Règlement « ePrivacy » : va-t-on « rejouer le match » du RGPD ?

La proposition de Règlement « ePrivacy » sur la protection de la vie privée et des données personnelles dans les communications électroniques, actuellement en cours de négociation,aura vocation à compléter le RGPD pour encadrer la fourniture et l'utilisation de services de communications électroniques et le traitement de données relatives aux équipements terminaux des utilisateurs. En pratique, le futur Règlement ePrivacy régulera directement l'économie des données européennes, car il s'appliquera à tout ce qui touche de près ou de loin à l'identification et à la traçabilité des terminaux, des usages et des comportements européens sur les réseaux de communications électroniques.Avec lui, la pluralité et la pérennité de la presse et des médias et de leur financement publicitaire sont en jeu, de même que l'écosystème européen de la publicité en ligne

Règlement « ePrivacy » : va-t-on« rejouer le match »du RGPD ?*Etienne DrouardJoséphine BeaufourCabinet K&L Gates*La proposition de Règlement « ePrivacy » sur la protection de la vie privée et des données personnelles dans les communications électroniques, actuellement en cours de négociation,aura vocation à compléter le RGPD pour encadrer la fourniture et l'utilisation de services de communications électroniques et le traitement de données relatives aux équipements terminaux des utilisateurs. En pratique, le futur Règlement ePrivacy régulera directement l'économie des données européennes, car il s'appliquera à tout ce qui touche de près ou de loin à l'identification et à la traçabilité des terminaux, des usages et des comportements européens sur les réseaux de communications électroniques.Avec lui, la pluralité et la pérennité de la presse et des médias et de leur financement publicitaire sont en jeu, de même que l'écosystème européen de la publicité en ligne

1. Des tractations à la hauteur des enjeux pour l'Union européenne
Des tractations intenses qui fragilisent le consensus européen autour du RGPD
La Commission pensait pouvoir faire vite dans le sillage du RGPD
Le 10 janvier 2017, la Commission européenne publiait une proposition de Règlement « ePrivacy »1 sur la protection de la vie privée et des données personnelles dans les communications électroniques (ci-après la**«** Proposition **»**). Les services de la Commission espéraient alors que cette Proposition de Règlement pourrait entrer en vigueur en mai 2018, en même temps que le Règlement Général sur la Protection des Données (ci aprèsRGPD) n° 2016-6792, puisque le futur Règlement ePrivacy a vocation à compléter le RGPD en se substituant à l'actuelle Directive ePrivacy 2002/583.
La Présidence de l'Union à la recherche d'un consensus européen
La Présidence autrichienne de l'Union européenne depuis juillet 20184 tente activement, comme la présidence bulgare avant elle (janvier-juillet 2018), de trouver un consensus entre, d'une part, la

position du Parlement européen issue d'un vote à faible majorité en octobre 20175, celle du Conseil (les États membres) et celle de la Commission européenne, qui espère renouveler auprès des citoyens européens le succès politique qu'a représenté le RGPD. Ainsi, la Présidence autrichienne espère pouvoir ouvrir à l'automne 2018 un « trilogue » entre les institutions européennes, qui permettrait de voter début 2019 un futur Règlement ePrivacy qui pourrait entrer en vigueur en 2020.
Les tractations en cours sont à l'image des enjeux de ce futur Règlement ePrivacy sur l'économie et l'innovation européennes. Elles révèlent de manière inquiétante que les antagonismes et les frustrations étouffés par l'adoption du RGPD, refont surface dès que la construction européenne s'affaiblit face aux stratégies nationales ou extra-européennes.

Le Règlement ePrivacy n'est pas une norme technique subsidiaire

Les points d'achoppement qui entourent la discussion de la Proposition ne sont pas anecdotiques ou technologiques. Ils touchent aux fondamentaux de la stratégie européenne en matière de protection des données personnelles, qui avait pourtant été déjà arbitrée durant quatre années de discussion du RGPD jusqu'en avril 2016 :

« on » veut écarter des bases légales pourtant consacrées par le RGPD (point REF _Ref519837776 \w \p \h 3 ci-dessous),

« on » présume que tout ce qui n'est pas consenti ou obligatoire, doit être interdit (point REF _Ref519837832 \w \p \h 2.2 ci-dessous),

« on » confierait aux géants américains et chinois qui conçoivent des logiciels de navigation, le soin de définir l'ergonomie de nos droits et relations entre un service en ligne et son visiteur (point REF _Ref519612586 \w \p \h 2.2.5(c) ci-dessous).

Ce faisant, on romprait les équilibres dégagés par l'Union européenne face au reste du monde à travers le RGPD.

La Proposition de Règlement ePrivacy n'est pourtant pas un texte technique et subsidiaire, sauf pour ceux qui ont intérêt à le faire croire en régulant l'informatique en latin, lorsqu'ils invoquent un statut de*lexspecialis*pour mieux déficeler les consensus politiques issus du RGPD.Cette Proposition déterminera très concrètement la stratégie numérique européenne. Elle aura des impacts sociaux, réglementaires et économiques bien plus approfondis sur les services en ligne que le RGPD, qui reste un texte général de définitions, de principes et de gouvernance de la conformité.

