Les sources d'inspiration du Règlement général sur la Protection des Données : la conformité, la réglementation de l'environnement, la responsabilité du fait des produits défectueux

Par Winston MAXWELL et Christine GATEAU
Avocats associés, Hogan Lovells

Le Règlement général sur la Protection des Données à caractère personnel (RGPD) s'appuie sur les mêmes principes que la directive 95/46, principes qu'on retrouve aussi bien dans la Convention 108 du Conseil de l'Europe de 1981 que dans les lignes directrices de l'OCDE de 1980, révisées en 2013. Ces mêmes principes se retrouvent dans la loi Informatique et Libertés (LIL) de 1978 et le *Privacy Act* américain de 1974. Les principes fondamentaux n'ont pas fondamentalement changé depuis quarante ans. Les données doivent être traitées de manière loyale et licite, collectées pour des finalités déterminées, légitimes et non excessives, elles doivent être exactes, et conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées.

Le RGPD représente néanmoins une rupture avec le passé dans la mesure où il prévoit un système de responsabilisation des entreprises et un régime de sanctions dissuasives, à un niveau inédit en matière de données à caractère personnel. Ce qui a changé avec le RGPD, c'est l'ampleur des risques − et des opportunités − liés à l'exploitation des données. Pour rester efficace, la régulation a dû changer d'échelle. Les données deviennent un sujet de conformité majeur, à l'instar des règles anti-corruption, du droit de la concurrence ou de la réglementation de l'environnement et des installations dangereuses. Le RGPD représente une prise de conscience similaire à celle qui s'est opérée à la fin des années 1970 et au début des années 1980 après le naufrage de l'***Amoco Cadiz*** en 1978 et la catastrophe de Seveso en 1976. Le RGPD s'inspire d'ailleurs de la réglementation des installations SEVESO puisque les mesures de traçabilité, de stockage et d'utilisation des données seront adaptées selon leur niveau de « toxicité » potentielle. L'exploitant doit identifier les risques à leur source et élaborer lui-même le plan de sécurité pour l'installation, sous la supervision du régulateur.

Les données à caractère personnel sont devenues indispensables à l'économie mais, comme le pétrole et d'autres produits chimiques, elles peuvent créer des externalités négatives importantes, nécessitant une intervention réglementaire musclée.

En Europe, les données à caractère personnel sont à la fois un objet de commerce et un droit fondamental. Le RGPD tente de réconcilier ces deux principes. L'objectif du règlement est de faciliter la libre circulation des données à caractère personnel et leur exploitation par les entreprises. En même temps, le RGPD nous rappelle que les données ne sont pas des services et marchandises comme les autres. Le règlement tente de gérer cette tension, ainsi que la tension qui existe entre différents droits fondamentaux eux-mêmes. Une mesure qui augmente la protection de la donnée à caractère personnel peut nuire au droit à l'accès à l'information ou au droit à la protection de la propriété privée. En cas de frottement entre plusieurs droits et libertés fondamentaux, une règle de proportionnalité s'applique afin d'assurer la limitation de chaque interférence au strict nécessaire.

Une direction : le principe d'*accountability*

Le RGPD oblige l'entreprise à mettre en place un cadre pour effectuer elle-même des analyses de risques et arriver à ses propres conclusions quant au caractère loyal, non excessif et adéquat des traitements et des mesures d'accompagnement. Ce cadre interne repose d'abord sur la création d'un registre pour chaque traitement de données à caractère personnel. Le registre oblige l'entreprise à répertorier chaque action de traitement, à identifier l'entité responsable du traitement, l'existence de sous-traitants et de transferts internationaux. Surtout, le registre contient une description précise de la finalité du traitement : pourquoi est-ce que je traite ces données ? Le registre est la clé de voûte du système de responsabilisation. Il permettra de mettre en évidence le traitement de données à risques. Il permettra d'identifier des traitements pour lesquels les finalités sont vagues ou mal définies. Il permettra d'identifier des traitements faisant appel à des sous-traitements ou à des transferts internationaux non encadrés.

