Sociétés et numérique

6023

Durée : 3h

Session : Mai 2018

Exercice : note d'analyse

A partir des dossiers documentaires fournis et des connaissances acquises en cours, vous produirez une note d'analyse relative **à l'un des deux** sujets qui suivent (au choix). Votre note d'analyse devra comprendre une courte synthèse des documents ainsi qu'une page (recto-verso) qui présentera votre analyse du sujet choisi.

Sujet n°1 : Apports et limites de la loi française « anti-fake news » (p.2-13).

Sujet n°2 : Les enjeux de la protection des données personnelles (p.14-21).

SUJET n°1 : Apports et limites de loi française « anti-*fake news* »

N° 799

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 21 mars 2018.

PROPOSITION DE LOI

relative à la **lutte contre** *les* **fausses informations**,

(Renvoyée à la commission des affaires culturelles et de l'éducation, à défaut de constitution
d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par Mesdames et Messieurs

Richard FERRAND, Yaël BRAUN-PIVET, Bruno STUDER, Naïma MOUTCHOU, Gabriel ATTAL, Patrice ANATO, Sophie BEAUDOUIN-HUBIÈRE, Barbara BESSOT BALLOT, Danièle CAZARIAN, Olivier DAMAISIN, Benjamin DIRX, Stéphanie DO, Coralie DUBOST, Frédérique DUMAS, Alexandre HOLROYD, Dimitri HOUBRON, Denis MASSEGLIA, Monica MICHEL, Pierre-Alain RAPHAN, Stéphane TESTÉ, Caroline ABADIE, Damien ADAM, Saïd AHAMADA, François ANDRÉ, Pieyre-Alexandre ANGLADE, Jean-Philippe ARDOUIN, Laetitia AVIA, Aurore BERGÉ, Danielle BRULEBOIS, Stéphane BUCHOU, Céline CALVEZ, Philippe CHALUMEAU, Fannette CHARVIER, Christine CLOAREC, Fabienne COLBOC, François CORMIER-BOULIGEON, Bérangère COUILLARD, Amélie de MONTCHALIN, Jennifer De TEMMERMAN, Audrey DUFEU SCHUBERT, Françoise DUMAS, Christophe EUZET, Valéria FAURE-MUNTIAN, Philippe FOLLIOT, Pascale FONTENEL-PERSONNE, Jean-Luc FUGIT, Séverine GIPSON, Joël GIRAUD, Fabien GOUTTEFARDE, Florence GRANJUS, Émilie GUEREL, Yannick HAURY, Philippe HUPPÉ, Monique IBORRA, Caroline JANVIER, Catherine KAMOWSKI, Rodrigue KOKOUENDO, Gaël LE BOHEC, Gilles LE GENDRE, Marion LENNE, Richard LIOGER, Brigitte LISO, Alexandra LOUIS, Jacques MARILOSSIAN, Sereine MAUBORGNE, Thomas MESNIER, Cécile MUSCHOTTI, Claire O'PETIT, Matthieu ORPHELIN, Catherine OSSON, Xavier PALUSZKIEWICZ, Sophie PANONACLE, Patrice PERROT, Anne-Laurence PETEL, Laurent PIETRASZEWSKI, Jean-François PORTARRIEU, Éric POULLIAT,

Hugues RENSON, Xavier ROSEREN, Bertrand SORRE, Vincent THIÉBAUT, Agnès THILL, Nicole TRISSE, Frédérique TUFFNELL, Marie-Christine VERDIER-JOUCLAS, Martine WONNER, Jean-Marc ZULESI et les membres du groupe La République en Marche et apparentés,

députés.

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

L'actualité électorale récente a démontré l'existence de campagnes massives de diffusion de fausses informations destinées à modifier le cours normal du processus électoral par l'intermédiaire des services de communication en ligne.

Si les responsabilités civiles et pénales des auteurs de ces fausses informations peuvent être recherchées sur le fondement des lois existantes, celles-ci sont toutefois insuffisantes pour permettre le retrait rapide des contenus en ligne afin d'éviter leur propagation ou leur réapparition.

Les mesures proposées dans cette perspective doivent toutefois être conciliées avec la préservation de la liberté d'expression. Cet enjeu majeur se pose avec d'autant plus d'acuité dans le cadre du débat électoral au cours duquel s'expriment par nature des opinions ou arguments que les adversaires des candidats peuvent estimer insincères.

Afin d'être en mesure de contrecarrer d'éventuelles opérations de déstabilisation qui pourraient survenir lors des prochaines échéances électorales, trois axes de réforme sont envisagés :

– d'une part, de nouveaux outils permettront de mieux lutter contre la diffusion de fausses informations durant la période électorale.

Il s'agit, durant les périodes pré-électorale et électorale (c'est-à-dire à compter de la date de publication du décret convoquant les électeurs) :

– en amont, d'imposer aux plateformes des obligations de transparence renforcées en vue de permettre, d'une part, aux autorités publiques de détecter d'éventuelles campagnes de déstabilisation des institutions par la diffusion de fausses informations et, d'autre part, aux internautes de connaître notamment l'annonceur des contenus sponsorisés ;

– en aval, de permettre que soit rendue une décision judiciaire à bref délai visant à faire cesser leur diffusion.

Tel est l'objet du titre I^{er}.

En amont, eu égard à l'intérêt s'attachant à la lutte contre la diffusion des fausses informations, des obligations relativement poussées de transparence seront imposées aux plateformes (réseaux sociaux, moteurs de recherche, plateformes de partage de contenus, portails d'information, etc.), dont les services sont utilisés de manière massive et sophistiquée par ceux qui souhaitent propager de fausses informations, sans porter une atteinte disproportionnée à la liberté du commerce et de l'industrie.

L'article L. 111-7 du code de la consommation impose d'ores et déjà aux opérateurs de plateformes en ligne une obligation de loyauté à destination des consommateurs. Cette obligation concerne leurs conditions générales d'utilisation, ou encore leurs modalités de référencement, de classement et de déréférencement des offres mises en ligne.

L'article L. 111-7 du code de la consommation prévoit également que ces plateformes doivent faire apparaître clairement l'existence éventuelle d'une relation contractuelle, de liens capitalistiques ou de rémunération à leur profit dès lors qu'ils influencent le classement des contenus, des biens et des services proposés ou mis en ligne. Cette obligation permet notamment d'imposer aux plateformes de signaler par une indication claire, par exemple par une icône, qu'un contenu est mis en avant contre rémunération.

