Le futur règlement ePrivacy va réformer le régime de protection de la vie privée appliqué aux communications électroniques : réseaux de télécommunications, services de messagerie, pistage en ligne et géolocalisation. **La Quadrature du Net défend sept positions précises protégeant la vie privée.**

1. Adopter un règlement spécifique aux communications électroniques

Le RGPD : un règlement général applicable à tout secteur d'activité

Au printemps 2016, l'Union européenne s'est dotée d'un règlement général sur la protection des données (RGPD). À compter du 25 mai 2018, ce règlement s'imposera à toute personne traitant des données personnelles, quel que soit son secteur d'activité : médical, bancaire, administratif, assurance, ressources humaines, services publics, sur Internet, etc.

Sur certains points, le règlement prévoit des règles communes à tous ces secteurs (obligations de sécurité, droits conférés aux individus, contrôle opéré par des autorités indépendantes, sanctions...). Ces règles communes ne sont pas remises en cause par le règlement ePrivacy : elles continueront à s'appliquer telles quelles aux communications électroniques.

L' « intérêt légitime » : une exception générale dangereuse

À côté de ces règles communes, le RGPD a dû répondre à la question fondamentale suivante : dans quels cas est-il acceptable de traiter des données personnelles sans le consentement des personnes concernées ?

Compte tenu de l'importante diversité des activités auxquelles le RGPD s'applique, le législateur européen a choisi de ne pas y dresser de façon exhaustive la liste des finalités justifiant de se passer du consentement. À la place, une solution particulièrement incertaine a été choisie, héritée de la directive de 1995 : chaque acteur définit lui-même, en fonction de son activité, quels sont les « intérêts légitimes » (objectifs qui produisent des bienfaits plus importants que les nuisances qu'ils causent) qui l'autorisent à traiter des données sans consentement.

Le danger de cette solution vient du fait que, dans un premier temps, **cet équilibre est défini de façon unilatérale par chaque acteur, qui se retrouve alors juge et partie**. Ce n'est que dans un second temps, et dans les rares cas où ils en sont saisis, que la CNIL et les juges peuvent contrôler cet équilibre et sanctionner les acteurs qui ne l'ont pas respecté.

Un danger injustifiable à défaut de définitions sectorielles

Le législateur a pu se permettre une solution à ce point contraire à l'objectif de sécurité juridique car d'autres textes européens peuvent ensuite définir, secteur par secteur, une liste concrète et limitative des finalités justifiant de se passer du consentement.

Le RGPD serait contraire au respect le plus élémentaire des données personnelles si l'Union européenne ne se saisissait pas de cette opportunité pour lister autant qu'elle le peut **les finalités justifiant de se passer du consentement dans chaque secteur d'activité**. C'est l'objectif principal que poursuivait la directive ePrivacy et que doit poursuivre le règlement.

Des précisions propres aux communications électroniques

Certaines règles générales posées par le RGPD nécessitent d'être affinées lorsqu'elles s'appliquent aux communications électroniques. Comment donner un consentement libre sur Internet ? Qui peut consentir au traitement de données personnelles qui concernent plusieurs personnes à la fois ? Comment les données collectées peuvent être réutilisées par les États pour surveiller des individus ?

Ces précisions sont d'autant plus importantes que les communications électroniques produisent **des données personnelles déjà structurées**, rendant leur analyse automatisée particulièrement efficace pour révéler l'état physique ou émotionnel des individus, leur localisation, leurs habitudes, leurs opinions ou leurs rapports sociaux.

En outre, le RGPD ne concerne que le droit au respect des données personnelles consacré à l'article 8 de la Charte des droits fondamentaux de l'UE. Le règlement ePrivacy, lui, concerne aussi le respect de la vie privée, consacrés à l'article 7 de la Charte, qui couvre la confidentialité des communications électroniques.

2. Définir limitativement les dérogations au consentement

La proposition de règlement définit les finalités qui, en matière de communications électroniques, justifient de traiter des données sans le consentement des personnes concernées. Ces finalités peuvent être résumées à trois objectifs : **la fourniture, la sécurité et la facturation des services demandés par les utilisateurs**. La liste de ces finalités est limitative, exhaustive : toute finalité qui n'y est pas définie ne peut être poursuivie qu'avec le consentement des utilisateurs.

Aucun « intérêt légitime » n'est justifiable

Certains acteurs proposent d'intégrer dans ePrivacy l'exception d'« intérêt légitime ». Cette proposition est contraire à toute la structure du droit européen des données personnelles : un texte sectoriel, comme ePrivacy, a justement pour but de contenir les risques de cette exception générale.