Est-il nécessaire de rappeler qu'entre janvier 2012 et avril 2016, l'élaboration du RGPD a fait l'objet de plus nombreux amendements que la Politique Agricole Commune durant 25 ans ?Pour rester crédible et compétitive sur les plans réglementaire et économique, l'Union européenne a besoin de stabilité et de cohérence. Ni les institutions, ni les entreprises ne peuvent s'aventurer vers une remise en cause des principes fondamentaux stabilisés il y a deux ans à peine avec l'adoption du RGPD et entrés en vigueur le 25 mai 2018.

Les services et secteurs concernés par ce futur Règlement ePrivacy

Le futur Règlement ePrivacy aura vocation à compléter le RGPD pour encadrer la fourniture et l'utilisation de services de communications électroniques (Article 1 de la Proposition) et le traitement

de données relatives aux équipements terminaux des utilisateurs (Article 2).En pratique, le futur Règlement ePrivacy régulera directement l'économie des données européennes, car il s'appliquera à tout ce qui touche de près ou de loin à l'identification et à la traçabilité des terminaux, des usages et des comportements européens sur les réseaux de communications électroniques. Ainsi, la connectivité GSM (3G, 4G, 5G, etc.), par câble, par fibre, par satellite, en wi-fi ou en bluetooth, l'usage d'un téléphone fixe, d'un téléphone mobile, l'accès à Internet en général, toute la navigation sur Internet, l'envoi d'un SMS, d'un fax ou d'un courriel commercial, l'existence et l'usage des annuaires téléphoniques, la géolocalisation des terminaux, le fonctionnement des véhicules connectés, la communication entre machines et, de manière générale, le traitement de toute donnée relative à l'utilisation de n'importe quel service ou terminal connecté, seront encadrés par ce Règlement européen.

Son impact sur l'économie et sur l'innovation européennes dépassera nécessairement celui du RGPD -et s'y ajoute-, puisqu'il ne s'agit plus « seulement » de définir des principes, mais de présumer que telle ou telle pratique, service ou traitement de données serait interdit*a priori*ou devrait être fortement limité.

Une association professionnelle américaine,*The Developpers Alliance*(regroupant notamment Facebook et Google) a récemment estimé que la Proposition, en l'état actuel, pourrait coûter aux entreprises européennes plus de 550 milliards d'euros en perte de revenus annuels6 et ferait chuter de 30 % les bénéfices produits par les secteurs touchant aux communications électroniques au sein de l'Union européenne.Ces chiffres alarmistes n'ont évidemment aucune neutralité et doivent être pris avec précaution. Mais il suffit d'envisager ce que l'industrie américaine dit craindre de perdre sur le marché européen, pour mesurer ce que l'économie européenne risque de perdre elle-même, si elle ne parvient pas à trouver un point d'équilibre entre efficacité des règles et innovation européenne.

Pourquoi faut-il un RÈglement ePrivacy en complÉment du RGPD ?

D'aucuns prétendent que le RGPD se suffirait à lui-même et que les régulateurs nationaux sauront très bien l'interpréter entre eux. C'est réglementairement juste, mais c'est politiquement faux et dangereux.Dès la publication de la Proposition en janvier 2017, on constatait déjà que laCommission européenne envisageait d'exclure certaines bases légales pourtant consacrées par le RGPD en avril 2016 et de poser des principes d'interdiction résultant de présomptions strictes selon lesquelles tout ce qui n'est pas nécessaire à la fourniture d'un service est interdit.Au prétexte d'un texte technique et sectoriel, cette évolution des règles vers la caricature démontre que l'Union européenne n'est pas encore parvenue à stabiliser sa politique de régulation de l'innovation, ni en son sein, ni à l'égard du reste du monde.

Des enjeux trop lourds pour n'être arbitrés que par des autorités nationales sectorielles

La version finale de la Proposition de Règlement se faisant attendre, la Directive ePrivacy n° 2002/58/CE du 12 juillet 20027*« concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques »*(ci après« la

Directive ePrivacy ») reste applicable.Elle complétait la Directive 95/46/CE du 24 octobre 19958 *« relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »*(ci-après « la Directive 95/46/CE **»**), qui est désormais abrogée depuis l'entrée en application du RGPD le 25 mai 2018.Il avait donc fallu sept ans aux États membres pour adopter une réglementation sectorielle en matière de communications électroniques. Durant cette période de gestation, l'Europe avait été traversée par une mutation sans précédent des communications électroniques : explosion de la téléphonie mobile, du courrier électronique et de l'internet, notamment marchand.

