[39] Groupe 29, Opinion 03/2013, précité, pp. 15-16 et 39. M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *J.D.E.*, 1997, p. 377 ; M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 685 et 686.

La finalité doit être précise afin de permettre à la personne concernée d'effectuer cette analyse et d'exercer les droits qui lui sont conférés par la loi. Cette précision permettra également au responsable du traitement de déterminer les données qui devront être collectées et traitées. En effet, comme on le verra plus loin, les données traitées doivent être pertinentes au regard de la finalité. Une finalité qui ne serait pas suffisamment précise et serait donc énoncée de manière trop large permettrait de traiter un ensemble bien trop vaste de données, toutes pouvant passer pour pertinentes par rapport à la finalité annoncée. Le Groupe de l'article 29 a signalé que, au risque de manquer de précision, la définition de la finalité des traitements ne peut se faire par la simple référence aux activités du responsable du traitement ou à ses missions légales[40]. La doctrine[41] a aussi pointé comme ne répondant pas au critère de spécificité les finalités trop vagues indiquées par Facebook, telles « *Provide, Improve and Develop Services* », « *Promote Safety and Security* » et « *Show and Measure Ads and Services* »[42].

b) Finalité explicite

10. La finalité doit également être explicite, ce qui signifie qu'elle doit être annoncée sans ambiguïté[43], ne pas être tenue « secrète » ou « camouflée »[44].

Ainsi qu'il a été dit plus haut à propos du principe de loyauté, la transparence des traitements de données fait partie intégrante du régime de

[40] Ainsi, pour les traitements de données effectués par les agences antidopage : « La simple référence au traitement des données par les organisations antidopage "dans le contexte de leurs activités antidopage" et une formule du type "les organisations antidopage ne doivent traiter les renseignements personnels que dans la mesure nécessaire et appropriée pour assumer les responsabilités qui leur incombent en vertu du code et des standards internationaux" ne suffisent pas. », Groupe 29, Deuxième avis 4/2009 du 6 février 2009 sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage, WP 162.

[41] B. Van Alsenoy *et al.*, « From social media service to advertising network : a critical analysis of Facebook's Revised Policies and Terms », 2015, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf ; H. Ursic, B. Custers, « Legal Barriers and Enablers to Big Data Reuse », *EDPL*, 2016/2, p. 213.

[42] Ces finalités publiées dans la version de 2015 des conditions générales de Facebook au moment des analyses doctrinales citées plus haut sont toujours valables au printemps 2018.

[43] Groupe 29, Opinion 03/2013 on purpose limitation, précité, pp. 17 à 19.

[44] C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 157.

protection. La ou les finalités du traitement entrepris sont parmi les éléments les plus importants à communiquer au nom de l'obligation de transparence. L'information sur la finalité poursuivie doit en principe être systématiquement dévoilée lors de la mise en œuvre de tout traitement[45].

c) Finalité légitime

11. Enfin, la finalité doit être légitime, ce qui signifie tout d'abord que l'objectif poursuivi doit être « compatible avec les missions de l'organisme » qui traite les données[46] mais également que la finalité ne peut induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement[47]. « *What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance ; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society* »[48]. La notion de légitimité invite donc à un examen de proportionnalité.

On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées. Les intérêts en jeu à prendre en considération sont, bien sûr, ceux de la personne concernée par les données, mais sont aussi, le cas échéant, l'intérêt de la société dans son ensemble. Une recherche médicale, par exemple, met en jeu l'intérêt des malades sélectionnés pour la recherche à voir garantir la confidentialité de leurs données, l'intérêt de l'équipe de chercheurs désireux de faire avancer l'état des connaissances scientifiques, mais également l'intérêt de

---

[45] Voy. sur cette obligation et le moment auquel elle doit être observée la contribution de Thomas Tombal dans le présent ouvrage.

[46] Commission Nationale de l'Informatique et des Libertés (CNIL), « Définir une finalité », https://www.cnil.fr/fr/definir-une-finalite.

[47] M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *op. cit.*, p. 145 ; J. Dumortier et F. Robben, note sous Prés. Comm. Anvers, 7 juillet 1994, et Prés. Comm. Bruxelles, 15 septembre 1994, *Computerr.*, 1994, pp. 244 et s. ; S. Gutwirth, « De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993/4, pp. 1409 et s. ; Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

[48] Protocole d'amendement à la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Rapport explicatif, 18 mai 2018, § 46.

la société, du point de vue de la santé publique, à voir progresser les possibilités de traitement de la maladie étudiée.

Pour être légitime, une finalité ne peut en définitive causer un préjudice plus grand à l'ensemble des intérêts en jeu que l'intérêt que représente le traitement. Dans le même sens d'ailleurs, dans le cadre de l'article 8, CEDH, la jurisprudence de la Cour européenne des droits de l'homme exige un juste équilibre entre les intérêts publics et privés en jeu lors de la mise en œuvre de traitements de données. Dans son arrêt *S. et Marper*, la Cour a ainsi affirmé que le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, nécessaire dans la mesure où il n'existe pas d'autres mesures appropriées moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société, et qu'il ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport aux bénéfices attendus par le responsable du traitement[49]. Pour sa part, la Cour de justice des Communautés européennes s'est prononcée dans le même sens en estimant, dans l'affaire *Österreichischer Rundfunk*, qu'en présence d'un traitement de données à caractère personnel, les objectifs listés dans l'énumération de l'article 8, § 2, CEDH (objectifs qui peuvent justifier des atteintes à la vie privée) sont légitimes mais qu'il convient de vérifier le respect de l'exigence de proportionnalité contenue elle aussi à l'article 8, § 2, CEDH[50] induisant que la mesure respecte « un juste rapport de proportionnalité entre les moyens utilisés et le but à atteindre »[51].

Par ailleurs, dans tous les cas, un traitement poursuivant une finalité contraire à la loi ne pourra être considéré comme poursuivant une finalité légitime[52].

A titre d'illustration de traitement ne pouvant passer pour poursuivre une finalité légitime car induisant une atteinte excessive aux droits et intérêts des personnes concernées, la Cour constitutionnelle belge s'est prononcée[53] dans un cas où, d'après un décret flamand, les suspensions disciplinaires des sportifs majeurs devaient être publiées sur un site Web

[49] Cour eur. D.H. (GC), 4 décembre 2008, req. n^os^ 30562/04 et 30566/04, *S. et Marper c. Royaume-Uni*, § 118.

[50] C.J.C.E., 20 mai 2003, arrêt *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, pts 81 et s. Voy. égal. C. const., arrêt du 10 novembre 2011, 166/2011, pt B 35.3, www.const-court.be. Égal. Cour eur. D.H., 4 mai 2000, *Rotaru c. Roumanie*, *Rev. trim. dr. h.*, 2001, pp. 137 à 183, obs. O. De Schutter.

[51] M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, p. 688.

[52] Groupe 29, Opinion 03/2013 on purpose limitation, précité.

[53] C.A., 20 octobre 2004, n° 162/2004, suspension, pt B.5.2 ; puis C.A., 19 janvier 2005, n° 16/2005, annulation, pt B.1, http://www.const-court.be.

créé par le gouvernement à cette fin et via les canaux de communication officiels créés par les fédérations sportives. Cette publication contenait les nom, prénoms et date de naissance du sportif, le début et la fin de la période de suspension et la discipline sportive qui avait donné lieu à l'infraction. Pour la Cour, il s'agit d'une ingérence dans le droit au respect de la vie privée. Assurer le respect effectif des sanctions imposées aux sportifs est un but légitime, mais « [l]a diffusion de données personnelles, prévue par le décret, sur un site Web non sécurisé et, partant, accessible à chacun va cependant au-delà de ce que cet objectif requiert ». La Cour conclut que « la publication entreprise n'est pas nécessaire pour atteindre l'objectif légitime poursuivi par le législateur, puisque cet objectif peut également être réalisé d'une manière moins dommageable pour les intéressés et, d'autre part, les effets de la mesure sont disproportionnés par rapport à cet objectif ».

§ 2. Pas d'utilisations ultérieures incompatibles

a) La règle

12. Après avoir spécifié que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, le RGPD dispose que les données ne peuvent pas « être traitées ultérieurement de manière incompatible avec ces finalités »[54]. Une fois qu'on a collecté des données à caractère personnel, on ne peut faire n'importe quoi avec ces données[55]. Seules les utilisations compatibles avec les finalités déterminées et annoncées au départ, au moment de la collecte, sont admises. Toute utilisation incompatible est interdite, sauf les deux exceptions évoquées ci-après (voy. le Chapitre 1, Section 2, § 3).

Par ailleurs, l'admissibilité de certains traitements ultérieurs des données à caractère personnel ne dispense pas de respecter dans ces cas toutes les autres règles de protection du RGPD. Ainsi, « En tout état de cause, l'application des principes énoncés dans le présent règlement et, en particulier, l'information de la personne concernée au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devraient être assurées »[56].

[54] Art. 5, § 1er, b), du RGPD.

[55] Voy. P. Van Eecke et Ch. Suffys, « Herbestemming van verzamelde persoonsgegevens voor andere doeleinden », in N. Ragheno (coord.), *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2017, pp. 61 et s.

[56] Considérant n° 50 du RGPD.

b) Les critères de la compatibilité

13. La notion d'utilisation « compatible » a suscité de nombreux questionnements dans la pratique et les auteurs du RGPD ont eu le souci de la baliser davantage. Le texte présente ainsi, à son article 6, § 4, une série de critères permettant d'établir si le traitement des données pour une autre finalité est compatible ou non avec la finalité de la collecte de départ[57]. Il s'agit de tenir compte :

– « du lien pouvant exister entre les deux finalités » : ce critère permet d'admettre toutes les utilisations ultérieures qui présentent un lien logique et cohérent avec les finalités annoncées ;
– « du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement » : pour être correctement cerné, ce critère doit être lu avec l'éclairage apporté par le considérant n° 50 qui précise : « du contexte dans lequel les données à caractère personnel ont été collectées, *en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données* »[58]. Ce critère des attentes raisonnables du sujet des données est particulièrement pertinent, étant donné qu'en limitant ce qui est fait avec les données à ce qui entre dans les prévisions de ce sujet, il permet à celui-ci de conserver le contrôle sur le sort de ses données[59].
– « de la nature des données à caractère personnel », ordinaires ou sensibles : on sera plus sévère pour admettre comme compatibles des utilisations à d'autres fins que ce qui était initialement prévu en présence de données sensibles, étant donné le risque accru que présente le traitement de ce type de données (ce qui rejoint le critère suivant) ;
– « des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées » : l'examen de ce qui est compatible et donc admissible comme traitement ultérieur de données est notamment

[57] Ces critères sont repris, pour l'essentiel, de l'avis du Groupe 29 sur la limitation des finalités, précité, pp. 23-27.

[58] C'est nous qui soulignons. Cette phrase est inspirée de l'Avis 03/13 du Groupe 29, précité, p. 40 et annexe 1.

[59] Dans le même sens, « Predictability is also relevant when assessing the compatibility of further processing activities. In general, further processing cannot be considered predictable if it is not sufficiently related to the original purpose and does not meet the reasonable expectations of the data subjects at the time of collection, based on the context of the collection » (Groupe 29, Avis 03/13, précité, p. 13).

fonction de l'impact[60] que ce nouveau traitement risque d'avoir sur les personnes concernées[61] ;

– et « de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation », le considérant n° 50 précisant qu'il s'agit de tenir compte de l'existence de « garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu ». Ces garanties appropriées doivent viser à assurer la séparation fonctionnelle des données[62].

c) Exemples d'incompatibilité des traitements ultérieurs

14. À titre d'exemple de réutilisations de données à caractère personnel qui ne sont pas compatibles, on citera :

– le cas d'une banque ayant également des activités d'assurance, qui identifie dans les virements effectués par ses clients ceux qui paient des primes d'assurance plus élevées que les primes de ses produits d'assurance et qui leur envoie un courrier les invitant sur cette base à changer de compagnie d'assurances[63] ;

– les cas traités par la Commission belge de la protection de la vie privée concernant un bourgmestre ayant utilisé le fichier des parents d'un enfant inscrit dans la crèche communale pour leur envoyer un courrier électoral pour les élections auxquelles il se représentait, un autre bourgmestre utilisant le registre des mariages pour envoyer ses vœux aux mariés de l'année en les invitant à se souvenir de lui dans les isoloirs et, encore, un autre bourgmestre utilisant le fichier des patients

---

[60] Pour reprendre le terme utilisé par le Groupe 29 dans son avis 03/13, précité, p. 40.

[61] Voy. égal. les Lignes directrices du Comité consultatif de la Convention 108 du Conseil de l'Europe du 23 janvier 2017 sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, Principe 3.1. : « Les données à caractère personnel ne devraient pas faire l'objet d'un traitement ultérieur que la personne concernée puisse considérer comme étant inattendu, inapproprié ou contestable. Exposer la personne concernée à des risques différents ou supérieurs à ceux envisagés pour les finalités initiales pourrait être considéré comme un traitement ultérieur inattendu ».

[62] Groupe 29, Avis 03/13, précité, p. 13. Égal. p. 27 : « *When trying to identify technical and organisational measures that qualify as appropriate safeguards to compensate for the change of purpose, the focus often lies with the notion of isolation. Examples of the relevant measures may include, among other things, full or partial anonymisation, pseudonymisation, or aggregation of the data, privacy enhancing technologies, as well as other measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')* ».