Néanmoins, certains acteurs ont bien compris que les finalités qu'ils souhaitent poursuivre sans consentement (des finalités publicitaires, typiquement) ne seront pas acceptées comme telles par le législateur. Ainsi, plutôt que de soumettre directement ces finalités au débat, ils préfèrent demander d'intégrer l'exception d' « intérêt légitime ». La validité de tels « intérêts légitimes » n'étant contrôlée qu'*a posteriori* et à l'initiative des autorités de protection, ces acteurs espèrent ainsi, en pratique, pouvoir se passer du consentement pour des finalités que le législateur aurait écartées s'il en avait été saisi *a priori*.

Admettre l' « intérêt légitime » revient à **accepter que le débat législatif puisse être entièrement contourné** et à dénier reconnaître au législateur le moindre rôle.

Les traitements ultérieurs : un « intérêt légitime » encore plus dangereux

Le RGPD prévoit (article 6, §4 et considérant 50) que des données dont la collecte a été autorisée par un « intérêt légitime », un consentement ou une autre base légale peuvent être ré-utilisées sans consentement si elles le sont pour une finalité « compatible » avec la première.

Cette exception a la même logique que l' « intérêt légitime » : le RGPD concernant une infinité d'activités différentes, le législateur a permis une exception particulièrement imprévisible et dangereuse. Cette exception n'a aucune place dans un texte sectoriel dont le but est de lister les finalités permettant de se passer du consentement.

Enfin, elle ne repose sur aucun équilibre des intérêts mais sur la notion singulièrement vague de compatibilité qui, tel que définie par le RGPD, **n'inclut aucun critère de proportionnalité**. De plus, ici aussi, la compatibilité est évaluée unilatéralement par celui qui en bénéficie, qui se fait juge et partie.

La pseudonymisation : une simple mesure de sécurité

Certains acteurs souhaitent pouvoir traiter n'importe quelle donnée ayant été pseudonymisée, pour n'importe quelle finalité et sans consentement. Techniquement, les données pseudonymisées sont des jeux de données personnelles répartis sur des bases de données distinctes. Cette répartition technique **n'empêche pas l'exploitant de recouper les données**, mais constitue une simple mesure de sécurité, notamment destinée à diminuer les conséquences de fuites.

La pseudonymisation est une mesure saine qui doit être mise en œuvre chaque fois qu'elle peut l'être. Mais un traitement ne doit jamais pouvoir se passer du consentement pour la simple raison qu'il applique une mesure de sécurité. **Le droit des données personnelles a toujours conditionné la licéité des traitements à leur finalité**, et jamais uniquement à leur niveau de sécurité. Il doit en rester ainsi.

3. Préserver la liberté du consentement

Le RGPD prévoit que « *le consentement est présumé ne pas avoir été donné librement [...] si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution* » (considérant 43, précisant l'article 7, §4).

Si le consentement est donné sous la menace d'une perte (ne pas accéder à un service ou payer de l'argent), il n'est pas valide. Ainsi, **le consentement ne peut jamais être la contrepartie d'un bien ou d'un service**. Il n'est valide que s'il concerne une opération demandée par l'utilisateur ou s'il est donné de façon désintéressée.

Les libertés n'ont pas de valeur économique

Admettre que le consentement puisse être une contrepartie économique reviendrait à distribuer les libertés fondamentales selon des critères économiques. La vie privée deviendrait **un luxe réservé aux plus riches**.

En dehors du secteur des communications, certaines pratiques illustrent déjà parfaitement ceci. Tel est le cas des cartes de fidélité proposées par la grande distribution et qui permettent de ficher les clients à partir de leurs consommations quotidiennes – les définissant dans leur plus totale intimité. Alors que les plus riches peuvent se permettre d'échapper à cette surveillance en n'utilisant aucune carte, les plus pauvres n'ont souvent aucun choix. Refuser de se soumettre à ce contrôle total les priverait de promotions souvent indispensables pour clore leur budget. Ils ne peuvent pas s'offrir le « luxe » de l'intimité ni le « confort » de ne pas être surveillé. Or, il ne s'agit ici ni de luxe ni de confort, mais de libertés fondamentales.

C'est pour lutter contre de telles dérives qu'ont déjà été placées hors du commerce **l'intégrité physique** (l'article 3(2)(b) de la Charte de l'UE interdit de vendre les parties de son corps), la **liberté de disposer de son corps** (l'article 5 de la Charte interdit de se soumettre au travail forcé), celle de **se marier, de voter**, etc. La vie privée et le secret des correspondances n'ont absolument aucune raison de connaître un sort différent.

