Juliette Grossmann

Master Ethires 2019 - Emmanuel Picavet

RSE et acquisition d'informations
Etude de cas : le Règlement Général de la Protection des Données

La commission européenne redéfinit en 2011 la responsabilité sociétale des entreprises (RSE) comme « la responsabilité des entreprises vis-à-vis des effets qu'elles exercent sur la société », et ce pour tous types d'organisations, quelle que soit sa taille. La RSE demande la prise en compte des attentes des parties prenantes, le respect des lois en vigueur et doit être en accord avec les normes internationales de comportement. La RSE ne se limite pas à un respect de la réglementation, c'est une attitude proactive, qui se fonde sur l'idée que l'entreprise est responsable des externalités négatives qu'elle entraîne ou influence. La RSE peut aussi désigner les stratégies mises en place dans l'ensemble d'une organisation et dans ses relations avec ses parties prenantes pour répondre aux exigences nouvelles de responsabilisation. Le concept de responsabilité sociale de l'entreprise et l'étendue de la responsabilité de celle-ci se sont largement modifiés au cours des 50 dernières années comme le montre Philip Cochran, mais ce qui semble se perpétuer à travers toutes les définitions est que la RSE se présente comme une réponse à une crise de confiance et un besoin de garanties internationales et locales d'une certaine éthique. La responsabilité se définit comme l'obligation de répondre de ses actes et d'en assumer les conséquences. Dans un monde où les organisations et les entreprises ont un pouvoir grandissant et un impact mondial, il est devenu indispensable que les pouvoirs publics et les organismes internationaux s'emparent de la question pour assurer un certain contrôle de ces impacts, en ouvrant un dialogue entre la monde des affaires et la société civile. C'est dans cette perspective que le Règlement Général de la Protection des Données est entré en vigueur le 27 avril 2016 pour encadrer les droits des personnes et la responsabilité des organismes dans le traitement de données personnelles. Le RGPD oblige toute organisation privée ou publique à mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'assurer la conformité de son organisation au règlement, et d'être en mesure de se justifier et la démontrer à tout moment. Cela amène ainsi à poser la question de la mesure des effets et de la capacité de l'organisme à rassembler les informations nécessaires pour assurer une telle conformité. La notion d'acquisition d'informations ramène au deux aspects de la définition du terme acquisition qui désigne à la fois l'action d'acquérir que la chose acquise. Il apparaît ainsi qu'il y a une double responsabilité de l'entreprise, celle vis-à-vis de l'information acquise, qui amène au problème de la protection des données, et celle vis-à-vis de l'obtention d'information, qui amène au problème plus stratégique du dialogue et de l'accès aux informations. Nous étudierons donc ces deux aspects en s'appuyant sur une analyse du RGPD, s'abord en montrant que la protection des données implique un devoir d'information et de transparence, puisque pour cela l'organisme se retrouve face à des problèmes techniques et contextuels liés à l'obtention d'informations. Pour finir nous verrons que l'introduction du DPO dans le RGPD constitue la matérialisation du besoin d'échanges d'informations et de dialogue transparent entre le régulateur, l'organisme, et ses parties prenantes, et que cette transparence est la condition de la RSE.

I) La responsabilité de l'organisation vis-à-vis des informations acquises

1. La protection des données : un droit des utilisateurs et une responsabilité des organisations

Le premier niveau auquel l'acquisition d'information est un enjeu de la RSE est celui de l'acquisition au sens de l'information acquise. Les organisations traitent de plus en plus d'informations sensibles de la société civile, et il apparaît indispensable de faire entrer la protection de ces informations dans la RSE. La protection des données personnelles s'inscrit dans l'esprit de la Commission Européenne dans les valeurs d'Ethique**,** de Respect des Droits de l'Homme et de la protection du Consommateur, qui sont citées dans sa déclaration de 2011. Elle y rappelle que « information des consommateurs et transparence » est l'un des huit domaines d'actions prioritaires pour l'action de l'UE en RSE. Le règlement général de protection des données ou RGPD qui est en vigueur depuis le 27 avril 2016, et d'application directe depuis le 25 mai 2018, s'inscrit dans cette volonté de définir les droits des personnes dans un monde numérique. C'est un règlement de l'Union Européenne, qui vise aussi à harmoniser les considérations de RSE et le droit à la vie privée des consommateurs entre les pays d'Europe. Dans les articles 1 et 4, le RGPD définit la protection des données à caractère personnel comme un droit fondamental, et considère que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité ». Ce règlement a pour but à la fois de définir les droits des individus sur les informations qu'ils donnent aux organisations, et du coup de responsabiliser les entreprises sur le traitement qu'ils en font. A partir du moment où l'individu a un droit sur ses données, il en va de la responsabilité seule et entière de l'organisation de mettre en place les processus nécessaires au respect de ce droit. Le RGPD propose ainsi de réguler la gestion par les organisations des données qu'ils traitent et qui sont de plus en plus vulnérables : entre les menaces de cybercriminalité qui augmentent, et les quantités de données de plus en plus importantes utilisées par les organisations, il apparaît comme une nécessité d'en assurer la sécurité par de nouveaux modes de gouvernances et de nouvelles mesures. En effet il s'agit aussi d'accompagner les entreprises dans la transition numérique en les invitant à renouveler leurs modes de fonctionnement à l'aune de la numérisation de la création de valeur. Il apparaît ainsi que l'acquisition d'information s'accompagne inévitablement d'une responsabilité vis-à-vis du traitement de celle-ci.