[63] Anvers, 3 mai 1999, *Ann. prat. comm.*, 1999, pp. 524 à 527 ; *A.J.T.*, 1999, p. 437, note C. De Vos ; cet arrêt est l'appel de la décision rendue par Prés. Comm. Anvers, 7 juillet 1994, *D.C.C.R.*, 1994-1995, p. 77, note Th. Léonard.

de l'hôpital établi dans sa commune pour leur souhaiter en son nom propre un prompt rétablissement ;

– le cas d'un club de sport qui céderait la liste de ses adhérents avec toutes leurs coordonnées à une entreprise vendant des produits de régime amincissant afin de permettre à cette entreprise de contacter les membres du club pour leur proposer ses produits ;
– le cas d'un établissement scolaire qui communique les informations sur ses élèves en difficulté à des sociétés proposant un soutien scolaire[64].

Ainsi qu'on va le voir ci-dessous (§ 3), le club de sport pourrait communiquer les données de ses adhérents, mais seulement en informant ceux-ci auparavant et en récoltant leur consentement pour ce faire. L'école, quant à elle, ne pourrait certes en aucun cas communiquer les données en question à des fins commerciales, mais pourrait, si cela entre dans sa politique de communication interne, appliquer la voie moins attentatoire consistant à faire circuler la publicité au sein de l'établissement.

C'était également un problème de compatibilité qui avait été mis en exergue par les velléités d'une banque néerlandaise ayant fait grand bruit en 2014. Cette banque révéla son intention d'exploiter les masses de données amoncelées dans ses ordinateurs et réseaux internes pour développer une stratégie *Big Data* aux fins de réaliser un ciblage ultra affiné de ses clients et de leur adresser des offres promotionnelles de sociétés tierces. Cette annonce provoqua un tollé immédiat « dans les médias et parmi les associations de consommateurs, la banque usurpant selon eux ses droits sur la confidentialité des données personnelles en les vendant »[65]. Il est clair que cette pratique ne pouvait passer pour compatible avec les finalités des traitements classiques d'une banque. C'est pourtant aujourd'hui l'ensemble du secteur bancaire qui étudie des projets d'utilisation de leurs trésors de données personnelles à des fins commerciales, bien au-delà des nécessités des services financiers offerts[66]. Les paragraphes qui suivent détaillent comment le RGPD offre un cadre juridique à ces perspectives

[64] Pour d'autres exemples, voy. Groupe 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, WP 203, Annexe 2 (Practical examples to illustrate the compatibility assesment), pp. 56 à 70 ; B. Docquir, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, pp. 128-129.

[65] M. Leblanc-Wohrer, « Le défi de la protection des données personnelles », *L'AGEFI Hebdo*, 5 juin 2014, http://www.agefi.fr/banque-assurance/actualites/hebdo/20160210/defi-protection-donnees-personnelles-154345

[66] H. Stefani, « Le Big Data au service d'une connaissance client affinée », *Revue-Banque.fr*, 25 février 2014, http://www.revue-banque.fr/management-fonctions-supports/article/big-data-au-service-une-connaissance-client-affine ; Ch. Lejoux, « Le Big Data, un enjeu crucial pour le secteur bancaire », *La Tribune*, 28 janvier 2016, http://www.latribune.fr/entreprises-finance/banques-finance/banque/le-big-data-un-enjeu-crucial-pour-le-secteur-bancaire-545979.html ; Ph. Gelis, « Le 'Big Data'… L'arme secrète des banques

en permettant, avec le consentement (libre, éclairé, spécifique et indubitable) des personnes concernées, ces traitements de données poursuivant une finalité incompatible avec la finalité initiale.

§ 3. Acceptation de certaines utilisations ultérieures incompatibles

15. Une nouveauté du RGPD est la clarification du fait qu'il est permis dans certaines circonstances de traiter des données à caractère personnel à une fin différente de celle pour laquelle les données ont été collectées même si cette nouvelle finalité n'est pas compatible avec la première. Dans ces deux cas, on peut donc effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité[67].

Le projet initial du texte ouvrait en fait largement cette possibilité, réduisant par là le principe de finalité à la portion congrue, tandis que le Conseil était allé plus loin encore, soulevant de vives critiques[68], en proposant d'autoriser les traitements ultérieurs réalisés par le même responsable à des fins incompatibles pourvu que les intérêts légitimes de ce responsable ou d'un tiers priment sur les intérêts des individus concernés[69]. Le principe de finalité aurait bel et bien été vidé de son sens.

Le texte final du règlement est revenu à la vocation protectrice du principe de finalité tout en l'assouplissant dans les deux seules hypothèses suivantes[70] :

– en cas de consentement de la personne concernée pour le traitement de ses données à caractère personnel à de nouvelles fins incompatibles ; le consentement dont question doit présenter les qualités requises de tout consentement servant de base pour traiter des données à caractère personnel : il doit s'agir d'une manifestation de volonté libre, spécifique, éclairée et univoque[71] ;

---

pour gagner plus », *Frenchweb.fr*, 22 janvier 2016, http://www.frenchweb.fr/le-big-data-larme-secrete-des-banques-pour-gagner-plus/224205#LwJh6OY7PyK6CFfy.99.

[67] Considérant n° 50 du RGPD.

[68] Voy. not. Groupe 29, Communiqué de presse du 17 mars 2015 sur le chapitre II du GDPR ; égal., Opinion 03/2013 on purpose limitation, 2 avril 2013, WP 203, pp. 36-37. Onze États membres, parmi lesquels la Belgique, avaient exprimé des réserves sur ce point.

[69] Cette proposition était destinée à faciliter les opérations de *Big Data* (C. BURTON *et al.*, « The Final European Union General Data Protection Regulation », *Privacy and Security Law Report*, 15 PVLR 153, 25 janvier 2016, p. 6).

[70] Art. 6, § 4, du RGPD.

[71] Art. 4, 10°, du RGPD ; voy. *infra* Chapitre 2, Section 2 ce qui est dit sur le consentement.

– ou si le traitement ultérieur des données à des fins incompatibles est basé sur le droit de l'Union ou d'un État membre visant à garantir un des objectifs énumérés à l'article 23, paragraphe 1, du RGPD, c'est-à-dire, en particulier « d'importants objectifs d'intérêt public général »[72] ; la norme juridique dont question doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir l'objectif visé[73].

16. Hormis ces deux hypothèses, on ne peut traiter pour un nouveau but incompatible avec le premier les données à caractère personnel dont on dispose, en s'appuyant sur les autres bases de légitimité des traitements (voy. *infra*, la présentation de ces bases). Certains auteurs ont expressément regretté cette situation[74], estimant que « [l]'interdiction de traitement en cas d'incompatibilité des finalités s'oppose à l'évolution d'un traitement de données qui est en quelque sorte "figé" par sa finalité réelle de départ. Si des données ont été traitées pour les besoins d'exécution d'un contrat, elles ne peuvent être traitées pour une communication à un tiers en vue d'alimenter un processus de profilage *Big Data*, sauf consentement de la personne ou autorisation légale »[75]. Ce que le législateur a voulu réaliser au travers de ce régime d'interdiction des traitements ultérieurs non compatibles avec les finalités de départ sauf consentement ou autorisation légale, c'est garantir que les personnes concernées conservent un certain contrôle sur le sort réservé à leurs données. En acceptant que les données soient réutilisées hors des attentes initiales des personnes concernées mais avec leur consentement ou en s'appuyant sur une base légale nécessairement transparente, le législateur européen veille à ce que l'individu puisse demeurer conscient de ce qui est fait avec ses données, au prix, certes, de freiner les opérations de profilage basées sur des *Big Data*.

Cette volonté de permettre, grâce à la transparence, le contrôle par les personnes concernées sur les usages successifs qui sont faits de leurs données, se traduit dans le devoir d'information prévu aux articles 13, § 3 et 14, § 4 du RGPD. Ces deux dispositions imposent que, lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données ont été recueillies ou obtenues, le responsable du traitement fournisse à la personne concernée des informations au sujet de cette autre finalité. Cette information doit être communiquée avant la nouvelle utilisation des données. D'après le Groupe 29[76], une

[72] Considérant n° 50 du RGPD.

[73] Art. 6, § 4, du RGPD ; voy. *infra* Chapitre 2, Section 5 ce qui est dit sur la base légale.

[74] Th. Léonard et D. Chaumont, « Article 6 Licéité du traitement », *GDPR-expert*, https://www.gdpr-expert.eu/article.html?id=6#difficultesprobables.

[75] *Ibid.*

[76] Groupe 29, Guidelines on transparency under Regulation 2016/679, précitées, § 48.

période de temps raisonnable doit pouvoir s'écouler entre cette information et le démarrage du nouveau traitement, permettant à la personne concernée de considérer l'opportunité éventuelle d'exercer ses droits à l'égard de cette nouvelle utilisation. L'établissement de ce qui est une « période raisonnable » dépend des circonstances, sachant que le principe de loyauté exige que, plus le traitement ultérieur sera intrusif ou inattendu, plus longue devrait être la période de temps de réflexion accordée aux personnes concernées[77].

§ 4. Traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

17. Enfin, on signalera que certaines réutilisations des données sont systématiquement considérées comme compatibles moyennant certaines conditions. Il s'agit des traitements ultérieurs « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques »[78].

L'intérêt que ces traitements présentent pour la société, couplé au faible niveau de risque qu'ils sont censés présenter[79], notamment lié au fait qu'ils ne débouchent normalement pas sur une prise de décision ou de mesure individuelle à l'égard d'une personne concernée, explique qu'on leur ait réservé un régime particulier, les acceptant comme compatibles avec toute finalité initiale du traitement pourvu toutefois qu'ils respectent des conditions ou garanties particulières. Ces conditions sont évoquées à l'article 89, § 1er, du RGPD qui invite les États membres à soumettre ces traitements à des garanties appropriées pour les droits et libertés de la personne concernée, notamment en imposant la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. L'article 89 cite à titre d'illustration des mesures pouvant être prises, la pseudonymisation et l'anonymisation des données, dans la mesure où cela n'entraverait pas la réalisation des finalités d'archivage, de recherche scientifique ou historique, ou de statistique.

---

77 *Ibid*.

78 Art. 5, § 1er, b), *in fine* du RGPD.

79 Rapport explicatif de la Convention 108 (version du 28 janvier 1981), § 59 : « 59. Le paragraphe 3 prévoit la possibilité de restreindre les droits des personnes concernées dans le cas de traitements ne présentant aucun risque. Un exemple est celui de l'utilisation de données à des fins statistiques, dans la mesure où il s'agit de données présentées sous une forme agrégée et séparées des identifiants. De même la recherche scientifique est mentionnée dans cette rubrique, conformément à une recommandation de la Fondation européenne de la science ».

La Directive indiquait clairement que les garanties qui doivent accompagner ces traitements pour qu'ils bénéficient du régime spécifique « doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne »[80]. Cette indication n'est reprise dans le RGPD que concernant les utilisations à des fins statistiques[81], les finalités de recherche scientifique, en particulier dans le domaine de la santé, pouvant éventuellement déboucher sur des résultats conduisant à la prise de mesures dans l'intérêt de la personne concernée[82].

La Directive prévoyait donc elle aussi cette compatibilité systématique pour ce genre de traitement. Selon son article 6, § 1er, b), un traitement ultérieur « à des fins historiques, statistiques ou scientifiques » devait être considéré comme compatible s'il respectait les « garanties appropriées » que chaque État membre devait prévoir en supplément de la Directive. On constate donc que la formulation du RGPD est quelque peu plus restrictive : c'est la *recherche* scientifique seule qui est visée et les finalités historiques sont divisées en deux catégories, les finalités de *recherche* historique et *l'archivage* mais seulement *dans l'intérêt public*.

Les considérants apportent des éclairages sur la portée des termes utilisés[83].

a) Traitement ultérieur à des fins archivistiques dans l'intérêt public ou à des fins de recherche historique

18. Les considérants précisent tout d'abord que les traitements à des fins archivistiques dans l'intérêt public et à des fins de recherche historique ne doivent être pris en considération pour l'application du RGPD que lorsqu'ils portent sur des personnes qui ne sont pas décédées[84].

Ils clarifient ensuite que les traitements à des fins de recherche historique comprennent les recherches à des fins généalogiques[85].

---

[80] Considérant n° 29 de la Directive.

[81] Considérant n° 162, *in fine* du RGPD : « Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier ». Cette précision a une incidence sur le développement de traitements de *Big Data* qui ne peuvent être considérés comme entrant dans la catégorie des traitements à des fins statistiques et bénéficier du régime spécifique s'ils débouchent sur une prise de mesure ou de décision concernant une personne individualisée. Ces opérations sont alors plutôt spécifiquement visées par la disposition sur le profilage (art. 22).

[82] Considérant n° 159, *in fine* du RGPD.

[83] Sur cette exception voy. P. Van Eecke et Ch. Suffys, « Herbestemming van verzamelde persoonsgegevens voor andere doeleinden », *op. cit.*, p. 71.

[84] Considérants nos 158 et 160 du RGPD.

[85] Considérant n° 160 du RGPD.

