Travail de fin d'études: "Comment les entreprises traduisent-elles les obligations légales contenues dans le Règlement (UE) 2016/679 relatif à la protection des données en obligations de compliance? Analyse comparative entre PME et grandes structures"

Auteur : Sikivie, Charlotte
Promoteur(s) : Van Cleynenbreugel, Pieter
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en gestion
Année académique : 2019-2020
URI/URL : http://hdl.handle.net/2268.2/10008

LIÈGE université
Droit, Science Politique & Criminologie

HEC Liège
Ecole de Gestion de l'Université de Liège

Comment les entreprises traduisent-elles les obligations légales contenues dans le Règlement (UE) 2016/679 relatif à la protection des données en obligations de *compliance* ? Analyse comparative entre PME et grandes structures.

Charlotte SIKIVIE

Jury

Promoteur :

Monsieur Pieter VAN CLEYNENBREUGEL, professeur à l'ULiège

Lecteurs :

Monsieur Axel GAUTIER, professeur à l'ULiège

Monsieur Nicolas HAMBLENNE, Senior Associate chez PwC Legal Luxembourg

Année académique 2019-2020

Mémoire présenté en vue de l'obtention du diplôme de Master en droit, à finalité spécialisée en gestion

RESUME

A l'heure où les évolutions technologiques ne font que croître, protéger les données personnelles par le biais d'une réglementation détaillée devenait inévitable. Ainsi, en mai 2018, un nouveau règlement européen relatif à la protection des données personnelles, dit « R.G.P.D. » est entré en vigueur. Toute organisation traitant des données personnelles, établie sur le territoire de l'Union européenne ou dont l'activité cible des citoyens européens, est concernée.

Le R.G.P.D., réglementation complexe, lourde de conséquences, et contenant une centaine d'articles, s'applique aux entreprises privées comme aux organisations publiques, aux entreprises dont le cœur de métier est le traitement de données personnelles comme à celles qui en traitent très peu, et enfin, aux grandes entreprises comme aux PME.

Les grands groupes disposent, selon nous, des moyens nécessaires pour surmonter les difficultés posées par le règlement et s'y conformer. Pour les PME, c'est une autre affaire. Elles sont dorénavant soumises à un tas d'obligations et de principes nécessitant du temps, de l'argent, du personnel, et des compétences et connaissances dans des secteurs particuliers comme le droit, la vie privée ou l'informatique.

Deux ans après l'entrée en vigueur du règlement, nous nous interrogeons sur la manière dont les PME et les grandes structures l'ont mis en œuvre et comment certaines dispositions telles la minimisation des données, la transparence ou encore le consentement sont appliquées. Nous nous demandons également si ces organismes ont rencontré des difficultés, si les difficultés sont spécifiques à la taille, et comment elles ont été abordées. Plus précisément, nous nous interrogeons sur les solutions que mettent en place les PME et les grandes structures afin d'appliquer le R.G.P.D. de manière optimale.

ABSTRACT

At a time when technological developments keep increasing, protecting personal data through detailed regulation was becoming inevitable. That is why, in May 2018, a new European Regulation about data protection, also known as « G.D.P.R. », came into force. Any organization processing personal data, established on the European Union territory or whose activities affect European citizens, is concerned.

The G.D.P.R., a complex and significant regulation containing about one hundred legal provisions, applies to private companies as well as public organizations, to companies whose core business is personal data as well as those that process very little of it, and finally, to large organizations as well as SMEs.

In our opinion, large groups have the necessary means to overcome the difficulties generated by G.D.P.R. and to comply with it. For SMEs, it is a different matter. They are now subject to a whole bunch of obligations and principles that require time, money, staff, but also skills and knowledge in particular areas such as law, privacy and I.T.

Two years after the entry into force of this regulation, we wonder how SMEs and large companies have implemented it and how certain provisions such as data minimization, transparency and consent are applied. We also wonder whether these organizations have encountered difficulties, whether those difficulties are specific to size, and how they have been addressed. More specifically, we would like to find out about solutions that have been put in place by SMEs and large organizations in order to apply G.D.P.R. in the best possible way.

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce travail.

Je remercie, tout d'abord, mon promoteur, le professeur Pieter van Cleynenbreugel pour avoir suscité mon intérêt dans le domaine du droit européen ainsi que pour m'avoir orientée et conseillée pour l'élaboration de ce travail. Je remercie également mes lecteurs, messieurs Axel Gautier et Nicolas Hamblenne pour l'intérêt porté à mon travail et le temps qu'ils y ont accordé.

Ensuite, je remercie les différents intervenants qui ont accepté de répondre à mes questions, malgré les circonstances économiques. Rien de cela n'aurait été possible sans leur bon vouloir.

Enfin, je remercie ma famille et mes amis, pour leur soutien moral au quotidien durant mon cursus universitaire. Je remercie particulièrement mon père pour ses encouragements ainsi que ma grand-mère pour ses longues relectures sur un sujet ne la passionnant pourtant guère.

TABLE DES MATIERES

INTRODUCTION…….....1

METHODOLOGIE……..5

1. Choix de la question de recherche …….....5
2. Méthode de recherche utilisée ……5
3. Limites…….....7

ANALYSE THEORIQUE DU R.G.P.D…….....9

A) CADRE JURIDIQUE EUROPEEN DE LA PROTECTION DES DONNEES PERSONNELLES 9
1. Charte et Traités…….....9
2. La directive 95/46/CE…….....9
3. Le règlement 2016/679 (R.G.P.D.) …….....9
B) DEFINITIONS ET CHAMP D'APPLICATION……..10
1. Définitions…….....10
1.1. Définition d'une donnée personnelle……..10
1.2. Définition d'un traitement……...11
1.3. Définition d'une donnée sensible……....11
1.4. Définition du responsable du traitement…….....12
1.5. Définition du sous-traitant……..13
2. Champ d'application……...14
2.1. Champ d'application matériel…….....14
2.2. Champ d'application territorial……...14
C) DISPOSITIONS-CLES……...14
1. Principes……....15
1.1. Principe de minimisation des données……15
1.2. Principe de transparence……16
1.3. Principe de responsabilité ou principe *d'accountability*……18
2. Obligations du responsable du traitement……20
2.1. Consentement libre, spécifique, éclairé et univoque……..20
2.2. Capacité à démontrer l'accord de la personne concernée……...24
2.3. Retrait du consentement……24
2.4. Principe de *privacy by design*……24
3. Outils à la conformité……..25
3.1. Changements organisationnels et techniques……..25
3.1.1. Désignation d'un délégué à la protection des données……25
3.1.2. Registre des activités de traitement……28
3.1.3. Analyse d'impact à la protection des données……..29
3.2. Code de conduite et certification……30
3.2.1. Code de conduite……31
3.2.2. Certification……32
D) BARRIERES A L'IMPLEMENTATION DU R.G.P.D……..32
1. Manque de sensibilisation et de compréhension……..32
2. Ressources financières……...33
3. Penser la gestion des ressources humaines……..33

ANALYSE CRITIQUE DE LA MISE EN PLACE ET DE L'APPLICATION DU R.G.P.D……**35**

A) DIFFICULTES PRATIQUES……..35

1. Contrainte budgétaire……..35

1.1. Externalisation des compétences……..35

1.2. Nouveautés technologiques……..37

1.3. Sensibilisation du management……38

2. Contrainte d'accès à l'information……..38

3. Contrainte liée aux ressources humaines……39

3.1. Sensibilisation, formation, information……40

3.2. Internalisation des compétences……...42

3.3. Formalisation……....43

B) APPLICATION DES DISPOSITIONS LEGALES……..45

1. Notions de responsable du traitement et de sous-traitant……..45

2. Principe de minimisation des données……46

3. Principe de transparence……..47

4. Principe de responsabilité……49

4.1. Délégué à la protection des données……49

4.2. Registre des activités de traitement……...51

4.3. Analyse d'impact à la protection des données……..52

5. Consentement……53

6. Principe de *privacy by design*……...54

7. Code de conduite et certification……..55

CONCLUSION……....56

ANNEXE……..59

BIBLIOGRAPHIE……..60

INTRODUCTION

Depuis les années 1940, la société est bouleversée par une révolution technologique, marquée par l'apparition des premiers ordinateurs[1]. Depuis lors, la place du digital dans la société ne fait que croître. On parle d'une véritable « vie sur écran » à partir des années 1990[2].

La directive 95/46/CE[3] est venue concrétiser cette révolution du numérique et incarne la première réglementation de la protection des données personnelles au niveau européen. La situation en 1995 n'est cependant en rien comparable à celle d'aujourd'hui. En effet, à l'heure actuelle, notre quotidien est affecté, d'une manière ou d'une autre, par l'évolution des technologies de l'information et de la communication[4]. Cette évolution spectaculaire peut se traduire par un progrès des libertés fondamentales : les réseaux sociaux, par exemple, encouragent plus que jamais la liberté d'expression. Cependant, d'autres libertés tout aussi, si pas plus importantes sont hautement menacées : nous pensons notamment au droit à la vie privée. Avoir la pleine maîtrise de ses données personnelles est devenu illusoire.

L'essor des nouvelles technologies occasionne un grand nombre de défis en termes de protection des données[5]. La directive de 1995 est devenue obsolète, et l'absence d'un cadre juridique adapté a mené à nombre d'abus, notamment par les géants du numérique (Google, Amazon, Facebook etc.)[6]. La protection des données personnelles est par conséquent devenue un enjeu de taille, qui a récemment fait couler beaucoup d'encre (Cambridge Analytica, Panama Papers, Google Spain, etc.).

Quoi qu'il en soit, adapter nos règles de droit et encadrer strictement les données à caractère personnel devenait inévitable[7]. L'Europe, avant-gardiste en la matière, qui s'est depuis longtemps montrée garante de la protection de la vie privée et des données à caractère personnel[8], s'est attelée à cette tâche.

Après des années de négociation, le Parlement européen et le Conseil adoptèrent, en 2016, le texte qui constitue aujourd'hui le texte de référence en matière de protection des données au niveau de l'Union européenne : le règlement général sur la protection des données[9] (ci-après,

---

1 S. VIAL, *L'être et l'écran. Comment le numérique change la perception*, Paris, Presses Universitaires de France, 2013, p. 19.

2 S. VIAL, *ibidem.*, p. 19.

3 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, 23 novembre 1995.

4 C. GIAKOUMOPOULOS, G. BUTTARELLI et M. O'FLAHERTY, *Manuel de droit européen en matière de protection des données.* Conseil de l'Europe, 2018, p3.

5 V. REDING, « Tomorrow's Privacy. The upcoming data protection reform for the European Union », *International Data Privacy Law*, Vol. 1, n°1, 2011, p. 3.

6 F. DEHOUSSE, « L'enfer bureaucratique du Règlement sur les données personnelles », *Le Vif*, n°3, 2019, p. 66.

7 G. DESGENS-PASANAU, « Avant-propos », G. DESGENS-PASANAU, *La protection des données personnelles : le RGPD et la nouvelle loi française*, 3e éd., Paris, LexisNexis, 2018, p. XIII.

8 C. GIAKOUMOPOULOS, G. BUTTARELLI et M. O'FLAHERTY, *op. cit*, p. 3.

9 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

R.G.P.D.). Il a pour objectif de renforcer la protection des données et de responsabiliser les entreprises dans la gestion des données personnelles. Avec ce règlement, toute une série d'obligations s'imposent désormais aux entreprises : principe de responsabilité accru, délégué à la protection des données, analyses d'impact, sanctions administratives, consentement de la personne concernée… Il est entré en vigueur le 24 mai 2016 mais a été rendu applicable bien plus tard, le 25 mai 2018, afin de laisser le temps aux responsables de s'adapter et de mettre tout en place pour se conformer à cette nouvelle réglementation.

Ce règlement est, selon nous, loin de résoudre tous les problèmes liés au développement des nouvelles technologies. Il semble en effet que, vu la complexité de la situation et la vitesse à laquelle les modèles économiques et les usages se transforment, il soit bien difficile de définir un cadre juridique efficace[10]. C'est probablement pour cette raison que le règlement se veut abstrait, laissant une grande marge de manœuvre aux organisations, qui devront s'assurer en permanence que leurs pratiques sont bel et bien conformes au règlement[11]. A ce propos, le Groupe de travail 29 rappelle qu'« il est fréquent que les principes et obligations à respecter dans l'Union européenne en matière de protection des données ne se traduisent pas suffisamment par des mesures et pratiques internes concrètes »[12]. Si le R.G.P.D. suppose certaines mesures spécifiques, la priorité est toutefois de créer un « cadre de compliance »[13] approprié pour assurer la protection des données personnelles et faire en sorte que les traitements de données respectent le R.G.P.D.[14].

L'objet de ce travail consiste à analyser comment précisément ces pratiques sont mises en œuvre sur le terrain. Nous étudierons quelques principes généraux, obligations légales et changements qu'impose le R.G.P.D, et nous nous intéresserons à la manière dont chacune de ces dispositions est appliquée en pratique. Si ces dispositions semblent plutôt limpides à première vue, nous verrons que s'y conformer n'est pas sans poser de difficultés. Par ailleurs, le R.G.P.D. fixe nombre d'objectifs à atteindre sans prescrire de règles bien déterminées, au point qu'il soit possible de considérer qu'il y a « autant de parcours pour se mettre en conformité que de responsables du traitement »[15]. L'implémentation du R.G.P.D. est donc spécifique à chaque organisation et doit être adaptée en fonction de la complexité de la structure et des facteurs de risque[16].

---

ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016.

10 T. SAMMAN et M. DREVON, « De la réglementation à la compliance, encadrer et accompagner la transformation numérique », *Les défis du numérique*, D. Rahmouni-Syed Gaffar (dir.), Bruxelles, Bruylant, 2019, p. 107.

11 B. VAN ASBROECK, et J. DEBUSSCHE, « Les obligations de « compliance » des entreprises », *Vers un droit européen de la protection des données*, B. Docquir (dir.), Bruxelles, Larcier, 2017, p. 91.

12 Groupe de l'article 29, « Avis n°3/2010 sur le principe de la responsabilité », WP 173, p. 2.

13 Traduit de l'anglais *(« compliance framework »).*

14 IT GOVERNANCE (ORGANIZATION). PRIVACY TEAM., *EU General Data Protection Regulation (GDPR) : an implementation and compliance guide,* Ely, IT Governance Publishing, s.d, 2017, pp .23, 24.

15 S. PARSA, « Le R.G.P.D. et la profession d'avocat, au-delà du secret professionnel et du principe de confidentialité », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020, p. 163.

16 MDC. FREITAS and M. MIRA DA SILVA, « GDPR Compliance in SMEs: There is much to be done », *Journal of Information Systems Engineering & Management*, vol. 3, issue 4, 30, 2018, p. 2.

Il existe heureusement certains outils ou mécanismes pour aider les entreprises à transformer les obligations légales engendrées par le règlement en obligations de *compliance*, nous pensons notamment au délégué à la protection des données ou aux mécanismes de certification. Les considérants du texte, les lignes directrices du Groupe de travail 29 et la jurisprudence sont également d'une aide précieuse.

La *compliance*[17] est le fait pour les parties prenantes de déterminer des moyens afin de rencontrer les objectifs fixés par la loi (au sens large)[18]. « Ce qui lui importe est moins de savoir si les entreprises enfreignent les règles qui s'appliquent à elles que de savoir si elles mettent en œuvre, en leur sein, un dispositif efficace pour prévenir le risque d'infraction à ces règles »[19].Le but principal du R.G.P.D. n'est effectivement pas seulement de créer un outil de contrôle quant à l'application de certaines règles concernant la protection des données personnelles mais aussi et surtout de pouvoir conscientiser et imposer l'importance de la protection des données personnelles au sein des organisations.

La mise en conformité au R.G.P.D. s'avère couteuse, que ce soit en termes de budget, d'efforts, ou de ressources (technologiques et humaines). En outre, l'approche est fonction du type de données traitées, de la fréquence à laquelle les données sont recueillies, du type de responsable du traitement (personne publique ou privée), mais aussi de la taille de l'entreprise (ou du groupe)[20].

Ce règlement s'appliquant aussi bien aux grandes structures qu'aux petites et moyennes entreprises (PME), nous nous interrogeons sur la capacité, en particulier pour les PME de se conformer à une telle réglementation, si vague et si lourde de conséquences.

Le règlement requiert que la situation particulière de ces entreprises soit prise en compte[21], mais elles restent soumises à la majeure partie des obligations entraînées par le règlement. Nous pensons qu'il peut être judicieux de comparer la façon dont les PME et les grandes structures mettent en œuvre et appliquent ce règlement, comme le suggèrent C.Tikkinen-Piri, A. Rohunen, et J. Markkula : *« To understand how companies are adapting to changes in legislation, implementing its new requirements and addressing related challenges, future empirical studies should be conducted among personal data intensive companies. It is also crucial to investigate the GDPR implementation in companies of different sizes to find out how the implementation is carried out and how the challenges are addressed, for example, in the SME context. Through empirical research of this kind, the means for implementing the changes and the appropriate concrete solutions can be followed and analysed, along with how field-specific data usage and management practices are formulated in companies »*[22].

---

17 Le vocable anglais est plus répandu que sa traduction française (« conformité ») dans le monde du droit et des affaires.

18 T. SAMMAN et M. DREVON, *op. cit.*, p. 107.

19 A. GAUDEMET, « Qu'est-ce que la compliance ? », *Commentaire*, vol. 165, 2019/1, p. 109.

20 S. CHATRY, « Les données collectées par l'entreprise : documenter sa conformité au RGPD », *L'entreprise face aux défis du numérique*, J.-M. Moulin, S. Chatry et A. Riera (dir.), Paris, Mare & Martin, 2018, p. 118.

21 Considérant 13 R.G.P.D.

22 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, « EU General Data Protection Regulation: Changes and implications for personal data collecting companies », *Computer Law & Security Review*, 2017, p. 18.

Il y a, par ailleurs, très peu d'études concernant les pratiques et problèmes de compliance relatifs au R.G.P.D. C'est encore plus vrai pour les PME qui représentent pourtant la majorité des organisations de l'Union européenne[23].

Pour tenter de répondre à la question qui nous occupe, c'est-à-dire comment les grandes structures ainsi que les PME traduisent les obligations légales du R.G.P.D. en obligations de *compliance*, nous avons choisi d'utiliser une démarche hypothético-déductive. Ainsi, l'objet de ce travail consiste en un approfondissement théorique permettant l'émission d'hypothèses que l'analyse empirique tentera de confirmer ou d'infirmer.

L'organisation de ce travail se présente comme suit. Nous commencerons tout d'abord par poser la base méthodologique suivie. Nous dédierons ensuite une partie de cet écrit à une analyse théorique ciblée du R.G.P.D. Nous définirons quelques concepts fondamentaux et préciserons son champ d'application. Ensuite, nous tenterons d'éclaircir certaines dispositions-clés, telles que quelques principes généraux introduits par le R.G.P.D. et diverses obligations mises à charge des entreprises ainsi que certains outils à la conformité. Nous exposerons également quelques barrières que les entreprises sont susceptibles de rencontrer lors de l'implémentation du règlement. Nous clôturerons ainsi la première partie de ce travail. Dans une seconde partie intitulée « analyse critique de la mise en place et de l'application du R.G.P.D. », nous interrogerons certains acteurs-clés et tenterons de voir comment ces derniers s'y prennent pour se conformer à la nouvelle réglementation : quelles difficultés ont-ils rencontrées ? Existe-t-il des zones grises ? Comment les abordent-ils ? Comment les évitent-ils ? Quelle(s) stratégie(s) utilisent-ils ? Les prescrits qu'ils ont mis en place vérifient-ils bel et bien les prescrits du règlement ? Il nous semble en effet, à première vue, que le R.G.P.D. laisse derrière lui certaines lacunes qu'il va falloir identifier et combler. Grâce aux données extraites du terrain, nous tenterons de répondre aux hypothèses, notamment en opérant une comparaison non seulement entre les données théoriques et les données empiriques mais aussi entre les résultats observés dans les PME et ceux dans les grandes structures. En guise de conclusion, nous tenterons de répondre à la question de recherche.

---

[23] Z. SHI LI *et al.*, « GDPR Compliance in the Context of Continuous Integration », *IEEE Transactions on software engineering*, 2018, p. 1.

METHODOLOGIE

Cette section est dédiée au détail de la méthodologie utilisée pour mener cette étude. Nous expliquerons le choix de notre question de recherche et présenterons les hypothèses qui y sont liées. Ensuite, nous ferons part de la méthode de recherche utilisée. Nous terminerons cette section en exposant les limites de notre recherche.

1. Choix de la question de recherche

Le chercheur doit, pour structurer son étude de manière cohérente, choisir un fil conducteur[24]. Une fois celui-ci déterminé, la question de recherche a été adaptée jusqu'à remplir les trois critères nécessaires à une bonne question de départ à savoir, selon Quivy et Van Campenhoudt, la clarté, la faisabilité et la pertinence[25].

La question de recherche s'est précisée et concrétisée au fur et à mesure de la lecture d'ouvrages scientifiques. Ces sources théoriques nous ont permis d'affiner la recherche mais également de découvrir si le sujet avait déjà été abordé antérieurement. Nous en avons profité pour nous inspirer des suggestions faites par différents auteurs. Les premières lectures et quelques discussions avec des professionnels nous ont permis d'établir une première hypothèse : le R.G.P.D. pose des difficultés pratiques, que ce soit dans sa mise en place ou dans son application.

Alors que nous pensions analyser la manière dont les entreprises en général traduisent les obligations légales du R.G.P.D. en obligations de *compliance*, nous avons décidé, au vu des difficultés propres aux PME et des propositions faites par certains chercheurs, de préciser notre question de recherche en opérant une comparaison entre PME et grandes structures. Notre deuxième hypothèse est ainsi celle-ci : les PME, faute de moyens, éprouvent davantage de difficultés pour se conformer aux obligations du R.G.P.D. que les grandes structures.