S'agissant de l'enjeu spécifique de la lutte contre les fausses informations en période électorale, ces obligations viendraient compléter les dispositions de droit commun en matière de transparence des plateformes qui découlent des articles L. 111-7 et suivants du code de la consommation.

Ces obligations de transparence concernent en particulier les contenus d'information mis en avant contre rémunération (contenus « sponsorisés ») par l'intermédiaire des réseaux et des moteurs de recherche, au-delà d'un certain seuil d'audience. Sans préjudice des obligations déjà applicables en vertu de l'article L. 111-7 du code de la consommation, elles portent sur l'identité de l'annonceur et des personnes qui le contrôlent ou pour le compte desquelles il agit, ainsi que, au-delà d'un seuil à définir par décret, les montants consacrés à la mise en avant de ces contenus. Sont donc en cause les contenus d'information liés à l'actualité, même lorsqu'ils ne se rapportent pas directement au débat électoral, qu'ils fassent ou non l'objet d'un traitement journalistique. En sens inverse, ne sont pas concernés les contenus visant à promouvoir des biens ou des services, tels que ceux publiés sur les plateformes de commerce en ligne.

De telles obligations de transparence doivent permettre, d'une part, aux autorités publiques de veiller au respect de l'interdiction de la publicité commerciale à des fins de propagande électorale (article L. 52-1 du code électoral) et de détecter d'éventuelles campagnes de déstabilisation des institutions ou de manipulation de l'opinion. Le recours à des contenus « sponsorisés » est en effet l'une des techniques d'acquisition d'audience utilisées en vue d'une large diffusion des fausses informations. Ces obligations peuvent, d'autre part, servir à informer et sensibiliser les internautes qui utilisent les plateformes en cause, en leur permettant, s'ils le souhaitent, de connaître notamment l'annonceur des contenus sponsorisés.

En aval, dès lors qu'une fausse information s'est propagée, seule l'intervention du juge est de nature à assurer la conciliation entre, d'une part, la liberté d'expression et le droit à l'information et, d'autre part, la préservation de la sincérité du scrutin.

L'approche pénale étant insuffisante à remplir l'objectif poursuivi, l'**article 1er** propose d'introduire, au sein du code électoral, une nouvelle action en référé devant le juge civil dont la mise en œuvre serait limitée aux périodes pré-électorale et électorale précitées. Le juge se verrait ainsi confier le soin de prononcer, à l'égard des tiers tels que les hébergeurs, plateformes et fournisseurs d'accès à internet, des mesures visant à faire

cesser la diffusion de fausses informations et ce indépendamment de toute mise en cause de leur responsabilité.

Le dispositif proposé à leur égard est inspiré du référé dit « LCEN ». Il sera applicable lorsque des fausses informations (à l'exclusion, naturellement, des contenus parodiques ou satiriques) et de nature à altérer la sincérité du scrutin à venir auront été diffusés en ligne, de manière à la fois massive et artificielle (c'est-à-dire, notamment, par le biais de contenus sponsorisés ou promus au moyen d'outils automatisés dits « bots »). Le juge, statuant en urgence (48 h), pourra ordonner le déréférencement du site, le retrait du contenu en cause ainsi que l'interdiction de sa remise en ligne, la fermeture du compte d'un utilisateur ayant contribué de manière répétée à la diffusion de ce contenu, voire le blocage d'accès au site internet. Ces mesures seront librement appréciées par le juge sous réserve de leur adéquation et de leur proportionnalité au regard de la liberté d'expression.

Compte tenu du caractère national de l'écho donné à la diffusion massive des fausses informations objet de la présente mesure, il est prévu de donner compétence exclusive au tribunal de grande instance de Paris pour connaître de ces actions, cette compétence étant fixée par un décret auquel il est renvoyé.

L'**article 2** a pour objet de rendre ces nouvelles dispositions applicables durant les élections sénatoriales et l'**article 3** durant les élections des représentants français au Parlement européen.

– d'autre part, de nouveaux pouvoirs sont conférés au Conseil supérieur de l'audiovisuel : le **titre II** vise à permettre au Conseil supérieur de l'audiovisuel d'empêcher, de suspendre ou de mettre fin à la diffusion de services de télévision contrôlés par un État étranger et qui portent atteinte aux intérêts fondamentaux de la Nation ou participent à une entreprise de déstabilisation de ses institutions.

La modification de l'article 33-1 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication par l'**article 4** vise en premier lieu à sécuriser la possibilité pour le Conseil supérieur de l'audiovisuel de refuser de conclure une convention avec un service n'utilisant pas de fréquences hertziennes, en explicitant la jurisprudence du Conseil d'État relative aux refus de conventionnement.

Le second alinéa autorise quant à lui le Conseil supérieur de l'audiovisuel à refuser un conventionnement à une chaîne lorsqu'elle est liée à un État étranger dont les activités sont de nature à gravement perturber la vie de la Nation, notamment par la « diffusion de fausses nouvelles », notion qui figure déjà dans la loi du 29 juillet 1881 sur la liberté de la presse. Afin de saisir la grande diversité des situations qui peuvent se présenter, le dispositif vise non seulement les chaînes contrôlées au sens du code du commerce, mais également celles qui sont « sous l'influence » d'un État étranger, notion beaucoup plus large qui devrait être appréciée à l'aide d'un faisceau d'indices. Enfin, il autorise le régulateur à prendre en compte les agissements de l'ensemble des sociétés liées à la société éditrice de la chaîne et les contenus édités sur tous les services de communication au public par voie électronique (notamment les réseaux sociaux ou les sites de presse en ligne) afin de lui permettre de saisir l'ensemble des stratégies qui pourraient être mises en place par certains États.

L'**article 5** insère un nouvel article 33-1-1 pour instituer une procédure exceptionnelle de suspension administrative de la diffusion d'un service conventionné, en période électorale (élections présidentielles, législatives, sénatoriales, européennes et référendum), si les agissements en cause ont pour objet ou pour effet d'altérer la sincérité du scrutin à venir.

Le nouvel article 42-6 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication créé par l'**article 6** organise un régime de sanction parallèle à celui créé pour le refus de conventionnement, permettant au Conseil supérieur de l'audiovisuel de retirer la convention en cas d'agissements postérieurs à sa signature, selon la procédure prévue par l'article 42-7 de la loi du 30 septembre 1986 (**article 7**).