2. Obligation d'accessibilité et de compréhensibilité : le devoir d'information

Un des points centraux du RGPD est le devoir d'information qui accompagne l'acquisition d'informations. En d'autres termes, si une organisation acquiert des informations dites personnelles (c'est-à-dire « toute information se rapportant à une personne physique identifiée ou identifiable »[1]), elle se voit obligée non seulement de protéger au sein de son système ces données des violations et des cyber attaques, mais aussi d'informer les concernés du traitement des données récoltées. Définie dans les articles 12, 13 et 14, cette obligation d'information contraint les organisations à fournir une série d'informations sur notamment l'intention et l'identité du responsable du traitement de données, sa finalité, et sa base juridique. Ceci est une application dans l'entreprise du droit de l'individu à connaître l'usage

[1] Chapitre 1, article 4, RGPD, 2016/679

qui sera fait de l'information qu'il divulgue, et lui assurer un droit de consentement réel. Ce devoir d'information impose une information claire et complète : « Le principe de transparence 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. »[2] Il faut d'abord que l'information soit accessible, que l'individu soit amené facilement à l'emplacement de l'information. Il faut ensuite qu'elle soit compréhensible, c'est-à-dire qu'elle s'adapte à la personne à qui elle s'adresse pour que la personne puisse consentir à donner ses informations personnelles en tout connaissance de cause. Il faut enfin qu'elle soit claire et simple, c'est-à-dire de proposer une information courte et adaptée aux supports sur lesquels elle sera communiquée. Ces trois modalités de l'information nous montre qu'il ne s'agit pas simplement de transparence au sens négatif, mais plutôt au sens positif : « qui est clair et lumineux »[3]. Etre transparent, pour l'organisation, ça veut dire devoir fournir aux usagers des informations claires et distinctes sur les traitements de leurs données, cela suppose ainsi une attitude proactive de création de nouveaux contenus et de nouveaux supports. Le RGPD invite donc les organisations à créer des espaces d'interaction avec les consommateurs et ouvrir une relation consentante mutuelle : l'usager fournit à l'organisation une information de manière volontaire, et en retour celle-ci doit fournir une information claire sur ce qu'il en fait. Comme on le verra plus tard, la communication, via principalement les rapports d'activités des entreprises, est très importante dans la mise en place d'une stratégie de RSE. Mais ce qui nous importe ici c'est qu'il s'agit moins d'une démonstration par l'entreprise de ses activités de RSE, qu'un échange d'information. Cet échange requiert donc un type de relation et de dialogue entre les consommateurs et les entreprises qui est assez inédit. Il s'agit, pour rétablir la confiance entre la société civile et les entreprises, de créer un nouveau type d'échange d'informations.