2. Méthode de recherche utilisée

Nous avons choisi d'utiliser, pour ce travail, la méthode qualitative. Par méthode qualitative, nous entendons « la recherche qui implique un contact personnel avec les sujets de la recherche, principalement par le biais d'entretiens et par l'observation des pratiques dans les milieux mêmes où évoluent les acteurs »[26]. La recherche est qualitative, notamment, lorsque « les instruments et méthodes utilisés sont conçus, d'une part, pour recueillir des données qualitatives (témoignages, notes de terrain, images vidéo, etc.), d'autre part, pour analyser ces données de manière qualitative (c'est-à-dire en extraire le sens plutôt que les transformer en pourcentages ou en statistiques) ».

---

24 L. VAN CAMPENHOUDT et R. QUIVY, *Manuel de recherche en sciences sociales*, Paris, Dunod, 2011, p. 40

25 L. VAN CAMPENHOUDT et R. QUIVY, *ibidem*, p. 43.

26 P. PAILLÉ et A. MUCCHIELLI, *L'analyse qualitative en sciences humaines et sociales*, Paris, Armand Colin, 2012, p. 13.

Pour récolter les données, nous avons choisi la méthode de l'entretien semi-dirigé, c'est-à-dire celui où le chercheur pose des questions ouvertes, préparées au préalable, afin d'orienter la discussion vers le sujet de recherche[27]. C'est la méthode la plus appropriée lorsque l'on souhaite étudier un domaine spécifique, sonder des hypothèses et laisser l'interlocuteur s'exprimer librement sur un sujet défini par le chercheur[28].

Dès lors, nous avons rédigé, en fonction de l'exploration de la littérature scientifique, un guide d'entretien[29] plutôt souple et nous avons tenté de cibler les questions dans le but de tester les deux hypothèses.

Les entreprises et organismes interviewés sont au nombre de quatorze : sept PME et sept grandes structures. Leurs caractéristiques sont diverses : nous nous sommes entretenus avec tous types de profils. Tout d'abord, nos interlocuteurs viennent tant du secteur public que du secteur privé. Ce critère ne nous a, en effet, pas paru pertinent dans le cadre de cette étude ; seul le critère de la taille du groupe faisant l'objet de notre recherche et le R.G.P.D. s'appliquant de la même façon, à peu de choses près, aux organisations publiques et privées. En outre, si la majorité des structures interviewées sont belges, certaines ont leur siège ailleurs dans l'Union européenne. Encore une fois, cette distinction est, à nos yeux, sans importance car toutes les entreprises situées sur le territoire de l'Union sont soumises au règlement.

Nous avons donc sélectionné quatorze groupes de taille différente et les avons rangés dans une des deux catégories : PME ou grande structure.

Par « petites et moyennes entreprises », nous entendons, conformément à la recommandation 2003/361/CE de la Commission, les entreprises qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros[30]. Les structures ne remplissant pas ces critères sont dès lors considérées comme « grandes ».

Certains entretiens ont été réalisés dans les lieux de travail des intervenants, mais la plupart se sont déroulés via des moyens multimédias, mesures sanitaires obligent. La durée des entretiens variait entre trente et quarante-cinq minutes.

---

27 R. SAUVAYRE, *Les méthodes de l'entretien en sciences sociales*, Paris, Dunod, 2013, p. 9.

28 R. SAUVAYRE, *ibidem*, p. 9.

29 Voy. Annexe

30 Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, annexe, art. 2, *J.O.C.E.*, L 124, 20 mai 2003.

Code	Nom	Taille	Date
I.1	Smals	Grande structure	02/07/2020
I.2	Citadelle	Grande structure	19/06/2020
I.3	Administration générale de l'enseignement de la Fédération Wallonie-Bruxelles	Grande structure	27/05/2020
I.4	Le Bon Coin	Grande structure	06/06/2020
I.5	Province de Liège	Grande structure	18/05/2020
I.6	ULiège	Grande structure	13/07/2020
I.7	Ortec Finance	Grande structure	18/06/2020
I.8	Wep	PME	16/06/2020
I.9	Sips	PME	03/07/2020
I.10	List Minute	PME	06/06/2020
I.11	Sauvons Maya	PME	18/06/2020
I.12	Heetch	PME	16/06/2020
I.13	Festiv@Liege/LesArdentes	PME	25/05/2020
I.14	Traiteur Les cours	PME	10/07/2020

3. Limites

Le temps est venu d'avertir le lecteur des limites de ce travail.

La première concerne la taille de l'échantillon. Si les quatorze entretiens nous ont permis, nous semble-t-il, de repérer les tendances générales, il est évident que ce nombre reste réduit et que les constats tirés sont à relativiser.

Ensuite, les critères de sélection des entretiens, que ce soit au niveau de la taille du groupe, du *core business*, ou de la dimension publique ou privée, tendent à être larges afin d'établir un

constat général. Par conséquent, la diversité des interviewés fait en sorte que chacun est peu représentatif.

La troisième limite concerne les choix théoriques. Parmi les nombreuses dispositions fondamentales introduites par le R.G.P.D., nous avons dû nous limiter à quelques-unes d'entre elles seulement. Nous justifierons nos choix le moment venu.

Enfin, au fur et à mesure des entretiens, certaines questions ont été adaptées ou revues en fonction des réponses obtenues. Partant, l'ensemble des interviewés n'a pas été confronté de façon exacte au même questionnaire.

ANALYSE THÉORIQUE DU R.G.P.D.

Cette première partie est dédiée à une analyse ciblée du nouveau règlement européen. Dans un premier temps, nous décrirons brièvement le cadre juridique européen de la protection des données personnelles qui nous amènera directement au R.G.P.D. Dans un second temps, nous définirons quelques notions fondamentales, et présenterons certains principes et obligations mises à charge des responsables du traitement. Nous évoquerons également les outils à la conformité. Enfin, nous dresserons une liste des potentielles barrières à l'application du R.G.P.D.

A) CADRE JURIDIQUE EUROPÉEN DE LA PROTECTION DES DONNÉES PERSONNELLES

1. Charte et Traités

Dans le droit de l'Union européenne, il n'y avait, à l'origine, pas de réel droit à la protection des données à caractère personnel. En 1995, ce droit est réglementé pour la première fois par la directive 95/46/CE, mais c'est en 2000, avec l'adoption de la Charte des droits fondamentaux de l'Union européenne, que le droit à la protection des données est finalement reconnu en tant que droit fondamental[31]. Ce droit trouve sa source à l'article 8 §1 de la Charte mais également à l'article 16 §1 du TFUE.

2. La Directive 95/46/CE

En 1990, la Commission européenne présente un premier projet afin de réglementer la protection des données à caractère personnel, qui mène en 1995 à l'adoption de la Directive 95/46/CE du Parlement européen et du Conseil 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[32]. Cette directive constituait, jusqu'à l'adoption du règlement général sur la protection des données en 2016, le texte de référence en matière de protection des données à caractère personnel[33].

3. Le règlement 2016/679 (R.G.P.D.)

Entré en vigueur le 24 mai 2016, le R.G.P.D (règlement général sur la protection des données) succède à la directive européenne 95/46/CE. La directive avait été adoptée au temps où à peine un pourcent de la population mondiale utilisait internet[34]. Le champ d'application de la directive

---

31 C. GIAKOUMOPOULOS, G. BUTTARELLI et M. O'FLAHERTY, *op. cit.*, p. 20.

32 B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Cambridge, Intersentia, 2019, p. 261 à 263.

33 B. VAN ALSENOY, *ibidem*, p. 279.

34 C. TANKARD, « What the GDPR means for businesses », *Network Security, 2016*, p. 5.

était donc devenu trop limité. Avec la montée en puissance des nouvelles technologies, l'accès aux données personnelles est plus que jamais facilité.

Par ailleurs, la directive ne permettait de toucher que des entreprises situées dans l'Union européenne. Or, à l'heure de l'ère numérique et de la mondialisation, il arrivait fréquemment que des citoyens européens voyaient leurs données personnelles utilisées par des entités non soumises à la réglementation européenne.

La CJUE a tenté, par sa jurisprudence, de se mettre à niveau et de combler ces lacunes, mais il devenait nécessaire de redéfinir un cadre juridique adéquat, plus strict et adapté aux avancées technologiques[35]. A titre d'illustration, dans l'arrêt Google Spain[36], Google avait recueilli et divulgué des informations relatives à la faillite d'une personne physique, résident espagnol, sans son consentement. A priori, Google avait donc commis une violation de la protection des données personnelles. Cependant, Google (le responsable du traitement) étant établi aux Etats-Unis, la directive européenne était difficilement applicable. Par une pirouette, la Cour était tout de même parvenue à faire appliquer la directive, mais son raisonnement a été extrêmement critiqué. Un des objectifs visés par le R.G.P.D. est, par conséquent, d'englober tous les cas où un citoyen européen serait impliqué[37].

Par ailleurs, le règlement poursuit un objectif d'uniformisation, et non plus d'harmonisation comme le faisait la directive[38]. L'ancienne législation sur la protection des données donnait lieu à des interprétations fort différentes au sein de l'UE. En se dotant d'un règlement, qui est par définition directement applicable, l'UE préconise un modèle uniforme et cohérent de protection des données personnelles et tente d'éliminer les divergences entre les réglementations nationales de protection des données[39].

B) DEFINITIONS ET CHAMP D'APPLICATION

Avant d'aller plus loin dans la réflexion, il nous semble indispensable d'aborder ici quelques définitions, et de délimiter le champ d'application du règlement.

1. Définitions

1.1. Définition d'une donnée à caractère personnel

L'article 4 du R.G.P.D. définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable (dénommée « personne concernée ») »[40]. Cela peut être un identifiant, un nom, une photo, un numéro de sécurité sociale, un matricule interne, une plaque d'immatriculation, une adresse postale, une adresse e-mail, un

---

35 C. TANKARD, *ibidem*, p. 5.

36 C.J., arrêt *Google Spain SL et Google Inc contre AEPD et Mario Costeja Gonzalez,* 13 mai 2014, C-131/12, ECLI:EU:C:2014:317.

37 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 5.

38 S. CHATRY, *op. cit.*, p. 111.

39 R. GOLA, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, vol. 59, no. 2, 2017, p. 30.

40 Article 4, § 1 R.G.P.D.

numéro de téléphone, des données de localisation, un identifiant en ligne, un enregistrement vocal…Cela peut viser également des données qui sont indirectement susceptibles de cibler une personne (âge, sexe, ville, diplôme…)[41]. En bref, s'il s'avère possible de relier telle information à telle personne, l'information en question est qualifiée de donnée à caractère personnel[42].

Ce type de données, qui peuvent sembler anodines à première vue, devront, comme nous le verrons, être traitées avec une extrême précaution.

La définition du concept de donnée à caractère personnel est formulée d'une manière particulièrement large, contrairement à celle qui était prévue dans la directive de 1995[43]. « C'est un choix délibéré du législateur qui se veut cohérent par rapport à d'autres textes de lois et de traités concernant la protection des données personnelles »[44]. D'ailleurs, la CJUE interprète la notion de « donnée à caractère personnel » très largement. Ainsi, dans un arrêt du 20 décembre 2017, la Cour de justice de l'Union européenne a par exemple considéré que les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses devaient être qualifiées de données à caractère personnel[45]. Selon la Cour, une information *concerne* une personne physique et est donc qualifiée de donnée à caractère personnel lorsque « en raison de son contenu, sa finalité ou son effet, l'information est liée à une personne déterminée »[46].

1.2. Définition de la notion de traitement de données

Le traitement de données est défini comme toute opération ou tout ensemble d'opérations appliquées à des données à caractère personnel[47]. Les opérations sont de toutes sortes, parmi elles : la collecte, la conservation, l'utilisation, la diffusion, la destruction… En somme, « tout ce qui peut être fait avec des données à caractère personnel »[48]. Pour être soumis au règlement, le traitement doit avoir été effectué à l'aide de procédés automatisés ou non automatisés[49].

La Cour d'appel de Liège a, par exemple, considéré que lorsqu'un gestionnaire de site internet enregistre et conserve les données relatives à un individu afin de lui envoyer des courriels non sollicités, il effectue un traitement de données[50].

1.3. Définition d'une donnée sensible

Attardons-nous un instant sur la notion de donnée sensible. L'article 9 du R.G.P.D. énumère une catégorie de données qui, en raison de leur nature, doivent être manipulées avec prudence.

---

41 Voir https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi

42 E. DEGRAVE (dir.), *L'ABC du RGPD : dictionnaire pratique à destination des administrations.* Namur, Union des villes et communes de Wallonie, 2018, p. 66.

43 C. PONSART et R. ROBERT, « Le règlement européen de la protection des données personnelles », *J.T.*, 2018/20, n°6732, p. 422.

44 A. FOCQUET et E. DECLERCK, *Gegevensbescherming in de praktijk,* Antwerpen, Intersentia, 2019, p. 5 et 6.

45 C.J., arrêt *Novak c. Data Protection Commissionner*, 20 décembre 2017, C-434/16, ECLI :EU :C :2017 :994, point 62.

46 C.J., arrêt *Novak c. Data Protection Commissionner*, 20 décembre 2017, C-434/16, ECLI :EU :C :2017 :994, point 35.

47 Art. 4, § 2 R.G.P.D.

48 C. TERWANGNE *et al*, *La protection des données à caractère personnel en Belgique. Manuel de base*, Bruxelles, Politeia, 2019, p. 17.

49 Art. 4, § 2 R.G.P.D.

50 Liège (7e ch.), 19 novembre 2009, *D.A.O.R.*, 2010/96, p. 453.

En effet, le traitement de ces données est a priori interdit, sous réserve d'exceptions[51]. Ces données sont : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique[52].

1.4. Définition du responsable du traitement

Le responsable du traitement, toujours selon l'article 4, est la personne (physique ou morale) qui, seul ou conjointement, détermine les finalités et les moyens du traitement[53]. C'est en principe celui qui sera tenu responsable sur la base du règlement en cas de violation de données personnelles[54].

Déterminer qui doit être qualifié de responsable du traitement poserait quelques difficultés pratiques. Pourtant, son identification est indispensable : en effet, c'est sur lui que reposent les principales obligations en matière de protection des données à caractère personnel[55]. Afin d'identifier le responsable du traitement, il faut prendre en compte divers critères et indices : « initiative du traitement et définition de la finalité/ des objectifs, influence de droit ou de fait sur le traitement et degré d'influence, autonomie et pouvoir décisionnaire (…) »[56].

La notion de « responsable du traitement » est une notion factuelle, et la Commission a déjà précisé qu'elle devait s'entendre largement[57]. Dans le célèbre arrêt Google Spain[58], la Cour avait considéré que l'exploitant du moteur de recherche (qui détermine les finalités et les moyens du traitement des données à caractère personnel) devait être considéré comme le responsable du traitement. En effet, « l'exploitant du moteur de recherche assume la responsabilité des conséquences que son activité a produite sur les personnes concernées, et, notamment, ses effets sur leur vie privée »[59].

Dans l'arrêt Wirtschaftsakademie Schlewig-Holsten[60], la Cour a conclu que l'administrateur d'une page fan sur Facebook, en offrant à Facebook Ireland la possibilité de placer des cookies sur l'ordinateur ou autre de la personne ayant visité sa page fan, devait être qualifié de responsable du traitement.

---

51 Article 9, §2 R.G.P.D.

52 Article 9, §1er R.G.P.D.

53 Art. 4, § 7 R.G.P.D.

54 Art.79 et s. R.G.P.D.

55 A. BEELEN, P. LAMBRECHT et F. DECHAMPS, *Guide pratique du RGPD : fiches de guidance,* Bruxelles, Bruylant, 2018, p. 33.

56 A. BEELEN, P. LAMBRECHT et F. DECHAMPS, *ibidem*, p. 33.

57 Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant », WP 169, p. 3.

58 C.J. (gde ch.), *Google Spain SL et Google Inc contre AEPD et Mario Costeja Gonzalez*, 13 mai 2014, C-131/12, ECLI:EU:C:2014:317, point 33.

59 M. POLIDORI, « L'arrêt *Google Spain* de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, 2015/1 n° 34, p. 247.

60 C.J. (gde ch.), *Unabhängiges Landeszentrum für Datenschutz SchleswigHolstein/Wirtschaftsakademie Schleswig-Holstein GmbH* , 5 juin 2018, C-210/16, ECLI:EU:C:2018:388, point 44.

Cette difficulté doit toutefois être relativisée car très souvent, le responsable du traitement correspond à l'employeur[61].

L'expression « seule ou conjointement » pose l'idée de « co-responsabilité »[62]. Lorsqu'il y a plusieurs responsables de traitement, ces derniers doivent déterminer de manière transparente leurs obligations respectives[63]. Cette précision vient complexifier davantage la matière, mais le R.G.P.D. y apporte un tempérament en prévoyant qu'en cas de difficulté, la personne concernée peut exercer ses droits contre le responsable du traitement de son choix[64].

1.5. Définition du sous-traitant

Par sous-traitant, il faut entendre celui qui « traite des données à caractère personnel pour le compte du responsable du traitement »[65]. Son existence dépend d'une décision du responsable du traitement qui peut faire le choix de « déléguer tout ou partie des activités de traitement à une organisation extérieure »[66]. Le responsable du traitement et le sous-traitant sont donc deux entités distinctes[67]. Alors que la directive de 1995 se concentrait principalement sur le responsable du traitement, le nouveau règlement européen met de nombreuses obligations à charge du sous-traitant. En effet, tout comme le responsable du traitement, le sous-traitant est soumis au principe *d'accountability*, principe que nous aborderons ultérieurement. Il peut faire l'objet de sanctions sévères ; il doit coopérer, sur demande, avec l'autorité de contrôle ; il doit, selon les cas, désigner un délégué à la protection des données (nous reviendrons également sur ce dernier point) et bien d'autres[68].

Il n'est pas toujours aisé de distinguer le responsable du traitement du sous-traitant. Pourtant, nous le rappelons, cette distinction est importante, en particulier pour la question de l'attribution des responsabilités[69].

Dans l'affaire SWIFT, qui concernait un transfert de données bancaires aux autorités américaines, il a été jugé que, malgré le fait que la société SWIFT s'était toujours présentée en tant que simple intermédiaire, elle ne pouvait être considérée comme sous-traitant. Il a en effet été démontré qu'elle était allée « au-delà de simples actions au nom de ses clients » et qu'elle avait endossé des responsabilités spécifiques, incompatibles avec celle d'un simple sous-traitant[70].

---

61 J. HICK et R. INVIJAJEV, *RGPD : quel impact sur la gestion du personnel ?* Waterloo, Kluwer, 2018, p. 7.

62 A. DELFORGE, *Les obligations générales du responsable du traitement et la place du sous-traitant*, Bruxelles, Larcier, 2018, p. 377.

63 Art.26, § 1 R.G.P.D.

64 Art. 26, § 3 R.G.P.D.

65 Art. 4, § 8 R.G.P.D.

66 Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant », WP 169, p. 1.

67 Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant », WP 169, p. 1.

68 B. VAN ASBROECK et J. DEBUSSCHE, *op. cit.*, p.113.

69 Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant », WP 169, p. 6.

70 Groupe de l'article 29, « Avis n°10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) », W 128, p. 9.

Il apparaît donc clairement que ce n'est pas moins la qualification donnée a priori aux entités qui déterminera le régime applicable, qu'une appréciation *de facto*. Un sous-traitant qui outrepasse son rôle sera requalifié en responsable de traitement[71].

2. Champ d'application

2.1. Champ d'application matériel

Conformément à l'article 2 du R.G.P.D., le règlement s'applique à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier[72].

Concrètement, cela signifie que les règles contenues dans le R.G.P.D. sont applicables, qu'il soit fait recours aux technologies de l'information et de la communication, ou pas (c'est-à-dire lorsque les traitements de données sont manuels)[73].

2.2. Champ d'application territorial

Aux termes de l'article 3 du R.G.P.D., le règlement « s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union »[74].

Ainsi que nous l'avons vu précédemment, un des points remarquables du R.G.P.D. est que son champ d'application est élargi par rapport à celui de la directive. Désormais, toute entreprise, même située hors de l'Union européenne, qui impacte une personne localisée dans l'Union, est soumise au nouveau règlement européen[75]. « *It is paramount to understand how the GDPR will change not only the European Data protection laws but nothing less that the whole world as we know it* »[76].

C) DISPOSITIONS-CLES

Le R.G.P.D instaure plusieurs principes fondamentaux, impose de nombreuses obligations aux organisations et entraîne certains changements aux niveaux organisationnels et techniques. Nous allons analyser certaines dispositions majeures que le règlement contient, et tenter de comprendre, en théorie, ce que ce dernier exige des entreprises ou organisations. Pour ce faire, nous nous aiderons notamment de recommandations ou de lignes directrices, le cas échéant, émises par le Groupe de Travail « Article 29 » (ci-après « G29 »), « acteur majeur de la

---

71 E. DEGRAVE (dir.), *op. cit.*, p. 116.

72 Art. 2, §1er R.G.P.D.

73 C. DE TERWANGNE, « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020, p. 17.

74 Art. 3 §1er R.G.P.D.

75 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 16.

76 J.P. ALBRECHT, « How the GDPR will change the world », *EDPL*, vol. 2, no. 3. 2016, p. 287.

protection des données au plan européen mais aussi mondial »[77]. Cet organe a été institué en 1996 par l'article 29 de la Directive 95/46/CE, et remplacé en 2018 par le Comité européen de la Protection des données, un organe européen indépendant chargé de garantir une interprétation précise du R.G.P.D.[78]. Notons qu'un des domaines que le R.G.P.D a bouleversé est celui des droits des personnes concernées (droit à l'oubli, droit d'accès, droit d'information, droit d'opposition…). L'objet de ce travail étant d'étudier le R.G.P.D. du point de vue des entreprises, nous avons préféré nous concentrer toutefois sur les obligations particulières mises à leur charge. Cette remarque est à nuancer, car il va de soi que les obligations des entreprises sont corrélées aux droits des individus.

1. Principes

Le R.G.P.D. énonce, en son article 5, plusieurs principes : la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité, la responsabilité.