L'**article 8** prévoit la modification de l'article 42-10 de la même loi qui organise le référé administratif audiovisuel permettant au président de la section du contentieux du Conseil d'État, à la demande du Conseil supérieur de l'audiovisuel, d'ordonner au responsable d'un service de communication audiovisuelle de se mettre en conformité avec ses obligations. Il vient compléter le dispositif en permettant au juge de suspendre en urgence la diffusion d'un service pour les mêmes motifs que ceux autorisant le Conseil supérieur de l'audiovisuel à résilier une convention. Cette procédure est complémentaire du pouvoir de résiliation conféré au Conseil supérieur de l'audiovisuel, en ce qu'elle permet de suspendre en urgence la diffusion d'un service sans attendre que la procédure de sanction engagée par le Conseil, encadrée par des contraintes procédurales spécifiques, ne soit parvenue à son terme. Elle est en revanche la seule voie d'action possible à l'encontre des chaînes relevant de la compétence de la France mais qui ne sont pas soumises à une obligation de conventionnement.

– enfin, le devoir de coopération des intermédiaires techniques est renforcé ; le **titre III** crée au sein du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique un article 7 *bis* visant à ajouter la lutte contre les fausses informations aux obligations de coopération imposées aux intermédiaires techniques I de l'article 6.

Ce devoir de coopération, élargi par l'**article 9**, implique des obligations renforcées pour les prestataires concernés. Au-delà de l'obligation de retirer promptement tout contenu illicite porté à leur connaissance (« *notice and take down* »), les prestataires visés sont soumis à l'obligation de mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance des contenus constitutifs de fausses informations, d'une part, et de relayer promptement auprès des autorités publiques compétentes les signalements relatifs à ces contenus transmis par les internautes, d'autre part. Ils doivent, enfin, rendre publics les moyens qu'ils consacrent à la lutte contre la diffusion de fausses informations. Cette troisième obligation est transversale et impose une transparence dans la mise en place des deux premières obligations.

Ce que le projet de loi français contre les fake news nous réserve

Sébastien Seibt, *France 24*, 13/02/2018

La ministre de la Culture Françoise Nyssen a présenté mardi son dispositif de lutte contre la prolifération de fausses informations. Emmanuel Macron, qui en a été la cible durant la campagne présidentielle, en a fait une priorité.

Fake news, gare à vous ! Emmanuel Macron et sa ministre de la Culture Françoise Nyssen ont fini d'aiguiser leurs armes contre les fausses informations sur Internet. Le projet de loi de fiabilité et de confiance de l'information, présenté aux éditeurs de presse mardi 13 février, vise à dépoussiérer l'arsenal juridique existant pour l'adapter à l'ère numérique.

Nouvelles obligations pour les Facebook, Twitter & co., pouvoir accru du Conseil supérieur de l'audiovisuel (CSA), possibilité de saisir le juge des référés en période électorale... Le président français ne veut pas d'une redite des campagnes de désinformation qui l'ont visé durant la présidentielle 2017.

Son constat : les dispositions héritées de la loi de 1881 sur le droit de la presse ne suffisent pas. Pour ce texte fondateur, le délit de fausse nouvelle désigne la publication d'informations erronées "par voie de presse ou par tout autre moyen de publication". Une définition suffisamment vague pour inclure le tweet mensonger ou encore la vidéo aussi virale que fallacieuse. Le problème est que cette loi "n'est pas adaptée à la vie sur les réseaux, marquée par la rapidité de diffusion et par la facilité pour tout un chacun de devenir diffuseur", explique Antoine Chéron, avocat au cabinet ABCM, spécialiste du droit des nouvelles technologies de l'information.

Du "bot" russe à l'article mensonger

Le nouveau dispositif doit permettre de sanctionner, avant qu'il ne soit trop tard, et de viser aussi bien le bot (compte automatisé) Twitter russe que l'article mensonger en ligne. Une attention particulière sera apportée aux périodes électorales. "La nouvelle loi cible deux vecteurs : les réseaux sociaux comme Facebook et les médias sous influence d'une puissance étrangère – essentiellement la Russie", résume l'avocat français.

Pour ce faire et pendant cinq semaines avant un scrutin, le CSA pourra "suspendre un média sous influence", c'est-à-dire retirer sa licence à un site ou une chaîne de télé réputée proche d'un gouvernement qui diffuserait des informations erronées. Le gendarme des médias aura aussi le droit de demander à des plateformes (YouTube, Facebook, etc.) de publier les noms des sponsors d'articles ou campagnes en ligne visant à influencer un vote à l'aide d'arguments mensongers. Ces sites devront également révéler les sommes dépensées pour de telles campagnes de désinformation.

Toujours dans un souci de rapidité, le juge des référés pourra être saisi par "toute personne intéressée à agir" pour faire cesser la circulation de *fake news*diffusées "massivement et artificiellement". Cette procédure est cependant soumise à une condition : "Le juge devra non seulement déterminer si la nouvelle est fausse, mais également caractériser la mauvaise foi de la personne à l'origine de la diffusion, et caractériser un 'trouble à la paix publique', ce qui n'est pas aisé", précise Antoine Chéron.

Trop d'urgence tue l'urgence ?

La priorité de ce texte musclé présenté par Françoise Nyssen – pouvoir dégainer la sanction plus vite que son ombre – a soulevé bon nombre de réticences. Lors de l'élection présidentielle américaine et du référendum sur le Brexit, les enquêtes ont mis du temps à établir avec certitude qu'il y avait eu un effort coordonné pour tenter d'influencer le scrutin à grand renfort d'informations trompeuses. Le projet de loi française pousse les juges et le CSA à agir à chaud.

Le risque étant que "l'urgence répondant à l'urgence, la recherche de la vérité passe au second plan", prévient Antoine Chéron. La tentation pourrait être grande de sanctionner d'abord pour éviter un emballement médiatique autour d'une information potentiellement "fake", et de réfléchir ensuite.

Il n'y a pas que la pression de l'urgence qui peut pousser à des dérives. Ce nouveau dispositif confère aussi au CSA et aux juges un droit de vie et de mort sur l'information. À eux de décider si le contenu d'un article est vrai ou faux. Certes, certains précédents, comme des articles durant l'élection américaine clamant à tort qu'Hillary Clinton était impliquée dans un scandale sexuel, avec pour décor une pizzeria de Washington, démontre que la tentative de manipulation peut être grossière. Mais lorsque les campagnes seront plus subtiles, la décision du CSA de suspendre, par exemple, une chaîne pourra sembler arbitraire.