3. <u>De la transparence à la confiance</u>

Il apparaît ainsi que l'enjeu de l'information, en tant qu'elle est acquise par l'entreprise, est celui de la création d'une relation de confiance entre celui qui fournit la donnée et celui qui la traite. La Commission européenne le dit : « La crise économique et ses conséquences sociales ont quelque peu mis à mal la confiance des consommateurs et le degré de confiance dans les entreprises. Elles ont cristallisé l'attention du public sur la performance sociale et éthique des entreprises. » On comprend ainsi que la RSE est en grande partie une réponse à l'enjeu de rétablissement de la confiance entre la société civile et les entreprises. Le RGPD s'inscrit dans ce besoin de confiance entre les citoyens et usagers, et les entreprises, sur les informations qu'elle accumule sur les concernés. On a vu que la protection des données était un enjeu majeur de la RSE. Mais si la notion de confiance a du sens quand il s'agit d'organes publics, puisqu'ils doivent servir les citoyens, peut-on parler de confiance quand il s'agit d'une relation commerciale entre un consommateur et une entreprise qui a forcément une intention de défense d'intérêts privés ? En effet la confiance est consensuellement définie en 1998 par Rousseau *et al*, par « un état psychologique comprenant l'intention d'accepter un état de vulnérabilité sur la base d'attentes positives à l'égard des intentions ou du comportement d'autrui ». Mais on ne peut pas envisager que les entreprises

[2] Considérant 58, RGPD, 2016/679

[3] Dictionnaire du Centre National de Ressources Textuelles et Lexicales (CNRTL)

aient des intentions positives, alors que leur objectif premier est le profit privé. Il est donc inévitable de penser différemment la confiance, non pas sur l'idée que les entreprises doivent avoir une intention positive pour que les individus leur fasse confiance, mais plutôt sur la notion de transparence, c'est-à-dire l'idée que ce qui est considéré sensible ou vulnérable (qui sont les données des usagers) soit laissé à la portée de celui à qui cela appartient. On n'attend pas aveuglément que les entreprises fassent de nos données des traitements bienveillants, mais la confiance sera basée sur le fait que les entreprises aient un minimum de pouvoir de discrétion, c'est-à-dire sur la transparence. La professeure américaine Suzanne J Piotrowski définit la transparence comme un flux ouvert d'informations. L'idée de la transparence est associée à celle d'imputabilité : à partir du moment où les informations sont divulguées, les individus peuvent surveiller les activités des entreprises, et celles-ci sont poussées à satisfaire leurs usagers. La transparence apparaît ainsi comme un moyen incontournable de garantir le droit des données personnelles, et permet dans un deuxième temps le rétablissement de la confiance. La confiance ici est donc basée sur une attitude proactive des entreprises et des usagers, non pas sur un état de confiance, mais plutôt sur un flux, un mouvement d'échange d'informations entre les uns et les autres. Ainsi la transparence n'est plus un symptôme de manque de confiance, mais plutôt une garante de la confiance en tant qu'elle établit un nouveau type de relation entre les parties prenantes, basée sur l'information.

Il apparaît ainsi qu'une donnée personnelle est une information sensible acquise par les organisations, qui les oblige à une certaine responsabilité quant à son traitement. L'entreprise a une responsabilité vis-à-vis de l'information qu'il acquiert, et par extension, de l'information qu'il doit restituer à l'usager en retour, basé sur le principe de transparence demandé par le RGPD. Il s'agit donc moins d'une acquisition d'information par l'entreprise (informations qui sont fondamentales à l'activité commerciale de la plupart des entreprises, particulièrement celles du secteur numérique), qu'un échange d'information. L'usager se voit aussi obligé d'user de son droit en acceptant activement l'usage de ses données personnelles. Pour pouvoir exercer cette responsabilité vis-à-vis de l'information acquise, l'entreprise se retrouve face au problème de devoir obtenir les informations nécessaires à la RSE.

II) La responsabilité vis-à-vis de l'obtention d'informations

1. L'analyse d'impact : nécessité, proportionnalité

Puisque la RSE est une affaire proactive, comme on l'a vu, il s'agit pour les entreprises de pouvoir assurer la transparence de leurs activités. Le cadre RSE de l'OCDE, qui est le plus exhaustif et contraignant juridiquement, demande une « transparence de l'information ». Celle-ci s'inscrit principalement dans l'obligation de produire des mesures d'impact et des rapports de RSE qui en tiendraient les comptes. En effet il apparaît inévitable pour pouvoir parler de la responsabilité d'une entreprise vis-à-vis de l'impact qu'elle a socialement et sur l'environnement, qu'elle puisse mesurer cet impact. Cette mesure présente plusieurs difficultés en terme d'acquisition d'informations. Il faut que l'entreprise puisse récolter les informations nécessaires à cette analyse, et qu'elle puisse justifier de la nécessité de faire ce type de mesure par rapport à ce type d'activité. L'analyse d'impact est forcément corrélative de l'activité particulière d'une organisation, et même du type d'organisation