Nous nous limiterons à deux d'entre eux, à savoir la minimisation des données et la transparence. Nous avons choisi d'étudier dans un premier temps ces deux principes car ils nous semblent essentiels. La transparence, par exemple, est un principe qui se manifeste tout au long du droit de l'Union[79].

Par ailleurs, ces deux principes diffèrent les uns des autres, et sont liés à d'autres principes, ce qui, selon nous, permettra de couvrir une partie assez importante de la matière. En effet, le principe de minimisation des données est intimement lié au principe de limitation des finalités : la « *véritable pierre angulaire de la protection des données* ». Ce principe exige que chaque traitement nécessite d'avoir une finalité déterminée, explicite et légitime, et que les données ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités[80]. Le principe de transparence, quant à lui, est relié au principe de loyauté[81], selon lequel « les personnes concernées doivent, en pleine connaissance de cause, pouvoir établir une relation de confiance avec ceux qui traitent leurs données à caractère personnel »[82].

Nous terminerons cette section par le principe de responsabilité qui pèse sur le responsable du traitement de démontrer le respect de ces principes. Il nous semble en effet inévitable de terminer par ce principe qui est en quelque sorte le prolongement logique des autres et qui est une des nouveautés du R.G.P.D.

1.1. Principe de minimisation des données

L'article 5 du R.G.P.D. vise le principe de minimisation des données, c'est-à-dire l'idée que les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est

---

77 S. NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *LEGICOM*, 2009/1, n° 42, p. 37.

78 Art. 68 et s. R.G.P.D.

79 Art. 1er TUE; art. 11, § 2 TUE; art. 15, § 3 TFUE.

80 Art. 5, § 1er, b), R.G.P.D. ; C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 22.

81 C. PONSART et R. ROBERT, *op. cit.*, p. 423.

82 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 34.

nécessaire au regard des finalités pour lesquelles elle sont traitées »[83]. Par « limitées à ce qui est nécessaire », le législateur vise à limiter la collecte de données tant en ce qui concerne la quantité qu'en ce qui concerne la qualité de celles-ci[84]. Ainsi, le but de cette disposition est que le responsable du traitement ne traite que les données essentielles au regard de la finalité poursuivie, et qu'il vérifie qu'un résultat identique ne peut être atteint grâce à des procédures alternatives sans traitement de données personnelles[85].

Nous allons à présent découvrir quelques exemples jurisprudentiels illustrant ce principe de minimisation des données.

Dans une décision du 17 septembre 2019, la chambre contentieuse de l'Autorité de Protection des Données a condamné un commerçant à une amende de 10.000 euros : la méthode utilisée pour la création de cartes de fidélité, en ce qu'elle nécessitait la lecture de la carte d'identité électronique, ne respectait pas le principe de minimisation des données énoncé à l'article 5, §1, c) du R.G.P.D. [86].

Par ailleurs, la chambre contentieuse a également jugé, le 2 avril 2019, que placer une caméra dans la cuisine commune d'un immeuble de chambres d'étudiants, bien que les exigences légales aient été remplies, était disproportionné et violait le principe de minimisation des données[87].

Il ressort de ce principe qu'il est important, avant tout traitement de données quel qu'il soit, que le consentement ait été obtenu ou pas, de procéder à une mise en balance des « intérêts, droits et libertés en jeu »[88].

1.2. Principe de transparence

Passons dès à présent au principe de transparence, énoncé à l'article 5, § 1er, a) R.G.P.D. Un traitement de données doit respecter, selon l'article 5, § 1er, les exigences de licéité, loyauté et transparence. Ce dernier principe vient s'ajouter à ce qui existait déjà dans la directive de 1995[89], c'est une des raisons pour lesquelles nous avons choisi d'expliciter ce principe de transparence particulièrement. Comme souligné ci-dessus, il est lié à l'exigence de loyauté qui « induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie »[90].

Ce principe est à nos yeux fondamental car il est favorable aussi bien pour les personnes concernées que pour les responsables du traitement. En effet, s'il est vrai que le R.G.P.D. représente pour beaucoup d'entreprises une contrainte, particulièrement en raison des

---

83 Article 5, § 1er, c) R.G.P.D.

84 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 23.

85 A. BEELEN, P. LAMBRECHT et F. DECHAMPS, *op. cit.*, p. 30 et 31.

86 A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO_fr.pdf.

87 A.P.D. (ch. contentieuse), décision 03/2019 du 2 avril 2019, https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG03-2019ANO_FR.pdf.

88 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 21.

89 Directive 95/46/CE, art. 6, § 1er, a).

90 C. TERWANGNE *et al*, *La protection des données…, op. cit.*, p. 34.

nombreuses obligations mises à leur charge[91], le principe de transparence peut être bénéfique à ces entreprises en ce qu'il redonne confiance aux citoyens[92]. « Plus qu'un ensemble de contraintes, les entreprises peuvent voir ce changement imposé comme un générateur de confiance, donc de croissance »[93]. Or la confiance est, aux yeux d'Isabelle Andoulsi, avocate au barreau de Bruxelles, « l'élément fondamental du règlement »[94].

La transparence n'est pas définie en tant que telle dans le R.G.P.D., mais le considérant 39 apporte des précisions sur la manière de comprendre ce principe. Il « exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples »[95]. « Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement »[96].

Le principe de transparence se manifeste de différentes manières. Il s'applique au fait de collecter, utiliser, consulter ou traiter les données à caractère personnel d'une personne physique ainsi qu'à la mesure dans laquelle ce traitement est effectué[97]. « *Het moet voor de betrokkenen perfect duidelijk zijn dat en hoe hun persoonsgegevens zullen worden verwerkt* »[98]. La transparence recouvre, selon les lignes directrices du G29, trois domaines : « 1) la communication aux personnes concernées d'informations relatives au traitement équitable de leurs données; 2) la façon dont les responsables du traitement communiquent avec les personnes concernées sur leurs droits au titre du R.G.P.D. et 3) la façon dont les responsables du traitement facilitent l'exercice par les personnes concernées de leurs droits »[99]. C'est un principe qui transparait également dans le droit d'accès de la personne concernée à ses données personnelles[100], que nous n'aurons pas l'occasion d'aborder dans le cadre de ce travail.

La transparence est primordiale, en interne comme en externe. En interne, elle passe par la sensibilisation du personnel au traitement des données au sein de l'entreprise. En externe, elle requiert d'informer clairement les personnes concernées au sujet du traitement de leurs données[101].

L'application pratique de ce principe ne va pas de soi. Certaines exigences pratiques spécifiques liées au principe de transparence sont listées aux articles 14 à 12 du R.G.P.D. On peut tout de

---

91 A titre d'exemples : l'obligation d'obtenir le consentement de la personne concernée (art. 6, § 1, a)), l'obligation de désigner un délégué à la protection des données (art. 37 R.G.P.D.), l'obligation de réaliser une analyse d'impact (art. 30 R.G.P.D.), l'obligation de tenir un registre des activités de traitement (art. 30 R.G.P.D.) …

92 R. GOLA, *op. cit.*, p. 29.

93 A. BEELEN, P. LAMBRECHT et F. DECHAMPS, *op. cit.*, p. 334.

94 I. ANDOULSI, « Le Règlement général sur la protection des données personnelles : un état des lieux après plus d'un an d'entrée en application », *Ann. dr.*, vol. 78, 2018/3, p. 471.

95 Art.15 R.G.P.D.

96 Art. 15 R.G.P.D.

97 Considérant 39 du R.G.P.D.

98 A. FOCQUET et E. DECLERCK, *op. cit.*, p. 82

99 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01, p .4.

100 Art. 15 R.G.P.D.

101 COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, « RGPD. Vade-mecum pour les PME » 2018, p. 5.

même s'interroger sur le sens à donner à ces dispositions. Heureusement, le G29 fournit, dans ses lignes directrices, une aide à l'interprétation quant à cette obligation de transparence en détaillant et illustrant presque chaque exigence[102]. Par exemple, pour l'obligation d'utiliser « des termes clairs et simples », il livre aux entreprises des exemples de mauvaises et de bonnes pratiques quant aux phrases à utiliser pour informer les personnes concernées des finalités et fondements juridiques du traitement de leurs données à caractère personnel.

Le G29 rapporte, dans ses lignes directrices, l'existence d'un conflit entre l'exigence d'utiliser des « termes clairs et simples » et celle de fournir des informations complètes [103]. Il appartient au responsable du traitement de hiérarchiser les informations à fournir en fonction de plusieurs critères (nature, circonstances, portée et contexte du traitement), des exigences légales et des lignes directrices du G29. Le G29 estime en effet opportun de catégoriser les différentes informations à fournir dans le but d'éviter que certaines informations soient noyées. Les détails de la finalité du traitement, l'identité du responsable du traitement et une description des droits des personnes concernées font partie, selon le G29, du premier niveau d'informations[104]. Il est recommandé que soient abordées en premier lieu les informations relatives aux activités de traitement susceptibles d'impacter le plus la personne concernée ainsi qu'à celles auxquelles elle s'attend le moins[105].

Penchons-nous à présent sur un exemple tiré de la jurisprudence qui nous éclairera davantage sur la notion de transparence (et sur la notion de consentement également, que nous analyserons dans la prochaine section). En 2018, Facebook a été condamné pour avoir suivi le comportement de navigation de non-utilisateurs en dehors du domaine du réseau social[106]. Certains internautes étaient en effet traqués par l'intermédiaire de « cookies » placés par Facebook, alors même qu'ils n'avaient pas de compte Facebook. Le Tribunal de première instance de Bruxelles a considéré que ces internautes n'étaient pas suffisamment informés quant à l'utilisation de leurs données personnelles, et qu'ils n'avaient pas la possibilité de marquer expressément leur consentement à cette pratique attentatoire à la vie privée. Facebook a été contraint, entre autres d'assurer une transparence totale s'agissant de l'utilisation de cookies[107].

1.3. Principe de responsabilité (ou principe d'accountability)

Le principe de transparence nous amène directement au principe de responsabilité. En effet, il appartient au responsable du traitement de prouver qu'il respecte les principes généraux du R.G.P.D., parmi eux, le principe de transparence[108]. Parallèlement, « le principe de responsabilité exige la transparence des opérations de traitement afin que les responsables du

---

102 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01.

103 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01, p. 2.

104 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01, p. 22.

105 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01, p. 22 et 23 ; A. FOCQUET et E. DECLERCK, *op. cit.*, p. 85.

106 M. TAEYMANS, « Facebook mag geen gegevens van-niet gebruikers verzamelen », *Juristenkrant*, 2020, p. 3.

107 Civ. néérl. Bruxelles (24e ch.), 16 février 2018, *R.A.G.B.* 2019/9, p. 698.

108 Art.5, § 2 R.G.P.D

traitement puissent démontrer qu'ils satisfont aux obligations leur incombant en vertu du R.G.P.D. »[109].

C'est une nouveauté du R.G.P.D. et c'est un des « changements les plus importants rencontrés à l'occasion de la réforme »[110]. La responsabilité du responsable du traitement, connue également sous le terme anglais *d'accountability* se traduit par le fait que ce dernier doit être constamment en mesure de prouver sa conformité au R.G.P.D[111]. Le responsable du traitement doit non seulement pouvoir démontrer qu'il a pris en compte les risques que peuvent engendrer les traitements de données dans la mise en œuvre des dispositions du règlement, mais aussi qu'il a pris les mesures adéquates pour que les droits et libertés des personnes concernées soient protégés[112], l'idée étant de le responsabiliser. Il y a un allègement de la charge de la preuve en faveur de la personne concernée, à qui il incombait, auparavant, de prouver la faute, le dommage et le lien causal[113].

La responsabilité du responsable du traitement est prévue à l'article 24 R.G.P.D. Ce dernier doit prendre des mesures appropriées (le R.G.P.D. parle de « mesures techniques et organisationnelles ») visant à assurer l'effectivité du règlement. Les mesures qu'il met en œuvre dépendent « de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques »[114]. Le R.G.P.D. impose toutefois au responsable du traitement la mise en œuvre de certains outils visant à l'aider dans sa mise en conformité. Parmi eux, la désignation d'un délégué à la protection des données, la tenue d'un registre des activités de traitement, et, dans certains cas, la réalisation d'une analyse d'impact[115]. L'application d'un code de conduite ou d'un mécanisme de certification peut également servir à démontrer le respect des dispositions du règlement[116]. Nous reviendrons ultérieurement sur ces notions.

« Les entreprises vont devoir agir et être en mesure de prouver, de tracer ce qui a été fait. Cela passera notamment par l'implémentation de documentations adaptées et de politiques de traitement des données écrites et contraignantes, ou encore de procédures de vérifications (régulièrement testées) pour s'assurer de l'effectivité et de l'efficacité des mesures mises en œuvre pour le respect des dispositions applicables »[117].

---

109 Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01, p. 5.

110 S. PARSA, « Le R.G.P.D. et la profession d'avocat… », *op. cit.*, p.133.

111 S. PARSA, « Le RGPD, dans la pratique – Entre principes généraux et obligation, que faire ? », *R.G.F.C.P.*, 2019/4, p. 31.

112 B. VAN ASBROECK et J. DEBUSSCHE, *op. cit.*, p. 105.

113 S. PARSA, « Le RGPD, dans la pratique… », *op. cit.*, p. 31.

114 Article 24, §1 R.G.P.D.

115 G. DESGENS-PASANAU, *La protection des données personnelles : le RGPD et la nouvelle loi française,* 3e éd., Paris, LexisNexis, 2018, p. 34.

116 Art. 24, § 3 R.G.P.D.

117 A. BEELEN, P. LAMBRECHT et F. DECHAMPS, *op. cit.*, p. 33.

2. Obligations du responsable de traitement

Dans cette section, nous nous attaquerons à l'obligation du consentement, considérée comme la base de tout le droit de la protection des données personnelles[118]. Le Parlement européen considère en effet le consentement comme « 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 »[119].

Un traitement de données, pour être licite, doit reposer sur un des six fondements juridiques offerts par le R.G.P.D. L'article 6 § 1er est ainsi libellé : « *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie: a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; b) le traitement est 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; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».*

Les principales bases de licéité invoquées par les PME sont, selon la Commission de la protection de la vie privée : le consentement, le contrat, le respect d'une obligation légale et l'intérêt légitime[120].

Notons que nous n'aborderons pas la question du consentement des mineurs. Nous évoquerons l'obligation qui pèse sur le responsable de traitement de pouvoir démontrer à tout moment que l'accord de la personne concernée a bel et bien été donné et qu'il est valide en regard de la loi. Nous terminerons par le retrait du consentement, auquel le R.G.P.D. accorde une place importante.

2.1. Consentement libre, spécifique, éclairé et univoque

Le responsable de traitement a l'obligation, dans certains cas, de recueillir le « consentement de la personne concernée à ce que ses informations fassent l'objet d'un traitement »[121], c'est la première hypothèse de licéité[122]. Le consentement doit, pour être valable, revêtir quatre

---

118 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.* n° 122-123, 2019 p. 4.

119 Comité LIBE du Parlement européen, 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, COM(2012)0011, C7-0025/2012, 2012/0011(COD), 21 novembre 2013, pp. 218-219.

120 COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, « RGPD. Vade-mecum pour les PME » 2018, p. 8.

121 G. DESGENS-PASANAU, *op. cit.*, p. 89.

122 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 26.

qualités : il doit être libre, spécifique, éclairé et univoque. Chacun de ces termes sera explicité ci-dessous.

Ce consentement, notion centrale dans le droit de la protection des données et suscitant bon nombre de commentaires, serait moins fréquemment requis que ce que l'on pourrait penser, et ce pour plusieurs raisons. Vu la dureté extrême des conditions de validité du consentement, comme nous aurons l'occasion de nous en rendre compte incessamment, il est courant que les entreprises choisissent de s'appuyer sur d'autres hypothèses de licéité, notamment sur l'article 6, §1, f) qui rend le traitement licite à condition qu'il soit nécessaire aux fins de réalisation d'intérêts légitimes[123]. Ensuite, selon un article d'Yves Poullet et un avis du G29[124], le responsable du traitement doit choisir le fondement juridique le plus approprié, le consentement devant être considéré comme une base subsidiaire, qui servirait uniquement pour « ce qui ne peut être justifié par les autres fondements »[125]. Enfin, le R.G.P.D. prévoit que la personne concernée peut retirer son consentement à tout moment[126], ce droit est abordé *infra* mais notons d'ores et déjà que cette possibilité fait du consentement une base juridique incertaine[127]. « Si la tentation pourrait être grande pour les responsables du traitement de privilégier le consentement, il pourrait aussi être tout autant avisé de lui préférer d'autres fondements plus sûrs si cela est possible »[128]. Il y a toutefois des cas où la loi exige purement et simplement l'existence d'un consentement, et malgré l'usage apparemment limité qui en est fait, il nous paraît indispensable de s'étendre sur cette notion, tant discutée.

Précisons que l'obtention d'un consentement ne dispense pas le responsable du traitement de l'obligation de proportionnalité[129] et donc d'effectuer une mise en balance des intérêts entre ceux du responsable du traitement d'un côté, et ceux de la personne concernée de l'autre[130]. Yves Poullet souligne en effet que « si les conditions de licéité constituent une condition nécessaire de la validité des traitements, elles ne sont pas suffisantes et exigent une analyse *in casu* du respect des principes de base de légitimité des traitements »[131].

Le consentement est défini à l'article 4, 11° : c'est « 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 »[132]. Les conditions applicables au consentement sont listées aux articles 7 et suivants, et la définition est détaillée par de nombreux considérants[133]. Le législateur européen a en effet dû s'attacher à préciser la notion pour faire face à la quantité de consentements de

---

123 G. DESGENS-PASANAU, *op. cit.*, p. 89.

124 Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187.

125 Y. POULLET, *op. cit.*, p. 17.

126 Art. 7, §3 R.G.P.D.

127 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, p. 306.

128 O. TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, p. 130.

129 Cf. Principe de minimisation des données.

130 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 42.

131 Y. POULLET, *op. cit.*, p. 18.

132 Art. 4, § 11 R.G.P.D.

133 Considérants 32, 33, 42, 43 et 44 du R.G.P.D.

mauvaise qualité faisant office de base juridique pour les traitements de données[134]. Chaque terme de la définition est, de surcroît, longuement explicité dans les lignes directrices et avis du G29[135]. Passons dès maintenant certains de ces qualificatifs en revue (« libre », « spécifique », « éclairé » et « univoque »).

Tout d'abord, le consentement doit être libre, autrement dit, selon le G29, il doit être issu d'un choix réel de la personne concernée, elle ne doit avoir subi aucune contrainte. Le consentement ne sera pas considéré comme libre si, en ne consentant pas au traitement de ses données, la personne concernée s'expose à des conséquences négatives[136]. Elle doit pouvoir refuser ou retirer son consentement sans subir de répercussion[137]. Nous reviendrons sur le retrait du consentement en fin de section, mais concernant le refus de la personne concernée, précisons d'ores et déjà que le consentement ne peut être qualifié de libre s'il est « présenté comme une partie non négociable des conditions générales »[138]. Cette condition est illustrée dans une décision de l'Autorité de protection des données que nous avons déjà mentionnée, relative à l'utilisation d'une carte d'identité comme carte de fidélité[139]. Dans cette affaire, le commerçant ne proposait aucune autre alternative pour l'obtention d'une carte de fidélité. La personne qui refuserait de donner son consentement au transfert de ses données personnelles via la lecture de sa carte d'identité ne pourrait dès lors pas bénéficier d'une carte de fidélité ni par conséquent de réduction[140]. Par ailleurs, l'usage de la carte d'identité n'est pas, aux yeux de l'A.P.D., nécessaire pour créer une carte de fidélité, et elle estime que l'intérêt du plaignant, et des clients en général (étant la protection de leurs données personnelles) prime, en l'occurrence, celui du commerçant (la création d'une carte de fidélité sur la base d'une carte d'identité)[141].

Enfin, et ce point pose particulièrement problème, il faut un certain équilibre entre les deux parties (responsable du traitement et personne concernée)[142]. On peut dès lors naturellement se demander si le consentement d'un employé au traitement de ses données par un employeur est considéré comme valable. Le G29 est conscient qu'un consentement donné dans le contexte professionnel est assez fragile, mais l'autorise « à condition qu'il existe des garanties suffisantes que le consentement est véritablement libre »[143]. Le consentement comme base juridique pour le traitement de données dans ce contexte particulier n'est donc pas exclu.

---

134 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 26.

135 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01 ; Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187.

136 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 6.

137 Considérant 42 du R.G.P.D.

138 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 6.

139 Cf. Principe de minimisation des données.

140 A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, p. 7. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO_fr.pdf.

141 A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, p. 7. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO_fr.pdf.

142 Considérant 43 du R.G.P.D.

143 Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187, p. 16.

Un consentement ne sera valable que s'il est spécifique, c'est-à-dire donné pour « une ou plusieurs finalités spécifiques »[144]. « Un consentement général sans que soit spécifié exactement l'objet du traitement des données n'est pas acceptable[145] ». En outre, dans le cas où le traitement poursuivrait plus d'une finalité, la personne concernée doit pouvoir consentir à certaines d'entre elles et pas à d'autres[146].

Le consentement doit également être éclairé. Nous retrouvons, une fois de plus, cette exigence de transparence. Afin d'être valable, le consentement doit être informé[147]. Il faut transmettre à la personne concernée toutes les informations dont elle a besoin, en termes clairs et simples, pour pouvoir consentir en connaissance de cause[148]. Le G29 a établi, dans ses lignes directrices, la liste des informations qu'il estime nécessaires[149]. Parmi elles, l'identité du responsable de traitement[150], la finalité[151], les types de données[152], l'existence du droit de retirer son consentement[153], etc. Précisons encore que, suivant le considérant 42 du R.G.P.D., si le consentement est demandé dans le cadre d'une déclaration écrite relative à une autre question (par exemple, comme c'est souvent le cas, l'acceptation des conditions générales), « il convient, dans un tel cas, de s'assurer que la personne concernée soit consciente du consentement donné et de sa portée »[154]. Autrement dit, le consentement doit se distinguer clairement parmi l'ensemble des informations.