Ils seront investis du droit de vie et de mort sur une information – décider si elle est "vraie" ou "fausse" –, et devront décider au plus vite si un internaute a fait circuler une *fake news* de bonne ou mauvaise foi. Autant de questions qui ne manqueront pas d'être évoquées au cours des mois qui viennent, puisque Françoise Nyssen a précisé que les organes de presse seront consultés pour que d'éventuelles modifications au projet de loi puissent aboutir à un texte qui satisfera tout le monde d'ici à l'été 2018.

La ministre de la culture précise les contours de la loi contre les « fake news »

Le Monde, 13 février 2018

Surveillance des réseaux sociaux et médias sous influence d'un Etat étranger, procédure de référé pour pouvoir bloquer rapidement les fausses informations… Françoise Nyssen a précisé les contours de la proposition de loi contre les « fake news ».

Légiférer sur les fausses informations – ou *fake news* – en ligne, c'est l'ambition du gouvernement depuis l'annonce d'Emmanuel Macron lors de ses vœux à la presse au début de janvier. Un sujet complexe qui soulève de nombreuses questions, notamment parmi les journalistes.

La ministre de la culture, Françoise Nyssen, a précisé, mardi 13 février, les contours de la proposition de loi qui sera déposée dans les prochains jours, et également lancé une consultation pour réformer la loi Bichet qui régit la distribution de la presse.

Autorités de régulation, représentants des éditeurs, des diffuseurs et des dépositaires de presse seront consultés jusqu'à avril-mai afin qu'un texte de loi soit présenté à l'Assemblée nationale *« avant l'été »*.

- **Surveillance des réseaux sociaux et des médias sous influence d'un Etat étranger**

La loi contre les *fake news*, rebaptisée loi sur *« la confiance et la fiabilité de l'information »* se concentrera sur les *« tuyaux »*, c'est-à-dire sur les modes de diffusion des fausses nouvelles que sont les réseaux sociaux et les *« médias sous influence d'un Etat étranger »*, avec une attention particulière durant les périodes de campagne électorale, a précisé le ministère de la culture.

Il s'agira, pendant une période de cinq semaines au maximum, de permettre au Conseil supérieur de l'audiovisuel de *« suspendre la convention d'un média sous influence étrangère »* et d'obliger les plates-formes numériques à signaler les contenus sponsorisés, en publiant le nom de leur auteur et la somme perçue.

Le ministère justifie cette loi en citant trois cas où la circulation des fausses nouvelles aurait été massive et déterminante : la campagne du Brexit, la dernière élection états-unienne et le référendum catalan, souligne-t-on au ministère.

- **Procédure de référé pour pouvoir bloquer rapidement les « fake news »**

Elle prévoit une procédure de référé pour pouvoir faire cesser rapidement la circulation de fake news diffusées *« massivement et artificiellement »*.

C'est le juge des référés qui qualifiera la fausse information, dont la définition existe déjà dans la loi de 1881 sur la liberté de la presse.

- **Devoir de coopération des plates-formes Web**

Du côté des plates-formes Web (Facebook, YouTube, etc.), le *« devoir de coopération »* qui existe déjà pour les contenus pédopornographiques ou d'apologie du terrorisme sera étendu aux fausses nouvelles, avec une obligation pour elles de se donner les moyens d'une vigilance accrue en période électorale.

Le projet de loi est moins sévère que la législation allemande – en Allemagne les retraits de publication sont jugés trop automatiques par le ministère de la culture français –, mais plus contraignant que ce qui se fait en Grande-Bretagne, où il n'existe aucun devoir de coopération des plates-formes.

- **Réformer la loi sur la distribution de la presse**

  La ministre Françoise Nyssen, qui présentait ces points dans le cadre de la quatrième conférence des éditeurs de presse, a également lancé une concertation de la filière pour réformer la loi Bichet de 1947 sur la distribution de la presse.

  « Toutes les pistes sont ouvertes » précise le ministère, qui souhaite que cette réforme soit aussi large que la future loi sur l'audiovisuel public, prévue pour la fin de 2018.

L'Union Européenne s'attaque aux « fake news »

Sylvestre Huet, Blog « Sciences » de la plateforme du Monde, 11 mars 2018

Le comité d'experts sur les fake news mis en place en novembre dernier par la Commission Européenne vient de rendre public son rapport. Issu de quatre réunions et d'intenses échanges, il survient alors que les études scientifiques sur la diffusion préférentielle des fausses nouvelles sur les réseaux sociaux comme Twitter ont fait la Une de la revue *Science* vendredi dernier. Ou qu'Emmanuel Macron annonce une intervention législative favorisant l'action judiciaire contre la diffusion de fausses informations.

Ce texte de 46 pages met d'emblée le sujet au niveau d'un «*risque pour nos processus démocratiques, la sécurité nationale, le tissu social, et peut miner la confiance dans une société de l'information et le marché unique numérique*». Un risque dont l'origine est précisée rigoureusement : la propagation volontaire d'information fausses, imprécises ou trompeuses conçues et diffusées pour nuire au public ou pour en obtenir un profit économique, financier, politique (en particulier lors des élections) ou idéologique. Le rapport ne s'intéresse donc que très peu à la propagation d'une fausse information par des personnes ne les ayant pas identifiées comme telles, et donc victimes de la désinformation.

Crise de confiance

En revanche, il insiste pour placer le problème dans une vision large de la manière dont l'information est produite, distribuée dans la sphère publique. Une vision qui inclut le journalisme, les média numériques et la montée des plate-formes (Facebook, Google, Twitter…) mais aussi le contexte de crise de confiance des citoyens envers les institutions publiques nationales et européennes. Cette vision s'interroge sur le rôle des médias numériques mais tout le monde en prend pour son grade.

Les responsables politiques pour disséminer de fausses informations (ci-contre un exemple célèbre) ou vouloir contrôler la presse à leur profit. Les journaux qui n'ont pas tous «*le même standard de professionnalisme ou d'indépendance éditoriale*». Voire les acteurs de la société civile, comme les ONG qui peuvent certes jouer un rôle de fact-checking ici, mais aussi désinformer à leur tour là. Quant aux « platforms US-based » – le texte désigne ainsi Facebook, Twitter, Google… – leur « *pouvoir croissant* » dans la circulation de l'information en font les vecteurs principaux des fake news et doit aller avec un responsabilité croissante, estiment les experts européens.

