

Nouvelle réglementation européenne des données personnelles : une simplification limitée mais une protection augmentée

Description

En mai 2018, un nouveau droit des données personnelles reposant sur le RGPD (Règlement général pour la protection des données personnelles) entrera en application. D'importantes obligations pèseront sur les auteurs de traitements de données, afin de mieux protéger la vie privée. En cours de discussion, un second règlement « ePrivacy », venant en complément, suscite l'inquiétude des entreprises de presse, dont le modèle économique repose sur la collecte des données de leurs clients.

Moderniser, simplifier et unifier le droit européen des données personnelles

Le règlement n° 2016/679 du Parlement européen et du Conseil, promulgué le 27 avril 2016 et 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, constitue une étape importante dans la construction européenne d'un droit des données personnelles. Ce RGPD prend la suite de la directive 95/46/CE du 24 octobre 1995, qui avait été conçue alors que l'internet et le web faisaient tout juste leur entrée dans les foyers. Le règlement l'abroge et la remplace. La principale différence entre une directive et un règlement de l'Union européenne est que ce dernier est directement applicable sur l'ensemble du territoire des États membres, tandis que les directives nécessitent des transpositions qui sont parfois tardives et aléatoires. Ainsi, le nouveau texte sera applicable de plein droit à compter du 25 mai 2018 sans nécessiter de lois locales d'application.

Les entreprises, administrations et autres acteurs manipulant des données disposent donc de quelques mois pour se mettre en conformité avec les nouvelles dispositions. Certains dénoncent une réforme risquant de freiner l'innovation en matière de nouvelles technologies de l'information et de la communication. En effet, il sera difficile pour les entreprises émergentes du *big data* et de l'intelligence artificielle, dont les outils reposent sur l'exploitation automatique d'immenses bases de données, de se conformer aux nouvelles normes sans brider leurs services. Le but affiché du règlement est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs informations personnelles. Le moyen associé à cette fin ne peut qu'être un renforcement des exigences à l'égard des auteurs de traitements de données personnelles, lesquels devront opérer une importante mise à niveau juridique.

L'ambition est de simplifier et d'unifier le droit des données personnelles à l'échelle de l'Union européenne. D'ailleurs, en France, des points importants ont déjà été introduits par le biais de la loi « Pour une République numérique » du 7 octobre 2016, à l'instar, par exemple, de la portabilité des données personnelles (voir [La rem n°41, p.15](#)). L'unification est évidemment un progrès en ce qu'elle permettra aux entreprises, nombreuses au demeurant, qui proposent leurs services dans différents États de l'Union d'avoir

affaire à un seul et même régime juridique.

Pour ce qui est de la simplification, la nouvelle réglementation ne devrait pas permettre de se passer de spécialistes du droit des données personnelles, bien au contraire. Le règlement est le résultat de quatre années d'après négociations et de près de 4 000 amendements. Il en résulte un ensemble de dispositions relativement complexe et technique. Mais ces normes n'en apparaissent pas moins bienvenues, eu égard aux menaces de plus en plus grandes qui planent sur la vie privée des internautes.

De nouvelles contraintes à la charge des entreprises et administrations

Parmi les dispositions issues du règlement européen, certaines augmenteront sensiblement la responsabilité des auteurs de traitement de données personnelles. Par exemple, avant de mettre en place un tel traitement, il faudra désormais réaliser une étude d'impact. Le règlement européen précise les actions à diligenter dans le cadre d'une telle étude. Il introduit de la sorte le concept de prise en compte du respect de la vie privée dès la conception du traitement : les différentes normes relatives à la collecte des données devront être intégrées dès la création du traitement de données (*privacy by design and by default*). En d'autres termes, une obligation de moyens est mise à la charge des entreprises et administrations, tant au moment de l'initiative du traitement qu'au moment de sa réalisation. En particulier, les auteurs de traitements sont invités à privilégier l'utilisation de pseudonymes avant et pendant les opérations. Cette « pseudonymisation » doit permettre de conserver les données sous une forme ne permettant pas l'identification directe d'un individu.