L'adoption d'une Directive sectorielle était alors perçue comme essentielle pour définir des règles spéciales dans ce secteur en pleine évolution économique et technologique. Les États, les entreprises et les régulateurs ont alors estimé qu'ils ne pouvaient se contenter d'une réglementation générale en matière de protection de données personnelles, qui aurait conduit à des insécurités réglementaires face à des enjeux d'innovation, d'économie, de société et de compétition intra et extra-européenne.Ces mêmes enjeux adjacents à la protection des données personnelles motivent aujourd'hui l'adoption d'un futur Règlement ePrivacy en complément du RGPD, car il ne suffit pas de confier à des régulateurs nationaux indépendants, si spécialisés et légitimes soient-ils, le soin d'appliquer des principes de protection des données personnelles, pour avoir déterminé une politique européenne cohérente, efficace et équilibrée, au cœur de l'innovation.Il s'agit de s'accorder sur un consensus politique donnant un cap à nos démocraties et déterminant la compétitivité de nos économies nationales et européennes, au sein de l'Union européenne et face au reste du monde. Cette tâche n'est pas celle des administrations chargées de protéger la vie privée et les données personnelles, fussent-elles indépendantes et expertes.

Les principales définitions et règles posées par la Proposition de Règlement

Des définitions nouvelles

La Proposition de Règlement introduit en son article 4, trois nouvelles définitions parmi lesquelles deux nouvelles catégories de données :

Les « données de communications électroniques »

Cette notion très large englobe à la fois le « contenu des communications électroniques » et les « métadonnées de communications électroniques ».

Le « contenu de communications électroniques »

Il s'agit de tout*« contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'image et de son »*.

Les « métadonnées de communications électroniques »

Il s'agit de toutes les données relatives à la transmission, la distribution ou l'échange de contenu de communications électroniques dans un réseau,

qui permettent de retracer une communication et d'en déterminer l'origine et la destination ou la localisation d'un terminal et,

qui sont produites à l'occasion de la fourniture de services de communications électroniques,

incluant la date, l'heure, la durée et le type de communication.

Annuaires téléphoniques

Si les coordonnées des personnes physiques sont aujourd'hui (et depuis 1948) publiées par défaut dans les annuaires, sauf opposition de leur part, l'article 15 de la Proposition inverse la tendance et pose un principe de non-publication dans les annuaires : les personnes physiques ne doivent plus pouvoir y être recherchées, sauf si elles y ont préalablement consenti (mécanisme de l'opt-in). Il s'agit donc de mettre fin aux annuaires, qui constituent pourtant, en France, un service public « universel ».

La confidentialité des données de communications électroniques

L'article 5 de la Proposition de Règlement pose**un principe général d'interdiction**, pour les personnes autres que l'utilisateur final, d'interférer avec des données de communications électroniques (par exemple, issues d'écoutes ou d'enregistrements), qui sont et doivent rester confidentielles et ne pourraient être traitées que sous réserve d'un strict principe de nécessité. Cependant, le texte admet, en l'état, que des interférences puissent être autorisées dans certaines situations spécifiques énoncées par le Règlement.

Le traitement et la conservation des données de communications électroniques

L'article 6.1 de la Proposition autoriserait les fournisseurs de service en ligne à traiter des données de communication, mais seulement si ce traitement est strictement nécessaire pour établir la communication ou assurer la sécurité des réseaux et services de communications électroniques, pendant une durée tout aussi nécessaire à ces fins.

Des traitements nécessaires ou soumis au consentement des personnes

Le traitement des métadonnées de communication

Les fournisseurs de services en ligne ne pourraient traiter des métadonnées de communication, que dans deux hypothèses seulement, décrites à l'article 6.2 de la Proposition de Règlement :**on ne pourrait traiter ces données que si on le doit**, car elles seraient indispensables au respect des obligations légales de qualité de service, pendant la durée nécessaire à cette fin, ou aux fins d'établir des factures ou de détecter ou faire cesser des fraudes à l'usage et à l'abonnement,**ou** ;**on ne pourrait traiter ces données que si les personnes y ont préalablement consenti**pour une ou plusieurs finalités précises. Toutefois, si un traitement d'informations anonymisées permettait de satisfaire ces mêmes finalités, le consentement ne devrait même pas être sollicité de la part des personnes.

Le traitement des contenus de communication

Le troisième et dernier paragraphe de l'article 6 de la Proposition de Règlement exigerait des fournisseurs de services de communications électroniques d'avoir recueilli le consentement valable des utilisateurs finaux pour pouvoir traiter des contenus de communications électroniques, à condition :

que tous les utilisateurs finaux concernés aient consenti au traitement de leurs communications électroniques pour un ou plusieurs objectifs spécifiques, et ;