« fake news » ou « false news »

La «*désinformation*» doit être affrontée tout «*en respectant la liberté d'expression, de recevoir et de donner de l'information*», posent en préalable les 39 experts nommés par la Commissaire Européenne en charge de « la société et l'économie numérique » Mariya Gabriel. Ils ne sont donc pas très chauds pour une intervention législative lourde… Alors que de son côté Tim Berners-Lee, l'un des créateurs des protocoles logiciels du web au Cern, appelle à une régulation des plate-formes. Une pierre dans le jardin d'Emmanuel Macron. Leur rapport s'inscrit dans une démarche résumée ci-dessous :

Le texte se heurte d'emblée à un problème de vocabulaire puisque toute cette action de la Commission Européenne a été présentée sous l'appellation « fake news », et est d'ailleurs titré « *Rapport du groupe d'expert de haut niveau européen sur les fake news* » dans sa version draft. Or, les experts recommandent justement de ne pas utiliser ce terme, en particulier en raison de son utilisation par des politiciens pour désigner une couverture médiatique à leur

désavantage. Il est à craindre que cette volonté de pureté de vocabulaire soit d'une totale inefficacité dans la sphère médiatique, même non anglophone, tant la formule « fake news » se coule dans le moule journalistique : court, évocateur, attractif et tranchant.

Les articles de *Science* se heurtaient à ce même problème, mais si les éditeurs de la revue scientifique l'ont contourné dans leur titre de Une (utilisant la formule «*false news*») il est à parier qu'ils ne seront guère suivis par la presse généraliste (démonstration avec le titre de cette note….).

Transparence des algorithmes

Très dense, ce rapport émet de nombreuses analyses et recommandations qu'il est difficile de résumer. Je vais donc en choisir quelques unes, un choix sans rapport avec l'équilibre du texte, qui montrent à quel point l'action proposée est vaste et va se heurter à des résistances.

► Le rapport souligne la nécessité d'un accès des chercheurs et des autorités d'enquête ou d'audits aux origines et chemins de dissémination des informations sur les réseaux numériques. Autrement dit, un peu comme le secret commercial est inacceptable lorsque la santé publique est en jeu, les experts estiment que la « santé politique » de nos sociétés s'oppose à toute tentative de secret des Facebook, Twitter ou Google sur le fonctionnement de leurs réseaux. Cette transparence, y compris pour les médias qui doivent être informés lorsque les algorithmes de classement sont changés, sera nécessairement un objet d'affrontement violent mais elle est jugée indispensable par les experts.

► Les experts soulignent la puissance des technologies dans la propagation de l'information (vraie ou fausse) mais également qu'aucune technologie ne peut résoudre seule un problème social et politique et que des personnes sont responsables de la manière dont ces technologies sont développées. Bref, ils récusent l'excuse « c'est pas Zuckerberg, c'est le robot ».

► Il faut créer une culture de l'information et des médias numériques – autrement dit une lecture critique de leurs contenus, le texte anglais utilise le mot literacy qui peut se traduire par alphabétisation, mais je préfère « culture » car il faut aller bien au delà d'un apprentissage primaire – et la diffuser, à l'école et dans la société, tant près des jeunes que des adultes. Elle doit devenir une «*compétence essentielle*» pour une citoyenneté active et la participation à la sphère publique numérique. Le texte insiste sur le caractère «*préventif*» de cette action vis à vis des fausses informations. Le « vaccin » est donc jugé plus efficace que le « médicament » avalé après exposition au risque de la fausse information. Cette culture doit être introduite «*à une échelle massive*» dans les programmes scolaires et la formation des enseignants, précise le texte.

► Les pouvoirs publics doivent favoriser l'environnement d'une presse pluraliste, tant privée que publique (le nombre de journalistes titulaires de la carte de presse a chuté de 37 390 en 2009 à 35 047 en 2017. Et ils sont de plus en plus souvent précaires, partent de moins en moins souvent en reportages.) Le communiqué de la Commission européenne accompagnant la publication du rapport précise que «Selon la dernière enquête Eurobaromètre (environ 26 000 personnes interrogées), le public a le sentiment que beaucoup de fausses informations circulent dans l'UE, 83 % des participants indiquant que ce phénomène représente un danger pour la démocratie. Cette enquête met également en exergue l'importance de la qualité des médias: les participants voient dans les médias traditionnels la source d'information la plus fiable (radio 70 %, télévision 66 %, presse écrite 63 %). Les sources d'information en ligne et les sites d'hébergement de vidéos seraient les moins dignes de confiance, 26 % et 27 % des participants, respectivement, leur accordant du crédit.»

►Les pouvoirs publics doivent soutenir la création de centres de recherches publiques sur la véracité des informations sur les affaires d'intérêt général (politique, santé, science, éducation,

finance…), l'identification et la cartographie des sources de désinformation et les mécanisme de leur amplification numérique.

► Il faut « démonétiser » la diffusion de fausses informations (interdire la publicité sur des pages internet dont le contenu est faux). Voir l'analyse des décodeurs du Monde sur ces sites commerciaux dont le modèle économique accentue leur propension à diffuser des informations fausses mais qui attirent du clic par leur contenu « insolite ». C'est l'application au monde numérique du vieil adage journalistique «un chien mort un homme, rien, un homme mort un chien, un papier». Ces usines à fausses informations doivent être frappées au portefeuille si l'on veut stopper la machine infernale. Même motif même punition pour Facebook, la plus puissante source de fake news.

►Informer clairement l'internaute de ce qu'une information, surtout présentée en priorité a été payée, par qui et dans quels objectifs (publicité commerciale, propagande politique…) et donc qu'elle ne provient pas d'une source journalistique. Egalement informer de l'intervention d'un robot ou d'un paiement dans l'amplification de la diffusion d'une information.

Sujet n°2 : Les enjeux de la protection des données personnelles

Facebook : la lucrative économie des données personnelles

Emmanuelle Réju, *La Croix*, 12 avril 2018

Le PDG de Facebook Mark Zuckerberg a dû s'expliquer mardi 10 et mercredi 11 avril devant le congrès américain sur l'utilisation des données personnelles des utilisateurs du réseau social. Le scandale lié à la société Cambridge analytica met en lumière le fonctionnement de l'économie numérique. Explications

► De quelles données parle-t-on ?

Ce serait le nouvel or noir, le pétrole du XXI[e] siècle, le gisement dans lequel puiseraient les nouveaux géants de l'économie mondiale. Votre nom, votre âge, votre lieu d'habitation… Mais aussi vos centres d'intérêt, vos voyages, vos habitudes de consommation ou encore vos préférences politiques. Que vous réserviez un voyage en ligne ou que vous partagiez une photo avec vos « amis » Facebook, il en restera une trace sur Internet, qui sera dûment stockée.

