CEPS
Centre d'Étude et de Prospective Stratégique

AVRIL 2018

LE CYBER SOUS LE PRISME EUROPÉEN

EN PRÉALABLE, comme de coutume : l'actualité du numérique [actualisée au 25 mai] – Après son adoption par le Parlement, le texte de loi transposant la directive NIS (Network Information Security, SRI en français) vient d'être promulgué en France. Le texte s'inscrit dans le prolongement du dispositif de cybersécurité des opérateurs d'importance vitale (OIV) introduit par le législateur en 2013. Il permet, au-delà de ces OIV, de renforcer la protection de nombreux autres acteurs indispensables à la vie quotidienne des citoyens. Nombre d'entre eux, qu'ils appartiennent au secteur public comme au privé, demeurent encore très vulnérables aux attaques informatiques comme l'ont montré les récentes campagnes d'attaques informatiques mondiales WannaCry et NotPetya.

Par ailleurs, le texte rendant applicable le règlement européen sur la protection des données (RGPD, devant entrer en application le 25 mai) a été adopté le 14 mai à l'Assemblée nationale. Alors que l'Allemagne s'est déjà mise en conformité depuis plus d'un an, la France accusait du retard sur son calendrier d'adaptation de la loi Informatique et Liberté de 1978. Il est probable que des parlementaires saisissent le Conseil constitutionnel. À quelques jours de la date butoir l'exercice était éminemment risqué, mais qu'on se rassure : sur 24 régulateurs des données personnelles en Europe, 17 affirment qu'ils n'auront pas les moyens immédiats de faire appliquer le RGPD…

S'agissant justement du Conseil constitutionnel, ce dernier a été saisi sur une question prioritaire de constitutionnalité portant sur la « pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie ». Dans son avis, rendu le 30 mars, le Conseil affirme que cette obligation figurant à l'article 434-15-2 du code pénal ne porte atteinte ni au droit de ne pas s'accuser, ni au respect de la vie privée et au secret des correspondances, ni aux droits de la défense, ni à la liberté d'expression. En vertu du code pénal, ce refus est donc susceptible d'être puni de trois ans d'emprisonnement et de 270 000 euros d'amende dès lors que le moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit (la peine peut être portée à cinq ans d'emprisonnement et 450 000 euros d'amende si ce refus a permis la commission d'un crime ou d'un délit).

Enfin, l'actualité c'est aussi le *Cloud Act*, littéralement *Clarifying Lawful Overseas Use of Data Act* : par cette nouvelle loi les autorités américaines ont récemment renforcé leur ingérence sur les opérateurs de Cloud. C'est un pied de nez aux souverainetés étrangères. Aussi la Commission européenne propose-t-elle de doter l'Union d'une réglementation similaire. L'objectif est d'optimiser l'accès aux preuves électroniques utiles aux autorités policières et judiciaires pour mener à bien leurs enquêtes. Parmi les mesures proposées, l'une d'elles cible les prestataires de services numériques non européens proposant leurs services dans l'UE afin qu'ils soient soumis à des obligations

identiques que les prestataires européens en cas de demande de preuves électroniques d'une autorité judiciaire.

***

CRÉER, ENFIN, UN VÉRITABLE MARCHÉ EUROPÉEN DU NUMÉRIQUE

Le Règlement général sur la protection des données (RGPD) est une riposte à l'arrivée tonitruante et extrêmement puissante de nouveaux acteurs économiques disposant d'une capacité à s'affranchir des règles des pays dans lesquels ils opèrent.

L'idée d'un nouveau cadre réglementaire pour l'économie numérique est née en 2012, à l'initiative de Viviane Reding, alors commissaire européenne à la Justice, aux Droits fondamentaux et aux Citoyens, qui estimait, à raison, que les textes de l'Union européenne étaient dépassés par les évolutions du numérique. Il est vrai que personne n'aurait pu anticiper la complexité des usages qui se sont développés avec Internet (réseaux sociaux, moteurs de recherche, géolocalisation mobile, publicité programmatique...). Aussi les textes en vigueur ne protégeaient-ils ni les citoyens, ni les entreprises européennes. Les entreprises américaines ont eu beau jeu de s'engouffrer dans les flous juridiques pour se soustraire aux lois de l'UE, et gagner ainsi une irrattrapable longueur d'avance dans l'économie numérique.