d’avoir préalablement consulté l’autorité de contrôle compétente.
Toutefois, si un traitement d’informations anonymisées permettait d’atteindre ces mêmes finalités, le consentement ne devrait même pas être sollicité de la part des personnes.
La conservation et l’effacement des données de communications
La Proposition imposerait aux fournisseurs de service ligne d’effacer le contenu des communications électroniques ou d’anonymiser les données après réception de ce contenu par le ou les destinataires.Les métadonnées de communications électroniques devraient être effacées ou anonymisées dès qu’elles ne sont plus nécessaires au maintien de la communication, sauf si leur traitement est nécessaire à des fins de facturation. Dans ce cas, elles pourraient être conservées jusqu’à la fin de la période de contestation ou du litige relatif au paiement.
Le stockage et la lecture de données dans les – ou liées aux — terminaux des utilisateurs
Il s’agit du sujet le plus controversé de la Proposition, traversant les articles 8 à 10 du texte en discussion, qui touchent, avec l’article 6 (point REF _Ref519607709 \w \p \h 2.2.4(a)(i) ci-dessus), à l’identification et à la traçabilité des terminaux connectés et, par conséquent, au cœur de la protection et de l’économie européennes de la donnée.*L’article 8 pose, en l’état, deux interdictions qui ont vocation à réguler les fichiers« cookies »*et les traceurs ou identifiants utilisés systématiquement dans l’internet fixe ou mobile.Réguler les communications
« machine-to-machine »
En régulant le fait de lire ou d’écrire une information issue d’un terminal connecté, on régule directement les communications « machine-to-machine », que celles-ci soient associées ou non à des données relatives à un utilisateur, car l’individualisation d’un terminal relève déjà du champ de la vie privée, même si elle n’est pas forcément corrélée à des données susceptibles de permettre, même indirectement, l’identification d’un utilisateur.Ces identifiants des terminaux et logiciels que nous utilisons au quotidien ont des fonctionnalités et des noms très divers. Ils peuvent servir, par exemple, à authentifier les utilisateurs accédant à leur propre compte afin de leur donner accès à celui-ci, à personnaliser les contenus éditoriaux et les services en ligne, ou encore à permettre l’affichage, le plafonnement ou l’adaptation des publicités en ligne selon la navigation des personnes.Ces identifiants peuvent être constitués de fichiers bruts au format « texte »et contenant un identifiant technique. Ils peuvent être propres à un logiciel de navigation sur un terminal déterminé (les cookies), ou être attachés au système d’exploitation d’un terminal mobile (IdFA). Ils peuvent aussi se rapporter à un composant logiciel d’une application mobile (SDK), par exemple.
Des traitements nécessaires ou soumis au consentement des personnes
À l’article 8 de la Proposition, une interdiction de principe serait faite aux fournisseurs de services en ligne d’utiliser des capacités de traitement et de stockage du terminal d’un utilisateur ou de collecter des informations provenant du terminal d’un utilisateur final, y compris sur les logiciels et le matériel. Cette interdiction ne pourrait être levée que si :
le traitement est nécessaire pour établir une communication électronique ou pour fournir un service demandé par l’utilisateur, pendant la durée nécessaire à cette fin ;

le traitement est nécessaire pour mesurer des résultats d'audience, si cette mesure est réalisée par le fournisseur du service demandé par l'utilisateur final ;
le fournisseur de services en ligne a recueilli le consentement préalable et valide de l'utilisateur, sous réserve d'une information préalable et complète de ce dernier, conforme à l'article 13 du RGPD relatif à la collecte directe de données personnelles.

Le logiciel de navigation, seul gestionnaire des choix des personnes ?

L'article 10 de la Proposition modifiée par le Parlement européen en octobre 2017 prévoit que les internautes européens devront pouvoir choisir dès l'installation d'une nouvelle version de leur logiciel de navigation, de consentir ou de refuser l'inscription de cookies dans leur terminal, avant même d'accéder à Internet. Simple, voire simpliste - comme les fausses bonnes idées -, au point de contrevenir à la fois au RGPD et à l'intérêt de l'Union européenne.En effet, les fournisseurs de services en ligne ne pourraient plus utilement informer leurs visiteurs de la finalité des cookies présents sur leurs services, ni solliciter efficacement leur consentement libre, spécifique et éclairé. Le logiciel de navigation - américain ou chinois - poserait seul cette question, sans information ni explication et sans contrôle effectif des régulateurs européens.

Une fois sur internet, si les personnes ont déjà exprimé leur refus lors de la mise à jour de leur navigateur, le recueil de leur consentement à l'implantation de certains cookies ayant certaines finalités et provenant uniquement du service qu'ils visitent, ne serait pas pris en compte par leur navigateur : celui-ci continuera de rejeter tous les cookies, à moins que l'utilisateur ne modifie les paramètres de son navigateur et se résolve inversement à accepter tous les cookies de quiconque.

Pour quelle protection, finalement ?

Contrairement au RGPD, la Proposition substituerait ainsi au choix individuel, contextualisé, spécifique et informé des personnes, à l'occasion de l'accès à un service déterminé, un choix préalable, global, aveugle et décontextualisé, visant à accepter ou rejeter des cookies, sans information préalable conforme aux principes du RGPD. En outre, la Proposition ne traite pas des conditions ultérieures dans lesquelles les personnes pourraient modifier leurs préférences, dans quelque sens que ce soit, à tout moment, ni la manière dont ces modifications pourraient être prises en compte par les logiciels de navigation ou par les acteurs qui émettent des cookies ou autres traceurs.