Autre exemple, les entreprises et administrations devront désormais désigner un « délégué à la protection des données » – sorte de nouveau « correspondant informatique et libertés » – dans les cas suivants : lorsque le responsable de traitement est un organisme public ; lorsque l'activité du responsable de traitement « exige un suivi régulier et systématique à grande échelle des personnes concernées » ; lorsque l'activité du responsable de traitement consiste en un « traitement à grande échelle » de données sensibles telles que celles relatives à la santé, aux opinions politiques ou religieuses, à l'orientation sexuelle, etc. Si la présence d'un tel délégué n'est exigée que dans certains cas, il semble préférable de le désigner systématiquement puisque toute entreprise ou administration peut être sommée à tout moment de s'expliquer quant aux traitements de données auxquels elle procède. Au-delà, chaque responsable de traitement de données devra tenir à jour un registre contenant un certain nombre d'informations obligatoires.

Réalisée par le cabinet de conseil en management Sia Partners, une récente étude estime le coût de la mise en conformité à environ 30 millions d'euros en moyenne pour un groupe du CAC 40, sachant que les moyens à mettre en œuvre varient selon la taille, la structure et l'état du système informatique de chaque entreprise, et surtout du niveau de traitement que celle-ci fait des données personnelles de ses clients. Le montant de la facture est estimé à 100 millions d'euros pour les banques et les assureurs, contre 11 millions pour les groupes dont la clientèle est constituée d'entreprises. En cas de violation du règlement européen, les autorités de contrôle pourront prononcer des amendes administratives qui devront être « *effectives, proportionnées et dissuasives* ». Les sanctions pourront aller jusqu'à 20 millions d'euros, et dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent.

La protection de la vie privée confortée

Si les auteurs de traitements de données personnelles doivent se conformer à d'importantes exigences, c'est bel et bien afin de renforcer la maîtrise par chacun des informations relevant de sa vie privée. Le RGPD développe en différents points les droits reconnus aux individus dont les données sont collectées : droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données vers un autre fournisseur de services, droit d'opposition (notamment au profilage), etc. De façon générale, le droit des personnes d'accéder aux données à caractère personnel qui les concernent est renforcé.

Les principes posés par la loi « Informatique et libertés » du 6 janvier 1978 restent d'actualité dans le cadre de la nouvelle réglementation européenne : proportionnalité de la collecte de données par rapport à la finalité du traitement, loyauté de cette collecte, droit d'opposition, droit de rectification ou de suppression, droit d'accès ou encore interdiction de principe de la collecte de données sensibles. Pour ce qui est du devoir d'information des personnes concernées et des cas dans lesquels leur consentement est requis avant toute collecte, les exigences sont renforcées.

La directive de 1995 proposait une définition du consentement à la collecte des données évasive qui a été transposée de manière très différente dans les législations nationales, tantôt en exigeant un consentement explicite, tantôt en retenant la possibilité d'un consentement implicite. Selon la nouvelle réglementation, le consentement 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* ». Le consentement à la collecte d'informations privées devra donc désormais être exprès. D'ailleurs, le règlement insiste sur le fait qu'« *il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité* ». En outre, une personne qui a accepté que ses données soient collectées sera en droit de revenir sur son consentement à tout moment.

Le contraste entre le droit des données personnelles européen et le droit des données personnelles américain, l'un étant de plus en plus exigeant quand l'autre est de plus en plus réduit à la portion congrue, est ainsi

saisissant.

Toutefois, le règlement européen établit la liste des différents cas dans lesquels un traitement de données pourra être réalisé sans besoin d'obtenir de consentement des personnes concernées : lorsque ce traitement est nécessaire à l'exécution d'un contrat ; lorsqu'il procède d'une obligation légale ; lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne ; lorsqu'il est utile à l'exécution d'une mission d'intérêt public ; pour tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne. Ce dernier cas de figure, fort imprécis, ne manque pas d'interroger tant il pourrait être la porte ouverte à des interprétations divergentes tant de la part des responsables de traitements que de la part des tribunaux.