Enfin, le R.G.P.D. pose que le consentement doit être univoque. Cette condition implique un acte positif clair de la part de la personne concernée[155]. Le G29 ajoute que « le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix »[156]. Il précise d'ailleurs qu'une case cochée par défaut ne peut être considérée comme un consentement, comme cela a été illustré dans un arrêt de la CJUE[157] et comme cela est spécifié dans le considérant 32 du R.G.P.D. Toujours selon les lignes directrices du G29, le consentement ne peut être considéré comme valablement obtenu s'il a été donné « moyennant la même action

---

144 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 13.

145 Dix-septième rapport du groupe de travail « Article 29 » sur la protection des données, *Justice et consommateurs*, 2013, p. 8.

146 C. DE TERWANGNE, « Présentation générale du R.G.P.D… », *op. cit.*, p. 27.

147 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 14

148 D.VANDENBUSSCHE, « Qu'est-ce qu'un consentement valable au sens du RGPD ? », 10 octobre 2018, disponible sur https://jura.kluwer.be/secure/documentview.aspx?id=kl2265042&state=changed.

149 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 15.

150 Considérant 42 du R.G.P.D.

151 Considérant 42 du R.G.P.D.

152 Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187, p. 21 à 22.

153 Art. 7, § 3 R.G.P.D.

154 B. VAN ASBROECK et J. DEBUSSCHE, *op. cit.*, p. 94.

155 Considérant 32 du R.G.P.D.

156 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 18.

157 C.J. (gde ch.), arrêt *Bundesverband der Verbraucherzentralen und Vervraucherverbände – Verbraucherzentrale Bundesverband eV/ Planet 49 GmbH*, 1er octobre 2019, C-673/17, ECLI:EU:C:2019:801.

que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service » [158].

2.2. Capacité à démontrer l'accord des personnes

L'article 7, §1 prévoit que le responsable de traitement doit être « en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant »[159]. Il doit également « démontrer que la personne concernée a été informée et que le flux de travail respectait tous les critères pertinents pour un consentement valable »[160]. Cela découle naturellement du principe de responsabilité vu précédemment, mais le fait que l'article 7 R.G.P.D. le rappelle au sujet du consentement fait penser qu'une attention particulière doit lui être portée dans ce contexte.

2.3. Retrait du consentement

Aux termes de l'article 7, §3, « la personne concernée a le droit de retirer son consentement à tout moment »[161]. Cela résulte du fait que la personne concernée doit avoir le contrôle sur ses données personnelles. La personne concernée doit être informée de ce droit avant de donner son consentement. Le retrait n'a pas d'effet rétroactif[162], mis notons que ce point doit être nuancé par le droit de la personne concernée à l'effacement des données la concernant[163].

L'article ajoute que le responsable de traitement doit faire en sorte que retirer son consentement soit aussi simple que de le délivrer[164]. Le R.G.P.D. ne précise pas que le consentement doit pouvoir être donné et retiré moyennant la même action[165]. Toutefois, lorsque la personne concernée a donné son consentement « par voie électronique uniquement par un clic, une frappe ou en balayant l'écran »[166], elle doit pouvoir retirer son consentement par ce même moyen. Lorsqu'elle retire son consentement, la personne concernée ne doit subir aucun préjudice[167]. Si le retrait de consentement engendre un coût ou une baisse de la qualité du service, le traitement ne sera pas licite[168].

2.4. Principe de privacy by design

Le principe de *privacy by design* est un concept introduit par l'article 25 du R.G.P.D., porteur de l'idée que le responsable du traitement doit inclure les principes de protection des données

---

158 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 19.
159 Art. 7, § 1 R.G.P.D.
160 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 24.
161 Art. 7, § 3 R.G.P.D.
162 Art. 7, § 3 R.G.P.D.
163 Art. 17 R.G.P.D.
164 Art. 7, § 3 R.G.P.D.
165 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 25.
166 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01, p. 25.
167 Considérant 42 du R.G.P.D.
168 Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP259 rev.01, p. 25.

personnelles dès la conception du traitement[169]. Il doit prendre en compte l'état des connaissances, les coûts de mise en œuvre et la nature, la portée, le contexte, les finalités du traitement ainsi que les risques que présente le traitement[170]. Selon Olivia Tambou, cette obligation est particulièrement lourde pour les responsables du traitement[171].

Ce principe s'impose au responsable du traitement, en ce qu'il doit « implémenter des mesures techniques et organisationnelles appropriées et des procédures de façon à ce que les traitements de données rencontrent les exigences du R.G.P.D. et assurent la protection des droits des personnes concernées »[172], mais avant toute chose, lui vient en aide dans la mise en conformité au R.G.P.D. En effet, il y a beaucoup moins de chance d'enfreindre le règlement si le principe de *privacy by design* est respecté « puisque le logiciel a été codé afin d'empêcher techniquement ses utilisateurs de traiter les données de manière contraire aux règles fixées dans le système de gestion de ces bases de données »[173].

La formation du personnel est, afin de respecter ce principe, indispensable. En effet, les développeurs de logiciels, par exemple, doivent être en mesure d'intégrer les éléments de protection des données au moment de concevoir leur logiciel[174].

3. Outils à la conformité

3.1. Changements organisationnels et techniques

Nous avons évoqué *supra* qu'en vertu du principe d'*accountability*, le responsable du traitement doit prendre des mesures organisationnelles et techniques afin d'assurer sa mise en conformité au R.G.P.D[175]. Par mesures techniques, il y a lieu d'entendre par exemple, la pseudonymisation et le chiffrement des données à caractère personnel. Nous n'en dirons pas plus à ce sujet, nous nous étendrons par contre plus longuement sur la question des mesures organisationnelles. Plusieurs outils sont mis à la disposition du responsable du traitement afin de documenter sa conformité au règlement (registre des activités de traitement, analyse d'impact…)[176]. Nous nous limiterons toutefois à trois grands changements apportés par le R.G.P.D. : la désignation d'un délégué à la protection des données, l'acteur clé du droit à la protection des données, (articles 37 et suivants), la tenue d'un registre des activités de traitement (article 30 R.G.P.D.), et enfin l'analyse d'impact (articles 35 et suivants). L'objectif principal de ces dispositions est de faciliter la tâche du responsable du traitement dans sa mise en conformité au R.G.P.D.

3.1.1. Désignation d'un délégué à la protection des données

Le R.G.P.D. impose, dans certains cas, aux responsables du traitement et sous-traitants de désigner un délégué à la protection des données (ci-après « DPO »[177]). C'est en quelque sorte

---

169 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 82.
170 Art.25, §1er R.G.P.D.
171 O. TAMBOU, *op. cit.*, p. 256.
172 Traduction libre de C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 9.
173 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 83.
174 C. TERWANGNE *et al*, *ibidem*, p. 83.
175 Considérant 78 du R.G.P.D.
176 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 9.
177 « Data Protection Officer » en anglais.

la personne de référence en matière de protection des données[178]. Il est « au cœur du processus de mise en conformité de l'entreprise, il conseille et accompagne les organismes qui le désignent dans la réalisation de leurs obligations »[179]. Le G29 l'envisage encore comme une des « pierres angulaires du régime de responsabilité » et estime que sa désignation peut « faciliter le respect des règles et, en outre, devenir un avantage concurrentiel pour les entreprises »[180]. Il doit être vu comme « vecteur de sécurité juridique »[181], ménageant la responsabilité du responsable du traitement.

La désignation d'un DPO n'est, suivant l'article 37 §1 R.G.P.D., obligatoire que dans les cas suivants : a) lorsque le traitement est effectué par une autorité ou un organisme public, b) lorsque les activités de base consistent en des opérations qui exigent un suivi régulier et systématique à grande échelle des personnes concernées, ou c) en un traitement à grande échelle de catégories particulières de données visées aux articles 9 et 10[182]. La plupart de ces notions ne sont pas définies dans le R.G.P.D. Nous allons préciser certaines d'entre elles mais renvoyons aux lignes directrices du G29 et au considérant 91 pour plus de détails[183].

La première catégorie appelle peu d'explications. C'est le droit national qui définit les notions d' « autorité publique » et d'« organisme public ». Les deux autres catégories sont plus subtiles. Nous allons tenter d'éclaircir les notions d'« activités de base » et de « traitement à grande échelle ».

Les « activités de base » mentionnées dans les deux dernières catégories[184] visent les activités principales[185], » les opérations essentielles nécessaires pour atteindre les objectifs du responsable du traitement ou du sous-traitant »[186]. Le G29 précise que « les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant »[187] sont également considérées comme des activités de base.

Citons deux exemples des lignes directrices du G29[188]. Il apparaît clairement qu'une société de sécurité assurant la surveillance d'espaces publics compte parmi ses activités de base le traitement de données à caractère personnel. Quant à un hôpital, bien que l'activité de base soit de fournir des soins de santé, le traitement de données concernant la santé est nécessaire donc considéré comme l'une des activités de base de tout hôpital.

---

178 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 90.

179 S. PARSA, « Le R.G.P.D. et la profession d'avocat… », *op. cit.*, p. 154.

180 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 5.

181 G. DESGENS-PASANAU, *op. cit.*, p. 139.

182 Art. 37, § 1 R.G.P.D.

183 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01.

184 Art. 37, § 1, b) et c), R.G.P.D.

185 Considérant 97 du R.G.P.D.

186 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP243 rev.01, p. 8.

187 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 8.

188 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 8.

Concernant le traitement « à grande échelle », également évoqué dans les deux dernières catégories, la notion est mise en lumière par le considérant 91, et les lignes directrices viennent la détailler davantage. Afin de déterminer si un traitement est mis en œuvre à grande échelle, plusieurs critères doivent être pris en compte : « le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ; le volume de données et/ou le spectre des données traitées ; la durée, ou la permanence, des activités de traitement des données ; l'étendue géographique de l'activité de traitement »[189]. Malgré ces indications, l'impossibilité de donner un chiffre précis pour ces différents critères rend cette disposition difficile à appliquer en pratique. Le G29 vient en aide aux entreprises en fournissant quelques exemples de traitement à grande échelle mais constate qu'il existe une large zone grise en ce qui concerne cette notion[190].

La dernière catégorie vise les activités de base consistant en un traitement à grande échelle[191] de catégories particulières de données relatives à des condamnations pénales ou[192] à des infractions[193].

Dans les cas où le traitement ne rentrerait dans aucune de ces trois catégories, la désignation se fait sur base volontaire, sauf si le droit de l'Union ou d'un Etat membre l'exige[194] (en l'occurrence, la Belgique a introduit, dans la loi du 30 juillet 2018[195] exécutant le R.G.P.D., qu'un DPO devait être désigné en cas de traitement pouvant engendrer un risque élevé au sens de l'article 35)[196]. Le G29 encourage d'ailleurs les entreprises à désigner un DPO même lorsque le R.G.P.D. ne le requiert pas[197]. Signalons qu'en cas de désignation volontaire d'un DPO, celui-ci doit remplir les mêmes conditions qu'un DPO désigné sur la base de l'article 37, §1[198]. Quoi qu'il en soit, dans le cas où une entreprise choisirait de se passer de DPO, le G29 recommande de documenter l'analyse effectuée afin de justifier un tel choix[199]. « Cette analyse fait partie de la documentation requise au titre du principe de responsabilité »[200].

Les fonctions et missions du DPO sont énoncées respectivement aux articles 38 et 39 R.G.P.D. Il doit être « désigné sur la base de ses qualités professionnelles, et, en particulier, de ses

---

189 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 9.

190 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01. p.9, note de bas de page n°14.

191 Voir les développements *supra*.

192 L'art. 37, § 1, c) utilise le terme « et » mais le G29 préfère utiliser « ou », ne voyant aucune raison pour laquelle ces deux critères devraient être cumulatifs (Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 11).

193 Art. 37, § 1, c) R.G.P.D.

194 Art. 37, § 4 R.G.P.D.

195 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

196 Loi du 30 juillet 2018, *ibidem*, art. 190.

197 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 5.

198 A. FOCQUET et E. DECLERCK, *op. cit.*, 114.

199 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 7.

200 Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01, p. 7.

connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 »[201]. Il peut être interne à l'entreprise, ou externe (société de services ou cabinet d'avocats)[202]. En outre, la fonction de DPO nécessite une formation en continu : « *[Hij] moet zijn kennis en vaardigheden steeds actueel houden door onder meer zelfstudie, studiedagen, congressen, workshops, cursussen enz.* »[203].

Le DPO est indépendant, il ne peut recevoir d'ordre de la part de son employeur[204]. Parallèlement, il n'a pas de pouvoir de décision : il ne peut que donner des conseils au responsable du traitement, sous-traitant ou aux employés[205]. Il a d'autres missions comme contrôler le respect des dispositions du règlement[206], sensibiliser et former le personnel participant aux opérations de traitements, coopérer en tout temps avec les autorités de contrôle[207], faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement[208]… En outre, il ne pourra pas être tenu responsable personnellement en cas de non-respect du R.G.P.D.[209].

S'agissant de la surveillance du respect des règles, il semblerait, d'après les auteurs de l'ouvrage *Gegevensbescherming in de praktijk,* que les DPO doivent, en pratique, davantage « assumer le travail opérationnel résultant du R.G.P.D. »[210], que remplir leur rôle principal, c'est-à-dire celui de supervision. Cela peut effectivement s'avérer indispensable, selon les auteurs, le temps de mettre en place les processus nécessaires, et cela est d'autant plus vrai chez les PME.

3.1.2. Registre des activités de traitement

Il incombe, en principe, à tout responsable du traitement de tenir un registre des activités de traitement[211], c'est-à-dire un document reprenant les informations relatives aux traitements (finalité, catégorie de données traitées, catégories de personnes concernées…) qui permettra à l'Autorité de protection des données de vérifier la licéité de ce dernier[212].

Les PME sont dispensées de l'obligation de tenir un registre des activités de traitement à condition que le traitement ne soit pas susceptible d'entraîner un risque pour les droits de la personne concernée, qu'il soit occasionnel et qu'il ne porte pas sur des catégories particulières de données visées aux articles 9 et 10[213]. En pratique, un responsable du traitement devra presque toujours tenir un registre[214].

---

201 Art. 37, § 5 R.G.P.D.

202 J. DOORNAERT, *Le règlement général sur la protection des données et sa mise en oeuvre en droit belge*, Waterloo, Kluwer, 2019, p. 156.

203 T. BALTHAZAR en P. RAEYMAEKERS, *Gegevensbescherming in de zorg. Een praktische gids bij de GDPR*, Brugge, die Keure, 2018, p. 54.

204 B. VAN ASBROECK et J. DEBUSSCHE, *op. cit.*, p. 112.

205 C. TERWANGNE *et al*, *La protection des données…, op. cit.*, p. 93.

206 Art. 39, § 1er, b) R.G.P.D.

207 Art. 39, § 1er, d) R.G.P.D.

208 Art. 39, § 1er, e) R.G.P.D.

209 C. TERWANGNE *et al*, *La protection des données…, op. cit.,* p. 94 à 95.

210 Traduction libre de A. FOCQUET et E. DECLERCK, *op. cit.*, p. 117.

211 Art. 30 R.G.P.D.

212 C. DE TERWANGNE, K. ROSIER, et B. LOSDYCK, *op. cit.*, p. 309.

213 Article 30, §5 R.G.P.D.

214 J. HICK et R. INVIJAJEV, *op. cit.*, p. 73.

3.1.3. Analyse d'impact à la protection des données

L'article 35 prévoit que « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires »[215].

En résumé, en cas de traitement risqué pour les droits des personnes concernées, une analyse d'impact relative à la protection des données (ci-après « A.I.P.D. ») devra être réalisée et documentée par le responsable du traitement qui y identifiera les risques possibles, et proposera comment les limiter ou les réduire[216]. « Il s'agit, dans les situations les plus délicates, de mener une analyse approfondie sur le respect du règlement et les risques pour les droits et libertés »[217].

Il existe trois hypothèses dans lesquelles les entreprises peuvent, à certaines conditions, échapper à l'obligation d'analyse d'impact : a) le traitement est nécessaire au respect d'une obligation légale nationale, b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public, c) le responsable du traitement est une autorité publique[218].

Cette A.I.P.D. vise non seulement à garantir la conformité d'un traitement au R.G.P.D. mais aussi à aider le responsable du traitement dans la démonstration de cette conformité[219]. Considérée comme un « outil d'aide à la prise de décisions en ce qui concerne le traitement »[220], elle doit, naturellement, être effectuée *avant* le traitement[221]. Il faudra toutefois penser à actualiser cette analyse qui relève d'un processus continu[222].

L'A.I.P.D. contient au moins : « a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du

---

215 Art. 35, § 1er R.G.P.D.

216 B. VAN ASBROECK et J. DEBUSSCHE, *op. cit.*, p. 110.

217 S. CHATRY, *op. cit.*, p. 126.

218 Art.35, §10 R.G.P.D.

219 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p. 4.

220 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p. 17.

221 Art. 35, § 1er R.G.P.D.

222 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p. 17.

présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées »[223].

Tout comme la désignation du délégué à la protection des données, l'analyse d'impact est obligatoire dans certains cas uniquement et un des grands enjeux est précisément de savoir si oui ou non le responsable du traitement doit réaliser cette analyse. Le G29 a pris soin de nous éclairer sur ce qu'il fallait entendre par *traitement susceptible d'engendrer en risque élevé pour les droits et libertés des personnes physiques*[224]. Nous allons voir quels sont les cas de réalisation obligatoire d'une A.I.P.D. Notons qu'en cas de doute sur la nécessité d'effectuer une A.I.P.D., le G29 recommande d'en réaliser une malgré tout[225].

La règle générale pour que l'A.P.I.D. soit obligatoire est donc la possibilité de risques élevés liés au traitement. Les considérants 89 et 91 donnent quelques indications, comme le fait qu'une attention particulière doit être portée aux traitements de données à caractère sensible[226] ou aux traitements impliquant le recours à une nouvelle technologie[227]. L'article 35, § 3 dresse une liste non-exhaustive des cas où une A.I.P.D. est requise. Le G29 a, quant à lui, proposé neuf critères à prendre en compte pour juger de l'opportunité d'une A.I.P.D.[228]. Selon les lignes directrices du G29, plus un traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées. A partir du moment où le traitement remplit au moins deux critères, le responsable du traitement peut, en principe, considérer qu'une A.I.P.D. est nécessaire, mais il y a des cas où un seul critère suffit[229].

Dans le cas où les risques liés au traitement de données sont élevés et que le responsable du traitement est dans l'incapacité de les réduire, ce dernier est dans l'obligation de consulter l'autorité de contrôle[230].

3.2. Code de conduite et certification

Ce type de mécanismes doivent, suivant le règlement, être encouragés afin de favoriser la transparence ainsi que le respect des obligations engendrées par le R.G.P.D.[231]. Ils ne suffisent pas à prouver la conformité de l'entreprise au règlement mais que celle-ci a pris les mesures adéquates pour encourager une sécurité efficace de l'information[232].

---

223 Article 35, § 7 R.G.P.D.

224 Art. 35 § 1er R.G.P.D.

225 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p. 9.

226 Considérant 91 du R.G.P.D.

227 Considérant 89 du R.G.P.D.

228 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p. 11 et 12.

229 Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01, p.12 et 13.

230 Art. 36 R.G.P.D.

231 Considérant 100 du R.G.P.D.

232 IT GOVERNANCE (ORGANIZATION). PRIVACY TEAM., *op. cit.*, p. 304 à 305.

3.2.1. Code de conduite

« Un code de conduite est un outil de conformité sectoriel qui permet de répondre aux besoins opérationnels des professionnels concernés dans leurs démarches de mise en conformité au R.G.P.D. »[233]. Il prend en compte les exigences contenues dans le R.G.P.D. mais peut aller plus loin. Son but n'est pas de répéter ce qui est dit dans le règlement mais plutôt « codifier comment ce dernier doit s'appliquer d'une manière spécifique, pratique et précise »[234]. Il repose sur une démarche volontaire de la part de l'organisation et des professionnels concernés[235], qui peuvent adopter des codes de conduite dans le but de préciser les modalités d'application du R.G.P.D. compte tenu des particularités de leur secteur[236]. Ces codes sont spécialement bénéfiques aux micro, petites et moyennes entreprises en ce qu'ils leur permettent de se conformer au règlement d'une manière davantage rentable[237].

« *The provisions under Articles 40 and 41 of the GDPR in respect of codes of conduct ("codes") represent a practical, potentially cost effective and meaningful method to achieve greater levels of consistency of protection for data protection rights* »[238].

Un responsable de traitement/sous-traitant adhérant à un code prenant en compte les spécificités d'un secteur devrait être en mesure de démontrer que leur code « répond à un besoin particulier de ce secteur ou de cette activité de traitement, facilite l'application du R.G.P.D., précise l'application du R.G.P.D., offre des garanties suffisantes et prévoit des mécanismes efficaces pour contrôler la conformité avec un code »[239].

Le code de conduite prévu par l'article 40 du R.G.P.D. est un outil contraignant : à partir du moment où une entreprise a décidé d'y adhérer, elle doit le respecter[240]. Il doit être au préalable approuvé par l'autorité de contrôle[241], et un suivi par un organisme agréé est organisé par l'article 41 du R.G.P.D. Notons qu'il est intéressant pour une entreprise de faire usage de cet outil en ce que cela donne confiance aux individus en ce qui concerne leurs données personnelles[242].

---

233 Voir https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite, consulté le 2 mai 2020.

234 Traduction libre de European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019, p. 15.

235 Voir https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite, consulté le 2 mai 2020.

236 Art. 40, § 1er et 2 R.G.P.D.

237 European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019, p. 8.

238 European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019, p. 5.

239 Traduction libre de European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019, p. 14.

240 Voir https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite, consulté le 2 mai 2020.

241 Art. 40, § 5 R.G.P.D.

242 European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019, p. 10.

3.2.2. Certification

La certification est une procédure, prévue par les articles 42 et 43 R.G.P.D., permettant à un responsable du traitement ou sous-traitant d'obtenir de la part d'un organisme agréé une attestation de sa conformité au règlement[243]. La certification est volontaire[244].