L'affaire Snowden a donné le dernier coup d'élan nécessaire à la révision de la législation. La question des données est apparue plus politique que jamais, et dès lors très liée au droit fondamental européen qui consacre la vie privée comme une jouissance inaliénable et inviolable de chaque citoyen, *a contrario* des États-Unis qui en font un droit cessible. Le RGPD est le fruit de ces différents jeux de pression qui expliquent en partie le temps de sa conception : quatre années. Viviane Reding a affirmé qu'il s'agissait du texte ayant fait l'objet du plus intense lobbying de l'histoire.

Si le règlement reprend des principes qui ne sont pas nouveaux (le consentement, le droit à l'oubli, la suppression des informations au-delà d'un certain temps, le choix d'un responsable des données, etc.) sa principale nouveauté, et même force, réside dans l'approche harmonisée à l'échelle européenne qu'il introduit en matière de droit des données. L'autre changement majeur est dans les sanctions encourue : les médias ont beaucoup écrit sur l'amende pouvant s'élever à 4 % du chiffre d'affaires mondial de l'entreprise déclarée coupable ou 20 millions d'euros en l'absence de revenus mais, en réalité, le règlement donne aux autorités des données personnelles un large éventail de mesures. Les entreprises qui ne respecteront pas les efforts demandés en matière de cybersécurité des données pourront ainsi être épinglées publiquement pour leurs fautes.

CRÉER, PARALLÈLEMENT, UNE VÉRITABLE EUROPE DE LA CYBERSÉCURITÉ

La Commission européenne a profité du « Mois de la Cybersécurité » (octobre 2017) pour formuler en amont diverses préconisations. Elle a notamment proposé un train de réformes dès septembre que le Conseil européen a adopté en octobre en demandant l'élaboration d'une approche commune de la cybersécurité de l'Union.

L'automne 2017 a permis de réaliser au niveau européen des avancées significatives en matière de cybersécurité.

Constance LE GRIP, députée des Hauts-de-Seine
vice-présidente de la Commission des affaires culturelles et de l'éducation

L'actuelle agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), basée en Grèce, devrait ainsi voir ses compétences renforcées. Toutefois, son mandat arrivant à expiration en 2020, la Commission a décidé d'avancer l'évaluation et le réexamen de ce mandat étant donné les changements significatifs intervenus en matière de cybersécurité depuis l'adoption de son règlement. Si son rôle consistait majoritairement à fournir une expertise et des conseils, le nouveau train de réformes pourrait lui octroyer de nouvelles prérogatives. Elle deviendrait ainsi l'Agence de cybersécurité de l'UE et son mandat permanent. Son rôle principal consistera alors à aider les États membres à mettre en œuvre la directive SRI. Elle aura également un rôle à jouer dans la coopération opérationnelle et la certification de cybersécurité des technologies de l'information et des communications. Le paquet contient en effet la création d'un cadre européen de certification. Cet « étiquetage » des dispositifs informatiques permettra de garantir aux consommateurs la fiabilité des systèmes qui pilotent de nombreuses infrastructures-clés telles que les réseaux d'énergies, les voitures connectées, etc., et ce dans tous les États membres.

Le Conseil européen a également acté la création d'un Centre européen de recherche et de compétences en matière de cybersécurité, accompagné d'un réseau de centres similaires au niveau des États membres, et une nouvelle directive relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces devrait être adoptée. La prochaine étape sera la mise en place d'une coordination et d'une coopération internationale en matière de cybersécurité. Mais déjà une avancée de la fin d'année 2017 a été la création d'une équipe permanente d'intervention en cas d'urgence informatique (CERT-UE) pour les institutions, organes et agences de l'Union, afin de répondre de manière coordonnée aux cyberattaques visant les institutions. Elle vient renforcer une *task force* existante depuis 2012.