Un modèle économique contraire à la qualité de l'information

Divers sites internet prétendent ne pas pouvoir laisser le choix à leurs utilisateurs d'accepter la publicité ciblée ou non. Sinon, ces sites ne pourraient soi-disant plus se financer pour fournir leurs services. Ces prétentions sont probablement vraies s'agissant de certains sites (Facebook, typiquement), mais elle sont assurément fausses pour d'autres. C'est notamment le cas des éditeurs de presse, qui ont repris ce discours[1] pourtant opposé à leur situation.

Le modèle économique de la presse repose traditionnellement sur la vente et l'abonnement. Ce modèle demande de fidéliser un lectorat en lui donnant l'assurance de retrouver sur son média des analyses et des investigations de qualité. Or, il est désormais brutalement remis en cause par l'apparition d'acteurs concurrents qui proposent gratuitement sur internet des informations d'actualité ou de divertissement, simples et variées, demandant généralement peu de temps de lecture et destinées au plus large public possible. Ce nouveau modèle économique repose uniquement sur **la publicité ciblée, dont les revenus dépendent de la quantité de visiteurs touchés et non de la qualité de l'information.**

La concurrence imposée par ces nouveaux acteurs contraint une part importante de la presse traditionnelle à faire évoluer (non sans douleur) son modèle économique et la façon qu'elle a de produire de l'information — en investissant plus dans l'information « spectacle » et moins dans l'analyse et l'investigation, par exemple.

Cette évolution nuira forcément à la qualité du débat public, mais peut être limitée très simplement : en interdisant qu'un site puisse empêcher son accès aux utilisateurs qui refusent la publicité ciblée. Une telle protection des internautes remettrait profondément en cause le modèle économique fondée sur la publicité ciblée et, par effet de balancier, rendrait bien plus viables les modèles traditionnels fondés sur la fidélisation du lectorat et la qualité de l'information. Surtout, cette protection réconcilierait durablement le modèle économique de la presse avec le respect de droits fondamentaux de ses lecteurs.

Un consentement cédé n'est pas librement donné

Les fournisseurs de service doivent se souvenir du choix des utilisateurs de ne pas consentir. Ils ne doivent pas redemander le même consentement à la même personne jusqu'à ce que celle-ci cède. Autrement, ce consentement ne serait pas librement donné mais obtenu par harcèlement.

Par exemple, sur un site internet, un bandeau invitant l'utilisateur à consentir au dépôt de cookies ne doit pas réapparaître sur chaque page du site une fois que l'utilisateur a refusé. Autrement, fatigués par la gêne constante du bandeau, de nombreux utilisateurs finiraient par donner leur consentement pour ne plus subir cette nuisance. **Pour être libre, le consentement ne doit être demandé qu'une seule fois par site internet.**

Techniquement, une solution pour les sites internet pourrait être de déposer un simple cookie sur le terminal de l'utilisateur qui, identique pour tous, indiquerait simplement « *cookie: no* ».

4. Exiger un consentement complet pour l'analyse des communications

Le consentement de tous les correspondants

La proposition de règlement prévoit (article 6) que les communications électroniques ne peuvent être analysées que pour l'une des finalités envisagées (acheminement, sécurité ou facturation) ou si l'utilisateur y consent.

En matière de communication, il y a en principe plusieurs utilisateurs : l'expéditeur et le (ou les) destinataire(s). Or, l'actuelle proposition n'exige généralement le consentement que d'un seul des correspondants (sans qu'on sache s'il s'agit de l'expéditeur ou d'un des destinataires). Le règlement doit être modifié pour exiger clairement le consentement de l'ensemble des correspondants. **Un seul correspondant ne doit pas pouvoir consentir à la place des autres.** La CEDH a clairement reconnu que ce serait une violation du secret des correspondances[2].

Dans le cas du courriel, par exemple, un prestataire de communication souhaite analyser les métadonnées d'un message pour proposer de la publicité ciblée (Gmail[3], typiquement) à son utilisateur. Il devrait alors obtenir le consentement de son utilisateur (inscrit sur Gmail) ainsi que celui du correspondant extérieur (non inscrit) — en envoyant un courriel à ce dernier. Si le correspondant refuse, le prestataire de courriel devrait se souvenir de ce choix pour ne plus le lui redemander (en enregistrant

1 http://www.humanite.fr/sites/default/files/lettre_ouverte_tabloid-web.pdf

2 CEDH, *A c. France*, 23 novembre 1993, n° 14838/89 : l'enregistrement d'une conversation téléphonique autorisé par une seule partie est une atteinte au droit au respect des correspondances des autres parties impliquées dans la conversation.

3 Gmail prétend arrêter d'analyser le contenu des courriels à des fins publicitaires, mais semble manifestement continuer d'analyser les métadonnées. L'annonce de Google : https://www.blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

l'empreinte de son adresse de messagerie sur une liste, par exemple).

Enfin, par exception, il existe un cas (et un seul) où exiger le consentement de l'émetteur conduirait à des abus de droit : en matière d'anti-spam. Ici, seul le consentement du destinataire est obligatoire.

Le même consentement pour toutes les données

La proposition de règlement exige (article 6) un consentement différent pour analyser le contenu des communications électroniques ou leurs métadonnées (identité des correspondants, date et volume du message, pièce jointe...). Les métadonnées ne requièrent le consentement que d'un seul des correspondants, alors que cette exigence est variable et plus ambiguë s'agissant du contenu (article 6, § 3, a et b).

Cette distinction ne fait aucun sens : les deux types de données doivent être protégés de la même façon. Comme l'a récemment rappelé la Cour de justice de l'UE[4], les métadonnées « *sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes [...], telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés [...]. En particulier, ces données fournissent les moyens d'établir [...] le profil des personnes concernées,* ***information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications*** ».

5. S'opposer au consentement automatique pour le pistage

La proposition de règlement prévoit (considérant 24) que les utilisateurs puissent donner de façon automatique leur consentement au pistage en ligne *via* la configuration de leurs logiciels de communication. Par exemple, au moment de l'installation de leur navigateur Web, les utilisateurs pourraient accepter, par anticipation, tout futur dépôt de cookies.

Cette proposition est parfaitement contraire à l'exigence d'un consentement « informé » et spécifique » faite par le RGPD (article 4,§11) et doit être rejetée. Un consentement donné avant même que l'utilisateur ne connaisse l'auteur, la finalité et la nature du traitement, ou si les données pourront être transférées hors UE, **ne peut jamais être considéré comme étant informé.** De même, un choix unique visant une infinité de traitements est parfaitement **contraire à la définition de « spécifique »**.

6. Exiger le consentement pour la géolocalisation

En matière de géolocalisation des individus à partir des données émises par leurs terminaux, la Commission a proposé des considérants qui sont contradictoires et incohérents avec le corps des articles.

D'une part, les données émises par les terminaux afin de se connecter à un réseau sont considérés comme des métadonnées ne pouvant jamais être analysées sans consentement (cons. 17 et 20). D'autre part, leur analyse est autorisée pour n'importe quelle finalité et sans consentement (article 8).

La directive ePrivacy avait pris en compte le danger considérable posé par cette pratique en exigeant de façon parfaitement explicite le consentement des utilisateurs pour l'analyse de telles données (article 6 et considérant 35). Le règlement n'a aucune raison de réduire ici la protection de la vie privée des individus.

Les données émises ne doivent pas non plus pouvoir être utilisées pour contacter les utilisateurs sur leurs terminaux afin d'obtenir leur consentement. Cela conduirait à des pratiques de **« spam hors ligne » inacceptables** et incompatibles avec la liberté du consentement. L'utilisateur ne peut consentir que par une démarche proactive : en contactant lui-même l'exploitant pour lui donner son consentement (l'exploitant peut l'informer de cette possibilité sur des affiches exposées au lieu où l'analyse doit prendre place, par exemple).

7. Encadrer la surveillance d'État

L'article 11 de la proposition de règlement permet aux États membres d'autoriser ou de contraindre les acteurs du numérique à collaborer avec eux pour surveiller la population.

Contrairement à la directive ePrivacy, la proposition permet une telle surveillance pour « *un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale* ». Cette extension est injustifiable.

Plutôt que d'étendre les limites de la surveillance d'État, le règlement ePrivacy doit impérativement **intégrer dans le droit écrit les limitations décisives récemment posées par la Cour de justice**[5]. Il doit interdire aux prestataires de conserver de façon généralisées des informations concernant tous leurs utilisateurs. Les seules atteintes aux droits fondamentaux admissibles doivent permettre de lutter contre la **criminalité grave**, être **autorisées par un juge** et limitées dans le temps (à **deux mois** en matière de conservation de données) et cibler des personnes **individuellement désignées**.

4 CJUE, arrêt *Tele2*, rendu en grande chambre le 21 déc. 2016, C-203/15 et C-698/15.

5 CJUE, arrêt *Tele2*, précité.