Sur base de certains critères définis par l'autorité de contrôle ou le comité, les organismes de certification visés à l'article 43 ou l'autorité de contrôle délivrent une certification relative à un traitement [245] ; certification qui permettra aux entreprises qui en bénéficient de prouver que le traitement de données en question respecte le R.G.P.D. Elle est valable pour trois ans, renouvelable, et peut être retirée lorsque le traitement ne remplit plus les conditions requises par le règlement[246]. Enfin, le texte prévoit que les besoins spécifiques des micro, petites et moyennes entreprises doivent être pris en considération[247].

D) BARRIERES A L'IMPLEMENTATION DU R.G.P.D.

Les entreprises font, sans surprise, face à certaines difficultés quant à l'implémentation et l'application du R.G.P.D. Nous allons exposer certaines de ces difficultés évoquées dans des textes scientifiques. Il ressort notamment d'une étude menée en 2018 sur quatre entreprises que les principales barrières identifiées sont celles-ci : l'ambigüité de la législation européenne, la faible priorité de la part du management pour ce qui concerne le R.G.P.D., le manque de temps pour l'implémentation, le faible budget pour l'implémentation, le manque de personnel qualifié ainsi que le manque d'outils et de technologie disponibles dans les entreprises[248].

Nous avons choisi de classer ces différentes contraintes en trois problématiques : la problématique de sensibilisation et de compréhension du règlement par les entreprises, la problématique financière, ainsi que la problématique liée à la gestion des ressources humaines.

1. Manque de sensibilisation et de compréhension

Un des défis majeurs évoqué dans un article paru en 2017 est que les entreprises ne sont pas suffisamment conscientisées au R.G.P.D.[249]. Il semblerait, en outre, que le besoin de changement soit bien ancré, mais que les informations relatives au R.G.P.D. ne soient pas diffusées en temps utile[250]. Trois années plus tard, il apparaît opportun de nous interroger sur l'état actuel des choses.

---

243 Voir https://www.cnil.fr/fr/la-certification, consulté le 2 mai 2020.
244 Art 42, § 3 R.G.P.D.
245 Art. 42, §5 R.G.P.D.
246 Art. 42, § 7 R.G.P.D.
247 Art. 42, § 1 R.G.P.D.
248 A. FAIFR and M. JANUSKA, « Companies' readiness of GDPR and implementation barriers », *International Institute of Social and Economic Sciences*, 2018, p. 42.
249 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 2.
250 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *ibidem*, p. 2.

Un autre défi serait, toujours selon cet article, le manque de compréhension de la part des entreprises des exigences imposées par le R.G.P.D.[251]. Les difficultés quant à l'implémentation du nouveau règlement seraient notamment dues à la complexité de la règlementation et au temps nécessaire à une bonne compréhension des obligations légales qu'elle engendre.

Dans l'étude menée en 2018, trois entreprises sur quatre ont cité comme problème principal l'ambigüité de la législation. Non seulement la formulation du règlement lui-même n'est pas toujours limpide, comme nous avons pu le remarquer dans l'analyse des dispositions légales, mais la manière de l'appliquer poserait également problème[252].

2. Ressources financières

Le R.G.P.D. a des implications pour les entreprises sur la manière de gérer leurs ressources, notamment financières[253]. Cette contrainte se fait particulièrement ressentir chez les PME, qui n'ont pas nécessairement un spécialiste de la sécurité de l'information à disposition[254], et qui ne peuvent pas toujours se permettre une aide juridique extérieure pour se mettre en conformité avec les règles du nouveau règlement[255].

Enfin, si la conformité au R.G.P.D. est susceptible d'engager des coûts importants, la non-conformité l'est davantage car la sanction peut aller jusqu'à 4% du chiffre d'affaire annuel total de l'exercice précédent[256].

3. Penser la gestion des ressources humaines

Christina Tikkinen-Piri, Anna Rohunen et Jouni Markkula indiquent que l'implémentation du R.G.P.D. couvre différents aspects, parmi eux : la sensibilisation et la formation au niveau des entreprises, l'adoption de mesures organisationnelles et techniques de protection des données, et la documentation des opérations de traitement. « Dans cette optique, les entreprises ont indéniablement besoin de temps, de ressources et de conseils aux fins de mise en œuvre de la protection des données »[257].

Implémenter et appliquer le R.G.P.D. nécessite en effet l'attribution de nouvelles responsabilités, la formation du personnel, un changement au niveau des pratiques et processus organisationnels etc.[258] Cela signifie un besoin de revoir les pratiques et mesures de protection des données, ou éventuellement élaborer de nouvelles[259].

---

251 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *ibidem*, p. 2.
252 A. FAIFR and M. JANUSKA, *op. cit.*, p. 43.
253 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 1.
254 A. EJZYN et T. VAN DEN BERGHE, « Avant-propos », *Cybersécurité et RGPD : protégez-votre PME*, Limal, Anthemis, 2018, p. 11.
255 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit.*, p. 2.
256 Art. 83, §5 R.G.P.D.
257 Traduction libre de C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *op. cit*., p. 2.
258 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *ibidem*, p. 2.
259 C.TIKKINEN-PIRI, A. ROHUNEN, and J. MARKKULA, *ibidem*, p. 2.

Le principe de *privacy by design*, évoqué plus haut, implique que le personnel soit formé à intégrer la protection des données dès la conception du produit ou service, et que les tâches et ressources soit réparties de manière appropriée[260].

Nous avons l'intention de découvrir, par le biais de nos entretiens, comment s'est déroulée la gestion des compétences et comment s'est effectuée la répartition des tâches.

La gestion des compétences est définie comme le fait, pour une organisation de « chercher à acquérir les compétences individuelles et collectives dont elle a besoin, mais aussi de les stimuler et les réguler »[261]. En d'autres mots, c'est une manière de gérer le capital humain d'une entreprise afin d'optimiser les performances de celle-ci. La gestion des compétences couvre la formation, le recrutement, la rémunération, la promotion, l'organisation du travail et la mobilité professionnelle[262].

La gestion des compétences, qui n'était auparavant évoquée qu'à propos des grandes entreprises, a récemment fait son apparition chez les PME[263]. Il nous paraît dès lors judicieux, dans un travail réalisé au sujet de PME et de grandes entreprises, d'introduire cette problématique de gestion des ressources humaines.

---

260 O. TAMBOU, *op. cit.*, p. 255.

261 C. DEFÉLIX, « La gestion des compétences au défi de la mesure : des réceptions différenciées de la norme ISO 9001, Version 2000 », *La GRH mesurée*, Actes du XVe congrès de l'AGRH, Montréal, tome 3, p.1509, cité par M. Antoine *et al*, « La démarche compétences dans la littérature en gestion », *Faut-il brûler la gestion des compétences : Une exploration des pratiques en entreprise*, F. Pichault (dir.), Louvain-la-Neuve, De Boeck Supérieur, p. 12.

262 B. MERCK et P.-E. SUTTER, « Présentation », *Gestion des compétences, la grande illusion. Pour un new deal "compétences"*, B. Merck et P.-E. Sutter (dir.), Louvain-la-Neuve, De Boeck Supérieur, 2009, p. 38.

263 C. DEFÉLIX et D. RETOUR, La gestion des compétences dans la stratégie de croissance d'une PME innovante : le cas Microtek, *Revue internationale P.M.E.*, 16 (3-4), 2003, p. 35.

ANALYSE CRITIQUE DE LA MISE EN PLACE ET DE L'APPLICATION DU R.G.P.D.

Une fois l'état de l'art réalisé, nous avons questionné divers acteurs (issus de petites, moyennes et grandes structures) afin d'étudier comment les entreprises ont traduit les obligations légales du R.G.P.D. en obligations de *compliance*. Nous avons ainsi pu relever les différentes contraintes auxquelles ces entreprises faisaient face et dégager, le cas échéant, leurs solutions ou esquives.

Cette analyse critique est subdivisée en deux parties : les difficultés pratiques et l'application des dispositions légales. Dans la première partie, nous présenterons les contraintes fonctionnelles rencontrées par les interviewés : la contrainte budgétaire, la contrainte d'accès à l'information et la contrainte liée à la gestion des ressources humaines. Dans un second temps, nous nous focaliserons sur la manière dont les organismes interviewés appliquent les différentes dispositions étudiées dans la partie « analyse théorique du R.G.P.D. ».

A) DIFFICULTÉS PRATIQUES

1. Contrainte budgétaire

Durant les entretiens, nous remarquons qu'une tendance se dégage principalement : la contrainte budgétaire est difficilement appréhendable. Cette difficulté s'explique, partiellement en tous cas, par l'aspect transversal qu'elle impose. En effet, de la gestion des compétences aux investissements technologiques en passant par le temps à consacrer pour se conformer au R.G.P.D., l'ensemble des contraintes touchent, de près ou de loin, à l'aspect financier. Dans cette section, nous n'aborderons que les changements impliquant le budget à proprement parler, c'est-à-dire une sortie d'argent : l'externalisation des compétences et les nouveautés technologiques. Nous terminerons par la sensibilisation du management en ce qui concerne le budget consacré à la mise en place et à l'application du R.G.P.D.

1.1. Externalisation des compétences

D'un point de vue de la gestion des compétences, il arrive que les PME décident d'externaliser[264] une partie de la gestion du R.G.P.D., pour éviter des soucis d'accès à ces compétences mais aussi de temps à y consacrer. C'est en effet une possibilité offerte par le R.G.P.D. qui prévoit, en son article 37, que « le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service »[265]. Cette externalisation a un coût non négligeable, comme le soulignent ces interviewés.

---

264 « L'externalisation est un service défini comme le résultat de l'intégration d'un ensemble de services élémentaires, visant à confier à un prestataire spécialisé tout ou partie d'une fonction de l'entreprise « client » dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de service et une durée définis » (AFNOR, Association française de normalisation, 1995, cité par E. FIMBEL, « Nature et enjeux stratégiques de l'externalisation », *Revue française de gestion*, vol. n° 143, 2003/2, p. 28).

265 Art. 37, § 6 R.G.P.D.

I.8 : « *Nous nous sommes entourés d'un cabinet juridique spécialisé dans la matière. Au niveau des prestations de ce cabinet, ils ont décortiqué en 3 phases : la phase vente, la phase de support administratif et la phase RH. Ils ont établi une matrice et les choses à faire évoluer pour être compliant.* »

I.12 : « *Nous possédons une team de juristes qui ont travaillé et qui continuent de travailler sur les questions R.G.P.D. quotidiennement. Au fur et à mesure que Heetch a grandi, nos besoins se sont multipliés et nous avons eu recours à un cabinet d'avocats spécialisé sur ces questions. (…) Les coûts sont très importants, notamment à cause du partenariat avec le cabinet.* »

L'interviewé 9 n'a pas bénéficié d'aide extérieure mais partage l'avis des autres intervenants quant aux coûts que ça implique :

« *On a été contactés du jour au lendemain par des cabinets d'avocats qui proposent de vous aider, je ne sais pour combien de milliers d'euros…* »

Concernant les grandes structures, une seule a abordé la question de l'externalisation des compétences. Cette aide n'a toutefois été que temporaire, comme cet extrait le révèle :

I.2 : « *Un opérateur externe a été mandaté pour aider notre DPO à prioriser les actions et conscientiser l'ensemble au R.G.P.D.* »

Hormis ce cas isolé, aucune grande structure n'a choisi d'externaliser la gestion du R.G.P.D. Interrogé sur ce procédé, l'interviewé 5 ne fait pas dans la dentelle :

« *Faire appel à un cabinet externe, c'est stupide et inutile. Un consultant externe n'a pas de responsabilité, il prend juste l'argent, et la responsabilité reste sur la tête des décideurs en interne. Ils pensent qu'en payant, ils ne risquent rien et que le cabinet s'occupe de tout mais c'est un leurre.* »

A ce propos, dans son guide pratique destiné aux PME, la CNIL[266] met en garde : « *Soyez vigilants : certains acteurs peu scrupuleux profitent du R.G.P.D. pour proposer des prestations excessivement coûteuses ou générer des appels surtaxés. Renseignez-vous sur leurs compétences et références avant d'entrer en relations d'affaires* »[267].

Par ailleurs, l'externalisation des compétences pose un problème de viabilité sur le long terme. En effet, comme cela a été pointé du doigt par plusieurs entreprises (petites ou grandes), l'intégration du R.G.P.D. au sein d'une entreprise se fait d'une manière lente et permanente. Il n'y a pas de résultat strict à atteindre mais simplement une conduite à adopter pour se diriger vers la conformité.

I.1 : « *Ça demande beaucoup de travail pour se conformer et on ne sait pas tout mettre en place directement. En matière de nouvelle technologie/cyber sécurité par exemple, on doit continuellement travailler dessus, on ne sait pas faire un one shot puis s'arrêter, c'est vraiment en continu.* »

---

266 Autorité française chargée de vérifier le respect de la protection des données

267 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises », 2018, p. 21.

I.9 : « *L'application du R.G.P.D., on doit y veiller en permanence. Par exemple, si on pense à aménager les locaux, il faut penser à protéger les dossiers des patients donc penser aux serrures, à qui a la clé et tout ce qui s'en suit*. »

I.12 : « Ça nous a demandé beaucoup de travail pour s'y conformer et ça en demande encore aujourd'hui car on a tellement de données et on doit faire tellement de choses avec cette loi qu'on est toujours en train d'essayer de se conformer… C'est difficile surtout pour une petite société comme nous : on n'a pas nécessairement les ressources, on essaie petit à petit… »

Le coût de l'externalisation est immédiat au moment de la mise en place du règlement, mais les cabinets sont uniquement capables de gérer le R.G.P.D. en fonction de la situation actuelle de l'entreprise, à un instant T. Or, dès l'introduction d'une nouvelle pratique ou d'un nouveau *process*, il faut penser R.G.P.D. Le coût de l'externalisation doit donc être subi de manière constante afin de continuer à respecter le règlement, ce qui est difficilement supportable pour les PME qui finissent par abandonner l'idée d'une aide extérieure.

I.8 : « *Ça a été des dépenses importantes… On a dit au cabinet d'avocats : 'on a la matrice, la structure, on voit ce qu'il faut faire, on reviendra vers vous' parce que c'est énorme comme budget quand on se fait aider de cette manière-là. »*

I.12 : « *Maintenant on s'adresse au cabinet spécialisé de manière ponctuelle.* »

Si les entreprises font le choix d'internaliser la question des compétences liée à l'application du R.G.P.D., d'autres contraintes apparaissent mais elles sont moins liées au budget qu'à la gestion des ressources humaines. Nous traiterons donc cette question ultérieurement.

1.2. Nouveautés technologiques

Certains intervenants, issus de grandes structures comme de PME, mettent en évidence le coût lié à l'acquisition et à la mise en place d'outils technologiques qui découlent, selon elles, des obligations légales qu'impose le R.G.P.D. Il existe, en effet, des secteurs où investir dans de la nouvelle technologie peut s'avérer nécessaire au respect du règlement.

I.9 : « *Il y a une obligation de protection des données mais c'est très lourd, ça demande des investissements financiers. Vu qu'on a de l'informatique, il a fallu s'adapter. Il faut compter une vingtaine d'euros par an et par ordi, il faut avoir accès à un informaticien qui peut mettre les données sur des clouds… Il faut compter 4 ou 5000 euros sans compter le temps qu'on a dû passer.* »

I.5 : « *La moindre mesure qu'on prend, c'est du temps et du budget. Par exemple, si on fait un contrôle médical, on doit scanner les certificats, inventer un logiciel qui sépare les données de pathologie des données purement administratives. Ça veut dire qu'il faut des sommes pour acheter la machine, puis former le personnel à la machine …* »

I.7 : « *Notre matériel est protégé par des logiciels de sécurité de premier ordre. Mais tout ça coûte de l'argent.* »[268]

---

[268] Traduit de l'anglais.

Outre le coût du matériel adéquat, la formation du personnel à ces nouveaux outils est une difficulté supplémentaire. Ce point est abordé ultérieurement.

1.3. Sensibilisation du management

Une difficulté évoquée maintes fois par les grandes structures est celle liée à la sensibilisation du management quant au budget à prévoir pour la mise en place et l'application du R.G.P.D.

> I.1 : « *Une des difficultés qu'on a eues, ça a été de convaincre le management de libérer les ressources financières nécessaires pour tenir compte du R.G.P.D. et de l'absolue nécessité de s'y conformer afin d'éviter les sanctions. C'est difficile de faire payer pour un projet qui ne rapporte rien immédiatement.* »
>
> I.3 *« Le plus important, c'est avoir l'aval et le soutien de la direction (RH et financière) et qu'elle débloque les budgets. »*

Néanmoins, une fois le budget débloqué, les grandes structures bénéficient des moyens nécessaires pour faire face au règlement et échappent ainsi à de nombreuses difficultés qu'éprouvent les PME…

Au-delà du budget, les entretiens ont dévoilé que d'autres ressources sont sollicitées via la sensibilisation du management. Ainsi, cette dernière a permis d'accorder du temps, du personnel et du soutien, essentiels à la bonne application du R.G.P.D.

> *I.5 : « On était face à un mur, mais la haute direction nous a ouvert des portes, ça a facilité les choses, on nous a placés comme prioritaires dans cette action. »*
>
> *I.3 : « Heureusement, chez nous, la direction en RH a compris l'importance de mobiliser des personnes qui n'étaient pas toutes prévues, on leur a demandé de consacrer du temps au R.G.P.D. »*

Cette sensibilisation du management n'intervient apparemment pas dans les PME. La structure des organisations plus petites est, en effet, généralement plus informelle, ce qui implique des niveaux hiérarchiques plus flous. Par conséquent, le processus de décision y est appliqué de manière moins concrète.

Dans les PME, que la personne en charge du R.G.P.D. se soit auto-désignée ou qu'elle ait été choisie par un responsable de l'entreprise, il semblerait qu'elle ait un champ d'action assez libre dans la mise en œuvre et dans l'application du règlement dans l'entreprise. Précisons tout de même que son champ d'action est généralement limité par l'insuffisance des ressources, propre aux PME.

2. Contrainte d'accès à l'information

Plusieurs PME ont insisté sur le fait que, si elles avaient bel et bien toutes entendu parler du R.G.P.D. avant qu'il n'entre en vigueur, des informations concrètes et claires faisaient cruellement défaut. Elles se plaignent particulièrement du manque d'aide de la part des autorités publiques.

I.8 : « *Quand le R.G.P.D. est sorti, on en a fait tout un plat, ça a été l'afflux d'infos contradictoires. Les gens ont eu peur. Il y a des gens qui ne savent pas ce que ça veut dire, qui ne savent pas ce qu'ils doivent faire… »*

I.9. : « Au départ, on a eu tellement d'infos de sources différentes. Je suis allée à 6 ou 7 séances d'information, c'était le jour et la nuit, heureusement que j'ai fait du droit ! (…) On aurait dû accompagner les structures, d'un point de vue fédéral. L'Etat devrait mettre des trucs en place quand ça chamboule à ce point-là le travail des gens. Je travaille pour d'autres A.S.B.L. qui n'ont pas d'administration, pas de juriste, pas de gens qui connaissent la législation, qui n'ont pas envie de s'embêter avec ça… Pour eux, ça devient très lourd. »

I.14 : « La ligne conductrice n'était pas claire et il y a eu beaucoup d'incohérences dans les différentes informations reçues. Les PME n'ont pas non plus pris les mêmes mesures que les multinationales qui, elles, avaient les moyens de mettre 2 ou 3 personnes à temps plein dessus pour comprendre ce qu'elles pouvaient faire ou pas faire. »

I.10 : « Quand on nous a décrit le R.G.P.D., on nous a dit : tout est prévu, vous allez recevoir de l'aide de la part de l'Autorité de protection des données, il y aura des procédures mises en place, tout va rouler. Mais quand on a vu la masse de travail, il a fallu réfléchir dans toutes les directions. Les concepteurs n'ont pas pris la pleine mesure de ce qu'ils demandaient aux organismes. »

Il en ressort que nous nous retrouvons confrontés à des interviewés qui ne comprennent pas toujours l'ampleur du règlement ni les subtilités qu'il y a derrière. Ils savent qu'ils ne sont pas au point, mais ne vont pas plus loin.

Nous sommes d'avis que les organisations, et plus particulièrement les PME, auraient dû bénéficier de plus d'encadrement. Elles n'ont visiblement pas été suffisamment informées, ce qui est regrettable. Certains guides de conformité destinés aux PME sont pourtant mis à leur disposition[269], mais elles semblent ignorer leur existence.

3. Contrainte liée aux ressources humaines

Afin d'opérer la mise en place et l'application du R.G.P.D., tant les petites et moyennes entreprises que les plus grandes structures adaptent leur gestion des ressources humaines de manière spécifique.

Tout d'abord, nous constatons dans plusieurs interviews que la mise en place du R.G.P.D. et son application impliquent des compétences nouvelles ou plus spécialisées. L'obligation légale, dans la majorité des entreprises, de désigner un DPO formalise cette contrainte. Le DPO doit être une personne capable de maîtriser les exigences du R.G.P.D. tout en se positionnant comme

---

269 Voy. COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, « RGPD. Vade-mecum pour les PME » 2018 ; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises », 2018.

personne ressource pour les membres de l'entreprises, tant par une mission d'information, de sensibilisation et de formation.

Ces compétences sont, selon nous, cruciales pour une application optimale du R.G.P.D. Ce point s'explique, notamment, par la complexité du règlement et l'ambiguïté qui peut y être perçue, et par l'obligation de *privacy by design* qui impose un accès à des compétences-clés le plus rapidement et le plus qualitativement possible.

Enfin, l'application du R.G.P.D. modifie l'organisation du travail pour les membres de l'entreprise. En effet, les différentes obligations légales qu'il engendre tendent à modifier l'organisation du travail au sein des entreprises car il oblige, par exemple, à modifier les techniques utilisées, les programmes et *process* internes à l'organisation. Afin d'y arriver, les entreprises mettent en place une formalisation plus conséquente. Nous y reviendrons.