Un peu de sens (géo)politique ne nuirait pas

Pour permettre à leurs utilisateurs finaux d'accepter ou de refuser certains cookies, les entreprises soumises au RGPD doivent mettre directement à leur disposition des facultés concrètes d'exprimer des choix éclairés. La plupart des entreprises européennes le font dans le respect des recommandations publiées par les divers régulateurs nationaux entre 2010 et 2013, en application de la Directive ePrivacy 2002/58/CE actuellement en vigueur.

Après avoir analysé la Proposition, les associations professionnelles françaises ont alerté les pouvoirs publics dès juin 2017, à Paris, à Strasbourg et à Bruxelles, par une position commune inédite par sa convergence et sa représentativité :*« Déplacer le consentement au niveau de*

*l'installation et de l'utilisation du logiciel de navigation priverait les entreprises européennes de toute interaction avec les utilisateurs finaux et de la connaissance de leurs préférences et de l'exercice de leurs droits. La Proposition de Règlement semble en effet confier la mise en œuvre du dispositif de recueil du consentement à des entreprises américaines qui dominent le marché mondial de la publicité digitale et comportementale, au rang desquels les trois principaux éditeurs de logiciels de navigation […]. Ce simple fait permettra à ces acteurs d'avoir une position très favorable, renforcée par leurs relations directes avec les internautes. Ainsi, ils pourront notamment utiliser des cookies nécessaires au fonctionnement du navigateur lui-même pour l'ensemble des services qu'ils fournissent ailleurs sur le web (recherche, publicité, audience, etc.). »*En l'état, la Présidence autrichienne de l'Union européenne a proposé le 17 juillet 2018 aux États membres réunis au sein du Conseil européen, de supprimer purement et simplement le projet d'article 10 décrit au point REF _Ref519612586 \w \p \h 2.2.5(c) ci-dessus. Nous saurons en octobre 2018, date à laquelle le Conseil européen envisage de se positionner, si cette proposition réunit un consensus entre eux. Ces atermoiements ne sont pas des tempêtes dans un verre d'eau tiède, car les enjeux économiques en cause pour l'Union européenne se chiffrent en dizaines de milliards d'euros chaque année. Ces discussions démontrent que lorsque*« le diable est dans les détails »*, il est nécessaire que s'affirme une prise de hauteur politique et stratégique. Pour ce faire, la question se pose de savoir pourquoi certains régulateurs veulent « rejouer le match » du RGPD dans le cadre de l'élaboration du futur Règlement ePrivacy.

Quelles philosophies de rÉgulation se cachent derriÈre les bases lÉgales ?

Les bases légales selon lesquelles une donnée personnelle peut être traitée, sont listées à l'article 6 du RGPD. Elles sont restées identiques à celles retenues par l'Union européenne depuis 1995 et théorisées en France depuis 1978. Aucune base légale ne prime sur une autre : soit une base légale est applicable, justifiable et satisfaite par le responsable de traitement, soit-elle ne l'est pas.Une entreprise dispose schématiquement de quatre bases légales pour justifier de traiter des données personnelles : (i) l'exécution d'une obligation légale, (ii) l'exécution d'une obligation contractuelle, (iii) la démonstration d'un équilibre entre les intérêts légitimes de l'entreprise et les mesures de protection qu'elle met en œuvre, ou (iv) le recueil du consentement libre des personnes.Les deux premiers fondements (l'obligation légale ou contractuelle) s'imposent à l'entreprise. Le troisième (la balance entre des intérêts légitimes et des protections suffisantes) requiert de démontrer, sous le contrôle du régulateur, l'effectivité de protections suffisantes. Le quatrième et dernier (le consentement) échappe aussi à l'entreprise, puisqu'il résulte de la libre volonté des personnes.

Le consentement est un régime d'interdictionLe consentement de l'utilisateur final tient une place prédominante, voir exclusive, au sein de la Proposition. Sa définition à l'article 9 de la Proposition reprend (inutilement) celle édictée aux Articles 4.11 et 7 du RGPD. Il s'agit de*« 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 ».

Selon les récentes lignes directrices des régulateurs européens, le consentement est absolument discrétionnaire, il ne peut être général, il doit être sollicité à nouveau pour toute nouvelle finalité, il n’est soumis à aucune condition, avantage ou détriment, il est réversible à l’envi, il est d’une durée de validité limitée et il doit être renouvelé, il est indépendant de l’accès à un service, quel que soit le modèle économique en jeu.Ainsi, lorsque le consentement est requis, le traitement d’une donnée est interdit tant qu’un consentement valable, discrétionnaire, éclairé, explicite, précis et réversible, n’a pas été exprimé sur la base d’une information complète fournie aux personnes, dénuée de toute manipulation ou omission susceptible de les influencer dans leur libre choix.