Enfin, ils spécifient que les autorités publiques ou les organismes publics ou privés qui conservent des archives dans l'intérêt public « devraient être des services qui, en vertu du droit de l'Union ou du droit d'un État membre, ont l'obligation légale de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur, de diffuser des archives qui sont à conserver à titre définitif dans l'intérêt public général et d'y donner accès »[86]. Et ils apportent cette autre illustration de traitement ultérieur à des fins archivistiques que les États membres peuvent prévoir : le traitement des données à caractère personnel « en vue de fournir des informations précises relatives au comportement politique sous les régimes des anciens États totalitaires, aux génocides, aux crimes contre l'humanité, notamment l'Holocauste, ou aux crimes de guerre »[87].

b) Traitement ultérieur à des fins de recherche scientifique

19. La notion de traitement de données à caractère personnel à des fins de recherche scientifique doit être interprétée au sens large et couvrir, notamment, « le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé »[88] de même que « les études menées dans l'intérêt public dans le domaine de la santé publique »[89]. Elle couvre ainsi, par exemple, les traitements de données réalisés dans les laboratoires universitaires ou le cas d'un médecin désireux de réutiliser les données contenues dans les dossiers de ses patients pour alimenter la recherche d'un laboratoire pharmaceutique privé ou ses propres recherches[90,91]. Elle s'étend aussi à l'objectif de réaliser un espace européen de la recherche, mentionné à l'article 179 du Traité sur le fonctionnement de l'Union européenne[92].

---

[86] Considérant n° 158 du RGPD.

[87] Considérant n° 158, *in fine*, du RGPD.

[88] Considérant n° 159 du RGPD.

[89] *Ibid.*

[90] Voy. égal. à ce sujet, Comité des ministres du Conseil de l'Europe, Recommandation n° R (97) 5 sur la protection des données médicales, 1997, pt 12 (« Recherche scientifique ») : « 12.3 – Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels des soins de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données médicales qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée ».

[91] Voy. égal., concernant la participation à des activités de recherche scientifique dans le cadre d'essais cliniques, l'application du règlement (UE) 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE, *J.O.*, L 158 du 27 mai 2014, p. 1.

[92] Considérant n° 159 du RGPD.

c) Traitement ultérieur à des fins statistiques

20. Par « fins statistiques », le considérant n° 162 signale qu'il convient d'entendre « toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques ». Les statistiques visent à analyser et à caractériser des phénomènes collectifs ou de masse dans une population donnée[93]. Les résultats statistiques ne sont normalement pas une fin en soi[94] et peuvent eux-mêmes être utilisés à d'autres fins, notamment des fins de recherche scientifique[95].

Ce qui est important c'est qu'ainsi qu'il a été dit plus haut, les traitements de données à des fins statistiques ne peuvent déboucher que sur des résultats présentant des données sous forme agrégée et non plus individualisée et que ces résultats ne puissent servir à prendre des mesures ou des décisions concernant une personne physique en particulier[96]. Des opérations telles le « traçage, le profilage dans un but de marketing direct, la publicité comportementale, le *brokering* de données personnelles, la publicité basée sur la localisation ou les études de marché digitales basées sur le traçage »[97], ne correspondent donc pas à des traitements de données à des fins statistiques, étant donné que ces opérations se basent sur une analyse de données à un niveau individuel[98].

SECTION 3. – Principe de minimisation des données

§ 1. Données adéquates et pertinentes

21. Les données à caractère personnel faisant l'objet d'un traitement doivent, comme auparavant, être adéquates et pertinentes au regard des

[93] Comité des Ministres du Conseil de l'Europe aux États membres, Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, 30 septembre 1997, annexe, pt 1.

[94] Comité des Ministres du Conseil de l'Europe, Recommandation n° R (97) 18, précitée, annexe, pt 11.

[95] Considérant n° 162 du RGPD.

[96] Considérant n° 162 du RGPD. Égal. Rapport Explicatif de la version modernisée de la Convention 108 du Conseil de l'Europe, adopté le 18 mai 2018, § 48, disponible sur www.coe.int/dataprotection

[97] Notre traduction. P. Van Eecke et Ch. Suffys, « Herbestemming van verzamelde persoonsgegevens voor andere doeleinden », *op. cit.*, p. 71.

[98] *Ibid.*

finalités du traitement. Pour être jugées pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies[99].

De nombreux formulaires, jugés à l'aune de cette exigence de pertinence des données, devraient bien être allégés en termes de données recueillies.

§ 2. Données limitées à ce qui est nécessaire

22. Plutôt que de devoir être en outre « non excessives », comme dans les textes de la Convention 108 et de la Directive, les données à caractère personnel doivent désormais être « limitées à ce qui est nécessaire » au regard des finalités pour lesquelles elles sont traitées[100].

Le projet de texte émanant de la Commission ajoutait que le fait que les données soient limitées au minimum nécessaire exigeait de « veiller à ce que les données collectées ne soient pas excessives »[101]. Même si ce passage n'est pas repris dans le texte final du RGPD, il faut comprendre que les deux formulations « limitées à ce qui est nécessaire » et « données non excessives » se rejoignent en ce qu'elles sont toutes deux l'expression du principe de proportionnalité[102].

Il est à noter que le critère de nécessité s'exprime tant au niveau de la quantité des données que de leur qualité. Ainsi, s'il est clair qu'on ne peut traiter un nombre excessif de données[103] (demander à un employé l'ensemble de son dossier médical pour juger de son aptitude au travail, notamment), on ne peut davantage se lancer dans le traitement d'une seule donnée qui, même pertinente au vu de la finalité, porterait excessivement atteinte aux droits et intérêts de la personne concernée par

---

[99] M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *op. cit.*, p. 146.

[100] On notera que la directive 2016/680/UE 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, a, quant à elle, gardé la formulation initiale et son article 4, § 1er, c) établit que les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont traitées ».

[101] Considérant n° 30 de la proposition de règlement publiée le 25 janvier 2012 par la Commission européenne, COM(2012) 11 final.

[102] Dans le même sens, O. Santantonio, « Exposé introductif du règlement général sur la protection des données », *Data Protection. L'impact du GDPR en assurance*, *Bull. Ass.*, 2017, n° 22, pp. 30-31.

[103] « A l'heure du Big Data et donc de la collecte massive en tout genre de données, cette obligation peut relever du véritable challenge et est en contradiction avec les ambitions de bon nombre d'entreprises notamment dans le secteur des assurances » (*ibid.*, p. 31).

rapport à l'intérêt qu'elle présente pour la personne qui souhaite la traiter (collecter l'information sur la sérologie VIH ou sur la consommation de drogue dans le cadre privé d'un candidat dans une procédure de recrutement pour un poste administratif, par exemple)[104].

23. Par ailleurs, selon le considérant n° 39, le principe de minimisation des données conduit à ce que l'on ne puisse traiter des données à caractère personnel que lorsqu'il n'y a pas raisonnablement moyen d'atteindre la finalité sans cela. « S'agissant par exemple des données collectées par un véhicule concernant la manière de conduire de la personne, et qui seraient justifiées par une optimisation des entretiens ultérieurs réalisés par le constructeur, on peut sérieusement douter que l'enregistrement des données de localisation du véhicule ou de certaines informations sur le mode de conduite soient nécessaires à la finalité projetée. En général, il sera en effet possible d'atteindre le résultat attendu sans procéder à un tel traitement […] »[105].

§ 3. Recours à l'anonymisation ou à la pseudonymisation

24. Le recours à l'anonymisation des données, rendant la personne concernée non identifiable[106], permet dans nombre de cas d'honorer le principe de minimisation tout en continuant de traiter les données.

Si l'anonymisation n'est pas indiquée pour atteindre l'objectif du traitement, le recours au codage ou à la pseudonymisation des données peut s'avérer opportun. Il s'agit du « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin

[104] Dans ce sens, voy. l'explication de la notion de données « excessives » dans le Rapport explicatif de la Convention 108 modernisée du Conseil de l'Europe, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4b : « Cette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel. Des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées ».

[105] H. Jacquemin et J.-M. Van Gyseghem, « Le Big Data en matière d'assurances à l'épreuve du RGPD », *Bull. Ass.*, 2017, n° 22, p. 247.

[106] Considérant n° 26, *in fine*, du RGPD. Voy. ce qui est dit sur la notion de donnée anonyme dans la contribution du présent ouvrage : C. de Terwangne, « Définitions clés et champ d'application du RGPD », pt 6.

de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[107].

Les auteurs du règlement ont marqué leur intention d'encourager les opérations de pseudonymisation, instrument de réduction des risques pour les personnes concernées[108]. La pseudonymisation interne (sans avoir recours à un opérateur externe pour réaliser le codage) est expressément admise pourvu que des mesures techniques et organisationnelles garantissent que les informations supplémentaires permettant d'attribuer les données à une personne concernée précise soient conservées séparément. Le responsable du traitement en question doit en outre désigner les personnes autorisées à accéder aux informations identifiantes conservées séparément des données[109].

§ 4. Impact sur la durée de conservation des données

25. Il est précisé au considérant n° 39 que le principe de minimisation implique que la durée de conservation des données soit limitée « au strict minimum », ce qui renvoie au principe de limitation de la conservation développé ci-dessous (Section 5).

§ 5. Pas de nécessité de collecte d'informations supplémentaires pour les traitements ne nécessitant pas l'identification (art. 11 RGPD)

26. On évoquera enfin ici une disposition nouvelle qui peut être mise en regard du principe de minimisation des données, disposition particulièrement pertinente et bienvenue qui a été insérée dans le RGPD pour dispenser de collecter les données identifiantes des personnes concernées. Il s'agit de l'article 11 selon lequel si les données traitées par un responsable du traitement ne permettent pas à celui-ci d'identifier une personne physique, il n'est pas obligé d'obtenir des informations supplémentaires pour identifier la personne en question en vue de respecter le RGPD, notamment les droits des personnes concernées.

Cette disposition vise par exemple le cas où une caméra a été placée sur un immeuble filmant les allées et venues à l'entrée. Les images filmées sont des données à caractère personnel dès lors que les personnes sont identifiables, même si le propriétaire de l'immeuble ne procède pas

[107] Art. 4, 5°, du RGPD.
[108] Considérants n^os^ 28 et 29 du RGPD.
[109] Considérant n° 29 du RGPD.

lui-même à l'identification des personnes entrant et sortant. L'article 11 du règlement dispense le responsable de ce traitement de chercher à identifier les individus filmés juste pour être à même de leur répondre s'ils souhaitent exercer leurs droits d'accès, de rectification ou d'opposition. Dans le même sens, le chercheur qui travaille avec des données codées obtenues à diverses sources ne devra pas se fournir la clé des codes ni les informations de contact pour honorer son obligation d'information des personnes concernées.

L'idée est donc que les règles de protection des données n'aboutissent pas à la situation paradoxale où l'on doive en connaitre davantage sur les personnes à propos de qui on traite des données pour garantir la protection de leurs données.

SECTION 4. – Principe d'exactitude

27. Déjà présente dans les textes antérieurs, l'exigence que les données soient exactes et, si nécessaire, tenues à jour est reprise dans le RGPD[110]. Il incombe ainsi au responsable du traitement de veiller à la qualité des données à caractère personnel traitées. Toute inexactitude doit être corrigée ou les données à caractère personnel inexactes[111] doivent être effacées, l'article 5, § 1er, d), apportant cette précision que la rectification doit être faite « sans tarder ».

C'est une obligation de moyens qu'impose ici le RGPD car il précise qu'il s'agit de prendre « toutes les mesures *raisonnables* […] pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ». Cette obligation sera jugée plus ou moins sévèrement en fonction du contexte du traitement effectué. Qu'il y ait, par exemple, des erreurs dans un listing d'adresses utilisées pour l'envoi de publicité ne sera pas particulièrement dommageable pour ceux recevant un message publicitaire qui ne leur est normalement pas adressé ni pour ceux qui sont privés de ce message. Par contre, il a été jugé en matière de crédit que le prêteur qui transmet une information inexacte sur un débiteur soi-disant défaillant commet une faute[112].

[110] Art. 5, § 1er, d), du RGPD.

[111] Pour une clarification de la notion de données à caractère personnel inexactes (dans le cas où les données consistent en des réponses à un examen), voy. C.J.U.E., 20 décembre 2017, arrêt *Peter Nowak c. Data Protection Commissioner*, C-434/16, §§ 53 et 54.

[112] Civ. Bruxelles (72e ch.), 15 octobre 2003, *J.T.*, 2004, pp. 140 et 141.

Le droit d'accès octroyé aux personnes concernées[113] a notamment pour but de permettre à ces dernières de traquer les erreurs et de les faire corriger ensuite en invoquant leur droit de rectification[114].

On signalera ici que la directive 95/46 ajoutait aux données inexactes les données incomplètes. C'est d'ailleurs ce qualificatif qui justifiait très vraisemblablement la précision « au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement » qui y était accolée. Les auteurs du RGPD ont supprimé l'adjectif « incomplètes » de l'article 5, § 1er, d), pour le réserver à l'article 16 qui consacre le droit de rectification. Ce droit vaut tout d'abord pour les données inexactes mais l'article 16 poursuit : « Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire ». On notera qu'en ayant supprimé l'adjectif « incomplètes » de l'article 5, § 1er, d), les auteurs du RGPD auraient dû supprimer également la portion de phrase précisant au regard de quoi devait se vérifier l'incomplétude éventuelle des données. Ils l'ont toutefois laissée alors qu'elle ne se justifie plus dès lors qu'on ne parle plus que de données inexactes. Or, l'exactitude d'une donnée n'est pas, elle, une question de contexte : une donnée est exacte ou inexacte quelle que soit la finalité poursuivie.