Il est, dans les faits, facilement affirmable que la contrainte d'envisager différemment une partie de la gestion des ressources humaines apparaît comme une solution à une grande partie de la difficulté que pose le règlement. Face aux contraintes d'accès et de transmission des compétences, mais aussi à celle de modification de l'organisation du travail, les entreprises mettent en place divers moyens : sensibilisation, formation, information, internalisation des compétences ou encore formalisation.

3.1. Sensibilisation, formation, information

La sensibilisation du personnel est une solution constamment rencontrée lors des entretiens, autant dans les PME que dans les grandes structures. Tout d'abord, c'est un moyen adéquat pour remplir l'obligation de transparence que nous avons étudiée lors de la première partie. De plus, le R.G.P.D. induit un changement brutal pour le quotidien des employés. Il est primordial que le personnel accepte ce changement, en comprenant l'objectif et les intérêts que le règlement dégage. Le règlement a un impact relativement global : il est susceptible de toucher chaque membre du personnel, peu importe son niveau hiérarchique et sa fonction au sein de l'organisation. Ainsi, il est capital que la sensibilisation puisse avoir un effet sur l'ensemble du personnel.

> I.8 : « *Tout le staff a été sensibilisé à cette protection des données. (…)* O*n n'a pas développé d'outil spécifique pour le suivi de l'application du R.G.P.D. mais on sensibilise le staff via la formation*. »
>
> I.9 : « *Il faut prévoir un temps de formation des équipes pour qu'elles comprennent l'importance du R.G.P.D.* »
>
> I.14 : « *On a dû conscientiser l'équipe par rapport aux données des clients*. »
>
> I.7 : « *Les employés sont conscients qu'ils peuvent être licenciés pour ne pas avoir respecté les règles du R.G.P.D.* »[270]

[270] Traduit de l'anglais.

I.2. : « *Il a fallu convaincre du côté incontournable de se plier aux exigences mais maintenant il y a une prise de conscience de la valeur à accorder au traitement des données personnelles.* »

I.5 : *« Le R.G.P.D., c'est avant toute chose informer et sensibiliser. Sensibiliser le personnel, les cadres, les dirigeants…* »

Pour certaines entreprises, la sensibilisation a porté ses fruits ; pour d'autres, l'intégration du règlement au sein du personnel continue de poser problème.

I.14 : « *Malgré la sensibilisation, il y a toujours de vieux réflexes qui restent …* »

I.1 : « *Mon plus grand souci et regret est de ne pas réussir à toucher tous les travailleurs. Sensibiliser et donner aux gens l'envie de comprendre les obligations du R.G.P.D. et de s'impliquer, c'est ce qui est le plus compliqué* ».

I.5 : « *Malgré les sensibilisations, on se rend compte que les gens du personnel n'ont toujours pas les bons réflexes, et que les erreurs sont trop fréquentes. Les ordinateurs sont souvent égarés, par exemple*. »

La sensibilisation s'est effectuée, pour la plupart, via un processus d'information. Evidemment, ces deux phénomènes sont liés et se confondent sur le terrain. L'un comme l'autre permet de sensibiliser le personnel au R.G.P.D et à l'importance de son application.

I.9 : « *On a informé le personnel par rapport au R.G.P.D., j'avais fait un PowerPoint pour expliquer son importance, les 6 paramètres à respecter quant à l'application et m'assurer qu'on y veille à chaque fois.* »

I.1 : « *On a organisé des sessions d'informations R.G.P.D.* »

I.2 : « *On informe notre personnel par des séances de formation, par des courriers, en leur faisant signer des avenants…* »

La formation du personnel est également un outil destiné à ancrer le R.G.P.D. au sein du fonctionnement de l'entreprise. Elle est particulièrement nécessaire en cas de matériel ou logiciel nouveau. En général, il est fait usage de la formation dans les grandes structures et dans les PME d'un certain effectif.

I.9 : « *Il faut prévoir un temps de formation des équipes pour qu'elles comprennent l'importance du R.G.P.D.* »

I.2 : « *Le premier stade, ça a été la formation de notre personnel. Une formation @learning est donnée à tout nouvel agent.* »

I.5 : « *On a élaboré un processus de formation d'une journée complète, un quick win pour avoir les bons réflexes au quotidien***. »**

I.7 : « *Les employés sont formés et contrôlés de manière périodique.* »[271]

[271] Traduit de l'anglais.

La formation semble essentielle pour se préparer correctement à la mise en conformité au R.G.P.D. Elle est toutefois un poids pour le DPO qui ne parvient pas toujours à former les travailleurs comme il le souhaiterait et qui doit réfléchir à des processus de formation adaptés.

A travers les extraits suivants, les grandes structures relatent également un manque d'encadrement. Afin de faciliter la tâche des DPO, une formation obligatoire pour chaque travailleur touché par le R.G.P.D. aurait dû être organisée.

> I.1 : « *Il y a des points où je ne suis pas à l'aise par exemple pour la formation : je ne peux pas prétendre que tout le monde sait ce qu'est le R.G.P.D. et ce que ça implique. C'est dommage… J'ai pensé à imposer des formations, ça a été refusé par le syndicat.* »

> I.2 : « *Je passe 80% de mon temps à répéter tout le temps la même chose, à des horizons différents. Ce n'est pas très efficient au niveau de l'approche. Il aurait fallu une assistance importante pour développer des modules de formation, je ne peux pas tout faire non plus.* »

> I.5 : « *Après la sensibilisation, il y a eu une formation donnée aux communes et aux provinces. On doit adapter la formation au personnel qui souhaite la suivre. On fait des quizz, des blind test en interne. Il faut faire vivre la matière. »*

3.2. Internalisation des compétences

Nous avons abordé, dans la section dédiée à l'impact budgétaire du R.G.P.D., l'externalisation des compétences. Le temps est venu d'exposer l'alternative, à savoir le maintien de la gestion du R.G.P.D. en interne. Si l'externalisation se traduit par le fait *d'acheter* le capital humain, l'internalisation est le fait de le *créer*[272].

Si les entreprises font le choix d'internaliser la question des compétences liées à l'application du R.G.P.D., d'autres contraintes apparaissent. Ces contraintes se caractérisent par un coût, mais de façon indirecte cette fois, en particulier au niveau du temps à consacrer. En effet, en internalisant la gestion du R.G.P.D., les entreprises se retrouvent confrontées à un dilemme : l'engagement de personnel ou l'obligation de repenser l'organisation du travail afin d'assigner de nouvelles tâches aux travailleurs déjà en place. Dans les deux cas, les économies réalisées grâce à l'internalisation des compétences sont contrebalancées par le temps dédié à la mise en conformité au R.G.P.D. par les entreprises. Plusieurs interviewés ont mis ce phénomène en évidence. Nous remarquons, par ailleurs, que la contrainte « temps » se fait particulièrement ressentir chez les PME.

> I.11 : « *L'impact budgétaire a été minime pour nous parce qu'on a tout fait nous-mêmes pour que ça nous coûte le moins possible, mais l'impact n'est pas négligeable en terme de temps : vu qu'on n'est pas expert, il a fallu se renseigner, rédiger, revérifier…* »

---

272 T. DULAC ET N. DELOBBE, « Relations entre les modes de gestion du capital humain, la relation d'emploi et les attitudes et comportements au travail », *La société flexible*, M. de Nanteuil-Miribel et A. El Akremi (dir.), Toulouse, ERES, 2005, p. 181.

I.10 : « *Les coûts, nous, c'est plutôt du temps humain, pris par le personnel de l'équipe mais pas de coût direct, on n'a pas dû payer des consultants, des juristes etc.* »

I.13 : « *Il a fallu du temps pour mettre en place les différentes mesures et voir clair dans les textes, d'autant plus qu'on n'a pas pu se permettre l'intervention d'un juriste*. »

I.12 : *« Concernant le temps de travail, c'est un travail quotidien, qui mobilise des juristes chez Heetch mais également toutes les équipes selon les besoins. »*

I.4 : *« Plus de 100 personnes ont travaillé pour adresser les sujets R.G.P.D. et pour mettre à jour les outils. Pour nous, les coûts humains ont été énormes. »*

Il est aisément compréhensible que cette pratique a également des répercussions financières puisqu'il faut libérer les travailleurs de certaines tâches habituelles afin de leur permettre de consacrer du temps à la mise en œuvre du R.G.P.D. et à son application.

C'est toutefois cette pratique d'internalisation, considérée comme moins coûteuse, qui est retenue le plus fréquemment parmi les entités interviewées. Les PME choisissent en général de désigner un délégué à la protection des données parmi leur personnel pour s'occuper du R.G.P.D. Les grandes structures font également usage de leurs ressources internes ou embauchent un expert à cet effet. Ce point sera abordé plus longuement dans la partie « application des dispositions légales ».

3.3. Formalisation

Une des solutions apportées à la difficulté d'application du R.G.P.D. est la formalisation. En effet, cette dernière est source d'efficience et de productivité. Par ailleurs, elle facilite l'application du règlement et son contrôle. La formalisation entraîne toutefois des contraintes, par exemple, au niveau de la gestion des compétences et du management. En effet, il faut ancrer, dans le quotidien des travailleurs, des nouvelles pratiques et techniques qui vont leur rajouter une charge de travail supplémentaire. Au niveau du management, il faut convaincre les travailleurs de l'utilité et de la nécessité d'ancrer ces nouvelles pratiques et techniques dans leur quotidien professionnel.

La formalisation intervient, à quelques exceptions près, dans les grandes structures. Ce n'est pas surprenant puisque la formalisation, qui requiert une organisation et une instrumentation complexes, est une caractéristique des grandes entreprises[273].

I.9 : « *J'ai été aidée par notre fédération qui a permis de créer un groupe de travail pour avoir des documents types. J'ai aussi profité du Covid pour travailler sur le R.G.P.D. et créer des modèles sur base de modèles légaux déjà existants*. »

I.8 : *On a simplement dû formaliser des pratiques qu'on avait déjà. On a été de découverte en découverte mais la bonne surprise ça a été que nos pratiques étaient déjà bonnes.* »

---

273 D. BESSON et A. OLABA, « Une approche contextualiste des pratiques de gestion des compétences par l'informel : une enquête sur quatre PME », *Annales des Mines – Gérer et comprendre*, vol. 128, 2017/2, p. 14.

> I.1 : « *On a une méthodologie projet adaptée au R.G.P.D. qu'on a rendue incontournable*. »
>
> I.2 : *« On a créé des formulaires types, des modèles et des procédures*. »
>
> I.3 : « *On a mis en place un programme R.G.P.D. qu'on a documenté avec une feuille de route, on a une équipe avec différents réseaux, des modèles pour répondre à toute obligation. On a mis en place une série de politiques, de documents à mettre en œuvre, des contrats, des outils. »*
>
> I.7 : *« On a un plan d'action bien précis. »*[274]

Nous remarquons, en revanche, que les interviewés 5 et 6, bien qu'étant des grandes structures, ont du mal à formaliser leurs pratiques. Cela tient probablement au fait que leur taille est particulièrement grande, et, comme elles l'ont elles-mêmes souligné, qu'elles comprennent une variété de métiers impressionnante pour lesquels il est difficile de trouver une ligne de conduite unique.

> I.5 : « *On a une méthodologie bien pensée, un plan de bataille, mais la concrétisation est compliquée parce qu'après c'est le bon vouloir. En plus, vu l'ampleur de la tâche et la diversité des matières et des données, c'est un travail titanesque, surtout avec 6300 personnes et 24 compétences différentes. On a des milieux tellement variés…* »
>
> I.6 : « *J'essaie de mettre en place des procédures qui permettront de travailler de manière systématique, mais ça prend du temps car ça demande de la collaboration entre plusieurs personnes. Puis on a de tout dans les métiers, et je ne peux pas demander aux vétérinaires de travailler de la même façon que les architectes. Il faut tenir compte de la réalité du terrain. Le but est de systématiser l'application du R.G.P.D. mais pour nous, et pour toutes les universités d'ailleurs, c'est compliqué*. »

Nous avons, le long de ce travail, émis l'hypothèse que les grandes structures étaient plus équipées que les PME pour implémenter le R.G.P.D., que ce soit au niveau du budget, du personnel, mais aussi du fonctionnement. Les grandes structures sont davantage organisées, elles sont, par exemple, propices à la formalisation, comme nous venons de le souligner. L'ampleur de la structure peut toutefois être un frein à une application opportune du R.G.P.D. En effet, les grandes organisations ont généralement des procédures et techniques plus complexes, avec plus de personnes concernées.

---

274 Traduit de l'anglais.

B) APPLICATION DES DISPOSITIONS LÉGALES

Nous avons évoqué, dans le chapitre précédent, la contrainte liée à l'accès à l'information relative au R.G.P.D. Dans ce chapitre, nous exposons les difficultés liées au traitement de l'information par les entreprises, c'est-à-dire à l'application des dispositions légales. Nous tentons également de découvrir quelles sont les solutions proposées par ces entreprises.

1. Notions de responsable du traitement et de sous-traitant

Rappelons-nous que la distinction entre responsable du traitement et sous-traitant, tout comme le concept de « co-responsabilité », étudiés *supra*, semblaient poser quelques difficultés. Lors de nos entretiens, nous nous sommes attardés sur la manière dont les entreprises jonglaient avec ces notions. Alors que nous avions émis l'hypothèse que les grandes entreprises appliquaient les dispositions légales du R.G.P.D. avec moins de difficultés que les petites et moyennes entreprises, il se trouve que sur ce point particulièrement, l'inverse se produit.

Aucune PME ne semble rencontrer de difficulté pour distinguer le responsable du traitement du sous-traitant.

> I.8 : « *Nous, on est responsables du traitement. Nos sous-traitants, ce sont nos partenaires. C'est aussi notre consultant IT, qui traite notre site internet.* »
>
> I.9 : *Nous sommes responsables de tous les traitements, alors que notre informaticien, la mutuelle, etc. sont des sous-traitants* ».

Les grandes structures éprouvent, en revanche, quelque peine pour attribuer les rôles de chacun :

> I.3 : « *L'identification des rôles et des responsabilités est peut-être le travail le plus compliqué en regard du R.G.P.D., en particulier dans les grandes entreprises, où il y a des filiales par exemple. Nous, on a le Ministère de la Fédération Wallonie-Bruxelles puis on a différentes administrations. Au sein de ces administrations on a des partenaires, des écoles, des fédérations de pouvoir organisateur, des professeurs… C'est dur de savoir qui fait quoi et à quel stade…* »
>
> I.5 : « *Le plus dur c'est de savoir qui est co-responsable du traitement et qui est sous-traitant, mais finalement on profite de ce flou de connaissance pour tirer notre épingle du jeu. »*
>
> I.1 : « *Dès qu'on évoque le traitement de données on doit se demander 'de qui est-ce la responsabilité ?'… C'est assez lourd. »*

Cette difficulté à laquelle seules les grandes structures font face s'explique naturellement par le fait que les grandes structures possèdent plusieurs niveaux de pouvoir. Nous supposons donc que plus la structure est grande, plus la difficulté de distinguer le responsable du traitement du sous-traitant sera grande. La structure organisationnelle d'une PME étant logiquement plus simple, le travail d'identification des rôles l'est également.

A la question de savoir comment cet obstacle est surmonté, il n'y a pas vraiment de solution miracle. C'est un sujet qui implique débats et négociations, comme le souligne l'interviewé 3.

I.3 : « *Quand on a des débats, ils portent presque toujours sur la question des rôles car du rôle dépend les obligations respectives des parties, c'est donc l'exercice le plus compliqué qui implique le plus de négociations. Il faut faire des schémas, se poser la question, pour chaque traitement : qui détermine les finalités ? les outils ? les moyens* ? … »

2. Principe de minimisation des données

Le premier principe évoqué dans la partie « analyse théorique du R.G.P.D. » est celui de minimisation des données, c'est-à-dire l'obligation que les données récoltées soient limitées au strict nécessaire.

Pour les grandes entreprises, ce principe est, selon, nous, plutôt bien respecté. Les applications semblent propres au secteur et à l'entreprise. Pour les interviewés 1 et 2, par exemple, la minimisation des données est mise en œuvre par le biais du registre de traitement.

I.1 : « *On se sert du registre de traitement : pour chaque traitement, on se demande si c'est indispensable, sinon, on vire.* O*n a mis en place un monitoring pour voir ce qu'il se passe et pour diagnostiquer les erreurs*. »

I.2 *:* « *On définit nos besoins tant en termes de données que de délais de conservation lors de l'établissement du registre de traitement. »*

Les interviewés 3 et 5 insistent tous deux sur le fait que la minimisation des données doit être pensée à chaque nouveau projet.

I.3 : « *Quand on a un nouveau projet, on réalise une fiche dans laquelle on se demande quelles données sont nécessaires et on se rend vite compte, grâce à cette fiche, s'il y a un problème*. »

I.5 : « *Chaque fois qu'il y a un nouveau projet, on fait application de la minimisation et des principes de privacy by default et by design. Tous les documents sont vus et revus pour limiter les infos au strict nécessaire et éviter d'avoir des données parasites*. »

Pour les PME, en tout cas celles où le traitement de données personnelles joue un rôle-clé, ce principe semble plus contraignant. Même si certains interviewés n'ont fait part d'aucune difficulté liée à ce principe, comme par exemple les interviewés 13 et 14, une majorité d'entre eux semble avoir du mal à le respecter.

I.13 : « *Déjà avant, nous ne demandions que les informations de base*. »

I.14 : « *Nous mettons en place des systèmes et des process qui nous permettent de faire le tri, et des rappels afin de vérifier régulièrement que nous respectons le principe en question.* ***»***

I.8 : « *La minimisation des données est quasiment impossible à atteindre. »*

I.10 : « *J'avoue ne pas l'avoir encore mis en place (…) On sait que ça va être très complexe, on a des centaines de milliers d'utilisateurs, ça va prendre du temps… »*

I.9 : « *On a fait une liste de ce qui est indispensable ou pas, mais c'est difficile de connaître la limite entre ce que le règlement nous interdit de faire et ce qu'on nous oblige à faire. Par exemple, quand la Région wallonne nous demande des statistiques*

à la fin de l'année... Aussi, pour vérifier l'assurabilité, on est obligé de demander la carte d'identité. Ça nous donne un tas d'éléments dont on n'a pas spécialement besoin. C'est paradoxal. »

L'application du principe de minimisation des données semble laborieuse chez les PME et les raisons sont diverses : manque de moyens, manque de temps, ambigüité de la législation et surtout, non-appréhension de l'autorité de contrôle. Trois interviewés, interrogés sur le non-respect de ce principe, déclarent compter sur leur bonne foi. Au demeurant, pour toutes les dérogations en général, les entreprises avouent s'appuyer sur ce principe pour éviter la sanction.

I.8 : « *(…) De toute façon, je me demande sincèrement s'il y a des entreprises qui peuvent être vraiment compliant, mais on fait le maximum*. »

I.9 : « *On essaie de faire le maximum. On est déjà bien loin, et ça suffit*. »

I.10 : « *Si on se fait inspecter, il suffit de montrer sa bonne foi*. »

I.14 : « *On a fait le minimum qu'on nous demandait. De toute façon, ils ont beaucoup parlé d'amende de 4% du chiffre d'affaire mais personnellement, je n'ai jamais entendu qu'une entreprise avait vraiment eu une amende à cause du R.G.P.D.* »

Remarquons qu'a contrario, les grandes entreprises semblent craindre les représailles de l'autorité de contrôle, comme le révèle l'interviewé 4 :

« *Pour se mettre en conformité, on a dépensé plus ou moins 1 million d'euros mais c'est préférable vu le montant de la sanction…* »

Selon nous, il est regrettable que le principe de minimisation des données soit peu intégré au sein des PME. En effet, en plus d'être une obligation légale en vertu du R.G.P.D., le principe de minimisation des données est un atout pour la concurrence. Il implique un tri parmi les données afin d'éviter de noyer les données importantes. Si les entreprises prenaient le temps d'implémenter ce principe, elles en sortiraient probablement plus efficientes. L'interviewé 14 remarque, à ce propos :

« *Si les données marketing recueillies sont moins nombreuses, elles sont peut-être plus qualitatives* ».

3. Principe de transparence

Ce principe, exposé antérieurement, énonce que les personnes concernées doivent recevoir toute information relative au traitement de leurs données et que ces informations doivent être accessibles et faciles à comprendre.

L'obligation de transparence est mise en œuvre de différentes façons (politique de vie privée, affiches, prospectus, vidéos…) mais elle semble plutôt bien appliquée, que ce soit dans les PME ou dans les grandes entreprises. C'est un principe qui semble leur tenir à cœur.

I.2 : « *On met des infos sur notre site internet et sur les écrans disséminés dans l'hôpital.* »

I.3 : « *On a une fiche qui nous permet de voir qui sont les acteurs impliqués, donc quelles sont les personnes concernées et quels documents sont nécessaires pour les informer. Si on se rend compte que le projet concerne les élèves, par exemple, on réfléchit à l'intermédiaire qui les touche le mieux (…)* »

I.8 : « *On a mis à disposition une charte de protection des données sur notre site interne. Il y a toutes les infos. La transparence est importante, c'est la première chose sur laquelle il faut agir*. »

I.9 : « *Quand quelqu'un arrive, il est informé par des affiches visibles de tous et par des prospectus. Chaque accueillant a été formé pour leur expliquer ce qu'on fait avec leurs données. »*

I.13 : « *On a mis des avertissements sur notre site, l'utilisateur peut nous contacter pour plus d'infos*. »

I.12 : « *Heetch se veut proche des utilisateurs, donc nous n'hésitons pas à faire des tableaux, plutôt que d'écrire de longs textes. Nous essayons de respecter ce droit via différents supports : vidéos, etc. »*

Nous remarquons que pour l'interviewé 3, l'information est transmise par des canaux de communication différents en fonction de la personne concernée. Nous sommes d'avis que cette technique d'information « sur mesure » est la plus adaptée pour remplir au mieux l'obligation de transparence.

La question du conflit entre l'obligation d'utiliser des termes clairs et celle de fournir des informations complètes, abordée dans la partie « analyse théorique du R.G.P.D. », a été soulevée par maints interviewés, majoritairement des grandes structures.