Le consentement est donc un régime d’interdiction, qui déplace l'action de réguler sur les personnes, qui sont réputées aptes à décider souverainement du monde qui les entoure. Ce véritable « droit au caprice » qui place la volonté libre de l’individu au-dessus de toute autre considération, ne peut constituer le fondement d’aucun service (le consentement se distingue de l’adhésion à un contrat) ni d’aucun modèle économique.Quelqu'un a-t-il déjà donné pareil consentement sans contrepartie à un tiers qui ne lui promet rien ni ne lui retire rien ? Créé en France en 1978 pour interdire le traitement des données sensibles relatives aux opinions politiques, philosophiques, religieuses ou syndicales, ce consentement-là, absolu et sanctifié, n’a jamais été « lâché seul » dans la sphère économique sans coexister avec des alternatives tout autant protectrices de l’individu (et malgré lui) et économiquement compatibles.L’approche binaire de la Proposition, entre nécessité et interdiction (consentement), n’est pas celle du RGPD ni de l’Union européenne depuis 1995, ni de la France depuis 1978.

La balance des intérêts et des garanties serait-elle devenue épouvantable ?

La seule évocation de cette base légale provoque des pincements de nez incompréhensibles, alors que RGPD la consacre comme les autres et alors que c’est la seule base légale qui porte en elle l’exigence d’une démonstration de la protection effective des données personnelles.Si ce troisième régime inquiète, c’est parce qu'il n'est pas binaire. Il nécessite de réfléchir et de décider.

Il s'agit, tout d'abord, de poursuivre un intérêt légitime, c’est-à-dire un objectif qui ne serait pas illégal par nature. Il s'agit, ensuite, de démontrer la mise en œuvre de mesures de protection des données personnelles effectives prescrites par le RGPD, afin d'équilibrer l'objectif de l'un et les droits de l'autre. Informer les personnes. Leur permettre d'exercer leurs droits : consentement, opposition, accès, portabilité, rectification, limitation, effacement. C’est-à-dire : sécuriser les données et établir un maillage contractuel de la conformité auprès de ses prestataires et partenaires ; minimiser les données à celles qui sont nécessaires ; Limiter les durées de conservation à ce qui est obligatoire ou objectivement justifiable ; pseudonymiser les informations de manière irréversible lorsque la connaissance de l'identité des personnes n'est pas nécessaire ; mesurer et réduire l'impact sur la vie privée des personnes en anticipant les risques d'une faille de sécurité ou d’un détournement des données, s’interdire des ciblages ou profilages aux effets discriminatoires, etc.

Pour les entreprises

Lorsque toutes ces mesures ont été envisagées dans le cadre d'une analyse préalable de conformité, l'entreprise prend la responsabilité d'être contredite et devra justifier en permanence auprès des personnes et des régulateurs, sur simple demande de leur part, de l’efficacité des mesures de protection mises en œuvre. Elle s'exposera à un risque médiatique, économique et juridique, identique à ceux des autres bases légales, puisque le régulateur peut à tout moment rétablir des équilibres qu’il estime non atteints, recommander, contrôler, arbitrer, amender et sanctionner.Au regard des sanctions encourues en application du RGPD, ce régime légal positionne la protection des données au cœur du processus de décision stratégique, car on n'arbitre pas à la légère, en interne, quand on conçoit un modèle économique d'exploitation de données qui s'expose à la contradiction et à des amendes maximales de 10 à 20 millions d'euros ou de 2 % à 4 % du chiffre d'affaires mondial consolidé.

Pour les régulateurs

Ce régime d'équilibre impose aux régulateurs européens de prendre le risque de réguler et de se mettre d'accord entre eux. En effet, il revient au régulateur de justifier auprès des responsables de traitement de données de l'insuffisance des garanties offertes aux personnes et à leurs droits. Il lui revient également de se justifier de ses raisonnements et admissions, si on devait lui reprocher d'avoir été trop conciliant ou d'être incohérent avec ses homologues dans des situations comparables.

Sur le fond

Pour les entreprises, ce régime de justification soumise à la contradiction n'est pas confortable, loin s'en faut. Il leur incombe de démontrer ou de convaincre du point d'équilibre qu'elles prétendraient avoir atteint. Mais il présente deux intérêts mêlés qui sont déterminants pour le devenir de nos sociétés européennes dans leurs rapports de force culturels, régaliens et économiques avec le reste du monde.Tout d'abord, il présente l'avantage de ne pas être un régime d'interdiction a priori (comme le consentement) ou d'exécution servile d'une prestation demandée (comme le contrat) ou d’une obligation légale. Ensuite, il permet et impose de concevoir ensemble l'innovation et la protection. En effet, on ne saurait faire souscrire un contrat portant sur un service encore inexistant et on ne saurait obtenir un consentement valable si on ne sait pas expliquer pourquoi on souhaite le recueillir.

Pourquoi certains rÉgulateurs veulent-ils « rejouer le match » du RGPD ?

Le futur Règlement ePrivacy fera-t-il disparaître la balance des intérêts et des garanties ? Tel est le souhait de ses premiers rédacteurs au sein de la Commission européenne et d'une courte majorité des parlementaires européens qui l'ont encore durci davantage, dont certains se sont dits investis d'une mission univoque et noble de*« protection des citoyens européens face aux mensonges des lobbyistes »*.

L’enfer (réglementaire) est pavé de bonnes intentions

On ne concevra pas des villes intelligentes et les services publics ou le système de couverture

sociale de demain sans comprendre l'usage qu'en ont nos concitoyens. On ne mesurera pas la fréquentation et le parcours des usagers d'un aéroport, d'une gare ou d'un magasin en leur demandant leur identité pour recueillir leur consentement libre, explicite et individuel. On ne financera pas la presse professionnelle accessible gratuitement, sans comprendre les centres d'intérêt de ses visiteurs ni compter et facturer à des annonceurs les publicités qui s'y affichent. On ne gérera pas des crises sanitaires, sécuritaires ou climatiques sans observer les comportements de navigation sur Internet ou de localisation.

L'évolution de nos sociétés européennes ne peut se réguler par le seul consentement individuel ou par l'exécution servile d'un contrat, car nul contrat et nul consentement discrétionnaire, ne peuvent aujourd'hui fonder l'analyse quantitative, qualitative ou prédictive de nos comportements, tout en garantissant une protection effective des données personnelles.Disposer d'une telle capacité d'analyse n'est ni bien ni mal. Y renoncer ou prétendre l'interdire en laissant nos concitoyens seuls avec leur consentement face à ces enjeux, c'est permettre au reste du monde de recueillir des données en Europe - qu'on le veuille ou non -, de les analyser en Californie ou en Chine, puis de vendre des services monopolistiques à nos entreprises, dénuées d'un savoir-faire dont elles ne pourront bientôt plus financer les cerveaux.

Le RGPD n’a modifié ou supprimé aucune base légale ni établi de hiérarchie entre elles

Réguler l'innovation sans l'empêcher est possible. C'est le défi que nous, européens, nous sommes lancés. Personne ne nous y a forcés. Personne d'autre ne nous y aidera. Nous protégeons nos valeurs, notre vision des équilibres démocratiques et économiques. Nous avons le devoir impérieux de réussir le pari que nous nous sommes lancé il y a 40 ans et qui puise ses racines dans notre vision politique du rapport de l'individu au corps social.

Une stratégie européenne de conquête en matière de protection des données personnelles nécessite de balancer des intérêts et des garanties.A-t-on le courage de dire aux entreprises européennes que les amendes qu'on se targue de préparer à l'encontre des GAFAM posent des interdits qui s'appliqueront d'abord aux sociétés européennes ?Il est là, le mensonge dont on pourrait aisément se passer. Il n'est pas une seule décision prise en Europe à l'encontre d'un Google, d'un Facebook ou d'un Whatsapp, qui ne soit directement applicable à l'identique à nombre de champions européens. Et c’est juste.Cependant, tous les champions du monde (non européens) de la donnée ont fondé leurs empires numériques sur un consentement invalide au regard du droit européen et sur des contrats d'adhésion qui s'autorisent unilatéralement à peu près tout.Ces pratiques non conformes et ces excès pourront être appréhendés efficacement par nos régulateurs sur la balance des intérêts et des garanties, en étant compréhensibles par d'autres régulateurs non européens. C'est probablement là que les Européens peuvent encore se donner une chance d'exporter leurs arguments hors de leurs frontières et de garder une économie numérique européenne forte.

Protéger les personnes ne peut se borner à interdire a priori

Sur l’article 6 de la Proposition (métadonnées)

Le smartphone d’un parisien passe à portée de 1 000 bornes wi-fi par jour en moyenne, même lorsqu'il reste dans la poche de son propriétaire. On devrait certainement pouvoir réguler les traces de sa détection technique autrement qu'en laissant croire aux personnes qu’elles décideraient seules et de tout.Réguler la durée de conservation de nos traces ou l'obligation de les transformer en des données pseudonymes irréversibles, serait probablement plus utile que de soumettre ces situations multiples à un consentement invalide ou aveugle, ce qui reviendrait à un régime d'interdiction inapplicable et, par voie de conséquence, inopérant.

Sur l’article 8 (cookies)

L'article 8 (sur les cookies) ne comporterait plus le fondement de la balance des intérêts et des garanties. Hors du consentement explicite de l'utilisateur, point de salut. On prétendrait ainsi interdire la publicité (du simple affichage jusqu'au ciblage) tant que les personnes n'ont pas consenti discrétionnairement à des cookies publicitaires.Mais qui donnerait un tel consentement, librement et, pour être valide, sans la moindre contrepartie ? Personne. À charge pour les éditeurs de presse et de services en ligne, par exemple, de faire payer leurs contenus à tous les internautes, ou à mettre la clé sous la porte.

Le pire n’est jamais sûr

Dans la compétition mondiale entourant l’exploitation des données personnelles, aucune institution ni aucune entreprise ne peuvent s’offrir le luxe de l’erreur ou de l’inefficacité des protections en cause. L’insécurité juridique dans ce domaine consiste à ne plus savoir expliquer pourquoi - et, donc, à ne pas laisser comprendre comment - on a choisi telle ou telle orientation de la réglementation en vigueur.Une telle insécurité porte en elle un lourd potentiel de destruction de valeur ou d’innovation, bien supérieur aux sanctions applicables en vertu du RGPD.