Par contre, il ne peut être question de caractère exact ou inexact d'informations subjectives tels les avis ou opinions. On ne peut donc contester l'exactitude de telles informations[115]. Toutefois, il importe que l'opinion émise s'appuie sur des données objectives dont l'éventuelle inexactitude pourra, elle, être mise en question. La qualité du raisonnement ou de l'analyse effectués à partir des données pour conduire à l'avis ou l'opinion émis peut, elle aussi, être éventuellement contestée.

---

[113] Voy. la contribution de Thomas Tombal dans le présent ouvrage.

[114] C.J.U.E., 20 décembre 2017, arrêt *Peter Nowak c. Data Protection Commissioner*, C-434/16, § 56.

[115] Cela n'empêche pas ces données subjectives d'être considérées comme des « données à caractère personnel », le cas échéant. Pour un exemple, voy. l'arrêt *Nowak* dans lequel la Cour de justice a tranché en exposant que les évaluations d'un examinateur et le contenu de ses « annotations reflète[nt] l'avis ou l'appréciation de l'examinateur sur les performances individuelles du candidat lors de l'examen, et notamment sur ses connaissances et ses compétences dans le domaine concerné » et entrent dans la définition de données à caractère personnel (C.J.U.E., arrêt *Nowak*, précité, § 43).

SECTION 5. – Principe de limitation de la conservation

§ 1. Durée de conservation des données limitée au regard de la finalité du traitement

28. Le RGPD n'apporte pas de véritable changement à l'interdiction de conserver les données à caractère personnel sous une forme permettant l'identification des personnes au-delà du temps nécessaire à l'accomplissement des finalités liées au traitement de ces données[116]. C'est donc la détermination de la finalité d'un traitement qui permet de définir la durée de conservation des données à caractère personnel traitées.

La durée licite de conservation des données n'est dès lors pas uniforme, mais dépend de la finalité du traitement de ces données. Dès l'instant où les données ne sont plus nécessaires pour atteindre la finalité de leur collecte ou les finalités ultérieures compatibles, le responsable du traitement est tenu soit de les effacer, soit de les anonymiser, c'est-à-dire de faire disparaître irréversiblement leur élément identifiant[117].

Le responsable du traitement doit faire cette opération de suppression ou d'anonymisation des données spontanément, et non sur demande des personnes concernées.

29. Cette obligation d'effacement est une des facettes du « droit à l'oubli » qui est reconnu aux personnes concernées[118]. Cette facette est expressément consacrée en tant que telle à l'article 17, § 1er, a), du RGPD selon lequel le responsable du traitement a l'obligation d'effacer, dans les meilleurs délais, les données à caractère personnel qui sont conservées alors qu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière. Il n'est pas légitime, pour la plupart des traitements de données, de conserver *ad vitam aeternam* les données sous une forme permettant l'identification des

[116] Art. 5, § 1er, e), du RGPD. La version française de cette disposition (« […] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités […] ») diverge légèrement de la version de l'article 6, § 1er, e) de la directive 95/46 (« […] pendant une durée n'excédant pas celle nécessaire *à la réalisation des* finalités […] » – nos italiques) alors que le sens est normalement identique vu que les versions anglaises des deux textes sont sur ce point parfaitement les mêmes.

[117] Rappelons qu'il ne suffit pas de coder les données pour les anonymiser. Des données codées demeurent des données à caractère personnel tant que la clé du code est conservée (voy. C. DE TERWANGNE, « Définitions clés et champ d'application du RGPD », dans le présent ouvrage).

[118] C. DE TERWANGNE, « Internet privacy and the right to be forgotten/right to oblivion », *Revista de Internet, Derecho y Politica,* 2012, n° 13, p. 114, http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng.

personnes. Dès qu'elle ne se justifie pas par un critère de nécessité, une conservation des données « pour mémoire » n'est pas légitime.

Il est à noter toutefois que les données peuvent être conservées à des fins probatoires durant une période correspondant au délai de prescription.

Il existe des traitements de données dont la finalité est telle qu'elle permet la conservation des données illimitée dans le temps. Il s'agit, par exemple, de la tenue des registres de population par les communes ou de l'archivage des documents du secteur public contenant des données à caractère personnel.

30. Le considérant n° 39 du RGPD suggère que des délais soient fixés dès le départ par le responsable du traitement pour l'effacement des données ou pour une vérification périodique, afin de garantir que la conservation des données ne dépasse pas ce qui est nécessaire.

Par application du principe de *privacy by design* et *by default*[119], on peut mettre en place un mécanisme technique prévoyant que la conservation des données se termine automatiquement dès que le temps nécessaire pour atteindre la finalité annoncée est passé. Cette instauration de « dates de péremption » techniques des données assure efficacement la protection voulue des individus.

De telles possibilités de mettre en place un système automatique de destruction des données existent déjà. À titre d'illustration d'un système de ce type, le logiciel X-Pire, lancé en Allemagne[120], permet aux utilisateurs d'attacher une date d'expiration digitale aux images enregistrées sur des sites de réseaux sociaux comme Facebook.

§ 2. Exception pour les données conservées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

31. Il est des cas où l'on ne souhaite pas effacer, détruire ni anonymiser les données à caractère personnel une fois la finalité originelle atteinte. C'est lorsque ces données peuvent servir à des fins d'archivage, à des fins de recherche scientifique ou historique ou à des fins statistiques. Le RGPD a prévu cette situation et permet de conserver les données à caractère personnel « pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en

[119] Voy. la contribution d'A. Delforge, « Les obligations générales du responsable du traitement et la place du sous-traitant » dans le présent ouvrage.

[120] http://www.getxpire.com/.

œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée »[121].

Si la conservation « longue durée » est donc permise dans les cas visés, il faut toutefois mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les droits et libertés des personnes concernées. L'article 89, § 1er, du RGPD évoque, à titre de mesure permettant d'assurer le respect du principe de minimisation des données, la pseudonymisation et l'anonymisation des données, dans la mesure où cela n'entraverait pas la réalisation des finalités d'archivage, de recherche scientifique ou historique, ou de statistique.

SECTION 6. – Principe d'intégrité et confidentialité

32. Sous l'intitulé de principe d'« intégrité et confidentialité », c'est le devoir de sécurité des données qui figure désormais au rang des principes de base de la protection des données[122], devoir classique mais ô combien crucial aujourd'hui que les données à caractère personnel représentent un eldorado attisant les convoitises des cyber-criminels en tout genre[123].

Le responsable du traitement doit protéger les données à caractère personnel qu'il a collectées contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Il doit, selon les termes de l'article 5, § 1er, f), du RGPD, veiller à « garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ».

Les mesures de sécurité à prendre sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe renouvelés régulièrement, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures

---

121 Art. 5, § 1er, b), du RGPD.

122 Art. 5, § 1er, f), du RGPD.

123 European Commission, Joint communication to the European Parliament and the Council, « Resilience, Deterrence and Defence : Building strong cybersecurity for the EU », 13 September 2017, JOIN, 2017 450 final ; McAfee & Centre for Strategic and International Studies, *Net losses : Estimating the Global Cost of Cybercrime*, 2014 ; EUROPOL, *Serious and Organised Crime Threat Assessment*, 2017, https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment.

techniques (programme anti-virus fréquemment mis à jour, *firewalls, backup* de sécurité, *login*...).

Elles doivent assurer un niveau de protection approprié, adapté au risque que présente le traitement en question et tenant compte de différents facteurs[124]. Ainsi, plus les données en cause sont sensibles et les risques pour la personne concernée sont grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (p. ex., par une compagnie d'assurances pour octroyer une assurance-vie), devront être encadrées de mesures de sécurité sévères.

Une section entière du chapitre du RGPD dédié aux responsable et sous-traitant[125] développe ce devoir de sécurité en apportant la nouveauté de l'obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les violations de données. On renvoie ici à la contribution de Franck Dumortier « La sécurité des traitements de données à caractère personnel » dans le présent ouvrage, qui offre une analyse substantielle, particulièrement riche et précieuse, de l'obligation de sécurité liée au de principe d'« intégrité et confidentialité ».

SECTION 7. – Principe de responsabilité (*accountability*)

33. La liste des principes de base de la protection des données se termine par l'affirmation que revient au responsable du traitement la responsabilité du respect de tous ces principes et, nouveauté, que le responsable doit être à même de démontrer que son traitement est en conformité avec ces principes[126]. C'est « [l]a responsabilité comme moteur de l'application efficace des principes de protection des données »[127, 128].

Cette dimension d'« être en mesure de démontrer le respect des règles » n'apparait pas clairement dans le terme « responsabilité » auquel on

[124] Précisions qui sont apportées et plus amplement développées par l'article 32 du RGPD.

[125] Section 2 du chapitre IV consacré aux responsables du traitement et sous-traitant, articles 32 à 34 du RGPD. Voy. la contribution d'Antoine Delforge dans le présent ouvrage.

[126] Art. 5, § 2, du RGPD.

[127] Groupe 29, Avis 3/2010 sur le principe de responsabilité (principle of accountability dans la version anglaise), WP 173, 13 juillet 2010, § 5.

[128] Sur cette notion d'« *accountability* », la genèse de son importation en droit européen de la protection des données et sa portée, voy. R. Thomas, « Accountability – a modern approach to regulating the 21st century data environment », in H. Hijmans et H. Kranenborg (eds.), *Data Protection Anno 2014 : How to Restore Trust ?*, Intersentia, 2014, pp. 135-147.

préfère donc parfois le terme anglais d'« *accountability* » qui comprend bien, lui, l'idée de rendre des comptes[129]. Le Groupe de l'article 29 a clarifié la portée qu'il convient d'accorder à ce terme : « En anglais, on utilise le terme "*accountability*", […]. Globalement, on peut dire qu'il met l'accent sur la manière dont la responsabilité (*responsability*) est assumée et sur la manière de le vérifier. En anglais, les termes "*responsibility*" et "*accountability*" sont comme l'avers et le revers d'une médaille et sont tous deux des éléments essentiels de la bonne gouvernance. On ne peut inspirer une confiance suffisante que s'il est démontré que la responsabilité (*responsability*) est efficacement assumée dans la pratique »[130].

Au nom du principe de responsabilité, le responsable du traitement est donc tenu de mettre en œuvre des mesures appropriées et effectives pour réaliser la protection des individus à l'égard du traitement de leurs données, et il doit être à même de démontrer la conformité des activités de traitement avec le RGPD, « y compris l'efficacité des mesures »[131]. C'est en outre pendant toute la durée du traitement que le responsable du traitement doit garantir la conformité de celui-ci[132].

Cette obligation de s'assurer et d'être en mesure de démontrer que le traitement de données est effectué conformément au règlement est reprise et développée à l'article 24 du RGPD consacré à la responsabilité du responsable du traitement[133]. Certaines obligations nouvelles mettent en œuvre le principe d'*accountability* au travers de mesures concrètes, telles que l'obligation d'effectuer une analyse de risque, de mettre en œuvre une politique de sécurité ou de concevoir le traitement de manière à minimiser les risques pour les personnes concernées[134].

---

[129] Le principe d'« *accountability* » était déjà mentionné dans le tout premier texte de portée internationale relatif à la protection des données, les Lignes directrices de l'OCDE du 22 septembre 1980 dont l'article 14 est intitulé en anglais « Accountability Principle » et qui dispose : « *A data controller should be accountable for complying with measures which give effect to the principles stated above* ».

[130] Groupe 29, Avis 3/2010 sur le principe de responsabilité (principle of accountability dans la version anglaise), WP 173, 13 juillet 2010, § 21.

[131] Considérant n° 74 du RGPD.

[132] Th. Leonard et D. Chaumont, « GDPR-expert. Article 5 Principes relatifs au traitement des données à caractère personnel », https://www.gdpr-expert.eu/article.html?id=5#ouvaton ; A. Bensoussan *et al.*, *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques*, 2e éd., Bruxelles, Bruylant, 2018, p. 89.

[133] Voy. les développements centrés sur le devoir d'*accountability* dans la contribution d'Antoine Delforge dans le présent ouvrage.

[134] L. A. Bygrave, « Hardwiring Privacy », in *The Oxford Handbook of the Law and Regulation of Technology* (R. Brownsword, E. Scotford et K. Yeung eds), Oxford, Oxford University Press, 2017 ; University of Oslo, Faculty of Law, Research Paper No. 2017-02, https://ssrn.com/

En compensation de cet accent mis sur une responsabilisation accrue des acteurs[135] à travers l'*accountability*, le RGPD a supprimé la formalité de déclaration préalable des traitements à l'autorité de contrôle et a réduit la procédure de consultation préalable de l'autorité[136].

En définitive, en faisant peser sur le responsable du traitement le poids de la responsabilité d'une mise en œuvre des traitements respectueuse des principes de protection des données contenus dans le règlement, ce dernier « *shifts much of the burden of policing against bad actors and irresponsible data use from individuals to the organisations that derive value from data* »[137].

abstract=2901405 ; B. Van Asbroeck et J. Debussche, « Les obligations de 'compliance' des entreprises », in *Vers un droit européen de la protection des données* (B. Docquir coord.), Bruxelles, Larcier, 2017, pp. 105 et s.