Le registre impose une logique de traçabilité, comme pour la gestion de produits dangereux dans une usine. L'absence de registre ou un registre incomplet constitueront automatiquement des fautes aux yeux du régulateur. De même, si le registre contient un traitement à risque et si le responsable du traitement ne fait rien pour réduire ce risque, la faute sera là encore manifeste. Le registre a le mérite de forcer l'entreprise à se poser les bonnes questions : quel est le fondement juridique de ce traitement ? qu'en est-il du consentement des individus ou de l'intérêt légitime de l'entreprise ? le traitement résulte-t-il de l'exécution d'un contrat ? est-ce que la finalité en est suffisamment précise et légitime ? est-ce que les données collectées sont en adéquation avec la finalité ? est-ce que les individus ont reçu une information complète sur le traitement ? comment l'entreprise assure-t-elle l'exercice par les individus de leurs droits d'accès, de rectification, d'effacement et de portabilité ? quelles sont les mesures de sécurité mises en place ? comment avons-nous organisé les transferts de données au sein du groupe ainsi qu'avec nos partenaires et sous-traitants ?

À partir du registre et de cette liste de questions, l'entreprise effectuera un premier bilan des risques et des mesures de conformité mises en place pour les atténuer. Ce premier bilan permettra à l'entreprise de démontrer sa conformité pour l'ensemble des traitements à risque faible ou moyen. Lorsque le premier bilan conduit au constat que le traitement présente un risque élevé, il faut passer à une analyse d'impact détaillée.

Comme la directive SEVESO 2, le RGPD conduit les entreprises et les régulateurs à se concentrer sur les traitements à risques élevés. L'étude d'impact pour les traitements à risque élevé sera un document d'importance capitale pour prouver la conformité. Il s'agit d'un renversement de la charge de la preuve. Dorénavant, il incombe à l'entreprise de démontrer qu'elle a mis en œuvre toutes les mesures appropriées pour protéger les données à caractère personnel en sa possession et assurer le respect des droits des personnes.

Une boussole dans la détermination des « mesures appropriées » : le principe de proportionnalité

L'application du RGPD est un exercice d'équilibriste. La mise en balance de droits et intérêts concurrents, voire contradictoires, se trouve au cœur des concepts-clés du RGPD tels que ceux de « mesures techniques et organisationnelles appropriées », d'« intérêt légitime » et de « traitement loyal ». Ces concepts laissent une grande marge de manœuvre à l'entreprise, aux régulateurs et aux juges pour placer le curseur à différents endroits en fonction du contexte et des risques pour les individus. L'interprétation de ces termes sera différente entre une PME qui gère une base de données de quelques centaines de clients et un géant de l'Internet qui gère les données de dizaines de millions de consommateurs.

Ces multiples zones de frottement ont conduit le législateur à adopter une approche à géométrie variable, fondée sur les risques. Hormis certains cas de figure, il n'existe pas de réponse binaire et univoque dans le règlement. Il pose le principe de « mesures appropriées », concept souple similaire au concept de « bon père de famille » figurant anciennement dans le Code civil et dorénavant remplacé par le terme « raisonnable ». Le règlement met l'accent sur les moyens mis en œuvre par l'entreprise pour assurer une gestion responsable des données à caractère personnel. L'accent mis sur les moyens organisationnels et techniques de protection vient du monde de la conformité ou *compliance*. Les autorités américaines exigent la mise en œuvre de politiques de conformité efficaces en matière de lutte contre la corruption et de droit de la concurrence. Le RGPD s'inspire directement de cette tradition.

L'entreprise doit mettre en œuvre des moyens appropriés, compte tenu des risques pour les individus, de l'état de l'art et des coûts de mise en œuvre. Il s'agit d'une protection raisonnable et non d'une protection absolue.

Mais qu'est-ce qu'une protection raisonnable ? L'analyse d'impact prévue par l'article 35 du RGPD ressemble aux analyses de risques qu'effectuent les entreprises en matière de sécurité des produits avant leur mise sur le marché. En termes d'analyses économiques, des mesures raisonnables doivent correspondre au point où le bien-être social est maximisé. Des mesures de protection trop draconiennes peuvent conduire à un appauvrissement de la société. Par exemple, une régulation qui limite la vitesse des voitures à 30 km/heure réduirait le nombre de victimes d'accidents mais réduirait fortement l'utilité de la voiture. De même, une régulation qui rendrait les plateformes responsables de tous les contenus mis en ligne par les utilisateurs conduirait les plateformes à limiter drastiquement les informations mises en ligne, ce qui conduirait à un appauvrissement de la liberté d'expression. Chaque régulation et chaque mesure de protection peuvent ainsi créer des effets secondaires qui doivent être pris en compte pour déterminer le niveau optimal de régulation.