(quand il s'agit de récolter des données, il ne s'agit pas de la même mesure d'impact que quand il s'agit de sous-traiter à une entreprise chinoise, même si cela se passe au sein de la même organisation). En ce qui concerne le RGPD, il propose comme outil d'analyse d'impact l'AIPD, Analyse d'Impact sur le Protection des Données. Celle-ci a pour objectif de contraindre les entreprises à se responsabiliser sur les impacts de leurs activités, pour pouvoir être en conformité avec le droit à la vie privée défendu par le RGPD. En effet, plus l'impact est risqué, plus la sécurité doit être renforcée. Il est fondamental de pouvoir réunir les informations nécessaires à la mise en place de la protection des données recueillies, et de pouvoir prouver à la CNIL que ce travail d'analyse a été fait pour éviter les sanctions. Cette analyse d'impact se fait en trois parties : d'abord la description du traitement de données, puis une évaluation de la nécessité et de la proportionnalité de celui-ci, et enfin une étude de la sensibilité des données traitées et des risques potentiels pour la vie privée. L'article 5 dispose que « les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Le principe de nécessité correspond à ce que la CNIL caractérise de minimisation des données, c'est-à-dire une analyse de la pertinence de la finalité du traitement de donnée. Le principe de proportionnalité correspond à l'étude du rapport entre les finalités du traitement de données et la nature des données. En effet il faut que la sensibilité de la donnée récoltée soit proportionnelle à la nécessité de son traitement : plus une donnée est sensible, plus la finalité de son traitement doit être pertinente. Par exemple, la CNIL a jugé illicite en octobre dernier l'utilisation de caméras et portiques intelligents dans des lycées à Nice et Marseille pour surveiller les entrées. Un tel usage des données personnelles, basé sur une technologie de reconnaissance faciale, a été considérée « disproportionnée par rapport aux enjeux de sécurité et intrusive pour les élèves »[4]. La Région Sud n'a pas pu démontrer la proportionnalité de l'enjeu de sécurité par rapport à un traitement de données aussi sensibles que celles utilisées pour la reconnaissance faciale, étant donné en plus le caractère particulièrement sensible des données d'individus mineurs. Il apparaît ainsi que l'analyse d'impact pose une difficulté pour les organisations à savoir quelles informations réunir pour être en conformité avec le RGPD.

2. <u>Obtenir des informations des parties prenantes : responsabilité, loyauté, licéité</u>

Un autre problème que pose l'acquisition d'informations dans la mise en place de la RSE dans les organisations est celui de l'obtention d'informations entre les parties prenantes. En effet, autant pour produire les mesures d'impact que dans le devoir d'information, il s'agit de collecter ou de communiquer sur des informations qui ne sont pas issues de l'organisation en tant que tel, mais des parties prenantes (ça peut être des sous-traitants, des usagers, des collaborateurs, etc). Comme on a vu en première partie, l'entreprise a une responsabilité quant au traitement des données qu'elle récolte, et se voit ainsi obligée de donner une information claire et transparente. Mais pour cela, il faut qu'elle ait la possibilité de produire une telle information. Cela pose problème à plusieurs niveaux : d'abord celui de la récolte d'informations auprès des collaborateurs. Si l'entreprise est responsable du traitement des données, elle est toujours en relation avec d'autres entreprises ou sous-traitants qui participent à ce traitement, et qui ne fournissent pas forcément une information claire et transparente que l'entreprise est pourtant contrainte de fournir. Particulièrement en ce qui concerne les