[135] C. de Terwangne, K. Rosier et B. Losdyck, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017, pp. 308 et s.

[136] Art. 36 du RGPD.

[137] R. Thomas, « Accountability – a modern approach to regulating the 21st century data environment », *op. cit.*, p. 147.

CHAPITRE 2. Hypothèses de licéité des traitements

SECTION 1. – Hypothèses ou conditions

34. L'article 6, § 1er, du règlement stipule que le traitement de données à caractère personnel n'est licite « que si, et dans la mesure où, au moins une des conditions suivantes est remplie ». Il ne s'agit pas à proprement parler de conditions à remplir mais plutôt d'hypothèses dans lesquelles les traitements sont admis[138].

Ces hypothèses sont les seules dans lesquelles il est permis de traiter des données à caractère personnel[139]. Elles correspondent à celles déjà admises par la Directive, même si certains changements ou précisions sont apparus. La Cour de justice a eu l'occasion d'insister sur la nature « exhaustive et limitative » de la liste des hypothèses énoncées à l'article 7

---

[138] La traduction française de la proposition de texte publiée par la Commission européenne en début de processus législatif diffère d'ailleurs, alors même que les mots anglais n'ont pas changé. Ainsi, la version anglaise énonce que le traitement de données n'est licite que si « *at least one of the following applies* », ce qui a d'abord été traduit par « l'une au moins des situations suivantes s'applique », avant de devenir, dans la version finale « au moins une des conditions suivantes est remplie ».

[139] C.J.U.E., 24 novembre 2011, arrêt *ASNEF et FECEMD c. Administracion del Estado*, C-468/10 et C-469/1.

de la Directive, équivalant à l'article 6, § 1er, du RGPD[140]. Elle a souligné que « les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la directive 95/46 ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article »[141].

35. Avant de parcourir ces différentes hypothèses, il est important de bien comprendre l'articulation entre les articles 5, et singulièrement l'article 5, § 1er, b), et 6 du RGPD qui doivent être lus conjointement[142]. Le fait de se trouver dans une des situations énoncées à l'article 6 n'implique pas que l'exigence de finalité légitime de l'article 5 soit *ipso facto* rencontrée. Les hypothèses visées dans la première disposition n'empêchent pas un contrôle sur la base de la deuxième[143]. En fait, on peut considérer que l'article 6 prévoit des situations abstraites dans lesquelles il y a une présomption d'équilibre des intérêts en présence, sans préjudice d'un contrôle concret, sur la base de l'article 5, permettant, le

[140] C.J.U.E., 24 novembre 2011, arrêt *ASNEF et FECEMD c. Administracion del Estado*, précité, pt 31.

[141] *Ibid*, pt 32. Voy. toutefois, *infra* Chapitre 2, Section 5, § 3, la nuance apportée par l'article 6, § 2, du RGPD concernant les traitements fondés sur une obligation légale ou une mission d'intérêt public.

[142] Pour le même raisonnement transposé à la directive 95/46/CE, voy. C.J.U.E., 24 novembre 2011, arrêt *ASNEF et FECEMD contre Administracion del Estado*, précité, pt 26 : « Tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncés à l'article 6 de ladite directive et, d'autre part, répondre à l'un des six principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette même directive ». L'exigence de respecter cumulativement le contenu de ces deux dispositions se retrouve, *mutatis mutandis*, clairement exprimée dans le Rapport explicatif de la version modernisée de la Convention 108, précité : « Les paragraphes 1, 2, 3 et 4 de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données » (§ 39). Le paragraphe 1er en question énonce l'obligation de respecter le principe de proportionnalité (« Le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu »), tandis que le paragraphe 2 correspond à l'exigence d'un fondement légitime pour traiter les données (l'équivalent donc de l'article 6 RGPD) et que les paragraphes 3 et 4 correspondent aux principes de licéité, loyauté, finalité et de qualité des données.

[143] Voy. Groupe 29, Guidelines on consent under Regulation 2016/679, 28 November 2017, last revised and adopted on 10 April 2018, WP 259 rev.01, p. 3 : « *obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity an proportionality [...]* ». Égal. M. Van Overstraeten et S. Depre, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 689 et 690.

cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu[144]. Ce n'est pas parce qu'on a le consentement d'une personne à ce que l'on traite les données la concernant (ce qui correspond à une des hypothèses de légitimité de l'article 6) que le traitement est d'office admissible. Le Rapport explicatif de la Convention 108 modernisée le dit explicitement : « L'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être évaluée »[145]. Ainsi, un traitement basé sur le consentement de la personne concernée porte peut-être atteinte de manière disproportionnée à un intérêt collectif qui n'a forcément pas été pris en compte par la personne concernée qui n'a envisagé, comme il se doit, que ses propres droits et intérêts pour donner son consentement. La condition de finalité légitime de l'article 5, § 1er, b), n'est, dans ce cas, pas rencontrée alors même que l'article 6 est respecté. Le traitement de données envisagé doit être déclaré illégal.

Pour être admis, tout traitement de données doit donc poursuivre un objectif qui respecte le principe de proportionnalité (art. 5, § 1er, b) tout en reposant sur un fondement licite, c'est-à-dire en correspondant à l'une des six hypothèses énoncées par l'article 6 du RGPD. Ces hypothèses sont les suivantes.

SECTION 2. – Le consentement de la personne concernée

36. Un traitement sera considéré comme licite s'il est effectué avec le consentement de la personne concernée pour une ou plusieurs finalités spécifiques[146]. Au-delà de la définition du consentement donnée à l'article 4, 11°, du RGPD qui est enrichie par rapport à la définition contenue

[144] M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *op. cit.*, p. 148, n° 41 ; J. Dhont, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 2000/1, pp. 324 et 325.

[145] Rapport explicatif de la version modernisée de la Convention 108 du Conseil de l'Europe, adopté le 18 mai 2018, précité.

[146] Art. 6, § 1er, a), du RGPD. On notera le paradoxe de la version française du RGPD qui définit la notion de consentement à l'article consacré aux définitions mais n'utilise pas expressément ce terme dans les hypothèses de licéité des traitements puisqu'il est dit à

dans la Directive (§ 1 ci-dessous), deux articles[147] apportent encore des précisions sur le sujet et de longs considérants[148] viennent éclairer l'ensemble. Il y a là les traces des discussions nourries sur la question qui ont émaillé l'action législative du Parlement européen et du Conseil et le trilogue qui a pris place avec la Commission par la suite[149].

§ 1. Un consentement de qualité comme fondement de licéité du traitement

a) Renforcement de la qualité du consentement

37. Le Parlement européen a clamé l'importance de la place du consentement dans l'édifice de protection des données : « Le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données »[150]. Toutefois, le législateur européen a fortement insisté durant le processus d'élaboration du RGPD sur la nécessité de veiller à ce qu'il ne soit plus abusé du recours au consentement et à ce que, lorsqu'un traitement repose sur le consentement des personnes concernées, ce consentement soit de qualité et soit donné dans un contexte tel qu'on se trouve face à la véritable expression de l'autonomie du sujet. Le législateur a voulu réagir à la multiplication des situations dans lesquelles un consentement de (très) mauvaise qualité servait de fondement de licéité au traitement des données, soit « le consentement basé sur le silence »[151]. Ce sont les cases pré-cochées et les configurations par défaut que la personne concernée doit modifier si elle ne souhaite pas voir ses données traitées, qui se sont retrouvées dans le collimateur des auteurs du règlement. En renforçant les

---

l'article 6, § 1er, a), que le traitement est licite lorsque « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques » plutôt que lorsqu'elle a « donné son consentement », comme mentionné dans la Directive.

147 Art. 7 et 8 du RGPD.

148 Considérants nos 32, 33, 42, 43 et 44.

149 Les discussions ont été éclairées notamment par l'opinion émise par le Groupe 29 sur la notion de consentement (Groupe 29, Avis 15/2011 du 13 juillet 2011 sur la notion de consentement, WP 187).

150 Comité LIBE du Parlement européen, 21 novembre 2013, Rapport sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Rapporteur J. Ph. Albrecht, « Exposé des motifs », pp. 218-219.

151 Groupe 29, Guidelines on consent under Regulation 2016/679. Last revised and adopted on 10 April 2018, 28 novembre 2017, WP 259 rev.01, p. 16.

exigences relatives à la qualité du consentement, ces derniers ont veillé à ce que, désormais, soit le responsable du traitement s'appuie sur un consentement de bonne qualité, soit il utilise une autre base de légitimité pour traiter ces données[152].

Aux termes de l'article 4, 11°, du RGPD, il faut entendre par « consentement » de la personne concernée « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Le consentement doit donc être, comme sous l'empire de la Directive, libre (point b *infra*), spécifique (point c) et éclairé (point d). Il doit par ailleurs être univoque et manifester la volonté de la personne concernée par une déclaration ou un acte positif clair de sa part (point e).

b) « libre »

38. Le consentement sera considéré comme ayant été librement donné uniquement si la personne concernée dispose d'une véritable liberté de choix ou est en mesure de refuser ou de retirer son consentement sans subir de préjudice[153]. Il ne doit y avoir aucun risque « de tromperie, d'intimidation, de coercition, ou de conséquence négative significative (comme un substantiel supplément de coût) »[154].

À titre d'exemple, le consentement est présumé ne pas avoir été donné librement si l'exécution d'un contrat est suspendue au consentement pour le traitement de données qui ne sont pas nécessaires à ce contrat[155].

---

[152] Le renforcement des exigences relatives à la qualité du consentement s'inspire des recommandations émises dans l'avis n° 15/2011 par le Groupe 29 sur la définition du consentement, 13 juillet 2011, WP 187.

[153] Considérant n° 42 du règlement. Voy. égal. Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 3 : « *Consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment* ».

[154] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 7 (traduction libre).

[155] Art. 7, § 4, et considérant n° 43 du RGPD. E. Plasschaert transposant cette disposition dans le contexte professionnel, même si ce contexte n'était sans doute pas, d'après lui, la cible de l'article 7, § 4, énonce comme exemple d'application qu'« il y aura lieu de tenir pour vicié le consentement du travailleur qui serait en mesure de démontrer *in concreto* que son consentement au traitement de ses données personnelles à une ou plusieurs finalité fut érigé en condition de la conclusion ou de la poursuite de son contrat de travail » (E. Plasschaert, « La licéité du traitement de données personnelles du travailleur au regard du nouveau règlement (UE) 2016/679 sur la protection des données », in *Data protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk*, *op. cit.*, p. 115).

D'autres situations de pression ou d'influence inappropriées peuvent également illustrer le déséquilibre qui peut exister entre la personne concernée et celle qui veut traiter ses données[156]. Les situations mettant en jeu les autorités publiques sont ainsi des situations de déséquilibre des pouvoirs[157], accentué par le fait qu'il n'existe souvent pas d'alternative pour le citoyen que d'accepter que ses données soient traitées[158]. Dans un contexte d'emploi, également, le rapport de forces déséquilibré existant entre les parties explique que l'employeur ne puisse revendiquer de s'appuyer sur le consentement de ses employés pour traiter leurs données[159].

c) « spécifique »

39. Le consentement ne peut être un feu vert général ; il doit porter sur un traitement de données précis, pour une finalité correctement identifiée[160]. Le considérant n° 32 apporte cette précision que « [l]e consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités ». Si l'on est en présence d'un traitement poursuivant des finalités distinctes, le consentement doit alors être donné

[156] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, pp. 5-6.

[157] Le Groupe 29 (Guidelines on consent under Regulation 2016/679, précité, p. 6) reconnait qu'il peut exister des cas rares dans lesquels une autorité publique pourrait s'appuyer sur le consentement pour traiter des données à caractère personnel. Ainsi, lorsqu'une municipalité offre aux citoyens la possibilité de s'abonner à une newsletter.

[158] On ne peut considérer, comme l'a fait le législateur belge, qu'un demandeur d'asile donne librement son consentement à ce que les instances administratives chargées de l'instruction de sa demande de protection internationale aient accès, pour disposer de tous les éléments nécessaires pour étayer la demande, à « toute pièce, tout document, tout objet, tout appareil de communication (téléphone portable, tablette, ordinateur portable, ...), tout compte de réseau social sur Internet (Facebook, Twitter...), tout support informatique (clé USB, CD-(ROM), carte mémoire, ...) susceptible de contenir les éléments susvisés » (Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, Exposé des motifs, *Doc. parl.*, Ch. repr., 2016-2017, n° 54-2548/001, p. 36). « Cette nouveauté est apparentée à une véritable « perquisition numérique » du demandeur d'asile, dans la mesure où son smartphone, son ordinateur, son compte Facebook... – et toutes les données qu'ils contiennent (liste de contacts, conversations, e-mails, photos, ...) – pourront être passées au crible » (J. Mont, « Fouille numérique des demandeurs d'asile. Et la protection de la vie privée ? », *R.D.T.I.*, 2017, pp. 120 et s.) Fonder une telle perquisition sur le consentement libre du demandeur de protection internationale est une ineptie. Voy. par ailleurs les critiques très pertinentes quant aux autres qualités d'un tel consentement (spécifique, éclairé et non univoque), développées par Julie Mont dans l'article précité.