En termes économiques, le niveau approprié des mesures de protection correspond au point où le coût marginal d'une unité supplémentaire de mesures de protection est égal au bénéfice marginal résultant de cette mesure [(1)]. Au-delà de ce point, les mesures de sécurité supplémentaires coûtent plus cher à la société que le bénéfice qui en découle. Elles vont réduire le bien-être social dans son ensemble, au lieu de l'augmenter.

Le niveau optimal des mesures de protection se situe au point C* dans la figure suivante :

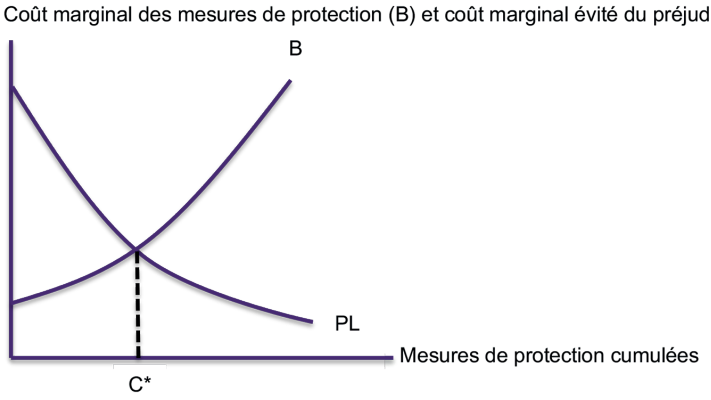

Figure 1 : Illustration de la règle de Hand.
Source : Richard Posner, Economic Analysis of Law, Aspen Casebook Series, 8th Edition, 2011.

(1) Cette règle découle d'une décision de justice américaine rendue par le magistrat Learned Hand en 1947. Depuis lors, cette règle s'appelle la « Règle de Hand ». Elle est utilisée pour définir un comportement fautif.

Dans ce diagramme, la courbe PL représente les coûts liés au risque du préjudice, P étant la probabilité de l'occurrence du préjudice et L étant le niveau de préjudice qui résulterait si le risque se réalisait. Par exemple, si le coût social (L) lié à la perte d'un million de numéros de cartes de crédit est égal à 100 millions d'euros (soit 100 euros par carte) et la probabilité de cette perte (P) est de 0,1 % (une chance sur mille), le produit «PL» est égal à 100 000 euros. Cette courbe PL décroît lorsqu'on ajoute des mesures de protection mais n'atteint pas zéro. La courbe s'aplatit, ce qui signifie qu'au-delà d'un certain seuil, chaque mesure de protection supplémentaire contribue faiblement à la diminution du risque.

La courbe B représente les coûts liés aux mesures de protection. Généralement, les premières mesures de protection, peu onéreuses et très efficaces, ont un impact important sur le risque (diminution de la courbe PL). Mais au-delà d'un certain seuil, les mesures de protection deviennent très chères pour un impact plus faible sur le risque. Par exemple, une mesure de protection qui réduit la probabilité « P » de 100 % à 0,5 % pourrait coûter le même montant qu'une mesure supplémentaire qui réduirait la probabilité « P » de 0,5 % à 0,1 %, ou de 0,1 % à 0,08 %. Chaque incrément de protection devient plus cher lorsqu'on approche un niveau de risque zéro. La courbe B grimpe de manière exponentielle.

Une autre façon de présenter le niveau optimal de mesures de protection est un graphique montrant le point où le bien-être social atteint son niveau maximum :