I.1 : « *On essaie d'avoir le libellé le plus complet, le moins discutable possible de la part de l'Autorité de protection des données, mais en même temps on préfère ne pas noyer la personne dans un document de 20 pages pour expliquer ce qu'on fait. Il y a des documents pondus par des juristes qui sont imbuvables et parfois ils le font exprès ! Nous on veut éviter ça, on fait donc le minimum pour être en règle, on recouvre tous les points qui sont exigés sans rentrer dans les détails, et si les gens ont des questions, ils peuvent envoyer un mail. C'est une balance à avoir*. »

I.2 : « *La politique de confidentialité, si on veut qu'elle soit complète, elle devient incompréhensible donc on ne sait jamais si on a rempli l'objectif. Il faut trouver un juste milieu, et on modifie l'info en fonction des retours qu'on a. C'est un tuning permanent. »*

I.4 : « *C'est très difficile d'expliquer à Monsieur Tout le monde ce qu'est un algorithme par exemple, comment ça fonctionne… On a dû changer nos conditions générales et ajouter des infos qui expliquent mieux quelle donnée est utilisée, quand, comment et pourquoi, mais on ne va pas dans les détails.* »

I.12 : « *Nous essayons d'adopter un ton léger, et d'avoir des réponses et des textes ludiques et facilement compréhensibles.* »

Nous pensons que la raison pour laquelle cette difficulté se fait ressentir particulièrement dans les grandes entreprises est que ces dernières, possédant plus de moyens (humains, financiers, techniques) sont davantage armées pour faire face au R.G.P.D. et vont donc plus loin dans l'application des principes. Elles exposent des barrières que les PME, n'ayant pas les outils pour approfondir le règlement à ce point, n'envisagent même pas. Comme nous avons pu remarquer au point précédent, cette attitude est, selon nous, justifiée par le fait que les PME semblent se reposer sur le principe de bonne foi. Elles posent ainsi des limites qui leur sont spécifiques.

Pour appréhender au mieux cette incompatibilité entre exhaustivité et clarté, les entreprises fournissent des informations supplémentaires à qui le demande, et adaptent la politique de confidentialité en fonction des questions ou critiques récurrentes de la part des personnes concernées. En outre, plusieurs entreprises tentent simplement de trouver un juste milieu, même si elles semblent généralement privilégier la clarté.

4. Principe de responsabilité

Passons dès maintenant au principe de responsabilité ou principe *d'accountability*. Pour rappel, ce principe oblige le responsable du traitement à documenter ses choix en matière de protection des données. Nous avons vu que plusieurs outils sont mis à disposition du responsable du traitement pour respecter ce principe, notamment le délégué à la protection des données, le registre de traitement, et l'analyse d'impact. Passons en revue ces trois éléments.

4.1. Délégué à la protection des données

Le délégué à la protection des données est présent dans la majorité des entreprises interviewées. Le plus souvent, il est désigné sur une des bases obligatoires[275]. Même quand il n'est pas obligatoire, il semble que certaines entreprises font le choix d'en désigner un malgré tout. Le DPO joue un rôle-clé dans le respect du R.G.P.D. et les entreprises l'ont bien compris. Il est difficilement imaginable, selon nous, de se conformer au règlement sans l'aide de cette personne de référence.

L'interviewé 11 remplit, selon nous, les conditions pour être exempté de l'obligation de désigner un délégué à la protection des données. Pourtant, à la question de savoir si l'entreprise compte un DPO, il répond :

> « O*ui, c'est moi. On a des clients qui sont des consommateurs directs, on est confrontés à la protection des données via notre site internet donc il faut une personne de référence.* »

L'interviewé 14 est également hors du champ d'application de cette obligation, et en est conscient, mais a tout de même décidé de désigner un DPO :

> « *J'ai une DPO dans mon entreprise, ce n'était pas obligatoire mais ça me semblait normal d'en avoir. Elle se fait même aider par deux autres : une personne du commercial et une personne de la RH.* »

Nous avons observé, lors de nos divers entretiens, que les PME prennent généralement la décision de désigner un délégué à la protection des données parmi leur personnel, celui-ci devant se former à cette fin. C'est la question de la gestion des ressources humaines et plus particulièrement de l'internalisation des compétences, dont nous avons discuté précédemment.

> I.8 : « *J'ai plusieurs casquettes, je suis quality manager, je suis responsable du département programme scolaire, et j'ai été nommée DPO donc point de contact pour le R.G.P.D.* »

---

[275] Pour rappel, un délégué à la protection des données doit être désigné dans 3 cas : a) lorsque le traitement est effectué par une autorité ou un organisme public, b) lorsque les activités de base consistent en des opérations qui exigent un suivi régulier et systématique à grande échelle des personnes concernées, ou c) en un traitement à grande échelle de catégories particulières de données visées aux articles 9 et 10.

I.9 : « *A la base, je fais de la gestion journalière, et j'ai postulé au poste de coordinatrice. Vu que je fais de la gestion journalière, j'ai dû mettre en place le R.G.P.D. Je me suis formée, et j'ai été aidée par notre fédération (…)* »

I.10 : « *Je suis responsable de l'I.T. dans la boîte, j'ai pris la fonction de DPO. On m'a ajouté plus de travail, mais on n'a recruté personne parce qu'on est encore une petite équipe de 18 personnes.* »

I.11 : « *Nous n'avons recruté personne car nous sommes bien trop petits !* »

I.13 : *« On a demandé à une personne de l'équipe de dédier une partie de son travail à la mise en place et au suivi du R.G.P.D.* »

Dans les grandes entreprises, le DPO est parfois désigné parmi le personnel, parfois embauché aux fins spécifiques de conformité au R.G.P.D.

I.1 : « *J'ai rejoint Smals en 2009, j'étais chef de projet puis en 2016 j'ai été désigné au poste de responsable de la sécurité de l'information donc quelques mois avant le R.G.P.D., j'ai pris en charge les aspects de sécurité*. »

I.2 : « *Je suis responsable juridique de la Citadelle. A ce titre, j'ai à connaître du R.G.P.D. Nous sommes 2 DPO : un DPO juridique et un DPO informatique*. »

I.3 : « *Je suis juriste-nouvelles technologies, on m'a embauché comme responsable R.G.P.D. pour l'Administration générale de l'enseignement de la Fédération Wallonie-Bruxelles. Avant, j'étais consultant dans une boîte spécialisée*. »

I.4 : « *Je suis ingénieur informatique, on m'a embauché comme DPO*. »

I.5 : « *Je suis premier attaché juriste à la direction générale de la province de Liège depuis 2011, aujourd'hui je fais partie d'une équipe de 5 DPO*. »

I.7 : « *On a de base une équipe compliance et on a engagé un DPO qui fait maintenant partie de cette équipe.* »[276]

Il semblerait donc que les PME, probablement parce qu'elles n'ont pas les ressources nécessaires pour embaucher un spécialiste en la matière, choisissent une option différente, à savoir, la formation en interne. Cette solution a indéniablement des avantages, notamment financiers, en revanche, nous avons remarqué certaines lacunes d'un point de vue des compétences du DPO. Quand ils sont désignés parmi les employés de l'entreprise, les DPO des PME, à nos yeux, ne prennent pas le temps de comprendre le R.G.P.D. en profondeur, ou n'ont tout simplement pas la formation nécessaire pour assimiler un règlement d'une telle ampleur.

L'interviewé 8, par exemple, nous a fait part de l'aide reçue par le cabinet spécialisé, dont ils ont dû se séparer, faute de moyens financiers suffisants. La personne qui faisait le lien avec le service externe est donc devenue la personne compétente et référente pour le R.G.P.D. et a appris sur le tas. Interrogé sur les principes généraux du R.G.P.D., l'intervenant déclare « *ne faire que de la pratique* ».

L'interviewé 9 nous confie :

[276] Traduit de l'anglais.

« *En dehors du Sips, je suis consultante, c'est un sacré avantage, je me suis formée à titre personnel, mais en général ce n'est pas évident de trouver des gens qui comprennent la complexité du R.G.P.D.* »

L'interviewé 11, interrogé sur les difficultés pour traduire les obligations légales du R.G.P.D. en obligations de *compliance*, répond :

« *Je ne sais pas moi, je ne me suis pas tapé tout le texte européen.* »

De manière générale, lorsqu'il parle des actions entreprises pour se conformer au R.G.P.D., il a, à plusieurs reprises, avoué ne pas être certain d'être en conformité avec le règlement :

« *On a mis en œuvre un process qui, on suppose, est conforme à la réglementation*. »

« *On a regardé sur internet ce qu'il fallait faire, c'est très vulgarisé, ce n'est pas 'legit' à 100%, on le sait bien.* »

Partant, nous nous demandons comment les PME parviennent à mettre en pratique un règlement dont elles ne connaissent pas le contenu. En outre, vu que l'application du R.G.P.D. se fait en continu, si une entreprise comme celle de l'interviewé 8 décide de renoncer au soutien du cabinet externe, se pose la question de savoir comment chaque nouvelle difficulté sera surmontée…

Ce problème de compétence à propos des PME ne se retrouve toutefois pas au niveau des grandes structures, même quand le DPO est désigné parmi le personnel. En effet, les DPO avec qui nous avons discuté semblent être à la pointe du R.G.P.D. Cela s'explique par le fait que, contrairement aux PME, les grandes structures ont généralement parmi leur personnel un service juridique et/ou un service informatique et/ou un service de sécurité. Les PME ont rarement, en interne, une grande administration et les ressources nécessaires pour mettre en place un tel règlement.

Compte tenu du coût auquel elles s'exposent si elles choisissent de faire appel à de l'aide extérieure, les PME sont contraintes d'affecter un travailleur déjà présent dans l'entreprise à une tâche qui ne lui était pas réservée au départ et pour laquelle il n'est pas nécessairement compétent. Nous estimons que c'est précisément ce souci de compétence, propre aux PME, qui complique leur application du R.G.P.D.

4.2. Registre des activités de traitement

Le registre des activités de traitement est, à la différence du DPO, présent uniquement lorsqu'il est obligatoire, c'est-à-dire, pour faire simple, dans toutes les structures excepté dans les PME où le traitement de données personnelles est secondaire. Lorsqu'un registre est établi, c'est l'outil principal utilisé pour prouver sa conformité et remplir ainsi l'obligation *d'accountability*. La tenue du registre est, manifestement, un travail considérable pour le DPO :

I.1. : « *Pour tous les traitements que nous opérons, on peut présenter le registre de traitement, les contrats avec nos clients et fournisseurs ainsi que les analyses d'impact* (…) *On a pris la décision de démarrer le registre de traitement pour toutes les applications que nous développons : ça a été un bouleversement pour les équipes de développement car ils ne le faisaient pas avant. Tenir un registre c'est du travail mais ça permet d'être droit dans nos bottes, si on a un contrôle : aucun souci !* ».

I.2 *« Si on a un contrôle, le premier document qu'on va donner c'est le registre de traitement. On a plus de 500 traitements donc c'est très lourd*. »

I.5 : « *On a mis en place un formulaire qui va constituer la base du registre de traitement (…) On va dans l'ensemble des services provinciaux (il y en a plus de 500 !) pour compléter le registre de traitement et l'affiner et proposer en fin d'année des perspectives d'aménagement du service. (…) On a un registre de traitement qui est très complet, même trop, comparé à ce que l'Autorité de protection des données demande*. »

I.6 : « *Le registre de traitement, c'est une de mes grosses tâches. Ce n'est pas juste un acte écrit, le but c'est de mener une forme d'audit dans les différents services, dresser un bilan des pratiques et puis d'apporter une série de conseils*. »

I.12 : « *On tient un registre de traitement donc on collecte les données de manière régulière pour faire un point sur les traitements et recenser les catégories de données traitées, c'est un travail documentaire et de mise à jour en fonction des évolutions, ça demande beaucoup de travail*. »

Nous remarquons, en lisant ces extraits, que plusieurs interviewés, outre l'ampleur du travail qu'exige la tenue du registre, insistent sur le fait que c'est un travail permanent, continu. Nous comprenons dès lors pourquoi les PME exemptées de cette obligation ne s'attèlent pas à cette lourde tâche. Toutefois, alors que les autres s'appuient sur ce registre pour documenter leur conformité, ces PME semblent incapables de répondre à leur devoir *d'accountability*. En effet, concernant la manière dont elles mettent en œuvre ce principe, leur réponse fut soit « *je ne sais pas ce que c'est* » soit « *on ne le met pas en œuvre* ».

4.3. Analyse d'impact à la protection des données

Le troisième élément analysé *supra* pour prouver sa conformité au règlement est l'analyse d'impact. Elle peut être définie comme une analyse des risques liés à un traitement qui doit être effectuée a priori. Elle doit être réalisée dans certains cas uniquement : lorsque le traitement est susceptible d'engendrer un risque élevé pour la personne concernée, par exemple, lorsque l'entreprise effectue des traitements à grande échelle de données sensibles.

Les analyses d'impact sont apparemment loin d'être la priorité des PME. Nous avons exposé dans la partie « analyse théorique du R.G.P.D. » qu'il n'était pas toujours aisé de déterminer si une analyse d'impact devait être effectuée. Nous avons remarqué par le biais de nos entretiens que toutes les PME interviewées, même quand elles manipulent des données sensibles en assez grande quantité, préfèrent se considérer comme n'étant pas visées par cette obligation. Pourtant, le G29 précise qu'en cas de doute, une analyse d'impact est opportune… Cela s'explique par le fait que cette analyse est, pour les petites entreprises, éprouvante et contraignante en termes d'énergie et de temps.

Chacune des grandes structures interviewées, à l'inverse, dit avoir recours aux analyses d'impact, aussi pénibles soient-elles.

I.1 : « *On essaie d'éviter les analyses d'impact comme la peste car c'est un travail monstrueux, si on avait le choix on n'en ferait pas mais on ne décide pas, c'est le client qui l'initie et nous on contribue à la faire.* »

I.2 : *« Les analyses d'impact, c'est extrêmement lourd. Forcer les équipes à en faire, c'est ce qui a été le plus difficile, mais il faut bien passer par là, tout est potentiellement critique chez nous*. »

I.3 : « *Les analyses d'impact c'est très contraignant. Ce n'est pas vraiment notre priorité. D'abord il faut identifier les traitements, puis mettre en place les modèles,*

puis après, dans un second temps, on met en place les procédures internes et si on a l'occasion et que certains traitements sont sensibles, alors seulement on se concentre sur les analyses d'impact. »

I.5 : « *On doit en faire pour chaque nouveau projet, c'est super important (…) Une analyse d'impact approfondie a déjà permis de changer la vie d'un élève, le traitement en question menaçant son accès à la profession.* »

Pour ces grandes structures, donc, la réalisation d'analyses d'impact semble inéluctable. L'interviewé 5 semble penser qu'elles sont bénéfiques et justifiées, tandis que la majorité s'y soumet malgré elle et s'en plaint grandement, vu la complexité de la tâche.

Quelques interviewés font toutefois part de moyens pour pallier cette difficulté :

I.3 : « *Une fois qu'on a identifié les traitements les plus à risques, on fait une analyse des traitements à risque c'est-à-dire une pré-analyse pour voir si une analyse d'impact est nécessaire*. »

I.2 : « *Nous avons implémenté une analyse de risque R.G.P.D. sur les traitements avec les mesures de sécurité sur le système d'information. Cela permet de faire une analyse d'impact systématique sur l'ensemble de nos traitements.* »

5. Consentement

Le consentement, notion au cœur du nouveau règlement, est *de facto* pratiquement inexistant. La partie « analyse théorique du R.G.P.D. » nous a enseigné que les entreprises choisissaient, pour diverses raisons, de privilégier d'autres bases légales que celle du consentement. Cela nous a été confirmé par les différents entretiens, que ce soit pour les PME ou les grandes entreprises. Il y a tout de même une distinction à faire entre les deux types d'entreprises. Les grandes sont tout à fait conscientes qu'elles se passent de cette base légale et leur réponse est très explicite :

I.1 : « *Le consentement est un pilier des droits du citoyen. Néanmoins, dans le cas particulier de Smals, il n'est que rarement requis compte tenu du contexte particulier, à savoir le traitement de données internes ou dans le cadre de projet pour la Sécurité Sociale ou les Soins de Santé, dont la finalité et les données traitées sont presque toujours couverts par un contexte légal. »*

I.2 : « *Dans le domaine médical, le consentement R.G.P.D. est très peu utilisé.* »

I.3. : « *On essaie de se baser le moins possible sur le consentement. On a besoin de bases légales solides et sur la durée, donc on se base sur les obligations légales dans le cadre de nos missions de service public, et sur l'exécution du contrat. De temps en temps, effectivement, on ne pourra pas se baser là-dessus donc on aura affaire au consentement. La personne doit alors être suffisamment informée, elle peut retirer son consentement à tout moment, il faut documenter les consentements. C'est une base légale comme les autres mais c'est loin d'être la privilégiée. »*

I.5 : « *C'est loin d'être la base légale préconisée car on fonctionne beaucoup sur la mission de service public ou sur la loi. »*

I.6 : « *En 2010, on nous disait que le consentement c'était la clé mais finalement on s'est vite rendus compte que c'est une base de licéité qui pose des difficultés pratiques.*

On a tendance à aller vers d'autres bases de licéité. Déjà à cause du retrait du consentement et en plus parce qu'il peut être facilement invalidé par les tribunaux. »

Certaines PME, quant à elles, affirment utiliser la base légale du consentement (à tort, selon nous). Le consentement doit en effet, selon le R.G.P.D., être tel que son refus ne peut entraîner aucune conséquence négative. Or, ces PME expliquent que le non-consentement implique l'impossibilité de la fourniture de services ou encore un désavantage financier.

I.8 : « *Si on veut aller plus loin avec un dossier, le R.G.P.D. est invoqué et les personnes doivent marquer leur consentement. Si elles ne veulent pas le donner, ce n'est pas possible d'aller plus loin… Certaines données sont nécessaires au bon déroulement du projet*. »

I.9 : « *Avant, on ne demandait pas aux gens et on prenait toutes les données dont on avait envie. Maintenant, on doit expliquer et demander l'autorisation. Si quelqu'un nous répond qu'il ne veut pas nous donner ses infos, il sera obligé de payer sa consultation dans son entièreté parce qu'on ne pourra pas facturer donc la mutuelle ne pourra pas intervenir*. »

Toutefois, en visitant le site internet de certaines entreprises et plus particulièrement leur politique « vie privée »[277], le seul traitement justifié sur la base du consentement est celui lié à la publicité ciblée, ce qui est bien différent de ce qui a été abordé. Autrement dit, il semblerait que les PME fassent un amalgame entre *consentement* et *licéité*. Bien qu'elles ne semblent pas bien informées (c'est le problème de compétence qui refait surface), ces PME, elles aussi, ont tendance à écarter la base légale du consentement, trop instable, trop stricte, et subsidiaire.

6. Principe de *privacy by design*

Le principe de *privacy by design*, selon lequel la protection des données doit être intégrée dès la conception du traitement, est considéré par la majorité des entreprises comme une difficulté non négligeable mais il est unanimement appliqué.

I.8 : « *A chaque fois qu'on veut mettre quelque chose en place on doit se demander 'qu'est-ce que dit le R.G.P.D. ?'* »

I.1 : « *On a dû réviser l'approche projet pour y intégrer la notion de privacy by design et s'assurer de la production des activités et documentations exigées. On a adapté la méthodologie projet et on y a intégré toutes les étapes pour le respect du R.G.P.D.* »

I.5 : « *Dès qu'un projet est initié, on demande de s'assurer que les aspects du R.G.P.D. seront pris en compte*. »

I.3 : « *Les gens, quand ils constatent que leur projet va impliquer des données personnelles, doivent compléter une fiche descriptive de leur projet et, ensemble, on analyse des mesures à mettre en place pour faire en sorte que leur projet soit en*

[277] Voy. la Charte de protection des données à caractère personnel de WEP : https://www.wep.be/fr/charte-de-protection-de vos-donnees-a-caractere-personnel ou encore les conditions générales de ListMinut : https://listminut.be/p/condgen?locale=fr

conformité, on va analyser les gros points d'attention pour penser la protection des données dès le départ. C'est ce qui a le plus changé, avant, on mettait en place le projet et par après on regardait si on pouvait mettre en conformité. »

I.7 : « *Vu que j'ai participé au développement de la nouvelle division, j'ai dû garder à l'esprit la protection des données pour la création de tous les process*. »[278]

L'obligation de placer le R.G.P.D. a priori est certainement une contrainte car elle impose une charge supplémentaire et un changement par rapport aux habitudes et pratiques antérieures. Comme nous l'avons souligné dans le chapitre précédent, certains travailleurs éprouvent quelques difficultés à abandonner leur routine et adopter les bons réflexes pour se conformer aux R.G.P.D.

Toutefois, puisque l'application du R.G.P.D. se fait généralement de manière permanente, le principe de *privacy by design* correspond, sur le long terme, à un gain de temps pour l'entreprise car il facilite son application et la couvre en cas de contrôle. En effet, plusieurs références théoriques mettent en avant que le principe de *privacy by design* est une aide à la bonne application du R.G.P.D.

Les différents intervenants ont eu, selon nous, l'occasion de s'en rendre compte et c'est la raison pour laquelle ce principe est implémenté et respecté dans chaque structure, petite ou grande.

7. Code de conduite et certification

Le R.G.P.D. recommande aux entreprises d'adhérer à des codes de conduite et/ou d'être certifié « R.G.P.D. » par un organisme agréé. Cependant, à ce jour, il n'y a, à notre connaissance, aucun organisme de ce type ni code auquel se référer. Il semble donc qu'il est encore un peu tôt pour analyser ce point, en pratique. Nous avons toutefois questionné les intervenants à ce sujet.

Alors que la théorie nous a enseigné que les codes de conduite étaient particulièrement bénéfiques pour les PME, ces dernières semblent se sentir particulièrement peu concernées à ce sujet. Parmi les grandes structures, le sujet est abordé mais aucune n'adhère à ce type de mécanisme. L'effort à fournir est apparemment trop important comparé au bénéfice retiré.