[4] Communiqué de la CNIL

entreprises du numérique, qui comme le montre le sociologue Antonio Casili dans son essai *En attendant les robots*, sont fondées sur la division du travail en micro-tâches externalisées. Un deuxième problème est l'acquisition d'informations auprès des consommateurs. En effet, pour que l'entreprise soit conforme aux exigence de la RSE portées par le RGPD, il faut qu'elle puisse faire consentir par les concernés au traitement de leurs données personnelles. En effet, sauf exceptions, « le traitement n'est licite que si la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques »[5]. Il en va de la responsabilité de l'organisation de pouvoir acquérir des informations quant au consentement du consommateur à la récolte et au traitement de ses données, ce qui concrètement est très difficile à mettre en place. La numérisation des activités commerciales et publiques a rendu la récolte permanente de données indispensable au bon fonctionnement des organisations. Antonio Casili défend même l'idée que cette récolte invisible et permanente de données des usagers fait partie intégrante du modèle économique des plateformes. A partir du moment où il est dans l'intérêt des organisations d'invisibiliser l'acquisition de données, et que récolter le consentement des consommateurs reviendraient à revoir tout l'organisation communicationnelle, il apparaît difficile de contraindre les organismes à de telles dispositions. Cette récolte frauduleuse de données est appelée déloyale par le RGPD, qui impose dans l'article 6 que « les données [soient] collectées et traitées de manière loyale et licite ». Le principe de loyauté exige la mise en place d'une interface qui permette au consommateur de consentir au traitement, et qui exige de l'organisme qu'il respecte jusqu'au bout son engagement : si les modalités du traitement de données d'un individu changent en cours de route, peu importe la raison, il faut pouvoir l'en avertir et lui laisser la possibilité de revenir sur son consentement de départ. Il faut donc que non seulement l'organisation soit capable de demander le consentement de la personne qui fournit ses données personnelles, mais en plus qu'elle soit capable de maîtriser derrière toute la chaîne du traitement de ces mêmes données, au risque de déroger au principe de loyauté et ainsi rendre illicite son activité. Un dernier problème est qu'il est théoriquement impossible de réunir toutes les informations nécessaires autant pour mesure l'impact de ses activités que pour juger l'étendue des risques encourus d'un traitement de données : l'analyse d'impact (sur laquelle se base les mesures prises pour assurer le droit et la sécurité des informations personnelles) est à une échelle tellement vaste et complexe que cela demanderait une quantité d'informations que personne ne peut fournir. Ceci est d'autant plus vrai dans un monde numérique où les données circulent à une vitesse infernale et où les notions de propriété et de sécurité sont remises en cause. Il s'agit donc de savoir comment imposer aux organismes une acquisition d'information qui puisse être contrôlable et personnalisable, tout en étant respectueuse des libertés individuelles et publiques.

3. <u>L'interprétabilité de la norme</u>

La question qui se pose alors c'est : quelle acquisition d'information est demandée ? Rappelons que le RGPD est un règlement, c'est-à-dire un ensemble de règles et de principes qui cherchent à encadrer un type de pratique. Comme tout règlement il assure deux fonctions : encadrer ce qui se fait ou non dans le déploiement d'une activité, et laisser de l'espace entre les règles pour permettre une certaine adaptation des règles aux cas particuliers. Cette double

[5] Chapitre 2, article 6, RGPD, 2016/679

fonction est d'autant plus vraie quand il s'agit de RSE à cause de la double injonction qu'elle représente : à la fois celle du respect de règles internationales ou locales qui intègrent la responsabilité de l'entreprise, et celle de la bonne volonté des organisations à prendre en compte leurs externalités et leurs responsabilités liés aux impacts de leurs activités. Il s'agit donc pour le régulateur de trouver un équilibre entre droit faible et droit fort, entre contrainte et incitation, pour pousser l'économie plutôt que la brider. Cet équilibre repose en partie, pour le RGPD, dans une certaine interprétabilité de la norme. Il y a plusieurs raisons qui la nécessitent, entre autres le fait que la RSE s'applique à toutes les formes d'organisations (petites, grandes, publiques, privées, plateformes et entreprises traditionnelles) ce qui demande une adaptabilité des règles ; que les traitements de données personnelles peuvent prendre une multitude de formes et de finalités ; que la stratégie de RSE dépend des moyens qui peuvent être mis en place au sein d'une structure. Les problèmes liés à l'acquisition d'information démontrent bien ce dernier point. En effet, on voit bien que les analyses d'impact et la nécessité d'échanges d'informations entre les parties prenantes demande à l'entreprise de pouvoir repenser son organisation, de pouvoir créer un nouveau type de dialogue avec ses collaborateurs et ses consommateurs, et de pouvoir mettre les moyens nécessaires pour produire toutes les informations nécessaires à la RSE. L'acquisition d'informations nécessaire à la conformité au RGPD dépendra forcément des moyens matériels et de l'adaptabilité de l'organisation. Cela ne veut pas dire que tout le monde ne peut pas s'y conformer, au contraire, la norme est pensée dans cette perspective, d'où une certaine interprétabilité et adaptabilité des règles. Toute la sémantique du RGPD est orientée vers l'idée que nous vivons dans un monde de plus en plus numérique, où tous les organismes (privés ou publics) se retrouvent à utiliser du traitement de données à une moment donné de leur chaîne de création de valeur, et il est du devoir d'un organisme d'état d'accompagner toutes les structures dans cette transition. Comment la CNIL compte-t-elle alors accompagner les organismes, et qu'est-ce que cela implique pour elles ?