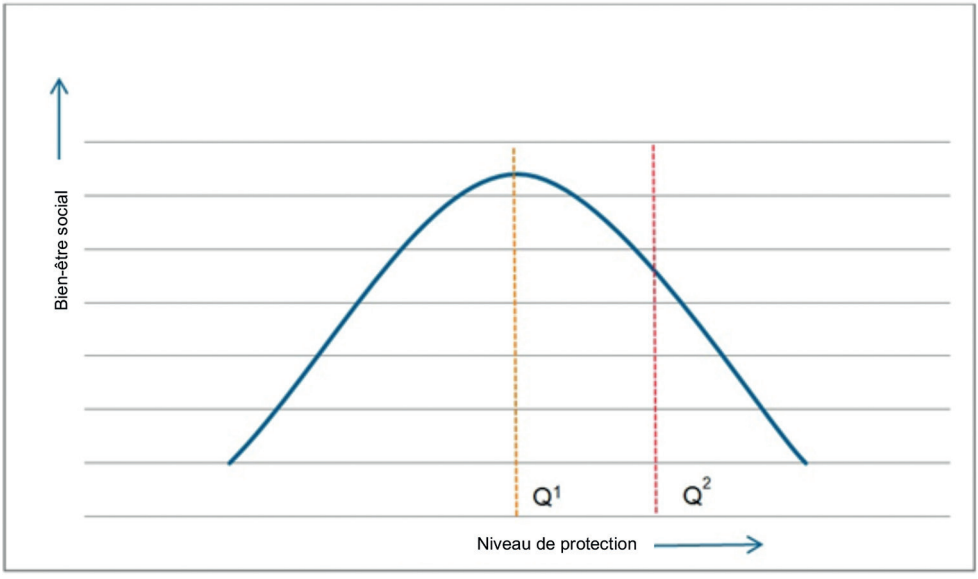

Figure 2 : Maximisation du bien-être social selon le niveau d'efficacité des mesures de protection (Winston Maxwell, *Smarter Internet Regulation Through Cost-Benefit Analysis*, Presses des Mines, 2017).

Même si la mesure de prévention Q2 fournit un niveau de protection supérieur à la mesure Q1, le niveau optimal se trouve au point Q1, car le bien-être social trouve son maximum à ce point.

L'analyse d'impact prévue par l'article 35 du RGPD permettra de mettre en lumière les risques ainsi que les différentes mesures qui peuvent être mises en œuvre pour réduire ces risques. Il appartiendra à la direction de la société de décider quel niveau de risque résiduel est acceptable ou non. Cela dépendra de la culture de l'entreprise et des pratiques de l'industrie dans laquelle l'entreprise évolue. En cas, par exemple, d'une fuite de données, il incombera ensuite à l'entreprise de justifier ses choix en démontrant, étude d'impact à l'appui, que les mesures mises en œuvre étaient raisonnables, même si elles n'ont pas permis de réduire le risque à zéro.

Au bout du chemin, l'application d'un régime strict de responsabilité aux responsables de traitement

Le RGPD impose un régime strict de responsabilité aux responsables de traitement : dès lors qu'une violation est constatée, sa réparation sera automatique. Les personnes concernées peuvent intenter une action sans avoir à prouver une faute ou une négligence de la part du responsable de traitement. La charge de la preuve que « le fait qui a provoqué le dommage ne lui est nullement imputable » [(2)] (à savoir que le traitement de données à caractère personnel est réalisé conformément au RGPD et aux droits nationaux transposant le RGPD) pèse sur le responsable de traitement défendeur. Les sociétés doivent en outre être préparées à ce que les personnes concernées exercent leur droit d'introduire une réclamation auprès d'une autorité de contrôle pour avoir accès aux conclusions de l'enquête administrative. Il est probable que les personnes concernées utiliseront ces informations dans le cadre de procédures civiles. Du fait de cette approche, les personnes concernées peuvent facilement créer une présomption de violation de la protection des données à caractère personnel et une charge administrative encore plus lourde pèse sur les responsables de traitement.

Les dispositions de responsabilisation du RGPD exigent des défendeurs de prouver qu'ils ont mis en œuvre les « mesures techniques et organisationnelles appropriées ». Les responsables de traitement doivent considérer la logique de responsabilisation du RGPD comme une stratégie précontentieuse, conçue pour créer des documents permettant de démontrer que le défendeur a appliqué les mesures techniques et organisationnelles appropriées. Le registre des opérations de traitement et l'analyse d'impact seront déterminants pour renverser la présomption de faute de la part du responsable du traitement.

En conclusion, à l'avenir, on peut s'attendre à ce qu'il y ait une convergence dans les démarches des entreprises en matière de risques RGPD et en matière de risques liés à la sécurité des produits ou à la pollution de l'environnement. Les analyses d'impacts et analyses de risques seront similaires, encourageant une mutualisation d'expertises au sein du groupe sur la gestion des risques et la préparation d'analyses d'impacts. Le programme RGPD de l'entreprise devra naturellement s'intégrer dans le dispositif général de gestion des risques du groupe.

(2) Article 82-3, RGPD.