I.5 : « *Il y a la norme ISO 27 001 mais c'est beaucoup trop contraignant et on ne voit pas trop la plus-value.* »

I.6 : « *On pourrait s'appuyer sur les normes ISO 9 001 ou 27 001 mais pour une entreprise qui comme nous ne travaille pas selon des procédures formelles, c'est compliqué et c'est un gros investissement…* »

[278] Traduit de l'anglais.

CONCLUSION

Ce travail avait pour ambition de découvrir comment les entreprises traduisent les obligations légales contenues dans le R.G.P.D. en obligations de *compliance*. Nous avions, de surcroît, le souhait d'opérer une comparaison entre PME et grandes structures.

Nous avons, dans un premier temps, réalisé un état de l'art du nouveau règlement. Vu l'ampleur de ce dernier, nous avons toutefois été contraints d'étudier un nombre limité de dispositions. Nous avons, dès lors, tenté de cibler les principes, obligations et mesures susceptibles de poser problème. Ensuite, nous avons interrogé 14 acteurs-clés, issus de PME et de grandes entreprises, afin d'observer comment le R.G.P.D. est implémenté et appliqué sur le terrain.

Notre première hypothèse, pour rappel, était celle-ci : le R.G.P.D. pose des difficultés pratiques, que ce soit dans sa mise en place ou dans son application. Pour tester cette hypothèse, nous avons décidé de diviser notre analyse critique en deux parties : la première concernant les difficultés fonctionnelles et notamment le problème des ressources, la deuxième, les difficultés relatives à l'application des dispositions légales.

Les interviewés nous ont effectivement fait part d'un certain nombre de difficultés, ce qui nous permet de confirmer la première hypothèse. Nous allons parcourir brièvement ces difficultés en précisant si elles sont spécifiques aux PME ou aux grandes structures. De cette façon, nous démontrerons que la deuxième hypothèse, à savoir que les PME éprouvent davantage de difficultés que les grandes structures concernant la conformité au R.G.P.D., s'avère vraie également.

Une des difficultés soulevées par les intervenants est, sans surprise, celle liée au budget. Petites, moyennes et grandes structures tentent naturellement de limiter l'impact budgétaire relatif au R.G.P.D. Par exemple, les interviewés ont unanimement refusé ou en tout cas renoncé à l'aide de services externes, leur coût étant trop élevé. Par contre, les investissements technologiques réalisés pour se conformer au règlement sont, pour certaines entreprises, inévitables. Pour les grandes structures, il « suffit » que le délégué à la protection des données (DPO) sensibilise le management afin de débloquer un *budget R.G.P.D*. Pour les PME, ce n'est apparemment pas une option. Elles font donc le nécessaire pour éviter des frais supplémentaires en compensant, quand c'est possible, leurs besoins par du temps et des moyens humains. Cette contrainte budgétaire se fait donc particulièrement ressentir chez les PME.

L'accès à l'information est, à nouveau, un problème assez spécifique aux PME. Elles estiment n'avoir pas pu se préparer correctement car des informations claires ne leur sont pas parvenues. Si leur manque de ressources complexifie la tâche des PME lors de l'application du R.G.P.D., le fait de recevoir peu d'informations ou des informations confuses n'allège en rien leur fardeau. Une attention particulière aurait dû leur être portée.

Les PME et les grandes structures doivent généralement adapter leur gestion des ressources humaines. Par exemple, la sensibilisation du personnel est indispensable pour que les travailleurs acceptent que leur quotidien professionnel soit modifié, et, a fortiori, que certaines tâches leur soient rajoutées. La nécessité, dans la majorité des cas, d'engager un DPO ou d'en désigner parmi le personnel est une difficulté supplémentaire. L'internalisation des compétences est en tout cas la solution retenue par les interviewés. Les grandes structures

embauchent un DPO ou en désignent parmi leur personnel en fonction de ce qu'elles ont « en stock », tandis que les PME n'ont d'autre choix, faute de moyens, que de désigner quelqu'un parmi les travailleurs déjà présents, quand bien même aucun d'entre eux n'aurait les compétences requises. Pour finir, la formalisation des pratiques R.G.P.D. facilite l'application du règlement. Elle est toutefois très peu présente dans les PME et dans les grandes structures complexes comme les organisations publiques.

Concernant l'application des dispositions légales, la distinction entre responsable du traitement, sous-traitant et co-responsable du traitement ne pose pas de difficulté chez les PME. Ce travail d'identification des rôles est, par contre, plus problématique pour les grandes structures avec une organisation complexe.

Le principe de minimisation des données, pourtant source d'efficience, est peu appliqué dans les PME, l'effort à fournir étant visiblement excessif. Ces entreprises, estimant qu'elles satisfont à la majorité des obligations mises à leur charge, se dispensent elles-mêmes de l'application de ce principe.

Le principe de transparence, important aux yeux des interviewés, est généralement respecté. Une application plus minutieuse du principe pourrait toutefois être faite si les responsables du traitement l'adaptaient en fonction des personnes concernées. Les grandes structures font parfois face à des difficultés que les PME ne perçoivent pas, comme le conflit entre exhaustivité et clarté. Cela s'explique par l'application moins scrupuleuse du règlement faite par les PME.

Le principe *d'accountability* est généralement incompris et donc peu respecté du côté des PME. Le registre de traitement, principal outil pour documenter sa conformité au R.G.P.D., y est pratiquement inexistant. Il représente une tâche considérable pour les entreprises, ce qui explique pourquoi celles qui en sont dispensées s'abstiennent de remplir cette obligation. Sans ce registre, toutefois, les PME risquent de manquer à leur devoir de responsabilité. Nous ne serons pas surpris de savoir que les analyses d'impact, qui demandent un travail encore plus colossal, font également défaut chez les PME.

Le consentement, instable et rigoureux, est, *de facto*, très peu utilisé. Les interviewés, PME ou grandes structures, préfèrent s'appuyer sur d'autres bases légales. Les PME semblent toutefois confondre consentement et licéité, ce qui, à nouveau, démontre un problème de compétence.

Quant au principe de *privacy by design*, il est appliqué par la majorité des interviewés. Il contribue à une application conforme au R.G.P.D.

Enfin, concernant les codes de conduite et mécanismes de certification, ils ne sont utilisés par aucun interviewé mais nous pensons qu'il est encore trop tôt pour étudier ce type de mécanisme.

Si, conformément au règlement, la situation des PME doit être prise en compte, nous constatons, dans les faits, peu de distinction. Le critère principal pour être dispensé de certaines obligations particulièrement pesantes du R.G.P.D. n'est pas celui de la taille mais bien du type et de la quantité de données traitées. Certaines PME, traitant par exemple des données sensibles, sont donc soumises aux mêmes obligations que les grandes structures, malgré la différence de moyens. Dans l'ensemble, le R.G.P.D. est plutôt bien respecté mais c'est un échec pour certaines PME qui, découragées par la complexité du règlement, manquant de temps, de personnel qualifié et de budget, font l'autruche. Par exemple, lorsqu'une obligation leur semble trop lourde, elles se disent non-concernées par cette obligation ou bien jouent sur leur bonne

foi. A force de vouloir être trop complets et trop méticuleux, les concepteurs du R.G.P.D. ébranlent le système. Comme dit le proverbe, *qui trop embrasse mal étreint…*

Les PME nécessitent une approche différente. Leur petite taille et leur manque de moyens justifient, selon nous, qu'une aide leur soit apportée, afin de faire face à une réglementation entraînant multiples mutations et bouleversant leur organisation.

A ce propos, l'Autorité de protection des données (APD) a, en 2019, réalisé une étude afin d'identifier les difficultés propres aux PME dans la mise en conformité au R.G.P.D. Le 1er janvier 2020, elle a lancé un projet, nommé « BOOST », qui a pour objectif d'accompagner et soutenir les PME dans la mise en œuvre du R.G.P.D.[279]. Cette étude se concentre principalement sur trois thèmes que l'APD estime préoccupants pour les PME. Il s'agit du principe de transparence, de l'analyse d'impact, et des concepts du « responsable du traitement » et du « sous-traitant », trois thèmes précisément abordés dans le cadre de cette étude.

279 https://www.dp-institute.eu/fr/newsletter-de-lapd-pours-les-pme/

ANNEXE

Guide d'entretien

1. Pouvez-vous vous présenter et décrire votre rôle chez xxxx ?
2. Quel est le nombre de travailleurs au sein de votre entreprise ?
3. Pouvez-vous présenter, brièvement, ce qu'est pour vous le Règlement Général de Protection des Données ?
4. Quel est votre rôle dans l'implémentation ou l'application du R.G.P.D. au sein de xxxx ? Y-êtes confronté ?
5. Pouvez-vous expliquer de quelle manière le R.G.P.D. a été abordé et mis en place au sein de xxxx ?
6. Quels ont-été, selon vous, les moyens utilisés pour mettre en place le R.G.P.D. ?
7. Quelles sont, selon vous, les conséquences relatives à la mise en place du R.G.P.D. au sein de votre entreprise ?
8. Pouvez-vous décrire comment s'applique (et/ou moyens d'application) le R.G.P.D. au sein de votre entreprise ?
9. L'application du R.G.P.D. se déroule-t-elle comme imaginée lors de la mise en place du R.G.P.D. ?
10. Quelles difficultés avez-vous rencontrées lors de la mise en œuvre et/ou l'application du R.G.P.D. ?
11. Quels sont, selon vous, les principes généraux du R.G.P.D. ?
12. Comment mettez-vous en œuvre la minimisation des données ?
13. Comment mettez-vous en œuvre la transparence ?
14. Comment mettez-vous en œuvre le principe de responsabilité ?
15. Pouvez-vous expliquer le rôle et l'importance du consentement dans l'application du R.G.P.D. ?
16. Existe-t-il, au sein de votre entreprise, des outils, techniques ou moyens utilisés pour assurer le suivi de l'application du R.G.P.D. ?
17. Avez-vous éprouvé des difficultés à traduire les obligations légales du R.G.P.D. en obligations de *compliance* (mise en conformité pratique) ?
18. *Avez-vous quelque chose à rajouter ? Un sujet sur lequel vous voulez revenir ?*

BIBLIOGRAPHIE

LEGISLATION

Traité sur le Fonctionnement de l'Union européenne (TFUE).

Traité sur l'Union européenne (TUE).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016.

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, 23 novembre 1995.

Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, annexe, art. 2, *J.O.C.E.*, L 124, 20 mai 2003.

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

JURISPRUDENCE

Cour eur. D.H. (gde ch.), arrêt *S. et Marper c. Royaume Uni*, 4 décembre 2008, §95.

Av. gén. E. SHARPSTON, concl. C.J.U.E., arrêts *Volker und Markus Schecke GbR c. Land Hessen*, 17 juin 2010, affaires jointes C-92/09 et C-93/02, ECLI:EU:C:2010:353, point 71.

C.J.U.E., arrêt *Google Spain SL et Google Inc contre AEPD et Mario Costeja Gonzalez*, 13 mai 2014, C-131/12, ECLI:EU:C:2014:317, point 33.

C.J.U.E., arrêt *Novak c. Data Protection Commissionner*, 20 décembre 2017, C-434/16, ECLI :EU :C :2017 :994, points 35 et 62.

C.JU.E. (gde ch.), *Unabhängiges Landeszentrum für Datenschutz SchleswigHolstein/Wirtschaftsakademie Schleswig-Holstein GmbH* , 5 juin 2018, C-210/16, ECLI:EU:C:2018:388, point 44.

C.J.U.E., (gde ch.), arrêt *Bundesverband der Verbraucherzentralen und Vervraucherverbände – Verbraucherzentrale Bundesverband eV/ Planet 49 GmbH*, 1er octobre 2019, C-673/17, ECLI:EU:C:2019:801.

A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, p. 7. https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO_fr.pdf

Civ. néérl. Bruxelles (24e ch.), 16 février 2018, *R.A.G.B.* 2019/9, p. 698.

DOCTRINE

AFNOR, Association française de normalisation, 1995, cité par E. FIMBEL, « Nature et enjeux stratégiques de l'externalisation », *Revue française de gestion*, vol. n° 143, 2003/2, p. 27 à 42.

ALBRECHT, J.P., « How the GDPR will change the world », *EDPL*, vol. 2, no. 3. 2016, p. 287 à 289.

ANDOULSI, I., « Le Règlement général sur la protection des données personnelles : un état des lieux après plus d'un an d'entrée en application », *Ann. dr.*, vol. 78, 2018/3, p. 471 à 484.

BALTHAZAR, T. en RAEYMAEKERS, P., *Gegevensbescherming in de zorg. Een praktische gids bij de GDPR*, Brugge, die Keure, 2018.

BEELEN, A., LAMBRECHT, P. et DECHAMPS, F., *Guide pratique du RGPD: fiches de guidance*, Bruxelles, Bruylant, 2018.

BESSON, D. et OLABA, A., « Une approche contextualiste des pratiques de gestion des compétences par l'informel : une enquête sur quatre PME », *Annales des Mines – Gérer et comprendre*, vol. 128, 2017/2, p. 14 à 33.

CHATRY, S., « Les données collectées par l'entreprise : documenter sa conformité au RGPD », *L'entreprise face aux défis du numérique*, J.-M. Moulin, S. Chatry et A. Riera (dir.), Paris, Mare & Martin, 2018.

COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, « RGPD. Vade-mecum pour les PME », 2018.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises », 2018.

DE TERWANGNE, B., ROSIER, K. et LOSDYCK, B., « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E*, n° 242, 2017, p. 302 à 316.

DE TERWANGNE, C., DEGRAVE, E., DELFORGE, A. et GÉRARD, L. *La protection des données à caractère personnel en Belgique. Manuel de base*, Bruxelles, Politeia, 2019.

DE TERWANGNE, C., « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020, p. 7 à 59.

DEFÉLIX , C. et RETOUR, D., « La gestion des compétences dans la stratégie de croissance d'une PME innovante : le cas Microtek », *Revue internationale P.M.E.*, 16 (3-4), 2003, p. 31 à 52.

DEFÉLIX, C., « La gestion des compétences au défi de la mesure : des réceptions différenciées de la norme ISO 9001, Version 2000 », *La GRH mesurée*, Actes du XVe congrès de l'AGRH, Montréal, tome 3, cité par Antoine, M. *et al*, « La démarche compétences dans la littérature en gestion », *Faut-il brûler la gestion des compétences : Une exploration des pratiques en entreprise*, F. Pichault (dir.), Louvain-la-Neuve, De Boeck Supérieur.

DEGRAVE, E., CANON, P., GÉRARD, L., GRÉGOIRE, D. et OURARI, Y., *L'ABC du RGPD : dictionnaire pratique à destination des administrations.* Namur, Union des villes et communes de Wallonie, 2018.

DEHOUSSE, F., « L'enfer bureaucratique du Règlement sur les données personnelles », *Le Vif*, n°3, 2019, p. 66.

DELFORGE, A., *Les obligations générales du responsable du traitement et la place du sous-traitant*, Bruxelles, Larcier, 2018.

DESGENS-PASANAU, G., *La protection des données personnelles : le RGPD et la nouvelle loi française,* 3e éd., Paris, LexisNexis, 2018.

DOORNAERT, J., *Le règlement général sur la protection des données et sa mise en oeuvre en droit belge*, Waterloo, Kluwer, 2019.

DULAC, T. ET DELOBBE, N., « Relations entre les modes de gestion du capital humain, la relation d'emploi et les attitudes et comportements au travail », *La société flexible*, M. de Nanteuil-Miribel et A. El Akremi (dir.), Toulouse, ERES, 2005, p. 179 à 203.

EJZYN, A. et VAN DEN BERGHE, T., « Avant-propos », *Cybersécurité et RGPD : protégez-votre PME*, Limal, Anthemis, 2018.

FAIFR, A. and JANUSKA, M., « Companies' readiness of GDPR and implementation barriers », *International Institute of Social and Economic Sciences*, 2018, p. 31 à 49.

FOCQUET, A. et DECLERCK, E., *Gegevensbescherming in de praktijk,* Antwerpen, Intersentia, 2019.

FREITAS, MDC. and MIRA DA SILVA, M., « GDPR Compliance in SMEs: There is much to be done », *Journal of Information Systems Engineering & Management*, vol. 3, issue 4, 30, 2018, p. 2 à 7.

GAUDEMET, A., « Qu'est-ce que la compliance ? », *Commentaire*, 2019/1, n° 165, p. 109 à 114.

GIAKOUMOPOULOS, G., BUTTARELLI, G. et O'FLAHERTY, M., *Manuel de droit européen en matière de protection des données.* Conseil de l'Europe, 2018.

GOLA, R., « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *LEGICOM*, vol. 59, 2017/2, p. 29 à 38.

HICK, J. et INVIJAJEV, R., *RGPD : quel impact sur la gestion du personnel ?* Waterloo, Kluwer, 2018.

IT GOVERNANCE (ORGANIZATION). PRIVACY TEAM., *EU General Data Protection Regulation (GDPR) : an implementation and compliance guide,* Ely, IT Governance Publishing, s.d, 2017.

MERCK, B. et SUTTER, P.-E., « Présentation », *Gestion des compétences, la grande illusion. Pour un new deal "compétences"*, B. Merck et P.-E. Sutter (dir.), Louvain-la-Neuve, De Boeck Supérieur, 2009, p. 38.

NERBONNE, S., « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *LEGICOM*, 2009/1, n° 42, p. 37 à 46.

PAILLÉ, P. et MUCCHIELLI, A., *L'analyse qualitative en sciences humaines et sociales*, Paris, Armand Colin, 2012.

PARSA, S., « Le R.G.P.D. et la profession d'avocat, au-delà du secret professionnel et du principe de confidentialité », *Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), vol. 195, Liège, CUP, Anthemis, 2020, p. 127 à 165.

PARSA, S., « Le RGPD, dans la pratique – Entre principes généraux et obligation, que faire ? », *R.G.F.C.P.*, 2019/4, p. 27 à 35.

POLIDORI, M., « L'arrêt *Google Spain* de la CJUE du 13 mai 2014 et le droit à l'oubli », *Civitas Europa*, 2015/1 n° 34, p. 243 à 266.

PONSART, C. et ROBERT, R., « Le règlement européen de la protection des données personnelles », *J.T.*, 2018/20, n°6732, p. 421 à 438.

POULLET, Y., « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.* n° 122-123, 2019, p. 3 à 37.

REDING, V., « Tomorrow's Privacy. The upcoming data protection reform for the European Union », *International Data Privacy Law*, vol. 1, 2011, p. 3 à 5.

SAMMAN, T. et DREVON, M., « De la réglementation à la compliance, encadrer et accompagner la transformation numérique », *Les défis du numérique*, D. Rahmouni-Syed Gaffar (dir.), Bruxelles, Bruylant, 2019.

SAUVAYRE, R., *Les méthodes de l'entretien en sciences sociales*, Paris, Dunod, 2013.

SHI LI, Z., WERNER, C., ERNST, N. AND DAMIAN, D., « GDPR Compliance in the Context of Continuous Integration », *IEEE Transactions on software engineering*, 2018, p. 1 à 14.

TAEYMANS, M., « Facebook mag geen gegevens van-niet gebruikers verzamelen », *Juristenkrant*, 2020, p. 3.

TAMBOU, O., *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020.

TANKARD, C., « What the GDPR means for businesses », *Network Security*, *2016*, p. 5 à 8.

TIKKINEN-PIRI, C., ROHUNEN, A. and MARKKULA, J., « EU General Data Protection Regulation: Changes and implications for personal data collecting companies », *Computer Law & Security Review*, 2017, p. 1 à 20.

VAN ALSENOY, B., *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Cambridge, Intersentia, 2019.

VAN ASBROECK, B. et DEBUSSCHE, J., « Les obligations de « compliance » des entreprises », *Vers un droit européen de la protection des données*, B. Docquir (dir.), Bruxelles, Larcier, 2017, p. 89 à 133.

VAN CAMPENHOUDT, L. et QUIVY R., *Manuel de recherche en sciences sociales*, Paris, Dunod, 2011.

VANDENBUSSCHE, D., « Qu'est-ce qu'un consentement valable au sens du RGPD ? », 10 octobre 2018, disponible sur : https://jura.kluwer.be/secure/documentview.aspx?id=kl2265042&state=changed.

VIAL, S., *L'être et l'écran. Comment le numérique change la perception*, Paris, Presses Universitaires de France, 2013.

AVIS, LIGNES DIRECTRICES ET DOCUMENT DE TRAVAIL DU GROUPE DE TRAVAIL « L'ARTICLE 29 »

Groupe de l'article 29, « Avis n°3/2010 sur le principe de la responsabilité », WP 173.

Groupe de l'article 29, « Avis n°1/2010 sur les notions de responsable du traitement et de sous-traitant », WP 169.

Groupe de l'article 29, « Avis n°10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) », W 128.

Groupe de l'article 29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » WP 260 rev.01.

Groupe de l'article 29, « Lignes directrices sur le consentement au sens du règlement (UE) 2016/679 » WP 259 rev.01.

Groupe de l'article 29, « Avis n°15/2011 sur la définition du consentement », WP 187.

Groupe de l'article 29, « Avis n° 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel », WP 48.

Dix-septième rapport du groupe de travail « Article 29 » sur la protection des données, *Justice et consommateurs*, 2013.

Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01.

Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé aux fins du règlement (UE) 2016/679 », WP 248 rev.01.

European Data Protection Board, « Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 », version 2.0, 4 June 2019.

RAPPORT SUR LA PROPOSITION DU REGLEMENT

Comité LIBE du Parlement européen, 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, COM(2012)0011, C7-0025/2012, 2012/0011(COD), 21 novembre 2013.

SOURCES INTERNET

https://www.dp-institute.eu/fr/newsletter-de-lapd-pours-les-pme/

https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-le-code-de-conduite

https://www.cnil.fr/fr/la-certification

https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi

https://www.wep.be/fr/charte-de-protection-de vos-donnees-a-caractere-personnel

https://listminut.be/p/condgen?locale=fr