Facebook a accès à un très grand nombre d'informations sur chacun de ses 2 milliards d'abonnés à travers le monde, au-delà même de ce que ces derniers écrivent sur leur page Facebook, des photos ou vidéos qu'ils y « postent », de leurs « amis » ou encore des contenus qui les intéressent grâce à la touche « like »…

Sa connaissance des habitudes des abonnés va plus loin, puisque ces derniers se connectent sur de nombreux sites via leur compte Facebook. Et que des échanges d'informations se produisent ensuite entre Facebook et ces sites. Résultat, Facebook est capable de dresser de ses utilisateurs une véritable identité numérique.

Auditionné mardi 10 avril par le Sénat américain, le PDG de Facebook, Mark Zuckerberg, n'a pas répondu à la sénatrice démocrate de Californie, Kamala Harris, lui demandant de confirmer que Facebook détiendrait jusqu'à 93 catégories d'informations sur ses abonnés

► Comment ces données sont-elles utilisées ?

Le réseau social ne vend pas directement les données ainsi collectées comme on vendrait par exemple un fichier d'adresses. *« Facebook vend de l'attention »*, affirme Alexandre de Cornière, professeur à l'école d'économie de Toulouse, spécialiste de l'économie d'Internet.

Deux milliards d'abonnés, qui passent en moyenne une heure par jour sur le réseau, *« représentent en effet le plus gros marché média en termes d'attention au monde »*, ajoute-t-il. Surtout quand l'utilisation de Facebook se fait de plus en plus sur téléphone mobile, avec peu de possibilités d'échapper à la publicité.

Bref, le réseau social vend des espaces publicitaires, comme un journal vend un espace de publicité, mais avec un atout considérable : sa capacité à cibler avec une grande précision le profil de consommateur visé par l'annonceur, grâce à la connaissance accumulée sur chaque abonné.

Facebook ne s'est lancé dans le marché de la publicité en ligne que depuis 2012. Un marché détenu aujourd'hui par un « duopole » constitué de Facebook et du moteur de recherche Google qui fonctionne sur le même modèle. L'an dernier, le marché publicitaire a représenté 98 % du chiffre d'affaires de Facebook qui a engrangé un bénéfice de 16 milliards de dollars.

► En quoi est-ce un problème ?

« Les publicités ciblées ne sont pas toujours considérées comme une nuisance, souligne Alexandre de Cornière. *Au contraire, certaines personnes y trouvent un intérêt puisque ces publicités sont faites pour les intéresser ! »*

Reste que de nombreuses personnes prennent aujourd'hui conscience de l'ampleur des connaissances personnelles accumulées – et stockées – par ces entreprises. Un fonctionnement que les internautes n'ont pas toujours voulu regarder en face.

« Les Américains sont tombés amoureux des réseaux sociaux et comme tous les jeunes amants, ils ont voulu vivre leur passion sans trop discuter », analyse ainsi dans une tribune publiée dans *Le Monde*, l'anthropologue américaine Sherry Turkle, spécialiste des réseaux sociaux.

Tout dépend aussi de l'utilisation qui est faite de ces données. Qu'elles aident à vendre des chaussures, pourquoi pas. Mais les enjeux sont différents quand il s'agit d'influencer le vote des électeurs. *« Le fait que des équipes de campagne envoient des publicités ciblées à certains électeurs, comme cela a été fait par Donald Trump, mais aussi par Barack Obama, est moins bien perçu »*, analyse Alexandre de Cornière.

Reste surtout la question cruciale du consentement, qui pèse lourd dans la tourmente dans laquelle se trouve Facebook aujourd'hui. Si l'utilisation des données personnelles figure dans les conditions générales d'utilisation de Facebook ou de Google, bien peu d'internautes se donnent la peine de les lire.

Et encore faudrait-il les comprendre. *« Votre agrément d'utilisation est nul,* s'est ainsi emporté le sénateur républicain John Kennedy, lors de l'audition du PDG de Facebook. *Rentrez chez vous et demandez à vos juristes payés 1 200 dollars l'heure d'écrire un texte en anglais ! »*

Cette question du consentement est aussi au cœur du scandale qui entoure la firme Cambridge Analytica. En répondant au test mis en ligne sur Facebook par ce cabinet spécialisé en marketing politique, les internautes ne savaient pas en effet que cette dernière pourrait ainsi « siphonner » les informations personnelles de leur groupe d'amis et récolter ainsi des informations sans leur consentement (sans compter que l'entreprise avançait masquée en se présentant sous les habits d'un projet de recherche universitaire).

La réglementation européenne sur les données personnelles, qui doit entrer en vigueur le 25 mai prochain prévoit que les internautes devront être informés de manière intelligible du traitement des données fournies lors d'une consultation sur Internet et donner leur accord de manière non ambiguë pour le traitement de leurs données. Celles-ci ne devront par ailleurs être stockées que *« le temps nécessaire »*. Pour le moment, aucune restriction de ce type n'existe aux États-Unis.

Ce qui est reproché à Google dans l'usage des données personnelles des enfants sur YouTube

Klervi Grouglazet, *L'Usine Nouvelle*, 11 avril 2018.

Lundi 9 avril 2018, une vingtaine d'associations de défense des droits numériques ont saisi la Federal Trade Commission (FTC) aux Etats-Unis. Elles accusent Google de collecter illégalement des données personnelles sur les enfants via la plateforme YouTube et de les utiliser pour de la publicité ciblée.

Alors que Facebook vacille suite au scandale Cambridge Analytica, c'est au tour de YouTube d'entrer sur le terrain glissant de la gestion des données personnelles : 23 associations de défense des droits numériques et de protection de l'enfance accusent la plateforme de vidéos d'exploiter les données personnelles d'enfants à des fins commerciales. *"Google amasse des informations sans informer au préalable les parents et il les utilise pour cibler des publicités vers les enfants partout sur Internet"*, indique le communiqué rendu public le lundi 9 avril 2018, adressé à la Commission fédérale du commerce (FTC) des États-Unis qui pourrait décider d'ouvrir une enquête.
Appareil de connexion, localisation ou encore numéro de téléphone portable… Selon ces associations américaines, Google, la maison-mère de YouTube, collecte les données personnelles des enfants alors qu'il est interdit d'avoir un compte YouTube avant l'âge de 13 ans. *"Depuis des années, Google a abandonné sa responsabilité envers les enfants et les familles en affirmant de façon trompeuse que YouTube – un site inondé de dessins animés, comptines et publicités pour des jouets – n'est pas pour les enfants de moins de 13 ans"*, assène Josh Golin, directeur de l'association signataire Campaign for a Commercial-Free Child Hood.