Les missions de la CNIL réinventées

Avec le nouveau règlement européen, la CNIL et ses homologues européennes ne sont pas appelées à disparaître, mais leurs fonctions seront largement repensées. En effet, le RGPD prévoit la suppression des formalités préalables auprès des autorités de contrôle. Sauf exception, il n'y aura plus de déclaration ou de demande d'autorisation préalable à la mise en place de traitements de données à caractère personnel. En revanche, les « CNIL » auront la charge de contrôler la bonne mise en œuvre du droit des données personnelles, donc du règlement européen. Celui-ci leur confère par ailleurs d'importantes missions de sensibilisation du public et d'information. Et les autorités de contrôle bénéficieront de forts pouvoirs d'enquête et de sanction. Elles devront donc constituer les relais nationaux indispensables à la politique européenne de conciliation du développement de l'économie numérique et de la protection de la vie privée des personnes.

En outre, la directive « ePrivacy » devra, elle aussi, être révisée, afin de s'adapter au nouveau règlement européen. En janvier 2017, le Parlement européen a présenté les mesures visant à sa mise à jour, sous la forme d'un second règlement venant compléter le RGPD. En l'état, ce projet suscite de vives inquiétudes, notamment de la part des entreprises dont l'activité repose sur la collecte des données privées. Il prévoit en effet de permettre à chaque internaute de choisir par défaut, dès qu'il se connecte, le niveau de protection de ses données personnelles qui s'appliquera ensuite à tous les sites qu'il visitera. C'est donc par l'intermédiaire du logiciel de navigation utilisé que l'internaute décidera d'accepter ou non l'usage des *cookies* qui enregistrent ses données personnelles, au lieu d'en décider au cas par cas, site par site, comme il peut le faire aujourd'hui.

Dans une lettre ouverte au Parlement européen et au Conseil de l'Union publiée le 29 mai 2017, trente-trois éditeurs de presse européens déclarent souscrire à l'objectif du règlement « ePrivacy », notamment en matière de transparence pour le traitement des données. Mais, rappelant que les interfaces de navigation sont les portes d'entrée du web, ils avertissent qu'« *étant donné que 90 % de l'accès à internet sur le territoire européen est contrôlé par quatre entreprises seulement – Google, Apple, Microsoft et Mozilla – l'orientation prise par la Commission aboutira à renforcer l'asymétrie du rapport entre les éditeurs de presse et les portails numériques mondiaux* ». Les éditeurs de presse craignent que, contrairement à ce que

prévoyait le RGPD, l'instauration d'un consentement unique au niveau de chaque navigateur envisagée par le règlement « ePrivacy » ne les empêche d'avoir une relation directe avec les internautes, afin de les informer eux-mêmes des enjeux liés à la collecte de leurs données, des avantages qu'elle pourrait leur procurer, comme des offres éditoriales et des services personnalisés, ainsi que des publicités adaptées. « *En privant les éditeurs de presse de proposer des publicités ciblées à leurs lecteurs, « ePrivacy » favorise la réorientation des annonceurs publicitaires de la presse vers les plates-formes numériques dominantes, et diminue donc l'investissement possible dans le journalisme de qualité, partout en Europe* », déplorent les signataires de la lettre. Des plates-formes qui monopolisent déjà à elles seules les revenus de la publicité en ligne...

Sources :

- « Règlement européen sur la protection des données : ce qui change pour les professionnels », cnil.fr, 15 juin 2016.
- « Protection des données : la Cnil appelle à préparer l'application du règlement européen », Amaëlle Guiton, liberation.fr, 28 mars 2017.
- « Dix points-clés du règlement européen sur les données à caractère personnel », Stéphanie Foulgoc, feral-avocats.com, 16 mai 2017.
- « Données personnelles : la presse s'inquiète d'un projet européen restrictif », AFP, tv5monde.com, 28 mai 2017.
- Lettre ouverte au Parlement européen et au Conseil de l'Union, 33 entreprises de presse signataires, *Les Echos*, 29 mai 2017.
- « ePrivacy : les éditeurs inquiets face au texte européen », Louis Adam, zdnet.fr, 29 mai 2017.
- « La facture du RGPD estimée à 30 millions d'euros », Sébastien Dumoulin, *Les Echos*, 29 mai 2017.

Categorie

1. Droit

date créée

11 octobre 2017

Auteur

borisbarraud