[159] *Ibid.*, p. 7. Le Groupe 29 admet, ici aussi, qu'il peut y avoir des circonstances exceptionnelles dans lesquelles le consentement pourrait être considéré comme librement donné car aucune conséquence négative ne s'ensuivrait d'un refus de la part de la personne concernée.

[160] Groupe 29, Avis n° 15/2011 sur la définition du consentement, 13 juillet 2011, WP 187.

pour chacune d'entre elles[161]. C'est ce qu'on a appelé la « granularité » du consentement[162]. La personne concernée doit donc pouvoir choisir la finalité de traitement qu'elle accepte tout en pouvant refuser d'autres usages de ses données. Elle ne peut être mise devant l'alternative d'accepter ou de refuser toutes les finalités annoncées à la fois. Cela signifie que dans certaines situations, il faudra recueillir plusieurs consentements de la personne concernée (ou un consentement découpé en plusieurs « *opt-in* ») avant de pouvoir commencer à traiter ses données pour différentes finalités[163].

d) « éclairé »

40. Alors que le terme anglais « *informed* » utilisé dans la définition du consentement donnée dans la Directive est maintenu dans la version anglaise du RGPD, cet adjectif qui était traduit dans la version française de la Directive par « informé » est cette fois traduit par « éclairé ». Aucune différence de portée ne doit être attachée à ce nouveau terme.

Pour que le consentement soit considéré comme éclairé, il faut que le responsable du traitement fournisse certaines informations à la personne concernée, sous une forme compréhensible et aisément accessible[164]. Le considérant n° 42 du RGPD réclame que la personne concernée ait connaissance au moins de l'identité du responsable du traitement et des finalités du traitement auquel sont destinées ses données à caractère personnel. La personne concernée donnant son consentement au traitement de ses données à caractère personnel « pour une ou plusieurs finalités spécifiques », ainsi qu'insiste l'article 6, § 1, a), l'information à lui donner doit en tout cas lui permettre de comprendre à quoi va servir le traitement de ses données.

Toutefois, le Groupe de l'article 29 estime que d'autres renseignements sont également cruciaux pour que la personne concernée puisse se décider en connaissance de cause et que son consentement soit valide. Il s'agit d'apporter des informations sur le type de données visées par le traitement envisagé, sur l'existence du droit de retirer le consentement donné (voy. art. 7, § 3, du RGPD), sur l'utilisation éventuelle des données pour une prise de décision automatisée (voy. art. 22, § 2, c), du RGPD) et, le cas

[161] Considérant n° 32 du RGPD. La traduction néerlandaise du considérant indique plus clairement que c'est bien pour chacune des finalités qu'il faut prévenir les personnes concernées : « *Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend* ».

[162] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 10.

[163] *Ibid.*, pp. 10 et 12.

[164] *Ibid.*, p. 13.

échéant, sur les risques liés au transfert des données vers un pays n'offrant pas de protection adéquate et en l'absence de garanties appropriées (voy. art. 49, § 1er, a), du RGPD)[165].

Le but de l'information de la personne concernée à ce stade est « *to allow the data subject to genuinely understand the processing operations at hand* »[166].

e) « univoque » et manifesté « par une déclaration ou un acte positif clair »

41. La définition du consentement énoncée à l'article 4, 11°, du RGPD reflète, ainsi que dit plus haut, l'attention particulière qui a été portée, au travers d'âpres discussions, à la qualité que doit présenter le consentement pour être admis comme fondement d'un traitement. Sous l'empire de la Directive, il devait être « indubitable » pour le traitement de données ordinaires et « explicite » pour les données sensibles. Dans les discussions concernant le projet de règlement, tant la Commission que le Parlement ont été d'avis que désormais il fallait exiger que le consentement soit explicite pour qu'il serve de fondement valide pour le traitement de toutes les données, ordinaires comme sensibles, afin de lutter contre la récolte facile de consentements de mauvaise qualité sur Internet. Le Conseil n'a pas suivi cette option et au final on est revenu à la notion de « *unambiguous* » déjà présente dans la Directive mais traduite cette fois, non plus par « indubitable », mais sans doute plus justement par « univoque ». Pour le traitement de données sensibles, un consentement explicite est, par contre, encore requis.

L'article 7, § 1er, du RGPD qui est consacré aux conditions applicables au consentement apporte un élément qui compense d'une certaine manière l'abandon du qualificatif « explicite » au profit de « univoque » pour les données ordinaires. Il s'agit de l'obligation qui est faite au responsable du traitement d'être en mesure de démontrer que la personne concernée a donné son consentement au traitement de ses données. La fourniture d'une telle preuve est, en effet, essentiellement envisageable en présence d'un consentement explicite.

42. Le RGPD ajoute par ailleurs que le consentement doit se matérialiser par une déclaration ou par un acte positif clair[167], rendant évident que la personne concernée accepte le traitement en question de ses

165 *Ibid.*
166 *Ibid.*
167 Art. 4, 11°, du RGPD.

données[168], « par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale »[169]. Le consentement peut également se manifester par la détermination de certains paramètres techniques de sites Web ou par le fait de cocher une case sur une page Internet[170]. Il peut aussi être donné par l'acceptation de termes et conditions, à condition que le consentement à ce traitement spécifique de données à caractère personnel soit clairement distinct des autres dispositions du document[171]. La demande de consentement dans ce cas doit être présentée sous une forme compréhensible, exprimée dans un langage clair avec des termes simples[172], « en évitant les termes techniques ou les formulations alambiquées qui génèrent de l'ambiguïté »[173]. La déclaration de consentement ne peut en outre contenir aucune clause abusive ni aucune clause contraire ou non conforme au RGPD, sous peine pour une telle clause d'être non contraignante[174].

A l'inverse, le consentement ne peut découler du silence, de l'inactivité de l'individu ou encore de cases pré-cochées[175]. On ne peut pas non plus inférer un consentement du simple fait de poursuivre la visite normale d'un site Web[176].

Cette précision dans le texte provient de la volonté de protéger les individus contre les consentements douteux, mais elle s'inscrit aussi dans la ligne de la nouvelle philosophie du RGPD. En effet, le principe d'*accountability* qui sous-tend le règlement[177] requiert que le responsable du traitement soit en mesure de démontrer qu'il a bel et bien recueilli le consentement de la personne dont il traite des données. Dès lors, en pratique, il faudra veiller à se ménager la preuve qu'un tel consentement a

---

[168] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 15.

[169] Considérant n° 32 du RGPD

[170] Considérant n° 32 du RGPD.

[171] Art. 7, § 2, du RGPD.

[172] *Ibid.*

[173] B. Docquir, « Consentement et intérêt légitime dans le secteur privé », in *Data protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk*, *op. cit.*, p. 33.

[174] Art. 7, § 2, *in fine*, et considérant n° 42 du RGPD. Le considérant n° 42 fait référence à la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs (*J.O.*, L 95 du 21 avril 1993, p. 29). Un exemple d'une telle clause est celle autorisant le co-contractant professionnel à modifier unilatéralement et sans raison valable les termes du contrat ou les caractéristiques du produit ou du service.

[175] Considérant n° 32 du RGPD.

[176] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 17.

[177] Voy. *supra*, pt 33.

bien été obtenu[178], en conservant par exemple les formulaires de collecte des données, ou des notes prises par l'opérateur en cas de consentement verbal lors d'un appel téléphonique[179].

43. Enfin, on signalera encore que si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, « cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé »[180].

§ 2. Validité des consentements obtenus avant l'entrée en application du RGPD

44. Qu'en est-il des consentements obtenus avant que le RGPD soit d'application ? Doivent-ils être donnés à nouveau ? La réponse à cette question dépend d'une évaluation au cas par cas. En effet, un considérant du RGPD indique que « lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement (…) »[181]. En pratique, il faut donc examiner si le consentement obtenu à l'époque a été donné par un acte positif clair, pour des finalités spécifiques et vérifier si le responsable du traitement est à même d'en rapporter la preuve[182]. Dans l'hypothèse inverse, un nouveau consentement doit être demandé aux individus dont les données sont traitées[183]. Au vu des coûts qu'une telle démarche peut engendrer et des informations additionnelles que le RGPD enjoint de transmettre aux individus dont les données sont traitées, il serait sans doute judicieux de profiter de la transmission de ces nouvelles informations pour obtenir systématiquement un nouveau consentement conforme aux exigences du RGPD.

---

[178] Art. 7, § 1er, du RGPD. Voy. égal. la précision apportée par le Groupe 29 sur la nécessité de pouvoir prouver que le consentement a été donné librement : « *In any event, the burden of proof in Article 7(4) is on the controller. This specific rule reflects the general principle of accountability which runs throughout the GDPR* » (Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 9).

[179] B. Docquir, « Consentement et intérêt légitime dans le secteur privé », *op. cit.*, pp. 31-32.

[180] Considérant n° 42 du RGPD.

[181] Considérant n° 171 du RGPD.

[182] Considérant n° 42 du RGPD.

[183] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, pp. 30-31.

§ 3. Retrait du consentement

45. Le règlement stipule que la personne dont les données sont traitées doit pouvoir à tout moment retirer son consentement aussi simplement qu'elle l'a donné[184]. Cela doit pouvoir se faire sans frais[185]. La facilité avec laquelle l'individu peut retirer son consentement depuis que le RGPD est applicable fait peser un risque important sur le responsable du traitement : celui de se retrouver du jour au lendemain sans fondement légal légitimant à l'avenir son traitement de données à caractère personnel. Précisons que la licéité du traitement fondé sur le consentement avant que celui-ci ne soit retiré ne se verra pas compromise[186]. Toutefois, l'article 17 du RGPD prévoit au profit de la personne concernée un droit à l'effacement des données la concernant lorsqu'elle retire son consentement et lorsqu'il n'existe pas d'autre fondement juridique au traitement[187]. En conséquence, le responsable du traitement, lorsqu'il traite des données sur la base du consentement, est susceptible non seulement de se retrouver inopinément sans fondement légal pour traiter ces données, mais de devoir également les effacer.

Le Groupe de l'article 29 a précisé qu'il n'était pas question, en cas de retrait du consentement, de migrer silencieusement vers une autre base légale permettant de traiter les données. Tout changement de base légale doit être notifié à la personne concernée conformément aux exigences découlant du principe de transparence (art. 13 et 14 du RGPD)[188].

§ 4. Le consentement des mineurs

46. Le règlement entend protéger davantage les mineurs dont les données à caractère personnel font l'objet d'un traitement. En effet, ceux-ci sont en général moins conscients des risques liés au traitement de leurs données à caractère personnel, ou des conséquences que ces traitements

---

184 Art. 7, § 3, du règlement. Cela ne veut pas nécessairement dire que le retrait de consentement doit se faire absolument par la même voie que l'obtention de celui-ci (Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 21).

185 Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 21.

186 Art. 7, § 3, du RGPD.

187 Art. 17, § 1er, b), du RGPD. Un autre fondement justifiant la poursuite du traitement malgré le retrait du consentement pourrait être une obligation légale de conservation des données (Commission européenne, « Reform of EU data protection rules. What if somebody withdraws their consent ? », https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent-en).

188 Groupe 29, Guidelines on consent under Regulation 2016/679, précité, pp. 22-23.

peuvent avoir pour eux et n'ont pas une bonne connaissance de leurs droits en la matière[189]. Or, ils ont recours de plus en plus tôt à toutes les possibilités qu'offre Internet. Par exemple, les écoles encouragent et optent de plus en plus pour l'utilisation de sites Web à des fins éducatives. De plus, l'âge auquel les enfants commencent à utiliser Internet, et avec lui ses réseaux sociaux, ne cesse de diminuer[190]. Au vu des risques significatifs que comportent ces traitements et afin de formaliser dans un texte les mesures protectrices pour les mineurs, un article spécifiquement dédié au consentement des enfants a été inséré dans le RGPD[191]. Cette disposition accorde donc une protection spécifique aux enfants[192] en raison de leur vulnérabilité et en fonction de leur degré de maturité, conformément à ce que préconisait le Groupe de l'article 29[193]. Cette protection spécifique s'ajoute aux éventuelles règles nationales issues du droit des contrats, notamment les règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant[194].

47. Dans le cadre de l'offre de services de la société de l'information, si le responsable du traitement envisage de traiter des données à caractère personnel se rapportant à un mineur sur la base de son consentement, il doit veiller à ce que celui-ci soit âgé de minimum 16 ans pour que le traitement soit licite.

Cela signifie que les responsables de traitement offrant des services de la société de l'information à des enfants, engendrant des traitements des données de ces derniers, doivent mettre en œuvre des moyens raisonnables pour vérifier que l'utilisateur de leur service a bien l'âge du « digital consent »[195]. Ces moyens devraient être proportionnés au risque lié aux activités de traitement des données en question[196].

48. Si l'enfant n'a pas encore atteint l'âge de 16 ans, le consentement devra être donné ou autorisé par le titulaire de la responsabilité parentale[197].

---

189 Considérant n° 38 du RGPD.

190 A ce sujet, voy. égal. K. Rosier, « Les réseaux sociaux et les jeunes : la Commission européenne exhorte à une protection renforcée de leur vie privée », *BSJ*, 2011, n° 460, www.lebulletin.be.

191 Art. 8 du RGPD.

192 Considérant n° 38 du RGPD.

193 Groupe 29, Avis 2/2009 sur la protection des données à caractère personnel de l'enfant, 11 février 2009, WP 160.

194 Art. 8, § 3, du RGPD.

195 Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 25.