III) L'échange d'informations entre l'organisme, le régulateur, et les parties prenantes : l'exemple du DPO

1. L'obligation de conformité au RGPD

A partir du moment où le RGPD est présenté comme un texte de RSE, cela implique qu'il s'inscrit dans la volonté des organisations publiques à encadrer les traitements de données et accompagner les entreprises dans les nouveaux enjeux de sécurité. L'enjeu du RGPD est avant tout celui de la conformité : comment énoncer des règles qui puissent être appliquées par les organismes, et comment les accompagner dans cette conformité ? Dans l'introduction de son guide 2018 pour la sécurité des données personnelles, à l'attention des organisations, la CNIL assume son rôle d'accompagnement des organisations : « il est parfois difficile, lorsque l'on n'est pas familier de ces méthodes, de mettre en œuvre une telle démarche et de s'assurer que le minimum a bien été mis en oeuvre. Pour vous aider dans votre mise en conformité, ce guide rappelle ces précautions élémentaires qui devraient être mises en œuvre de façon systématique. » On retrouve ici l'idée que le RGPD ne se veut pas contraignant mais cherche à pousser les entreprises à se réorganiser pour intégrer de manière systématique la protection des données. Toute réorganisation demande du temps, de

l'adaptation, et l'approche consiste à penser que des règles pas trop contraignantes permettent aux entreprises d'insérer au fur et à mesure les nouvelles normes, sans trop les affecter économiquement. Comme le montrait Wittgenstein dans ses *Recherches philosophiques*, il n'y a pas de règle qui nous dise de suivre la règle, et pourtant elle est la première de toutes les règles : le conformisme à la règle. C'est bien ce qui apparaît ici : la première des règles qu'implique le RGPD est la conformité, et c'est dans cette optique que le règlement est traversé par des considérations sur la capacité des organisations à se conformer. Ainsi le premier devoir d'information qui concerne l'entreprise est celui qu'il a envers le régulateur. Cette conformité est d'autant plus importante dans le cadre de la RGPD que l'entreprise est responsable de l'analyse d'impact. En effet, avant le RGPD une entreprise devait faire la demande auprès de la CNIL pour traiter des données sensibles. Alors que ce nouveau règlement est régit par le principe d'*accountability* qui oblige les entreprises à pouvoir prouver qu'elles sont conformes si quelqu'un se plaint de leurs pratiques auprès de la CNIL. Le rapport de pouvoir se voit ainsi modifié, la CNIL n'a plus d'autorité *a priori*, seulement une capacité à interdire ou punir après coup un traitement qui n'aurait pas été conforme. Pour reprendre l'exemple de la reconnaissance faciale utilisée par les mairies de Nice et Marseille dans deux lycées, c'est une association appelée la Quadrature du Net qui a mobilisé la CNIL sur ce traitement illicite, mais les caméras avaient déjà été mises en place dans l'un des deux lycées. Si les organisations, publiques en l'occurence, n'ont pas réussi à démontrer leur conformité auprès de la CNIL, elles ont prévenu qu'elles étaient choquées par la décision du régulateur d'interdire leur pratique de nouvelles technologies, et qu'elles allaient tout faire pour produire un dossier plus robuste pour se rendre conforme. Ceci nous montre bien l'aspect très réglementé de la CNIL : au sujet d'un même traitement, elle peut ou non la juger licite selon la robustesse des informations qui lui sont données. Pour être au plus proche des entreprises et permettre le dialogue entre les organismes et le régulateur, le RGPD place au coeur de son règlement ce que le Journal du Net appelle « la colonne vertébrale du RGPD »[6] : le Délégué à la Protection des Données (Data Protection Officer en anglais).