CYBERSÉCURITÉ ET SOUVERAINETÉ NUMÉRIQUE

Les institutions tant européennes que nationales ont pris conscience du fait que l'enjeu de souveraineté est l'enjeu « ultime » de la cybersécurité. C'est d'ailleurs cette prise de conscience, peut-être tardive, qui a incité la création au sein de l'Assemblée nationale française d'un groupe d'étude « Cybersécurité et souveraineté numérique », coprésidé par M. Florian Bachelier et Mme Laure de La Raudière et composé de 45 députés. Ce groupe de travail traitera des problèmes posés par le piratage informatique pour les entreprises mais aussi pour les services de l'État. L'enjeu de la souveraineté posera évidemment la question de la dépendance de certains pans entiers de la société et des administrations à des décisions commerciales ou des choix techniques venant de groupes privés étrangers. Et c'est évidemment ce groupe de travail qui sera en charge d'analyser les propositions de la riposte européenne à l'égard du *Cloud Act* américain.

Le RGPD va ancrer la cybersécurité dans l'esprit de tous les citoyens et tous les acteurs sont déjà progressivement en train de modifier leurs comportements.

Général Marc WATIN-AUGOUARD
fondateur du Forum international de la cybersécurité
directeur du Centre de recherche de l'École des officiers de la gendarmerie nationale

L'un des grands changements amorcés par le RGPD réside dans son champ d'application territorial. Jusqu'à présent le droit européen ne s'appliquait qu'aux responsables de traitements européens ou aux entreprises implantées sur le territoire d'un État membre ; donc seules les entreprises étrangères disposant d'un établissement ou d'une filiale sur le territoire de l'UE y étaient soumises. Dorénavant, le règlement laisse place à une application extraterritoriale du droit communautaire (c'est l'article 3 du règlement qui définit ce nouveau principe) : le règlement s'applique ainsi aux données personnelles exploitées par un responsable ou un sous-traitant situé sur le territoire de l'Union et, ce, peu importe que le traitement soit effectué en Europe ou non. La réelle nouveauté réside dans l'alinéa 2 de l'article qui élargit l'application du règlement aux acteurs non européens. L'alinéa précise les deux situations visées : lorsque l'activité de traitement est liée, d'une part, à l'offre de biens ou de services qu'un paiement soit exigé ou non ou, d'autre part, à des activités relatives au suivi du comportement des personnes.

Toutefois certains acteurs se demandent si le règlement ne va pas freiner le développement en Europe des technologies de traitement et d'analyse de données au détriment des entreprises spécialisées, en constituant pour elles un obstacle supplémentaire par rapport aux entreprises étrangères, en particulier chinoises.

LE RGPD : UN TIGRE DE PAPIER ?

Les organisations ne seront pénalisées que si elles n'informent pas l'autorité concernée dans les délais imposés de l'existence d'une attaque ou d'une fuite de données. Or une entreprise peut mettre beaucoup de temps à découvrir un incident de sécurité. Néanmoins, elle respecte la réglementation si elle signale simplement l'incident dans les délais légaux. Dans l'intervalle, un grand nombre de données peuvent avoir été volées, sans parler d'autres dommages. Il est également difficile de vérifier quand un incident a effectivement été découvert et si l'entreprise concernée ne l'a pas simplement dissimulé pendant un certain laps de temps. Dans ce cas de figure, elle ne sera soumise à aucune pénalité même si elle n'a pas pris les mesures de protection nécessaires. Ainsi, même si le RGPD est une première avancée positive, cette avancée ne va pas assez loin pour certains qui estiment que le législateur devra promulguer d'autres lois sanctionnant également des précautions de sécurité inadéquates.

De plus, le RGPD offre aux cybercriminels de nouveaux vecteurs d'attaque qui peuvent profiter des incertitudes et interrogations de beaucoup d'employés dans les entreprises, spécialement durant les dernières phases de mise en œuvre de la réglementation, estiment des experts en sécurité

informatique. Des campagnes d'hameçonnage ciblées ayant pour thème la conformité au RGPD ont déjà été observées, et leur nombre continuera d'augmenter dans les prochains mois.

Enfin, il sera intéressant de voir comment l'Union européenne va gérer les initiatives de certains États membres visant à affaiblir le règlement au niveau national avec des clauses de souplesse conçues spécialement à cet effet. Le premier exemple de ce comportement est fourni par l'Autriche. Dans ce pays, la législation nationale affaiblit le règlement européen à un point tel que même dans le cas d'une violation manifeste du RGPD, les entreprises ne risquent que très peu de pénalités, voire pas du tout. Le risque est de voir se former des enclaves où des cybercriminels pourront agir en toute impunité, en contrevenant légalement à des directives européennes.

FAKE NEWS : LE GRAND FLOU

Les cas de désinformation se multiplient, et des tentatives de manipulation des résultats électoraux ont été détectées dans dix-huit pays ces dernières années. En Allemagne, une loi « anti-fake news », entrée en vigueur le 1er janvier, crée la polémique ; elle prévoit des sanctions contre les auteurs et pointe la responsabilité des diffuseurs. [Actualisation] De son côté, à un peu plus d'un an des élections européennes de 2019, la Commission européenne a affirmé le 26 avril vouloir prémunir les Européens et contribuer à la naissance d'un « écosystème transparent, crédible et responsable ». Aussi a-t-elle proposer non pas une réglementation, mais les grandes lignes d'un « code de conduite » inspiré par les recommandations d'un groupe d'experts internationaux. Le principe est donc de faire confiance aux réseaux sociaux eux-mêmes.

En France, la ministre de la Culture Françoise Nyssen, pour qui « la capacité de discernement des citoyens ne suffit plus », est venue le 22 mai défendre devant la commission des Affaires culturelles de l'Assemblée nationale le projet de loi du gouvernement. Alors que la loi devrait être examinée en séance le 30 mai, plusieurs députés ont fait part de leurs réserves, à l'instar du Conseil d'État. Le talon d'Achille de cette loi de censure de l'information jugée fausse visant Internet et les réseaux sociaux réside dans l'établissement de la preuve de l'intentionnalité de nuire : comment distinguer entre une information erronée, mais publiée de bonne foi, et une information « de faussaire », en d'autres mots fausse et fabriquée ? Une loi ne ferait-elle pas aussi « doublon » avec la loi du 29 juillet 1881 sur la liberté de la presse qui permet déjà de réprimer les propos diffamatoires ou erronés ou encore le code électoral qui propose un cadre censé garantir la bonne tenue d'une élection en luttant notamment contre la diffusion de fausses nouvelles ?

Si nous sommes incontestablement entrés dans une nouvelle ère de la propagande et que les citoyens vont devoir réapprendre à démêler le vrai du faux, cet apprentissage ne prendra-t-il pas seulement un peu de temps, comme toute chose ? Il y a tout juste une quinzaine d'années, un secrétaire d'État a pu faire avaler des couleuvres aux Nations unies et au monde entier… et cela sans recourir à Internet ou aux réseaux sociaux.[1]

***

Le RGPD n'est-il pas déjà cliniquement mort, d'une part, parce qu'il a ouvert une guerre avec les États-Unis laissant peu de chance à une Europe désunie de l'emporter, d'autre part en créant de nouveaux handicaps pour les entreprises européennes face à leurs concurrentes étrangères ? Ces

[1] Discours de Colin Powell à l'ONU du 5 février 2003 sur les armes de destruction massive en Irak.

prochaines semaines, en tout cas, les internautes européens vont continuer de voir affluer dans leurs boîtes mail les vestiges numériques de leur historique de consommation, venant se rappeler à votre bon souvenir. Le moment est venu d'un grand ménage consistant à fermer des comptes et annuler des abonnements, finalement pas si utiles et surtout très encombrants. C'est aussi par sa mise en œuvre et par la jurisprudence qu'il va créer que le RGPD jouera son rôle de protection sans brider l'innovation. Très alerte dans la définition d'un nouveau droit, l'Europe va aussi devoir, pour aller jusqu'au bout de ses objectifs et faire appliquer ses lois, renforcer ses compétences numériques de haut niveau à la fois dans les ressources humaines et les logiciels.

Martine LE BEC
rédactrice en chef de la revue *Prospective Stratégique* – CEPS

CEPS
Centre d'Étude et de Prospective Stratégique

NOS PARTENAIRES

AIRBUS Atos babcock trusted to deliver Beijaflore Conseil en management

Capgemini cigref réussir le numérique DE GAULLE FLEURANCE & ASSOCIÉS SOCIÉTÉ D'AVOCATS Institut Robert Schuman pour l'Europe