196 *Ibid.*

197 Art. 8, § 1er, al. 1, du RGPD. Le considérant n° 38 précise toutefois que le consentement du titulaire de la responsabilité parentale n'est pas nécessaire dans le cadre de services

Dans ce cas, le responsable du traitement sera tenu de vérifier, dans la limite du raisonnable et en tenant compte des moyens technologiques disponibles, que la personne qui consent est bien titulaire de la responsabilité parentale à l'égard de l'enfant[198]. Dans des situations présentant un faible niveau de risque, la vérification de la responsabilité parentale par la voie d'un email peut être suffisante[199]. A l'inverse, en cas de risque élevé lié au traitement, la preuve de la responsabilité parentale devra se faire par une voie plus fiable, par exemple en demandant au parent d'effectuer un paiement de 0,01 € par transaction bancaire en indiquant en communication qu'il est titulaire de l'autorité parentale sur l'enfant en question[200]. Il faut donc désormais développer des processus permettant de s'assurer de la qualité de la personne qui va accorder le consentement au nom de l'enfant. A cette fin, l'exemple américain du *Children's Online Privacy Protection Act* (COPPA) pourrait inspirer les États membres de l'Union[201]. Ce texte fournit notamment des indications intéressantes sur les différentes méthodes qu'il est possible d'utiliser pour obtenir le consentement des parents de l'enfant[202].

49. Les États membres ont néanmoins la faculté d'abaisser l'âge à partir duquel le traitement des données d'un mineur peut être effectué licitement sans le consentement de son représentant légal[203]. Cette limite d'âge ne peut toutefois être inférieure à 13 ans[204]. Cette latitude étant offerte au niveau national, il se peut que, sur ce point, on retrouve une hétérogénéité qu'on avait voulu éviter en optant pour un règlement plutôt qu'une directive[205]. Les responsables offrant aux mineurs des services de la société de l'information transfrontières doivent vérifier l'état de la législation nationale (son contenu et son critère d'application territoriale)

---

de prévention ou de conseil proposés directement à un enfant. C'est le cas par exemple des services de protection de l'enfance et de la jeunesse offerts en ligne aux enfants au moyen d'un service de « *chat* » (Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 27).

198 Art. 8, § 1er, al. 3, du RGPD.

199 Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 26.

200 Exemple proposé par le Groupe 29, Lignes directrices relatives au consentement, précitées, p. 26, note 66.

201 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

202 À ce sujet, voy. Children's Online Privacy Protection Act, § 312.5.

203 Art. 8, § 1er, du RGPD.

204 Art. 8, § 1er, al. 2, du RGPD.

205 La loi française du 20 juin 2018 a opté pour l'âge de 15 ans, tandis que la loi belge du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a opté pour l'âge de 13 ans.

dans chaque pays de l'UE dans lequel ils offrent leur service, en vue de s'y conformer le cas échéant.

50. La portée de ce régime particulier réservé aux mineurs repose sur la notion de « service de la société de l'information ». L'article 4, 25°, du RGPD renvoie à la notion de service définie à l'article 1er, § 1, b), de la directive 2015/1535/UE[206] qui entend par là « tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ». La jurisprudence de la Cour de Justice a apporté quelques éclairages, précisant notamment que la notion couvre l'offre en ligne et la conclusion de contrats par voie électronique[207].

Ces services de la société de l'information doivent être offerts directement aux enfants pour entrer dans le champ de l'article 8 du RGPD. Ce n'est donc pas le cas si le service est clairement dirigé exclusivement vers les adultes de plus de 18 ans.

51. Enfin, les consentements donnés par les titulaires de l'autorité parentale peuvent être confirmés ou retirés une fois que la personne concernée a atteint l'âge du *digital consent*[208]. En cas d'inaction une fois passé cet âge, le consentement donné par le titulaire de l'autorité parentale à la place de la personne concernée demeure un fondement valide pour continuer de traiter les données à caractère personnel. Si par contre, la personne concernée retire le consentement précédemment donné en son nom, le traitement perd cette base légale et ne peut être poursuivi s'il n'y a pas d'autre fondement au traitement[209].

---

[206] Directive 2015/1535/UE du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.*, L 241 du 17 septembre 2015, p. 1.

[207] C.J.U.E., 2 décembre 2010, arrêt *Ker-Optika*, C-108/09, §§ 22 et 28.

[208] Groupe 29, Guidelines on consent under Regulation 2016/679, précité, p. 27.

[209] Si la poursuite du traitement s'appuie sur un autre fondement, il convient d'en informer la personne concernée qui pourrait légitimement croire qu'en retirant son consentement ses données seront effacées (obligation d'information prévue à l'art. 14, § 1er, c), du RGPD).

SECTION 3. – Le contrat

52. Dans sa liste des hypothèses de licéité des traitements de données, le RGPD reprend le cas où le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles. Le traitement de données à caractère personnel peut en effet être effectué lorsque le traitement s'avère « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci »[210].

Le cadre contractuel peut ainsi légitimement servir de fondement aux traitements de données à caractère personnel. Les contrats de travail, les contrats d'ouverture de compte ou d'octroi de crédit signés avec une banque, ceux passés avec une compagnie d'assurance, un site de vente à distance ou un voyagiste, par exemple, sont autant de cadres justifiant de nombreux traitements de données à caractère personnel.

> « Entrent clairement dans cette hypothèse les traitements effectués dans le cadre de la relation liant l'avocat à son client. Cela couvre même les hypothèses de remplacement de l'avocat aux audiences, dès lors que ces remplacements permettent une bonne exécution du contrat. Notons cependant que cette hypothèse n'autorise pas à traiter des données relatives à des individus qui ne sont pas eux-mêmes clients de l'avocat. On ne peut dès lors s'appuyer sur ce fondement pour recueillir des informations sur la partie adverse »[211].

53. Il faut toutefois répondre à deux conditions pour que ce fondement soit valablement invoqué.

§ 1. Condition de participation au contrat

54. Il faut tout d'abord que la personne concernée soit partie au contrat en question ou qu'elle ait demandé que soient prises des mesures précontractuelles nécessitant un traitement de données. Le contrat ne peut donc impliquer des données à caractère personnel concernant une personne

---

[210] Art. 6, § 1er, b), du RGPD.

[211] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », in *Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, pp. 159-160. Pour les traitements de données relatives à des personnes physiques autres que le client de l'avocat, d'autres bases légales peuvent être invoquées : la balance d'intérêt, la mission d'intérêt public ou l'obligation légale (*ibid.*, pp. 160-161).

qui n'y est pas partie. Si cela arrive, un autre fondement doit couvrir le traitement de telles données.

§ 2. Condition de nécessité du traitement

55. La deuxième condition consiste en ce que le traitement des données soit véritablement *nécessaire* à l'exécution du contrat en question ou des mesures précontractuelles. Cette condition de nécessité se retrouve formulée également dans les quatre autres bases légales des traitements, évoquées dans les points qui suivent ci-dessous. La Cour de justice a spécifié que « eu égard à l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres, la notion de nécessité [...] ne saurait avoir un contenu variable en fonction des États membres. Partant, il s'agit d'une notion autonome du droit communautaire qui doit recevoir une interprétation de nature à répondre pleinement à l'objet de cette directive tel que défini à l'article 1er, paragraphe 1, de celle-ci »[212]. Le Groupe de l'article 29 a aussi fait référence à la jurisprudence de la Cour européenne des droits de l'homme pour cerner l'exigence de nécessité[213]. Ainsi, sans atteindre le niveau d'« indispensable » l'adjectif nécessaire « n'a pas la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" »[214].

A titre d'exemple, la mise en place de caméras de surveillance dans les différentes zones d'une banque ne peut être jugée nécessaire à l'exécution des contrats liant la banque à ses clients. De même, la promotion par une agence de voyages des city-trips qu'elle organise auprès de ses clients ayant réservé par ses soins un week-end à Barcelone ne peut être considérée comme nécessaire à l'exécution du contrat de voyage relatif à Barcelone. Ces opérations ne sont pas illégales pour autant, mais, pour être admissibles, elles doivent s'appuyer sur un autre fondement légitime que l'exécution du contrat (la balance d'intérêts – voy. *infra* – dans le cas de la banque et le consentement dans le cas de l'agence de voyages).

[212] C.J.U.E., 16 décembre 2008, arrêt *Heinz Huber*, C-524/06, pt 52.

[213] Groupe 29, Avis 06/2014 du 9 avril 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, WP 217.

[214] Cour eur. D.H., 25 mars 1983, *Silver et autres c. Royaume-Uni*, § 97.

SECTION 4. – La sauvegarde d'un intérêt vital

56. Le RGPD reste aussi dans la ligne de la Directive en autorisant les traitements nécessaires[215] pour sauvegarder des intérêts vitaux de la personne concernée[216]. Il ajoute la précision qu'il peut s'agir également des intérêts vitaux d'une autre personne physique. D'après le considérant n° 46, on ne peut s'appuyer sur cette base légale et invoquer l'intérêt vital d'autrui que si le traitement ne peut manifestement pas être fondé sur une autre base juridique (issue de la liste de l'article 6, § 1er).

Cette base de licéité couvre l'hypothèse évidente où une personne accidentée nécessite des soins induisant de traiter ses données relatives, par exemple, à son groupe sanguin. Or, si elle a perdu connaissance, elle ne peut manifester son consentement. Ce sera donc en se fondant sur cette base de licéité que le traitement pourra avoir lieu. Le considérant n° 46 offre un autre exemple de situation où le traitement de données est justifié par la sauvegarde d'intérêts vitaux : lorsque le traitement est nécessaire à des fins humanitaires, notamment pour suivre la propagation d'épidémies ou dans le cas de catastrophes naturelles.

SECTION 5. – L'obligation légale ou la mission d'intérêt public ou relevant de l'exercice de l'autorité publique

§ 1. L'obligation légale

57. Aux termes de l'article 6, § 1er, c), du RGPD, identiques à ceux de l'article 7, e), de la Directive, le traitement peut aussi être considéré comme licite lorsqu'il « est nécessaire[217] au respect d'une obligation légale à laquelle le responsable du traitement est soumis ».

De nombreux traitements du secteur public entrent dans cette hypothèse de licéité. Le principe de légalité qui gouverne l'administration impose effectivement que les missions confiées aux entités du secteur public aient une base légale[218]. C'est sur une telle base de licéité que s'effectuent la tenue des registres de population, la publication des répertoires

[215] Voy. ce qui est dit *supra* au pt 55 sur la portée du terme « nécessaire ».
[216] Art. 6, § 1er, d), du RGPD.
[217] Voy. ce qui est dit *supra* au pt 55 sur la portée du terme « nécessaire ».
[218] Voy. en Belgique l'article 105 de la Constitution ; E. Degrave et Y. Poullet, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *J.T.*, 2008,

d'entreprises (la Banque carrefour des entreprises[219], en Belgique ; le Registre national du commerce et des sociétés (RNCS)[220], en France ; le Registre de commerce et des sociétés[221], au Luxembourg ; …), certaines communications de données entre administrations, etc.

Mais de nombreux traitements effectués hors du secteur public sur la base d'une obligation légale trouveront également ici leur base de licéité. Ainsi, les collectes et enregistrements de certaines données sur les employés par l'employeur afin de les communiquer à l'administration en charge de la sécurité sociale sont imposés par la législation. Le secteur bancaire et financier est aussi soumis à de nombreuses obligations légales qui justifient les traitements effectués. Ces obligations visent notamment à lutter contre le blanchiment d'argent et le financement du terrorisme en instaurant une obligation de vigilance à l'égard des clients[222], qui se traduit par le fameux KYC (« *know your customer* »), ou visent à garantir l'adéquation du produit ou service financier proposé à la situation et au profil du client (directive « MiFID » : *Markets in Financial Instruments Directive* – directive concernant les marchés d'instruments financiers[223]) et impliquent dès lors la récolte d'une série d'informations sur chaque client.

§ 2. La mission d'intérêt public ou relevant de l'exercice de l'autorité publique

58. D'une manière très proche de l'hypothèse précédente, l'article 6, § 1er, e), prévoit que sont licites les traitements nécessaires[224] « à l'exécu-

p. 280. Pour d'amples développements sur le principe de légalité et son implication en termes de protection des données à caractère personnel, voy. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014.

[219] https://kbopub.economie.fgov.be/kbopub/zoeknummerform.html?lang=fr.

[220] Accessible à travers le site Internet Infogreffe, https://www.infogreffe.fr/.

[221] Accessible à travers le site Internet du Luxembourg Business Registers, https://www.lbr.lu/mjrcs-lbr/jsp/IndexActionNotSecured.action?time=1527255600871&loop=2.

[222] Voy. en Belgique la loi du 18 janvier 2010 modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et le Code des sociétés.

[223] Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers (MiFID), modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil, *J.O.*, L 145 du 30 avril 2004, pp. 1-44 ; transposée en droit belge par la loi du 22 mars 2006 relative à l'intermédiation en services bancaires et en services d'investissement et à la distribution d'instruments, et par les articles 162 à 181 de la loi-programme du 27 avril 2007 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

[224] Voy. ce qui est dit *supra* au pt 55 sur la portée du terme « nécessaire ».

tion d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». Les traitements entrant dans cette hypothèse ne sont pas visés explicitement par une disposition légale comme dans l'hypothèse précédente mais concourent à la réalisation d'une mission d'intérêt public ou à l'exercice de l'autorité publique.