YOUTUBE INTERDIT AUX MOINS DE 13 ANS

La plainte accuse YouTube de faire preuve d'hypocrisie. Même si la plateforme est *"réservée aux utilisateurs de plus de treize ans, certains contenus ciblent les jeunes enfants"*, développent les plaignants. *"Des recherches montrent que plus de 80 % des enfants de 4 à 8 ans sont sur YouTube*". Selon une étude du cabinet Trendera, 45 % des enfants de 8 à 12 ans ont un compte YouTube. Mais rappelons qu'il n'est absolument pas nécessaire de posséder un compte pour visionner une vidéo sur la plateforme et qu'un jeune utilisateur peut très facilement mentir sur sa date naissance pour en ouvrir un.
En déposant plainte, les associations disent vouloir *"aider les parents et les enfants à prendre des décisions intelligentes quand ils sont en ligne. Pour que quand ils se connectent, ils n'aient pas à s'inquiéter des publicités et d'avoir leurs identifiants et data accumulées sur le long terme".*

QUE DIT LA LOI ?

Une loi est citée à plusieurs reprises dans le communiqué : *"Google réalise des profits gigantesques avec les pubs pour enfants et doit respecter la COPPA"*. Le Children's Online Privacy Protection Act (COPPA) est une loi américaine votée en 1998 et entrée en vigueur en avril 2000. Elle interdit la collecte en ligne d'informations personnelles sur les enfants de moins de 13 ans, sans le consentement vérifiable de l'un des deux parents.
Jusqu'en 2013, la loi COPPA s'appliquait uniquement aux sites Web. Depuis, elle concerne également également les jeux en ligne et les applications, très utilisés par les enfants sur smartphone ou tablette. Cette modification a permis notamment de réguler la collecte des informations par le biais des plugins.

QUE DIT YOUTUBE ?

Google a assuré, par la voix de son porte-parole, que la protection des enfants et les familles est *"une priorité". "Parce que YouTube n'est pas pour les enfants, nous avons investi de façon importante pour créer l'application YouTube Kids, qui propose une alternative spécialement destinée aux enfants"*, a insisté le géant de Mountain View.

L'application mobile YouTube Kids a justement été accusé mi-mars, d'exposer les jeunes enfants à des contenus complotistes, attestant par exemple que la Terre est plate (diffusé par le conspirologue David Icke), que les premiers pas de l'Homme sur la Lune ont été tournés en studio, ou encore que les pyramides de Gizeh ont été construites par des extraterrestres. En fin d'année dernière, le site américain The Verge pointait du doigt des commentaires à caractère pédophile.

Face à ces polémiques, YouTube a annoncé en décembre dernier, vouloir augmenter ses effectifs de modérateurs de 25 % d'ici la fin de l'année 2018. Et selon une information de BuzzFeed datant du 6 avril, YouTube Kids s'apprêterait à faire filtrer ses vidéos uniquement par des opérateurs humains et non pas des algorithmes comme c'est le cas aujourd'hui. Jusqu'à maintenant, l'algorithme de filtrage ne sait pas analyser le contenu verbal des vidéos et analyse uniquement les mots clés du contenu.

RGPD : 10 questions pour comprendre le nouveau règlement sur la protection des données

Julien Lausson, *Numérama*, 15 février 2018

Le Règlement général sur la protection des données, ou RGPD, est amené à prendre une place de plus en plus importante dans l'actualité. En effet, ce texte, voté en 2016, sera appliqué dans l'Union européenne à partir du 25 mai 2018. Voici donc une FAQ pour répondre à toutes vos questions.

RGPD par-ci, GDPR par-là… depuis près de deux ans, ces acronymes reviennent dans l'actualité avec une intensité croissante. Vous avez peut-être vaguement entendu parler qu'ils étaient en lien avec une loi européenne sur les données personnelles mais vous ne savez peut-être pas clairement de quoi il retourne. Aussi avons-nous eu l'idée d'écrire une foire aux questions pour répondre aux interrogations que vous pourriez avoir.

QU'EST-CE QUE LE RGPD ?

Le Règlement général sur la protection des données (RGPD ou GDPR, pour *General data protection regulation* en anglais) est le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces informations sur lesquelles les entreprises s'appuient pour proposer des services et des produits. Ce texte couvre l' ensemble des résidents de l'Union européenne.

Avant le RGPD — dont le nom plus solennel est le règlement du Parlement européen et du Conseil du 27 avril 2016 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 — existait une directive sur la protection des données personnelles qui date de 1995. Ce texte est abrogé par le RGPD.

QUEL EST L'OBJECTIF DU RGPD ?

L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles, en remplaçant une directive datant de 1995. Une réforme de la législation européenne apparaissait nécessaire au regard de sa relative vétusté, accentuée par l'explosion du numérique et l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques.

Il s'agit aussi d'harmoniser le panorama juridique européen en matière de protection des données personnelles, afin qu'il n'y ait qu'un seul et même cadre qui s'applique parmi l'ensemble des États membres, que ce soit en France, en Allemagne, en Italie ou en Espagne ainsi que dans la vingtaine d'autres pays de l'Union. De cette façon, la fragmentation juridique sur le Vieux Continent s'en trouve atténuée.

D'OÙ VIENT LE RGPD ?

L'idée initiale vient du constat fait par la Commission européenne que la législation d'alors, entrée en vigueur en 1995, avait besoin d'être actualisée pour tenir compte des évolutions technologiques. En 2012, Bruxelles a donc proposé un nouveau règlement, dont la carrière législative au niveau européen s'est étalée jusqu'en 2016, avec notamment le 15 décembre 2015, un accord entre le Conseil, le Parlement et la Commission.

Le parcours du texte au niveau européen s'est fait dans un contexte particulier : le 13 mai 2014, la Cour de justice de l'Union européenne rendait son fameux arrêt qui oblige essentiellement Google à donner satisfaction aux internautes du Vieux Continent qui demandent le retrait de résultats qui les concernent, consacrant ainsi l'existence d'un droit au déréférencement (sorte de droit à l'oubli *light*) sur le net.

Un an plus tard, le 1er octobre 2015, la même Cour de justice a invalidé le régime juridique dit du « Safe Harbor » qui permettait aux entreprises américaines d'importer aux USA des données personnelles de citoyens européens. Celui-ci a été jugé invalide en raison des révélations d'Edward Snowden sur le programme PRISM, par lequel la NSA accèderait aux données stockées aux USA.

QUAND LE RGPD entre-t-il en vigueur ?

Le déploiement du RGPD dans l'espace européen se fait en deux temps : il y a d'abord eu, le 14 avril 2016, l'adoption définitive du texte par le Parlement, suivi quelques jours plus tard, le 27, de sa promulgation au Journal officiel. Cependant, son application ne s'est pas déroulée au même moment : il a été décidé de la décaler de deux ans, au 25 mai 2018. Dans à peine plus de trois mois.

Ce laps de temps permet à la fois aux législations nationales et aux entités procédant à la collecte et au traitement des données personnelles de s'y préparer, en transposant dans le droit des États membres les dispositions du RGPD et en adaptant les traitements déjà mis en œuvre pour qu'ils soient en conformité avec le texte. Après le 25 mai, tout traitement en infraction avec le RGPD pourra déboucher sur des sanctions.

C'EST QUOI UNE DONNÉE PERSONNELLE ?

Une donnée personnelle (ou donnée à caractère personnel) est une information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

Certaines données sont sensibles, car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés :

Une opinion politique, une sensibilité religieuse, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des idées philosophiques sont des données sensibles. Elles ont un cadre particulier, qui interdit toute collecte préalable sans consentement écrit, clair et explicite, et pour des cas précis, validés par la Cnil et dont l'intérêt public est avéré.

QU'EST-CE QUE LE RGPD CHANGE POUR L'INTERNAUTE ?

Du point de vue de l'internaute, le RGPD met en place ou conforte un certain nombre de protections. Il faut par exemple que les entreprises récoltent au préalable un consentement écrit, clair et explicite de l'internaute avant tout traitement de données personnelles, ou qu'ils s'assurent que les enfants en-dessous d'un certain âge aient bien reçu l'aval de leurs parents avant de s'inscrire sur un réseau social.

Le RGPD inclut aussi une reconnaissance d'un droit à l'oubli pour obtenir le retrait ou l'effacement de données personnelles en cas d'atteinte à la vie privée, le droit à la portabilité des données, pour pouvoir passer d'un réseau social à l'autre, d'un FAI à l'autre ou d'un site de streaming à l'autre sans perdre ses informations, le droit d'être informé en cas de piratage des données.

Les internautes pourront aussi être défendus par les associations dans le cadre d'une action de groupe en vue de faire cesser la partie illicite d'un traitement de données.

QUI DOIT SE CONFORMER AU RGPD ?

Toute entité manipulant des données personnelles concernant des Européens doit se conformer, qu'il s'agisse d'une entreprise, d'un sous-traitant ou même d'une association. Attention : le texte ne s'applique pas qu'aux organisations établies sur le territoire du Vieux Continent. Un groupe américain, japonais ou chinois qui collecte et mouline des données personnelles européennes doit aussi s'y conformer.

Des géants comme Google, Facebook, Amazon ou encore Uber doivent donc tenir compte des modalités du RGPD s'ils veulent continuer sans risque à fournir des biens et des services à la population européenne. La taille de l'entreprise, son secteur d'activité ou son caractère public ou privé n'entre pas en ligne de compte. Même une petite startup qui se lance dans de l'e-santé doit aussi être dans les clous.

ON M'A CONTACTÉ POUR ME METTRE EN CONFORMITÉ, EST-CE LÉGAL ?

Dans un peu plus de trois mois, le RGPD sera appliqué. Si vous gérez une entreprisequi traite d'une façon ou d'une autre des données personnelles, il n'est pas encore trop tard pour adapter vos traitements informatiques. Mais attention, la précipitation peut être mauvaise conseillère : du fait de l'application imminente du Règlement, il faut prendre garde à ne pas faire appel à n'importe qui.

La Commission nationale de l'informatique et des libertés a ainsi mis en garde sur les risques d'arnaques autour du RGPD : si les grands groupes sont immunisés, parce que leur département juridique peut prendre en charge cette mise en conformité, les startups, les TPE et les PME sont plus exposés. Pour la Cnil, il vaut mieux se documenter en ligne avant de faire appel à tout prétendu expert.

Et si besoin, la Cnil peut vous conseiller par téléphone via une ligne dédiée : 01 53 73 22 22.

COMMENT LE RGPD SE TRADUIT EN FRANCE ?

En France, le cadre du RGPD est transposé dans la législation via un projet de loirelatif à la protection des données personnelles. Il a été présenté le 13 décembre 2017 par Nicole Belloubet, la ministre de la justice. Une procédure accélérée a été enclenchée par l'exécutif, pour aller rapidement, avec un seule lecture du texte devant chaque chambre parlementaire.

À l'assemblée nationale, le texte a été adopté le 13 février à une large majorité : sur les 547 votants, 505 ont voté en faveur du texte. Le texte doit encore passer devant le Sénat. S'il est voté dans les mêmes termes, le texte sera ensuite promulgué par le président de la République et publié au Journal officiel. Sinon, une commission mixte paritaire sera constituée pour unifier les deux versions.

QUELLES SONT LES SANCTIONS PRÉVUES PAR LE RGPD ?

Les organisations ont tout intérêt à respecter à la lettre le RGPD car les plafonds des sanctions sont particulièrement élevés : en cas d'infraction, des amendes jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent sont prévues pour l'organisme fautif, sachant que c'est le montant le plus élevé qui est retenu entre les deux cas de figure.

Il faut imaginer ce que cela peut représenter pour des géants du net si une procédure était lancée contre eux. L'amende pourrait atteindre des dizaines ou des centaines de millions de dollars, voir davantage. Il convient aussi de noter qu'une société doit veiller à ce que son sous-traitant reste bien dans les clous de la loi, sous peine d'en subir les conséquences, du fait de sa qualité de responsable du traitement.

Cela étant, les multinationales ne sont pas nécessairement les plus exposées : si ce sont elles qui risquent les amendes les plus fortes, elles ont des détachements de juristes et d'experts qui travaillent déjà à plein temps depuis des mois pour être absolument dans les clous du RGPD. Le risque est en revanche plus grand pour les entités plus petites, comme une TPE, une PME ou une association.

RGPD : se préparer en 6 étapes

Site de la CNIL, 12 avril 2018

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Etape 1 :**DÉSIGNER UN PILOTE**

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

Etape 2 **: CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES**

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

Etape 3 **: PRIORISER LES ACTIONS À MENER**

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Etape 4 :**GÉRER LES RISQUES**

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

Etape 5 : **ORGANISER LES PROCESSUS INTERNES**

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

Etape 6 : **DOCUMENTER LA CONFORMITÉ**

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.