La pluralité et la pérennité de la presse et des médias et de leur financement publicitaire est en jeu et, avec elle, l’écosystème européen de la publicité en ligne, déjà très fragilisé par la puissance des géants américains de l’internet sur ce marché, qui ont déjà conquis de l’ordre de 70 % des budgets publicitaires dans l’internet fixe européen et jusqu’à 90 % dans l’internet mobile européen.

Éviter une telle insécurité juridique en Europe consiste à réaliser des équilibres nécessaires entre une protection efficace des personnes et une compétition mondiale. Il s’agit évidemment de ne renoncer ni à l’une ni à l’autre. L’atteinte de ces équilibres exige d’exprimer les tenants et aboutissants de nos craintes, de nos convictions et des règles qui en résulteront.Tout soumettre au consentement, c'est renoncer à réfléchir, à infléchir et à exporter notre vision européenne des équilibres sociaux. Avec les pouvoirs de sanction dont nous nous sommes dotés, autorisons-nous à être intelligents et efficaces.

Le 17 juillet 2018, la Présidence autrichienne de l’Union européenne a proposé au Conseil européen de supprimer le projet d’article 10 qui plaçait l’expression du consentement dans le logiciel de navigation. En outre, la proposition formulée en avril 2018 par la Présidence bulgare, qui ferait référence au Considérant 47 du RGPD dans l’article 8 de la Proposition, permettrait d’évoquer à mots couverts une référence à la légitimité des activités commerciales.C’est encore insignifiant,

juridico-technique et abscons pour les non-spécialistes. Mais ces propositions d'évolution semblaient inenvisageables il y a encore quelques semaines. Le chemin vers des choix politiques cohérents avec le RGPD reste encore long à parcourir, mais gageons, pour la trêve estivale, que le pire n'est jamais sûr.

E. D. et J. B.

Auteur(s) :

Etienne Drouard - Avocat associé -

Président de la Commission juridique GESTE

Joséphine Beaufour - Avocat - Cabinet K&L Gates

Notes de bas de page :

1. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

2. http://data.europa.eu/eli/reg/2016/679/oj

3. http://data.europa.eu/eli/dir/2002/58/oj

4. https://ec.europa.eu/luxembourg/events/la-pr%C3%A9sidence-autrichienne-du-conseil-de-lunion-europ%C3%A9enne-se-pr%C3%A9sente_fr

5. http://www.europarl.europa.eu/news/fr/press-room/20171016IPR86162/communications-en-ligne-le-respect-de-la-vie-privee-renforce

6. « The Next Privacy Battle in Europe Is Over This Law », Natasha Singer, The New York Times, 27 mai 2018.

7. http://data.europa.eu/eli/dir/2002/58/oj

8. http://data.europa.eu/eli/dir/1995/46/oj

9. https://www.cnil.fr/fr/comment-ca-marche

10. https://fr.wikipedia.org/wiki/Cookie_(informatique)

11. Le numéro IdFA (ou « IFA » pour “Identifier for Advertisers”) est un identifiant temporaire d’un terminal mobile Apple, dédié à l’usage publicitaire. Il a succédé au numéro « UDId » (Unique Device Identifier), qui identifiait auparavant un terminal, quelle qu’en soit la finalité d’usage. L’IdFA est dédié à l’identification publicitaire des terminaux Apple depuis iOS6. Un identifiant équivalent de l’IdFA existe aussi dans les terminaux mobiles fonctionnant sous Android (Google).

12. L’acronyme anglais “SDK” (pour “Software Development Kit”) désigne un composant logiciel de programmation d’une application mobile. On distingue généralement trois types de SDK : (1) les SDK de programmation liés à un certain type de système d’exploitation (iOS, Android, Windows, etc.), (2) les SDK de maintenance, qui détectent et analysent des dysfonctionnements ou « crashes » au sein d’une application mobile et (3) les SDK de mesure d’audience et publicitaires, pour constater l’utilisation d’une application et y insérer des publicités.

13. https://www.ufmd.org/attachment/912353/: (juin 2017) Position interprofessionnelle sur la Proposition de Règlement e-privacy 2017/0003(COD), qui a rassemblé plus de 98% des acteurs français des divers métiers de l’internet, de la presse quotidienne, régionale aux medias et éditeurs de contenus et de services en ligne, aux TV et webTV, aux e-commerçants, aux agences de communication et régies publicitaires, jusqu’aux annonceurs.

14. Lignes directrices sur le consentement adoptées en novembre 2017 et déjà modifiées en avril 2018 : https://www.cnil.fr/sites/default/files/atoms/files/wp259_enpdf_consent.pdf.Lignes directrices sur la transparence adoptées en novembre 2017 et déjà modifiées en avril 2018 : https://www.cnil.fr/sites/default/files/atoms/files/wp260_enpdf_transparency.pdf.Lignes directrices sur le profilage adoptées en octobre 2017 et déjà modifiées en février 2018 : https://www.cnil.fr/sites/default/files/atoms/files/20171025_wp251_enpdf_profilage.pdfLignes directrices concernant l’analyse d’impact relative à la protection des données adoptées en avril 2017 et déjà modifiées en octobre 2017 : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf