governance & regulation

Fondation Paris-Dauphine

DAUPHINE UNIVERSITÉ PARIS | PSL

Règlement général sur la protection des données : Premiers retours d'expérience

Synthèse de conférence

Petit-déjeuner de la Chaire Gouvernance et Régulation

Université Paris-Dauphine, 28 juin 2018

DEBATE

Table des matières

Règlement général sur la protection des données : premiers retours d'expérience

Petit-déjeuner de la Chaire Gouvernance & Régulation
28 juin 2018

Un mois après l'entrée en vigueur du RGPD, comment les entreprises s'adaptent-elles à ce nouveau cadre réglementaire présidant à l'exploitation et à la valorisation des données ? Ce règlement constitue-t-il un frein à la bonne marche des affaires et à l'innovation, ou au contraire un vecteur de différenciation grâce à la relation de confiance qu'il institue entre les acteurs économiques et les consommateurs ?

Le RGPD, évolution ou révolution ?

Guillaume Buffet
Ancien président, Renaissance Numérique

Alors que la data est considérée comme le « fuel » de l'économie, la donnée responsable garantie par le règlement général sur la protection des données (RGPD) sera-t-elle « l'énergie verte » de l'économie numérique ? Outre la marée noire qu'il a suscitée dans les boîtes mail, qu'a changé le RGPD dans les entreprises depuis son entrée en vigueur le 25 mai 2018 ?

Thomas Dautieu
Directeur adjoint de la Conformité, CNIL

L'entrée en vigueur du RGPD s'est déroulée sans trop de heurts. Ce texte introduit certes des nouveautés – responsabilisation, analyses d'impact… –, mais il repose sur des principes fondamentaux de protection des données inchangés depuis la loi de 1978 relative à l'informatique, aux fichiers et aux libertés. Nous avons conscience que ni le secteur public, ni le secteur privé ne sont encore pleinement conformes au règlement. Ce qui importe avant tout est que les acteurs s'engagent dans une démarche de conformité, comprennent les changements à opérer et intègrent le principe de responsabilité. La CNIL entend les accompagner en leur fournissant un cadre de doctrine sécurisant.

Benoît Marichal
Responsable du programme data, RATP

Au quotidien, le RGPD n'induit pas une révolution à la RATP mais une évolution. Pour autant, la constitution du registre des traitements imposée par le règlement requiert un travail important. Bien que les nombreux traitements de données que la RATP avait déjà déclarés à la CNIL constituent un excellent socle, le périmètre élargi que recouvre désormais ce sujet génère chez nous une charge de travail conséquente.

Guillaume Buffet

Quel usage fait la RATP de ses données ?

Benoît Marichal

Nous possédons assez peu de données personnelles sur nos voyageurs, hormis celles qu'ils renseignent sur le site maRATP dans le cadre de notre programme relationnel, ou qui proviennent de nos contacts avec la clientèle. L'usage des données du programme relationnel est soumis à un consentement. Les données de télébillettique

issues du pass Navigo sont, quant à elles, rendues anonymes 24 heures après leur entrée dans le système. L'opération est réalisée par le GIE Commutitres grâce à une clé de chiffrement fournie par Ile-de-France Mobilités. Ces informations permettent uniquement de comptabiliser les voyageurs. Enfin, les images de vidéoprotection ne sont consultées qu'en cas d'incident ou pour s'assurer d'une absence de congestion, le plus souvent a posteriori et sur réquisition de la police. Leur durée de conservation est de 30 jours.

Guillaume Buffet

La donnée est au cœur du modèle des e-commerçants, qui ont besoin de connaître finement leurs clients. Les modifications induites par le RGPD sont-elles un motif d'inquiétude pour cette profession ?

François Momboisse
Membre du Conseil de Surveillance, Netwave & Président, Fevad

S'il est vrai que ce texte n'introduit pas de changement majeur par rapport à la loi de 1978, il porte néanmoins une approche fondamentalement nouvelle qui place les e-commerçants dans l'incertitude, là où prévalait hier une stabilité. A l'extrême, le comité de pilotage de tout projet devrait intégrer un juriste en charge de la protection des données ! Si les grandes entreprises ont les moyens d'y répondre, les PME sont submergées par la complexité du sujet.

Les e-commerçants ont le sentiment d'être les victimes collatérales d'un règlement visant avant tout les plateformes qui, comme Facebook, proposent des services gratuits en échange de données dont elles font un usage assez clandestin. Dans le e-commerce au contraire, l'usage des données est transparent et utile pour le client, puisqu'il permet de lui proposer des produits adaptés à ses goûts. En outre, les e-commerçants ne s'échangent que des données à caractère général, et préservent les informations stratégiques.

De la salle

Pourriez-vous citer des exemples de traitements qui entrent désormais dans le champ du RGPD ?

Benoît Marichal

Citons les fichiers Excel nominatifs que tout un chacun possède dans son ordinateur – permettant par exemple à un manager de gérer l'attribution des primes et des avancements. Ils relèvent du champ du RGPD. Peut-être étaient-ils même concernés précédemment pour l'obligation d'être déclarés à la CNIL, sans que leurs auteurs en aient conscience.

De la salle

L'élaboration d'un registre des traitements est-elle obligatoire pour toutes les sociétés, quelle que soit leur taille ? Au-delà, quels tableaux de bord est-il demandé aux entreprises de produire pour prouver qu'elles respectent leurs obligations ?

Thomas Dautieu

Le registre recensant les traitements et leurs caractéristiques s'impose à tous. Désormais – et c'est un important renversement de logique –, la CNIL demande aux organismes de prouver qu'ils sont conformes au RGPD. Outre leur registre, ils doivent être en mesure de lui communiquer la fiche de poste de leur délégué à la protection des données et la preuve de la mise en œuvre effective d'un plan de conformité (audits, formations, sensibilisations, etc.).

Guillaume Buffet

Le RGPD ne doit pas rester une affaire de spécialistes. Tant que les entreprises considéreront qu'il revient aux fonctions juridiques de traiter ce sujet, le fossé qui sépare ces dernières des opérationnels s'agrandira. Mieux vaut considérer que ce règlement place les utilisateurs au cœur du débat, et que c'est à partir d'eux que doit être réfléchi tout nouveau modèle. Or, qui est le mieux placé pour y procéder que les responsables du marketing, de l'innovation et de la communication ? En cela, le RGDP doit fédérer l'ensemble des départements d'une entreprise.

Benoît Marichal

Il est utile de s'appuyer sur le RGPD pour remettre en question les processus métier, dans le cadre du mouvement plus vaste de transformation digitale des entreprises. C'est l'occasion de se demander si toutes les données que l'on recueille sont vraiment nécessaires.

Quelle responsabilité pour les sous-traitants ?

De la salle

Le RGPD introduit-il une nouvelle répartition des responsabilités en cas de sous-traitance ? Est-il possible de déléguer totalement la responsabilité au prestataire qui traite les données ?

Thomas Dautieu

Le RGPD met fin à la fiction juridique dans laquelle la faute pesait nécessairement sur le responsable de traitement (c'est-à-dire le donneur d'ordres), quand bien même une faille de sécurité tenait à l'erreur d'un sous-traitant. Le règlement impose de répartir contractuellement les responsabilités entre le donneur d'ordres et son prestataire. Si, par exemple, une association sous-traite l'hébergement de sa base de données et précise contractuellement que la sécurité des informations relève de la responsabilité du prestataire, c'est à ce dernier que la CNIL infligera une amende en cas de manquement au contrat. Pour autant, le responsable de traitement ne peut se dégager de toute responsabilité : c'est lui qui définit la finalité et les moyens de mise en œuvre du traitement. J'ajoute que le contrat doit traduire les conditions d'exécution réelles. Un prestataire ne pourra pas être sanctionné pour avoir manqué à des obligations que, dans la pratique, seul le donneur d'ordres était en mesure de remplir. En outre, un sous-traitant ne peut pas lui-même sous-traiter sans l'accord du responsable de traitement.[1]

1 *Pour toutes ces questions, voir le Guide du sous-traitant disponible sur le site de la CNIL.*

Le consentement au cœur du débat

Guillaume Buffet

Dans le commerce physique, un vendeur n'a pas besoin du consentement de son client pour se souvenir qu'il aime les bananes bien mûres ! Dans le monde virtuel, jusqu'où est-il nécessaire de recueillir le consentement du consommateur ?

Thomas Dautieu

La règle du consentement comme base légale du traitement des données a été présentée à tort comme absolue. En réalité, elle n'est qu'une option parmi d'autres. Un cybercommerçant qui collecte des données pour vendre ses produits et effectuer quelques actions de marketing n'est pas soumis à des contraintes démesurées. Ses obligations sont plus poussées s'il met en œuvre des mécanismes de profilage, croise des données avec des tiers ou traite avec des *data brokers*. Ainsi, les contraintes sont d'autant plus fortes que la donnée est sensible, qu'elle est partagée et que son usage est complexe. Le seul fait d'analyser des achats pour effectuer une publicité ciblée ou lutter contre la fraude relève plutôt de l'intérêt légitime – dont la définition mérite toutefois, selon la CNIL, d'être précisée.

Outre le consentement, le traitement des données peut notamment s'effectuer sur une base contractuelle. Lors d'un achat en ligne, un cybercommerçant a besoin, pour exécuter son contrat, de recueillir les coordonnées et le numéro de carte bancaire d'un client. A ce stade, le consentement explicite de ce dernier n'est pas nécessaire. Le cybercommerçant pourra réutiliser l'adresse email de ce contact pour lui proposer des produits, à condition de le lui annoncer et de lui laisser la possibilité de s'y opposer. En revanche, son consentement pourra être requis si le vendeur s'enquiert d'éléments supplémentaires (âge, profession, centres d'intérêt…).

Guillaume Buffet

A quelles conditions une donnée est-elle considérée comme anonyme ?

Thomas Dautieu

Ce sujet complexe a fait l'objet d'un avis du Comité européen de la protection des données (G29). Pour être considérée comme anonyme, la donnée doit empêcher toute identification de la personne qu'elle concerne et ne pas être « individualisable ». Reconnaissons qu'aujourd'hui, vu la sophistication des croisements d'informations, il est extrêmement difficile de garantir un anonymat absolu. Il n'en reste pas moins que pour traiter de grandes masses de données, l'un des canaux les plus simples est celui de l'anonymisation.

Guillaume Buffet

Est-il illusoire d'espérer une traçabilité des données personnelles et des consentements ?

Thomas Dautieu

La CNIL travaille, avec les organisations professionnelles, à la mise en œuvre du principe de meilleure information des personnes, notamment en cas de collecte indirecte via des *data brokers*. Des obligations de transparence et d'information des personnes seront à la charge de ces derniers.

La *blockchain* pourrait également permettre de suivre les consentements. La CNIL est l'une des premières autorités de protection européennes à avoir travaillé sur ce sujet, et publiera prochainement ses orientations. Nous ne considérons pas la *blockchain* comme un traitement en soi mais comme une technologie pouvant être mobilisée afin de remplir un certain nombre de finalités, et pouvant dans certains cas respecter les obligations de protection des données.

De la salle

Les données de la blockchain sont ineffaçables, gravées pour l'éternité, voire accessibles à tous. N'est-ce pas contraire aux principes du RGPD ?

Guillaume Buffet

Il est possible de ne graver dans la *blockchain* que des clés d'accès à des données stockées par ailleurs et pouvant être supprimées. La *blockchain* offre une interopérabilité très intéressante pour le consommateur. Une fois son consentement donné, il a l'assurance que tous les acteurs peuvent s'y référer.

Le RGPD, entrave ou avantage concurrentiel ?

Guillaume Buffet

Les entreprises perçoivent-elles le RGPD comme une entrave à la bonne marche de leurs affaires, ou au contraire comme l'occasion de renforcer la relation de confiance avec leurs clients ?

Benoît Marichal

La Commission européenne évalue l'économie de la donnée à 300 milliards d'euros en Europe en 2016. Elle estime que ce montant pourrait atteindre 740 milliards d'euros en quatre ans, à condition que les conditions de confiance et d'éducation au numérique soient réunies . A cet égard, le RGPD pourrait avoir un effet favorable.

François Momboisse

Imaginez combien il est complexe pour une PME de se conformer au RGPD ! De notre point de vue, le grand gagnant du règlement sera Amazon. Aucun autre e-commerçant ne possède des données dans les 27 Etats membres et sur toutes les catégories de produits, lui permettant d'effectuer librement des croisements extrêmement fins. C'est aussi grâce à ce type de recoupements que les GAFA avancent aussi vite dans la e-santé. Je crains qu'en comparaison, nous soyons trop timorés, en particulier dans l'utilisation de données de santé anonymes.

Thomas Dautieu

Le RGPD est parfois avancé, à tort, comme prétexte au retard d'acteurs européens par rapport à leurs concurrents nord-américains. Reconnaissons que l'avance de ces derniers tient avant tout à leur efficacité.

Toute entreprise qui cible des consommateurs européens est soumise au RGPD. Cela induira une uniformisation des contraintes réglementaires en matière de protection des données, entre les acteurs continentaux et ceux qui sont implantés ailleurs mais visent une clientèle européenne. Le RGPD est même repris par des pays extracommunautaires et tend à devenir un standard en matière de protection des données.