2. Le DPO, un intermédiaire

La fonction de DPO est définie dans le RGPD du 27 avril 2016 principalement par le considérant 97 de sa section 4. La désignation d'un DPO est obligatoire pour tout organisme ayant une autorité publique, et tout organisme dont les activités de base comportent des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées, ou des traitements à grande échelle de catégories particulières de données. Il est un agent indépendant (il doit garder un statut d'externe pour garantir une certaine neutralité) dont la fonction est d'assurer la conformité d'un organisme au RGPD. Il apparaît ainsi comme un point de contact entre le régulateur et les organisations pour deux raisons : d'abord parce qu'il permet à l'organisme de centraliser les informations sur ses traitements de donnée et d'avoir un responsable au sein de sa structure, et il permet au régulateur d'assurer un certain suivi spécifique des organismes particuliers. La création de ce métier (qui est une redéfinition de ce que la loi Informatique et Libertés de 1978 appelait des Correspondants à la protection des données à caractère personnel), d'un médiateur entre le régulateur et l'entreprise a ainsi le double intérêt pour les entreprises de rester conformes et à jour sur les normes et régulations,

[6] https://www.journaldunet.com/management/expert/69000/le-dpo---de-la-contrainte-a-l-opportunite.shtml

et pour le régulateur de pouvoir prendre en compte les environnements spécifiques. Il est aussi un moyen pour la CNIL d'avoir des branches d'autorité au sein même des organismes. En effet, en cas de traitement de données non conformes, le DPO est tenu de divulguer les informations aux concernés et à la CNIL, mais cet aspect de son rôle est assez ambigu. Il doit à la fois être un lien entre l'autorité de contrôle, et les consommateurs puisqu'il est aussi un intermédiaire en cas de questions ou de réclamations des personnes au sujet de leurs données personnelles : une de ses missions décrite dans l'article 39 est de « coopérer avec l'autorité de contrôle ». Il devient le garant de la manière dont les informations personnelles sont récoltées, traitées et conservées au sein des infrastructures, même si la responsabilité incombe toujours au responsable de traitement qui sera jugé en cas d'infraction. Il apparaît que, plus qu'une simple conformité, le rôle du DPO est de définir et d'impulser une stratégie et une vision de l'entreprise en matière de collecte et de traitement des données personnelles. Le Data Protection Officer doit être au fait des derniers amendements à la loi afin d'assurer une protection optimale des données personnelles et de garantir la conformité de l'entreprise. Le DPO est ainsi un point de contact entre les organismes et la CNIL, et entre les organismes et les consommateurs. Et ce principalement parce qu'il est le garant de la fluidité de l'information, il est l'intermédiaire entre les différents acteurs de la protection des données : le responsable de traitement, le régulateur, la personne concernée par les données, les parties prenantes. L'idée est d'avoir un individu neutre qui serait capable de centraliser tout ce qui concerne les traitements de données d'un organisme.

3. L'échange d'informations au cœur de la protection des données, et de la RSE

Ce qui confère ce rôle d'intermédiaire au DPO est son rapport à l'information et au dialogue. Il permet un dialogue au sein de l'organisme puisqu'il est chargé d'informer et conseiller le responsable de traitement, les sous-traitants, et les employés sur tout ce qui est lié aux traitements de données ; un dialogue réciproque entre le régulateur et l'organisme ; un dialogue entre les organismes et les personnes qui exercent leur droit à la protection des données puisque « les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement », comme le stipule le considérant 4 de l'article 38. Le DPO fait aussi l'objet d'un devoir d'information puisqu'il doit faire en sorte que l'organisme notifie à la CNIL les violations aux traitements de données à caractère personnel, et communique envers les personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés. Le RGPD, conscient que le règlement est général, cherche ainsi à spécifier et contextualiser les problèmes de traitements puisque, selon l'article 39,2, « le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement. » On comprend ainsi que l'introduction du DPO est avant tout une manière de centraliser et rendre clairs les échanges d'informations entre ceux qui la traitent, ceux qui la produisent, et ceux qui la régulent, tout en permettant un passage de la règle générale à son application particulière. Si le DPO est intéressant pour ce qu'il représente pour le RGPD, aussi parce qu'il est une opportunité pour les organismes de pouvoir afficher une garantie du soucis de la protection des données, il ne s'agit pas non plus d'occulter le fait que le DPO n'est pas à la portée de tous les organismes et qu'il demande des moyens matériels non

négligeables. Le DPO est censé être une garantie de la conformité d'un organisme au RGPD, mais il ne faut pas oublier que le règlement a une marge d'interprétabilité et d'adaptabilité des règles qui le rendent assez souples et qui ne font pas de lui un cadre très contraignant. Malgré cela, le DPO avant d'être un garant de la conformité, est un garant du lien entre les différents acteurs. En étant en charge de l'information sur les traitements de données qui circule au sein de l'entreprise et ses collaborateurs, entre l'organisme et l'usager, et entre l'organisme et le régulateur, il garantit une certaine transparence et une communication entre les acteurs. Il apparaît que l'enjeu de l'acquisition d'informations dans la RSE réside principalement dans la notion de transparence, à la fois en tant qu'elle est une fin dans une société en mal de confiance, et le moyen de sa fin, par les modes de gouvernance et d'organisation qui ouvrent une certaine porosité entre les acteurs de la société, et ainsi fluidifient les flux d'informations.