On relèvera d'emblée une restriction apparue entre le texte de la Directive et celui du RGPD. La Directive admettait les traitements de données nécessaires à l'exécution d'une mission d'intérêt public dont est investi non seulement le responsable du traitement mais aussi un tiers auquel les données sont communiquées. Le règlement n'a pas repris cette hypothèse du tiers chargé d'une mission publique. Il faudra donc que ce tiers soit lui-même un responsable du traitement pour avoir désormais accès ou recevoir des données nécessaires à l'exécution de sa mission.

À titre d'illustration d'hypothèses s'appuyant sur cette base de licéité, l'enregistrement et la gestion des abonnés par les sociétés publiques de transports en commun se justifient pleinement au nom de l'exécution d'une mission d'intérêt public[225]. Le traitement des données des écoliers et des étudiants par les établissements scolaires et universitaires pour gérer leur parcours académique s'appuie également sur cette base[226], hors les traitements prévus spécifiquement par des textes légaux en la matière.

---

[225] Par contre, la mise en œuvre des cartes MoBIB dans le réseau de métro bruxellois n'a pas été sans susciter des problèmes de traitement illégitime de données à caractère personnel. En effet, en quoi une carte de tickets de voyage (et non pas un abonnement) nécessite-t-elle de comporter un identifiant personnel ? Sur cette question voy. F. DUMORTIER, A. ROUVROY, F. STANDAERT et F. KOEUNE, « Carte MoBIB : un bon exemple de mauvaise mise en œuvre », *Bruxelles en mouvements*, n° 240, 10 septembre 2010, pp. 9 et s., égal. disponible à l'adresse http://www.crid.be/pdf/crid5978-/6557.pdf. Pour une réflexion parallèle en France, voy. CNIL, « Délibération n° 03-008 du 27 février 2003 portant avis sur un traitement de la régie autonome des transports parisiens ayant pour finalité l'exploitation des données de validation des passes NAVIGO », 27 février 2003, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653732 et « Délibération n° 2004-100 du 09 décembre 2004 portant autorisation de la mise en œuvre par la SNCF d'un traitement automatise de données à caractère personnel relatif à la gestion des données de validation des passes "Navigo" chargés d'un abonnement annuel, mensuel ou hebdomadaire », 9 décembre 2004, https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653201.

[226] L'exécution de la mission d'enseignement ne couvre pas nécessairement tous les traitements réalisés par les établissements. Ainsi, la diffusion de photos sur le site de l'école n'est pas « nécessaire » à la mission et devra s'appuyer sur une autre base de licéité, le consentement des enfants voire de leurs parents en l'occurrence.

§ 3. Dispositions spécifiques d'application des deux hypothèses de licéité

a) Autorisation de dispositions sectorielles ou spécifiques à côté du RGPD

59. Ces deux hypothèses de licéité des traitements étaient déjà présentes dans la Directive[227] et le RGPD précise expressément[228] que les États membres sont autorisés à maintenir les dispositions nationales sectorielles ou spécifiques qu'ils auraient été amenés à adopter sur cette base avant l'entrée en vigueur du règlement.

Les États membres peuvent à l'avenir également introduire de telles dispositions sectorielles plus spécifiques pour adapter l'application des règles du RGPD « dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal »[229]. Le règlement laisse donc une marge de manœuvre aux États membres pour préciser ses règles dans des domaines qui requièrent des dispositions plus précises[230]. Les auteurs du texte ont clarifié la portée de cette possible intervention sur le plan national, en spécifiant que les précisions apportées peuvent porter sur les conditions générales régissant la licéité du traitement par le responsable du traitement[231], sur la détermination du responsable du traitement (s'il doit notamment être une autorité publique ou une personne physique ou morale de droit public ou de droit privé)[232], sur le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal[233].

---

[227] Pour l'articulation entre ces hypothèses et les principes du droit administratif de légalité, spécialité et proportionnalité qui gouvernent l'action des entités publiques, voy. M.-H. Boulanger *et al.*, « La protection des données à caractère personnel en droit communautaire », *op. cit.*, pp. 147-148.

[228] Art. 6, § 2, du RGPD.

[229] Art. 6, § 2, du RGPD et considérant n° 10 : « À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite ».

[230] Considérant n° 10 du RGPD.

[231] Art. 6, § 3, du RGPD.

[232] Considérant n° 45 du RGPD.

[233] Art. 6, § 3, du RGPD.

Cela a fait dire à certains auteurs : « La possibilité laissée aux États d'adapter les règles applicables aux traitements imposés par une loi nationale est par contre plus problématique. Elle est significative de la volonté des États de conserver une part de leur souveraineté dès lors qu'il s'agit d'une relation entre l'État ou une de ses entités et le responsable du traitement/citoyen. Aussi compréhensible qu'elle soit, cette possibilité de continuer à réglementer un grand nombre de traitements sur une base spécifique et nationale ouvre une brèche importante dans l'acquis censé être apporté par le règlement : l'unification des règles au niveau européen »[234].

b) Qualité des dispositions légales

60. Les paragraphes 2 et 3 de l'article 6 apportent des précisions sur les conditions encadrant ces hypothèses de licéité des traitements. Ainsi, le fondement de ces traitements doit être défini par le droit de l'Union européenne ou par le droit d'un État membre qui doit répondre à un objectif d'intérêt public et être proportionné à l'objectif légitime poursuivi. Le considérant n° 41 précise que « [l]orsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné ».

Le même considérant précise également que cette base juridique ou cette mesure législative doit répondre aux exigences mises en lumière par la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne. Elle doit en conséquence être claire et précise et son application doit être prévisible pour les justiciables. Pour être prévisible, une norme doit être suffisamment détaillée pour qu'à sa lecture, on soit à même d'envisager les traitements de données qui auront lieu. Dans son arrêt *Rotaru*[235], la Cour européenne des droits de l'homme a énoncé les ingrédients qui devaient se trouver dans une telle norme pour répondre à la condition de prévisibilité, ingrédients repris et étoffés à l'article 6, § 3, du RGPD (voy. point a) *supra*).

Toutefois, « Le présent règlement ne requiert pas de disposition légale spécifique pour chaque traitement individuel. Une disposition légale peut suffire pour fonder plusieurs opérations de traitement basées sur une obligation légale à laquelle le responsable du traitement est soumis ou

[234] Th. Leonard et D. Chaumont, « GDPR.expert, Article 6 Licéité du traitement », 20 avril 2016, http://www.gdpr-expert.eu/difficultes-probables.html?id=6.

[235] Cour eur. D.H., 4 mai 2000, arrêt *Rotaru c. Roumanie* ; égal. Cour eur. D.H., 4 décembre 2015, arrêt *Roman Zakharov c. Russie*.

lorsque le traitement est nécessaire pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique »[236].

Les finalités des traitements en cause doivent être définies dans cette base juridique ou être liées à la mission d'intérêt public ou à l'exercice de l'autorité publique[237].

On notera qu'il ne s'agit pas d'admettre des situations où des données seraient traitées sur la base d'une norme étrangère à l'Union européenne[238].

SECTION 6. – Les intérêts légitimes du responsable du traitement ou d'un tiers

§ 1. La balance des intérêts

61. Le RGPD apporte quelques modifications à cette dernière hypothèse de licéité des traitements qui est celle de la balance des intérêts. Derrière ces modifications somme toute mineures se cachent d'intenses discussions qui se reflètent quelque peu dans la densité des considérants attachés à cette disposition.

Le traitement de données est donc admis s'il est nécessaire « aux fins des intérêts légitimes »[239] du responsable du traitement ou d'un tiers, « à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »[240].

Le règlement offre des exemples de cas où le traitement peut légitimement se fonder sur une hypothèse de balance d'intérêts. Ainsi, il cite les traitements à des fins de prévention de la fraude ou à des fins de prospection commerciale[241] ou ceux visant à garantir la sécurité du réseau et des informations[242].

---

[236] Considérant n° 45 du RGPD.

[237] Art. 6, § 3, al. 2, du RGPD.

[238] Ch. KUNER, « The European Commission's Proposed Data Protection Regulation : a Copernican Revolution in European Data Protection Law », *Privacy and Security Law Report*, 11 PVLR 06, 2 juin 2012.

[239] Le texte anglais du règlement est resté le même que celui de la Directive sur ce point mais la traduction française a, elle, varié. On est passé de la formulation « nécessaire à la réalisation des intérêts légitimes (…) » à une formulation moins heureuse « nécessaire aux fins des intérêts légitimes (…) ».

[240] Art. 6, § 1er, f), du règlement.

[241] Considérant n° 47.

[242] Considérant n° 49.

62. C'est au responsable du traitement qu'il revient dans un premier temps d'effectuer lui-même la mise en balance et, s'il estime que la mise en œuvre du traitement de données qu'il envisage sert un intérêt supérieur à celui de la personne concernée ainsi qu'aux droits et libertés de celle-ci, il conclura que son traitement est légitime.

La personne concernée pourra, quant à elle, contester le résultat de cette mise en balance et invoquer son droit d'opposition si elle estime que ses intérêts, droits et libertés prévalent sur l'intérêt poursuivi par le responsable.

En dernier ressort, si les deux intervenants ne se mettent pas d'accord à la suite d'une opposition manifestée par la personne concernée, ils pourront s'adresser à l'autorité de contrôle ou au tribunal pour trancher sur les intérêts prévalant dans la situation en litige.

§ 2. Pas de listes préétablies

63. Le Parlement européen, fort dérangé par le flou attaché à cette hypothèse et l'insécurité juridique qui en découle inévitablement, a tenté de procéder à l'avance à la mise en balance des intérêts contradictoires en présence afin de déboucher sur une liste des traitements d'office autorisés et une liste de ceux *a priori* illicites[243]. Cette idée de listes a cependant soulevé de nombreuses critiques tenant à des problèmes de délimitation des traitements à classer d'un côté ou de l'autre, et à l'inévitable situation où l'on n'a pu tout prévoir et où une liste fermée bloque donc ce qui n'y figure pas. Le Parlement s'est donc ravisé et est revenu à une formulation générique de la mise en balance des intérêts contradictoires en présence.

§ 3. Balance d'intérêts et attente raisonnable de la personne concernée

64. Le considérant n° 47 apporte une précision qui provient également des discussions ayant eu lieu au Parlement mais qui n'est pas sans susciter la perplexité. Il indique que lorsque l'on met en balance les intérêts légitimes d'un responsable du traitement ou d'un tiers avec les intérêts ou les libertés et droits fondamentaux de la personne concernée, il faut

[243] Art. 6, § 1, b) et c), de la proposition de texte du Comité LIBE du Parlement européen (Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data [General Data Protection Regulation) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)], 17 décembre 2012, Rapporteur J. Ph. ALBRECHT).

tenir compte des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Le texte spécifie : « En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur ».

Faire intervenir le critère de l'attente raisonnable des personnes concernées est plutôt pertinent pour évaluer si une opération effectuée sur les données est bien compatible avec la finalité initiale[244]. Et le fait que le considérant évoque *in fine* l'hypothèse d'un traitement ultérieur appuie cette impression que les auteurs du considérant confondent la balance des intérêts avec l'évaluation de la compatibilité des utilisations ultérieures des données au regard de la finalité initiale.

Cette balance ne revient pas à mettre en jeu le fait que la personne concernée s'attend ou non au traitement effectué sur ses données. Des traitements de données peuvent s'avérer légitimes sur la base de la balance d'intérêts sans que la personne concernée ne s'attende nécessairement à ce que ses données fassent l'objet d'un traitement. C'est le cas par exemple d'un traitement de données effectué par un journaliste dans le cadre d'une enquête qu'il mène à l'égard d'un acteur politique. Ce dernier ne s'attend vraisemblablement pas à ce que des données soient rassemblées sur lui et pourtant l'intérêt de la liberté de la presse justifiera pleinement le traitement de données. De même, la collecte de données auprès de tiers à des fins de marketing direct échappe le plus souvent aux personnes concernées alors que de tels traitements sont reconnus comme légitimes. C'est le devoir d'information qui pèse sur le responsable[245] qui viendra éclairer les personnes concernées sur le sort réservé à leurs données.

§ 4. La personne concernée est un enfant

65. L'attention apportée à la fin de la disposition aux enfants (« notamment lorsque la personne concernée est un enfant ») ne doit être là sans doute que pour inviter à tenir compte, lors de la mise en balance, de

244 Voy. *supra*.

245 Voy. sur ce point la contribution de Thomas TOMBAL dans le présent ouvrage.

l'éventuelle qualité d'enfant de la personne concernée, car cette portion de phrase n'induit rien de véritablement concret. Aucun écho de cette attention particulière ne se retrouve par ailleurs dans les considérants.

§ 5. Base légale exclue pour les traitements des autorités publiques

66. Enfin, on signalera que les auteurs du RGPD ont expressément exclu de cette hypothèse de licéité les traitements effectués par les autorités publiques dans l'exécution de leurs missions[246]. Pour ces traitements, l'exigence de légalité impose au législateur de prévoir par la loi la base juridique justifiant le traitement des données à caractère personnel par les autorités publiques[247].

[246] Art. 6, § 1er, al. 2, du règlement.
[247] Considérant n° 47.