Somme toute, le meilleur promoteur du RGPD fut Facebook à travers le scandale Cambridge Analytica, société accusée d'avoir utilisé à leur insu les données de dizaines de milliers d'utilisateurs du réseau social, dans le but d'orienter l'opinion américaine en période électorale. Cette affaire a porté au grand jour les dérives potentielles d'une mauvaise protection des données, susceptible d'affecter le fonctionnement de nos sociétés démocratiques. Aux Etats-Unis est envisagée une loi non plus sectorielle (visant notamment la protection des enfants) mais générale à cet égard. Des sociétés de la Silicon Valley s'y disent favorables, conscientes qu'elles devront consolider leur relation de confiance avec les consommateurs pour poursuivre la collecte de données.

Au total, le RGPD devrait contribuer à créer de la valeur, car il induit un vecteur de différenciation pour les entreprises européennes. Certaines ont valorisé leurs pratiques vertueuses de protection des données pour remporter des marchés à l'international, y compris aux Etats-Unis.

Ajoutons que le droit à la portabilité des données, institué par le RGPD, libère les internautes qui étaient jusque-là prisonniers de plateformes. Il devrait fluidifier le jeu concurrentiel entre ces dernières.

François Momboisse

Initialement, cette disposition permettait aux abonnés de changer d'opérateur téléphonique en conservant leur numéro de téléphone, ce qui était pertinent. Le Royaume-Uni l'a transposée à l'électricité ou aux plateformes de *streaming*, services pour lesquels le consommateur recourt généralement à un fournisseur unique. En revanche, le droit à la portabilité est inapplicable dans le e-commerce, où un internaute effectue des achats sur de multiples sites. La liste des produits qu'il aura acquis chez l'un n'est pas transposable chez l'autre, à moins que les enseignes ne se livrent à un minutieux voire impossible travail de mise en correspondance de leurs catalogues.

Guillaume Buffet

Partant du principe que la portabilité est l'occasion pour un internaute de partager ses données avec plusieurs plateformes afin qu'elles coordonnent leurs services, la start-up française Onecub imagine des usages innovants. Elle a testé une mise en relation entre le site de covoiturage BlaBlaCar et le service d'acheminement de paquets entre particuliers Cocolis. Un conducteur BlaBlaCar peut ainsi prendre à son bord des voyageurs, mais aussi des colis. Il en résulte une commission d'apporteur d'affaires pour BlaBlaCar, de nouveaux clients pour Cocolis et un revenu pour le chauffeur. Sous cet angle, le RGPD n'est plus une contrainte, mais une source de revenus complémentaires pour toutes les parties.

Guillaume Buffet

Pour les acteurs publics, l'open data constitue-t-il plutôt une opportunité ou une menace ?

Benoît Marichal

L'*open data* est l'un des mécanismes par lesquels l'Union européenne entend stimuler l'économie numérique, et nous entendons poursuivre les mises à disposition de données dans ce but. Ceci étant dit, la RATP verra ses lignes de bus ouvertes à la concurrence à compter de 2024. Depuis 2017, la loi pour une République numérique (loi Lemaire), permet à n'importe quel citoyen ou entreprise d'obtenir la mise à disposition d'un très grand nombre de données. La refonte de la directive sur la réutilisation des informations de service public (PSI) est même susceptible de renforcer cette obligation. Or certaines de nos données touchent au secret industriel et commercial, et le risque de voir passer des

savoir-faire à de futurs concurrents est réel. La loi prévoit certes un cas d'exception à cet égard, mais la définition de ce secret industriel et commercial reste floue et sera soumise à l'appréciation d'un juge en cas de litige. Tout ceci contribue à créer de l'insécurité juridique et un terrain de jeu inégal entre les différents acteurs du secteur.

Guillaume Buffet

La donnée est un carburant central de l'innovation. Le RGPD prévoit-il des conditions d'utilisation des données personnelles propres aux projets de R&D ?

Thomas Dautieu

Une disposition du règlement autorise à modifier la finalité d'un traitement à des fins de recherche, à certaines conditions (vérifier que les finalités sont compatibles, « pseudonymiser » les informations…). Le RGPD n'est donc en rien incompatible avec la R&D, y compris sur des données qui ne seraient pas anonymes.

Chaire Gouvernance et Régulation
Fondation Paris-Dauphine
Place du Maréchal de Lattre de Tassigny - 75016 Paris (France)
http://chairgovreg.fondation-dauphine.fr