Ainsi l'acquisition d'informations dans la RSE pose problème à plusieurs niveaux : dans les relations entre les différents acteurs et parties prenantes (personnes, organismes, collaborateurs, autorité de contrôle) ; dans la forme qu'elle doit prendre selon le type d'acteur à qui elle s'adresse et selon la finalité de celui qui la produit ; dans son fond puisque selon le type d'information acquise la responsabilité ne s'applique pas de la même manière et dans la même mesure. L'étude de cas du RGPD nous permet de comprendre dans un texte précis de RSE comment les problèmes d'acquisition d'informations s'articulent et dans quelle mesure ils sont pris en compte dans l'écriture même des normes. L'introduction du DPO en est un parfait exemple puisqu'il incarne cette volonté pour le régulateur de créer les conditions pour que la protection des données soit mise en place dans un dialogue et une intermédiation. Finalement le problème de l'acquisition d'informations pose la question de l'établissement d'un dialogue de confiance au sein de l'entreprise, de ses parties prenantes, et avec la société extérieure (la société civile, et les organismes de régulations comme la Commission nationale de l'informatique et des libertés). Il s'agit avant tout de créer des modes de gouvernance et d'organisation basés sur la transparence et le flux d'informations pour rétablir le lien de confiance indispensable au bon fonctionnement économique et politique d'une société. La Commission Européenne rappelle dans son rapport de 2011, article 1.3, que « la crise économique et ses conséquences sociales ont quelque peu mis à mal la confiance des consommateurs et le degré de confiance dans les entreprises ». Il s'agit ainsi de rétablir ce lien de confiance par la mise en place de rapports transparents et fluides entre les différents acteurs d'une société.

BIBLIOGRAPHIE et rapports officiels de RSE

Casili, Antonio, *En attendant les robots*, 2019, Seuil, Paris

Cochran, Philip, « The evolution of corporate social responsibility », *Business Horizons*, 2007, vol. 50, issue 6, 449-454

d'Humières, Patrick, « La RSE, une valeur pour l'espace public », *Vraiment durable*, vol. 4, no. 2, 2013, pp. 65-74

Park, Heungsik, et John Blenkinsopp, « L'influence de la transparence et de la confiance dans la relation entre corruption et satisfaction du citoyen », *Revue Internationale des Sciences Administratives*, vol. vol. 77, no. 2, 2011, pp. 251-273.

Piotrowski SJ, Van Ryzin GG, « Citizen attitudes toward *transparency* in local government », *The American Review of Public Administration,* 37 (3), 306-323, *2007*.

Rivas, Sébastien. « L'acquisition d'informations, un facteur différenciant dans les marchés de délégation de service public », *Géoéconomie*, vol. 52, no. 1, 2010, pp. 55-70.

Rousseau DM, Sitkin SB, Burt R, Camerer C, Not so different after all : a cross-discipline view of trust », 1998, *Academy of Management Review*, vol 23, n°3, juillet, p 393-404

Wittgenstein, Ludwig, *Recherches philosophiques*, 1953

——

Règlement Général de la Protection des Données, CNIL : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

OCDE, *Les principes directeurs de l'OCDE à l'attention des entreprises multinationales – Éditions 2011,* éditions OCDE : www.oecd.org/fr/daf/inv/mne/48004355.pdf

Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, Groupe de travail «Article 29» sur la protection des données. Version révisée et adoptée le 11 avril 2018 : https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf

Lignes directrices sur le consentement au sens du règlement (UE) 2016/679, Groupe de travail «Article 29» sur la protection des données. Version révisée et adoptée le 10 avril 2018 : https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf

Rapport de la Commission européenne, « Responsabilité sociale des entreprises: une nouvelle stratégie de l'UE pour la période 2011-2014 », 2011 : https://www.diplomatie.gouv.fr/IMG/pdf/Communication_du_25_octobre_2011_de_la_Commission_europeenne_sur_la_RSE_cle434613.pdf

Guide de la CNIL sur la sécurité des données personnelles, *Les guides de la CNIL*, Edition 2018 : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf