N° 429

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 16 avril 2018

RAPPORT

FAIT

au nom de la commission des affaires européennes (1) sur la proposition de résolution européenne, présentée en application de l'article 73 quinquies *du Règlement, sur la* **régulation** *des* **objets connectés** *et le* **développement** *de l'***internet** *des* **objets** *en* **Europe***,*

Par M. André GATTOLIN,

Sénateur

et TEXTE DE LA COMMISSION

(Envoyé à la commission des affaires économiques.)

(1) Cette commission est composée de : M. Jean Bizet, *président* ; MM. Philippe Bonnecarrère, André Gattolin, Mmes Véronique Guillotin, Fabienne Keller, M. Didier Marie, Mme Colette Mélot, MM. Pierre Ouzoulias, Cyril Pellevat, André Reichardt, Simon Sutour, *vice-présidents* ; M. Benoît Huré, Mme Gisèle Jourda, MM. Pierre Médevielle, Jean-François Rapin, *secrétaires* ; MM. Pascal Allizard, Jacques Bigot, Yannick Botrel, Pierre Cuypers, René Danesi, Mme Nicole Duranton, MM. Thierry Foucaud, Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Daniel Gremillet, Mme Pascale Gruny, Laurence Harribey, MM. Claude Haut, Olivier Henno, Mmes Sophie Joissains, Claudine Kauffmann, MM. Guy-Dominique Kennel, Claude Kern, Jean-Yves Leconte, Jean-Pierre Leleux, Mme Anne-Catherine Loisier, MM. Franck Menonville, Georges Patient, Michel Raison, Claude Raynal, Mme Sylvie Robert.

Voir le numéro :

Sénat : **361** (2017-2018)

S O M M A I R E

Pages

AVANT-PROPOS

Madame, Monsieur,

En application de l'article 73 quinquiès du règlement du Sénat, la commission des affaires européennes a été saisie, le 15 mars dernier, d'une proposition de résolution européenne sur la régulation des objets connectés et le développement de l'internet des objets en Europe. Le rapport et la proposition seront ensuite transmis à la commission des affaires économiques pour examen.

Son auteure, Catherine Morin-Desailly, présidente de la commission de la culture, de l'éducation et de la communication, suit depuis plusieurs années les questions numériques et les développements de l'internet. Elle a notamment été la rapporteure de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'internet », à laquelle votre rapporteur a participé.

La proposition de résolution pose la question de la souveraineté de l'Union européenne dans le monde numérique à l'heure où les objets connectés envahissent nos vies et nos sociétés. Elle présente des pistes pour un développement économique des objets connectés en Europe respectueux de la vie privée et sécurisé.

Afin de l'analyser et de favoriser un travail efficace du Sénat, M. Jean Bizet, président de la commission des affaires européennes, et Mme Sophie Primas, présidente de la commission des affaires économiques, ont proposé que les rapporteurs des deux commissions mènent ensemble les travaux d'instruction de la proposition. Les auditions conduites par votre rapporteur ont ainsi toutes été faites en coopération avec M. Jean-Marie Janssens, rapporteur de la commission des affaires économiques.

On rappellera également la création, le 25 janvier dernier, du « groupe numérique » rattaché à l'ensemble des commissions permanentes du Sénat.

Les auditions ont permis de recueillir l'avis d'acteurs du monde économique et de la régulation du numérique en France, afin de mesurer les enjeux et les solutions prônées par la proposition de résolution. Le présent rapport expose le fruit de ces échanges et de la réflexion des rapporteurs, et présente les modifications qu'il est proposé d'apporter à la proposition de résolution européenne.

I. L'ESSOR DES OBJETS CONNECTÉS SOULÈVE D'IMPORTANTS ENJEUX AUXQUELS LES EUROPÉENS DOIVENT RÉPONDRE.

A. DES PERSPECTIVES DE DÉVELOPPEMENT IMPRESSIONNANTES

1. Le champ des objets connectés est potentiellement infini

Il convient d'abord de distinguer l'internet des objets et les objets connectés. Selon l'Autorité de régulation des communications électroniques et des postes (ARCEP)[1], *« **l'internet des objets** correspond à un ensemble d'objets connectés, de communications et d'internet, qui se conjugue avec les vagues du* cloud *et du* big data *:*

*- les **objets physiques** possèdent des technologies embarquées de capteurs, d'intelligence et de connectivité, leur permettant de communiquer avec d'autres objets ;*

*- les **réseaux de communications électroniques** permettent de transporter les données issues des objets ;*

*- **l'informatique**, plus ou moins distribuée, apporte les outils pour le stockage, la corrélation et l'analyse de ces données ».*

Les préoccupations en termes de sécurité et de protection des données à caractère personnel exprimées dans la proposition de résolution portent surtout sur le volet Objets physiques de l'internet des objets.

Selon le rapport d'information sur l'internet des objets des députées Corinne Erhel et Laure de La Raudière[2], les objets connectés sont *« l'ensemble des **objets traditionnels**, non technologiques, qui sont **augmentés d'au moins un capteur, une puce RFID[3] ou un QR-code[4]**. Le champ des objets connectés est donc potentiellement infini ».*

Dès lors, les objets connectés sont d'une très **grande diversité**. On peut toutefois les distinguer selon le public visé : certains sont destinés à l'usage des **consommateurs** (tels que les objets connectés portables, qui permettent une quantification de soi comme le poids de forme, le sommeil, la vitesse de course, etc), d'autres, aux **entreprises** (tels que les réseaux de capteurs sans fils permettant de mettre en place une maintenance prédictive).

---

[1] *Livre blanc du 7 novembre 2016 : Préparer la révolution de l'Internet des objets.*

[2] *Rapport d'information n° 4362 du 10 janvier 2017 de Mmes Corinne Erhel et Laure de La Raudière pour la commission des affaires économiques de l'Assemblée nationale intitulé L'internet des objets : le numérique à l'ère de la prédiction.*

[3] *Pour « radio frequency identification » : en français, il s'agit de radio-étiquettes.*

[4] *Pour « quick response » : il s'agit d'un code à barres pouvant être décodé rapidement et permettant de stocker plus d'informations qu'un code à barres classique et reconnues par des applications.*

2. Un développement rapide porteur d'opportunités économiques

a) Des perspectives économiques impressionnantes

Alors qu'entre 8,4[1] à 11,2[2] milliards d'objets connectés auraient déjà été utilisés en 2017, ce **volume est amené à s'accroître très fortement à l'avenir** : 20 milliards d'objets en 2020 selon certains[3], 35 milliards selon d'autres[4]… À ce jour, d'après le cabinet Idate[5], le marché des objets connectés apparaît surtout tiré par les applications industrielles pour répondre à des besoins métiers particuliers ; la valeur de ces objets connectés provenant principalement des logiciels et services informatiques qui leurs sont associés.

Le cabinet AT Kearney estime que **l'Union européenne gagnerait 7 points de PIB**, soit 1 000 milliards d'euros, d'ici à 2025, grâce à l'essor de l'internet des objets : 80 milliards d'euros proviendraient des ventes d'objets, 210 milliards d'euros seraient économisés par la réduction des risques de santé et le gain de temps dans la vie quotidienne des individus, 300 milliards d'euros proviendraient d'une hausse du pouvoir d'achat des ménages, notamment en raison d'une meilleure maîtrise des dépenses d'énergie, et 430 milliards d'euros seraient dus à l'augmentation de la productivité des entreprises[6].

b) Les acteurs économiques européens doivent se positionner pour participer à cet essor

Le développement des objets connectés soulève un enjeu d'ordre économique : il s'agit de la **capacité des acteurs de l'économie européenne à se saisir de l'opportunité économique qu'ils génèrent**. Or, comme le remarque l'Idate[7], les grands acteurs américains de l'internet – tels que Google, Apple, Facebook, Amazon et Microsoft (généralement désignés sous l'acronyme « GAFAM ») –, qui tirent une grande partie de leurs revenus de l'utilisation des données à caractère personnel, investissent le secteur des objets connectés de façon significative : *via* la commercialisation d'objets qu'ils ont conçus (assistants personnels, Google Glass, Apple watch) ou acquis (thermostat Nest acquis par Google), comme à travers le développement de plateformes logicielles (Android Wear, Google Fit chez Google, HelthKit et WatchKit chez Apple).

---

[1] *https://www.gartner.com/newsroom/id/3598917*
[2] *Idate, IoT Markets – Dataset and report, décembre 2017.*
[3] *Gartner, Leading the IoT, février 2017.*
[4] *Idate, IoT Markets – Dataset and report, décembre 2017.*
[5] *https://fr.idate.org/marche-internet-des-objets/*
[6] *AT Kearney, The Internet of Things : A New Path to European Prosperity, janvier 2016.*
[7] *https://fr.idate.org/marche-internet-des-objets/*

La production massive de données par les objets connectés[1] nécessitera de développer nos capacités de stockage, mais surtout de corrélation et d'analyse de données. Au demeurant, ces fonctions sont au cœur de la bataille économique en cours en matière d'intelligence artificielle. Or, comme le rappelle notre collègue député Cédric Villani[2], ces acteurs américains ainsi que leurs concurrents chinois – rassemblés sous l'acronyme BATX (pour Baidu, Alibaba, Tencent et Xiaomi) – sont également les plus avancés en la matière, son rapport évoquant même une « **asymétrie critique** » entre ces acteurs et les autres. Cédric Villani rappelle d'ailleurs, comme notre collègue Catherine Morin-Desailly, que l'enjeu est d'éviter que l'Europe devienne une « colonie numérique »[3].

Aussi, la capacité des organismes de **normalisation** européens à imposer leurs orientations au niveau international concourra à accroître la capacité des acteurs économiques européens à capter la valeur provenant de l'essor des objets connectés.

B. DES RISQUES ASSOCIÉS PRÉOCCUPANTS

Le développement des objets connectés dépendra de leur capacité à susciter la confiance de leurs utilisateurs. Cette confiance ne pourra être accordée que si, d'une part, les objets connectés sont suffisamment **sécurisés contre les cyberattaques** (1), et si, d'autre part, ils sont conçus, fabriqués et fonctionnent d'une façon qui garantisse la **protection des données à caractère personnel** (2), c'est-à-dire liées à une personne identifiée ou identifiable[4]. Or, l'**actualité est marquée par les questions de cybersécurité et de protection des données à caractère personnel**.

---

[1] *Amplifiant, en cela, une tendance déjà bien amorcée : 90 % des données dans le monde ont été créées depuis 2015 (Note d'information scientifique n°1 – mars 2018 - de l'OPECST sur les objets connectés).*

[2] *Cédric Villani, Rapport au Gouvernement : Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne.*

[3] *Catherine Morin-Desailly, L'Union européenne, colonie du monde numérique ?, Rapport d'information n° 443 (2012-2013), fait au nom de la commission des affaires européennes, déposé le 20 mars 2013.*

[4] *Selon l'article 4§1 du règlement (UE) 2016/679 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, et abrogeant la directive 95/46/CE, on entend par données à caractère personnel* « toute information se rapportant à une personne physique identifiée ou identifiable (…) ».

1. La vulnérabilité des objets connectés aux cyberattaques

Les deux dernières années ont apporté la preuve de l'essor des **cyberattaques**. La Commission européenne a dressé le constat[1] qu'en 2016, il y a eu 4 000 attaques par *rançongiciel* par jour, soit une hausse de 300 % par rapport à 2015. Au total, 80 % des entreprises européennes auraient été touchées par une cyberattaque en 2016. En 2017, les virus *Wannacry* et *Notpetya* ont frappé les ordinateurs dans le monde entier avec une ampleur jamais vue auparavant. Le premier a consisté à bloquer, par chiffrement, près de 300 000 ordinateurs dans le but de demander une rançon pour la restauration des données. Le second a détruit de nombreux systèmes informatiques utilisant un logiciel comptable ukrainien, Me.Doc. L'attaque a principalement frappé l'Ukraine, dont 80 % des entreprises utilisaient ce logiciel. Au-delà, elle a touché des groupes mondiaux comme le français Saint-Gobain, l'américain FedEx ou le danois Maersk, et les pertes financières totales sont estimées à plus d'un milliard d'euros. Plus grave, des hôpitaux au Royaume-Uni ont vu leur fonctionnement affecté par l'attaque.

L'évolution rapide des techniques et la connexion toujours plus grande des acteurs économiques à internet imposent aux autorités une adaptation permanente des méthodes et des règles de protection. Malgré le développement continu de la cybersécurité en France et en Europe, il semble que les attaquants, qu'il s'agisse de criminels ou d'acteurs étatiques, aient toujours un temps d'avance. Et la question est sans cesse posée de savoir si nous sommes assez protégés contre les cybermenaces.

S'agissant des objets connectés, plusieurs exemples récents attestent de leur vulnérabilité aux attaques. La campagne « Toyfail », menée par l'association norvégienne de protection des consommateurs, a montré que n'importe qui pouvait facilement avoir accès au microphone de la poupée connectée Cayla et ainsi parler avec l'enfant sans que ses parents le sachent. La campagne « WatchOut », menée par cette même association, a également montré les nombreux défauts de sécurité affectant les montres connectées.

Comme le rappelait le Livre blanc de l'ARCEP, *« les conséquences d'une sécurité informatique insuffisamment prise en compte lors de la conception, du développement ou de l'utilisation d'objets connectés peuvent être graves : pertes de vies humaines, atteinte à la vie privée ou aux biens, perte de compétitivité, nuisance dans la vie quotidienne, atteinte à la sécurité ou à la défense nationale »*. L'ARCEP souligne néanmoins que **l'enjeu de sécurité pourra être différent selon les cas d'usages** : par exemple, le niveau de sécurité exigé ne sera pas le même pour une pompe à insuline que pour un capteur de température.

[1] *Commission européenne, étude d'impact accompagnant la proposition de règlement sur la cybersécuritén SWD(2017) 500 final.*

2. Le risque de collecte et d'utilisation incontrôlées de données à caractère personnel

L'actualité montre aussi – hélas ! – que des pratiques légales et non agressives relèvent également de **l'atteinte aux libertés individuelles et à la vie privée**. L'affaire *Facebook/Cambridge Analytica* pourrait se révéler emblématique de pratiques dont la grande majorité des citoyens ignore tout. Le réseau social est accusé depuis plusieurs semaines d'avoir laissé les données de plusieurs dizaines de millions d'utilisateurs être récupérées, *via* un sous-traitant, par une entreprise spécialisée dans l'influence politique, *Cambridge Analytica*. Le patron de *Facebook* a évoqué 87 millions d'utilisateurs potentiellement touchés, dont près de 2,7 millions de personnes résidant dans l'Union européenne. Le système permettait à des applications autres que *Facebook* d'accéder non seulement aux données des utilisateurs du réseau social, mais aussi à celles de leurs amis, dans le but principalement de proposer des publicités ciblées. Si la licéité de la transmission des données à *Cambridge analytica* est sujette à question, l'affaire ne doit pas masquer le fait que l'économie du réseau social repose sur la collecte de données à caractère personnel, sans que l'utilisateur – voire les tiers – sache précisément jusqu'à quel point.

Dans la mesure où ils engendrent une production massive de données et que leur valeur dépend en grande partie de l'utilisation de celles-ci, **les objets connectés doivent également être conçus de telle sorte que les données à caractère personnel soient suffisamment protégées**[1]. Auditionnée par votre rapporteur, la Commission nationale de l'informatique et des libertés (CNIL) a souligné que, comme en matière de sécurité, les exigences relatives à la protection des données à caractère personnel feront l'objet d'adaptations selon le niveau de risques associé à l'objet connecté examiné. Par exemple, le degré de risque sera différent selon que l'objet est dit « *in-in* », c'est-à-dire qu'il ne transmet pas de données à l'extérieur et n'est donc susceptible de poser problème qu'au regard de la cybersécurité, ou « *in-out* », autrement dit, qui communique les données à l'extérieur et qui doit être appréhendé par les autorités de contrôle des traitements de données à caractère personnel

En France, l'affaire des compteurs Linky illustre la problématique du respect de la vie privée dans l'utilisation d'objets connectés. La CNIL a mis en demeure la société Direct Energie, à qui elle reproche de recueillir les données des utilisateurs sans leur consentement. Grâce aux relevés de consommation d'électricité et à leur transmission de ceux-ci pour analyse, les compteurs intelligents doivent permettre une meilleure maîtrise de cette

[1] *À ce sujet, il convient de rappeler que 60 % des flux numériques mondiaux sont constitués par des données à caractère personnel (Inspection générale des finances et Conseil général de l'économie, de l'industrie, de l'énergie et des technologies, Accord plurilatéral sur le commerce des services et partenariat transatlantique pour le commerce et l'investissement : enjeux numériques des négociations, avril 2016).*

consommation et une facturation au réel. Les informations sont récupérées par Enedis, société gestionnaire du réseau électrique en charge de l'installation des nouveaux compteurs, puis transmises à Direct Énergie. Or, pour la CNIL, il manque l'accord préalable et éclairé des consommateurs à cette collecte. En outre, elle conteste la finalité de la collecte dans la mesure où Direct Énergie ne propose pas de facturation au réel.

Ce dernier exemple n'est que l'embryon de ce que sera demain une société remplie d'objets connectés : les maisons connectées où les appareils correspondront entre eux (et avec leur fournisseur) pour offrir des services plus précis et plus économes en énergie ; les villes intelligentes où l'utilisation des données permettra de réguler le trafic et de réduire la pollution ; les grands réseaux de transport et d'énergie mieux régulés. Aussi, tout laisse à penser que l'utilisation des objets connectés devrait prendre une ampleur considérable tant ceux-ci seront présents dans nos sociétés, alors même que l'effectivité de la protection des données est déjà sujette à questionnements et à doutes.

C. LE NÉCESSAIRE RENFORCEMENT DU POSITIONNEMENT EUROPÉEN

1. Une législation européenne en constante adaptation

a) Le règlement général sur la protection des données à caractère personnel

L'évolution rapide et constante d'internet et de ses usages et les avancées d'une société toujours plus connectée ont amené l'Union européenne à proposer de nouvelles règles pour encadrer ces usages, en conformité avec les principes démocratiques qui la fondent et la nécessaire protection de ses ressortissants. Ces règles concernent en premier lieu la protection de la vie privée, donc des données à caractère personnel. Elles visent également à doter les Européens d'une cybersécurité plus robuste.

Si le règlement général sur la protection des données à caractère personnel (RGPD) a été adopté il y a déjà deux ans[1], son entrée en vigueur est prévue le 25 mai 2018[2]. Le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel définit un niveau cohérent et élevé de protection des personnes physiques et lève les obstacles aux flux de données à caractère personnel au sein de l'Union. Il harmonise à cet effet les règles de protection des droits et

[1] *Note d'information de la commission des affaires européennes n° 51 du 21 juillet 2016 sur la protection des données.*

[2] *En outre, un projet de loi relatif à la protection des données personnelles transpose la directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et précise les modalités d'application en France du RGPD. Il est en cours d'adoption par le Parlement français (http://www.senat.fr/dossier-legislatif/pjl17-296.html).*

des libertés des personnes physiques à l'égard du traitement de ces données dont il entend assurer une application homogène.

Or, comme le rappelle la note d'information de la commission des affaires européennes du 21 juillet 2016, le RGPD consacre, s'une part, le droit de la personne à donner et retirer son consentement et, d'autre part, « *il attribue des caractères au consentement. Ainsi, le traitement des données ne peut se faire sans le consentement de la personne concernée et uniquement à des fins déterminées jusqu'au moment où la personne décide de retirer son consentement. Ce dernier doit être « indubitable » pour les traitements de données sensibles et « explicite » dans tous les cas où il est exigé* ».

D'application directe dans les États membres sans qu'il soit besoin de procéder à une transposition, le RGPD constitue dorénavant le cadre général de la protection des données personnelles applicable aux opérateurs de l'Union européenne ou offrant des biens et services aux citoyens et résidents de l'Union. Il renvoie toutefois à des mesures d'application internes, comme la désignation de l'autorité nationale de contrôle compétente. Surtout, face à la grande inégalité des régimes de protection au sein de l'Union européenne et pour répondre à la sensibilité particulièrement forte en la matière de certains États comme la France, il autorise les États membres à maintenir ou à introduire des dispositions nationales pour préciser davantage l'application de ses règles, et leur laisse des « *marges de manœuvre* » pour compléter les dispositions concernant le traitement de catégories particulières de données à caractère personnel, dénommées « *données sensibles* ». Par ailleurs, il n'exclut pas que des législations sectorielles nationales spécifiques, dans des domaines qui requièrent des dispositions plus détaillées, précisent les circonstances des situations particulières de traitement, y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est alors licite.

b) La proposition de règlement sur la cybersécurité

Présentée en septembre 2017 par la Commission européenne, ce texte s'articule autour de deux axes. Le premier vise à faire de l'Agence européenne chargée de la sécurité des réseaux et de l'information une agence permanente de l'Union européenne, dont les objectifs et les missions seront étendus. Le second axe vise à mettre en place une certification européenne de sécurité des technologies de l'information et de la communication.

La certification s'effectue actuellement au niveau national sur la base de normes internationales de sécurité informatique, ce qui a engendré un paysage européen morcelé car seuls 13 États membres, dont la France, ont signé un accord pour des critères communs d'évaluation de la sécurité des technologies de l'information. La mesure s'appuierait sur un guichet unique à disposition des entreprises souhaitant faire certifier leurs produits : il leur suffirait d'obtenir un certificat dans un seul pays de l'Union et celui-ci serait

valable dans tous les États membres. Trois niveaux d'assurance sont proposés selon le type de produits (élémentaire, substantiel et élevé), sur la base de normes, de critères d'évaluation et de méthodes d'essai communs. La proposition est en cours de discussion à Bruxelles et donnera prochainement lieu à un examen de la commission des affaires européennes du Sénat, sur le rapport de nos collègues René Danési et Laurence Harribey.

c) La proposition de règlement sur la libre circulation des données à caractère non personnel

Enfin, on peut aussi évoquer une proposition de règlement visant à instaurer un cadre juridique pour la libre circulation des données à caractère non personnel dans l'Union européenne qui pose le principe de la libre circulation de ces données au sein de l'Union, interdisant – sauf exceptions – une localisation à des fins de stockage ou de traitement de ces données sur le territoire d'un seul État membre. Les objets connectés vont produire aussi des données à caractère non personnel et ils seront soumis à la future règlementation européenne en la matière.

2. L'action externe : la protection des données en dehors des frontières de l'Union et la question de l'extraterritorialité des mesures

Pour l'Union européenne, le transfert de données à caractère personnel en dehors de son territoire est en principe interdit. Il peut être autorisé si le pays ou le destinataire assure un niveau de protection suffisant, c'est-à-dire correspondant aux critères européens. L'autorisation s'appelle « décision d'adéquation ». Par cette décision, la Commission reconnait que le pays de destination assure un niveau de protection équivalent des données à caractère personnel en raison de la législation interne et des engagements internationaux auxquels il a souscrit. De telles décisions ont déjà été adoptées concernant notamment le Canada, la Suisse, l'Argentine, ou encore Guernesey.

Les décisions d'adéquation sont adoptées selon la « procédure de comité » qui comprend les étapes suivantes :

- la Commission présente une proposition ;
- le G29 (qui deviendra le comité européen de la protection des données, organe de l'Union doté de la personnalité juridique, créé par l'article 68 du RGPD) rend un avis non contraignant ;
- le comité réunissant les représentants des États membres rend un avis adopté à la majorité qualifiée ;
- le Parlement européen et le Conseil peuvent, à tout moment, demander à la Commission de maintenir, modifier ou retirer la décision d'adéquation au motif qu'elle excède les compétences d'exécution prévues par la Directive ;
- le collège des membres de la Commission adopte la décision.

Concernant les États-Unis d'Amérique, en raison de la domination des entreprises américaines sur l'internet mondial et de leur avancée technologique dans le traitement des données, c'est la décision la plus importante pour les données à caractère personnel des Européens. Pourtant, le doute persiste sur le niveau réel de protection.

Edward Snowden a mis en lumière la surveillance de masse qu'exercent les services de renseignement américains et britanniques sur l'internet mondial. Au-delà, il a porté le doute sur la surveillance que peuvent exercer ces services sur les données à caractère personnel des consommateurs européens. En effet, l'internet étant dominé par les GAFAM américains et l'ensemble de ces données étant transmises outre-Atlantique où elles sont traitées, comment ne pas suspecter un espionnage ?

Et derrière cette interrogation, pointe celle du respect des droits des citoyens européens quant au traitement de leurs données par les grands acteurs d'internet. L'action de l'avocat autrichien Max Schrems a entraîné l'invalidation du précédent accord juridique entre l'Union européenne et les États-Unis encadrant le transfert des données des Européens vers les entreprises américaines, le *Safe Harbor*, au motif qu'il n'assurait pas le respect du droit européen.

Cet accord a été depuis remplacé par l'accord *Privacy Shield*, censé apporter plus de garanties. Sa mise en œuvre fait l'objet d'un suivi attentif de la Commission européenne et du groupe rassemblant les autorités européennes nationales de protection des données personnelles – le G29 – auquel participe la CNIL française.

Dans son premier rapport d'application de l'accord présenté en janvier 2018, la Commission européenne estime que la mise en œuvre de cet accord doit être améliorée, en particulier la vérification de la conformité des entreprises qui se sont auto-certifiées. Un prochain rapport d'application doit être présenté en septembre.

Dans un internet qui se joue des frontières, les difficultés rencontrées avec les États-Unis soulèvent l'enjeu de l'extraterritorialité du droit applicable aux données à caractère personnel. Comme le relevait Simon Sutour dans son rapport[1] sur le projet de loi relatif à la protection des données, le RGPD organise une exportation contrôlée des données assortie d'une application extraterritoriale des règles européennes :

« Le règlement s'applique à tout établissement ou sous-traitant établi dans l'Union européenne, que le traitement des données à caractère personnel ait lieu ou non sur le territoire de celle-ci, comme à tout établissement ou sous-traitant qui n'est pas établi dans l'Union européenne pour les activités de traitement de données à caractère personnel de personnes physiques résidant dans l'Union européenne, dès

[1] *Rapport d'information fait au nom de la commission des affaires européennes par M. Simon Sutour sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à la protection des données personnelles (n° 296, 2017 2018).*

lors que ces activités de traitement sont liées à l'offre de services ou de biens à ces personnes, quand bien même aucun paiement ne serait exigé des intéressés, ou au suivi d'un comportement au sein de l'Union européenne.

Sauf si le traitement présente un caractère occasionnel, les données ne peuvent être transférées dans un pays tiers que si la Commission européenne a pris à son égard une décision d'adéquation du niveau de protection ou moyennant l'existence de garanties appropriées, et à la condition que la personne concernée dispose de droits opposables et de voies de recours effectives. Des mécanismes de coopération internationale devront être mis en place en la matière. »

Et comme le faisait remarquer l'auteur, *« l'Europe s'efforce de porter ce débat sur la souveraineté mais les discussions avec les États-Unis autour du « bouclier » sont loin d'être abouties ».*

3. Une démarche active en matière de normalisation

Le terme de « **normalisation** » renvoie aux normes d'application volontaire élaborées par des organismes réunissant les professionnels du secteur concerné pour leur propre usage. On peut le distinguer de celui de « standardisation », qui fait référence à la réunion de certains professionnels d'un secteur en vue de définir et de défendre un standard particulier. La normalisation est institutionnalisée et se veut un processus intégrant l'ensemble des acteurs de la filière concernée, là où la standardisation ne relève que de démarches *ad hoc* à la seule initiative de certains acteurs d'une filière.

La normalisation constitue, ainsi, un enjeu économique majeur. Consciente de cet enjeu, l'Union européenne est déjà très active en la matière. Au demeurant, l'internet des objets fait déjà l'objet de nombreux travaux de normalisation, tant au niveau national qu'européen ou international.

a) La normalisation : un enjeu économique majeur

Le rapport remis par Mme Claude Revel à la ministre du commerce extérieur résumait ainsi les **enjeux géopolitiques de la normalisation** : *« Il est de plus en plus difficile de séparer le « technique » du politique, les choix techniques étant non seulement souvent issus de la volonté d'ouvrir des marchés ou d'en fermer aux concurrents, mais aussi reflétant des choix politiques voire idéologiques, en tout cas de société de ceux qui les promeuvent ».* Comme le relevait notre collègue Elisabeth Lamure dans son rapport sur la normalisation[1], les acteurs nationaux de la normalisation *« se livrent à une **véritable course** pour être à même de proposer avant d'autres l'ouverture de*

[1] *Rapport d'information n° 627 (2016-2017) du 12 juillet 2017 fait au nom de la commission des affaires économiques par Mme Elisabeth Lamure, Où va la normalisation ? En quête d'une stratégie de compétitivité respectueuse de l'intérêt général.*

travaux dans les organismes européens ou internationaux de normalisation dans certains domaines ».

La normalisation : un système complexe à plusieurs niveaux

Comme le décrit le rapport d'Elisabeth Lamure sur la normalisation, il existe aujourd'hui trois niveaux de normalisation : international, européen et national.

1/ La normalisation au niveau international

Trois organismes principaux coexistent au niveau international, qui ont leurs caractéristiques propres quant à leurs compétences et à leur statut.

Le premier a une **compétence générale** : il s'agit de l'*International organization for standardization* (ISO)[1]. Les deux autres sont plus **spécialisés** : l'*International electrotechnical commission* (IEC)[2] concerne la filière électrotechnique, quand l'Union Internationale des Télécommunications (UIT) traite, plus largement, du domaine des technologies de l'information et de la communication.

Si l'ISO et l'IEC sont des **organisations non gouvernementales**, dans lesquelles la France est représentée par l'AFNOR, l'UIT est une institution spécialisée de l'Organisation des Nations unies (ONU). Elle réunit les 193 États membres et 800 entités privées ou universitaires y sont associées. Plus précisément, c'est l'UIT-T (pour télécommunications) qui est en charge de la normalisation.

Le fonctionnement de ces organismes est similaire. Une **assemblée plénière** définit les grandes orientations[3], et des **comités techniques**[4] composés d'experts nationaux élaborent les projets de normes.

Le principe d'adoption des normes est toujours le même : **chaque membre dispose d'une voix**[5]. Une nuance à ce principe est toutefois à souligner s'agissant de l'UIT-T : certaines résolutions élaborées par les commissions d'études sont considérées comme adoptées dès lors que la commission a élaboré un texte définitif. Elles ne sont donc pas soumises à approbation de l'ensemble des membres.

2/ La normalisation au niveau européen

Le « système » de normalisation européen est composé de trois entités qui répondent en partie aux trois entités internationales, à la différence qu'elles sont toutes des **organisations non gouvernementales**. Il repose aujourd'hui sur le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne.

---

[1] *163 Etats sont représentés à l'ISO.*

[2] *84 pays sont représentés à l'IEC.*

[3] *« Assemblée générale » de l'ISO, « Conseil » de l'IEC, « Assemblée mondiale de normalisation des télécommunications » de l'UIT-T.*

[4] *« Comités techniques » à l'ISO et à l'IEC, « commissions d'étude » à l'UIT-T.*

[5] *À l'ISO comme à l'IEC, chaque norme élaborée par un comité technique est soumis au vote de l'ensemble des membres – pour qu'elle soit adoptée, il faut une majorité des deux tiers des votes exprimés et que les votes négatifs ne représentent pas plus d'un quart du total.*

Recouvrant chacun un périmètre géographique différent[1], le Comité européen de normalisation (CEN) a une vocation **généraliste**, quand le Comité européen de normalisation électronique (CENELEC) et de l'*European Telecommunications Standards Institute* (ETSI) sont **spécialisés**, le premier en matière électrotechnique, le second en matière de technologies de l'information et de la communication.

Ces organismes sont composés de **délégations nationales**. Les normes ne sont, en revanche, pas votées selon le principe selon lequel « un État = une voix ». Au CEN et au CENELEC, le **vote est pondéré** en fonction de la population, quand à l'ETSI, les votes y sont pondérés en fonction de la contribution financière à l'organisme et les votes positifs doivent représenter 71 % des suffrages.

Ces organismes entretiennent des **liens étroits avec l'Union européenne**. En effet, la Commission européenne peut, d'une part, leur octroyer des subventions et, d'autre part, leur donner un mandat d'édiction de normes dans des secteurs et sur des questions qu'elle juge prioritaires. S'ils acceptent ce mandat, la Commission évalue la conformité des documents élaborés et, lorsqu'elle estime que la norme harmonisée répond aux exigences qu'elle vise à couvrir, elle publie une référence à cette norme harmonisée au *Journal officiel de l'Union européenne*.

3/ La normalisation au niveau national

Au niveau national, c'est **l'Association française de normalisation** (AFNOR)[2], association régie par la loi de 1901, qui assure le rôle d'animation de la normalisation en France et représente la France dans les organismes européens et internationaux de normalisation. À ce titre, l'AFNOR exerce une mission de service public et est dotée de prérogatives de puissance publique illustrées notamment par le pouvoir reconnu à son directeur général d'homologuer les normes afin qu'elles puissent rentrer dans le « catalogue », ou la « collection », des normes françaises.

b) Les outils mobilisés par la Commission pour renforcer l'influence européenne au niveau international

L'Union européenne agit en vue de renforcer l'influence européenne au niveau international en matière de normalisation à travers **deux outils** : la définition d'orientations en matière de normalisation et le soutien financier qu'elle apporte aux entreprises pour s'investir dans le processus de normalisation.

Afin que normalisation professionnelle et réglementation accompagnent efficacement le développement de l'activité économique sur un territoire donné, il importe que les **orientations** des acteurs de la

[1] Le CEN et le CENELEC réunissent 34 organismes membres, parmi lesquels ceux des 28 États membres de l'Union européenne ainsi que de la Suisse, de l'Islande, de la Norvège, de la Turquie, de la Macédoine et de la Serbie. L'ETSI réunit 68 pays différents.

[2] Depuis 2014, l'activité de normalisation dans le domaine électrotechnique - initialement exercée par l'Union technique de l'électricité (UTE) fondée en 1907 pour représenter les acteurs français à la Commission électrotechnique internationale (IEC), puis au Comité européen de normalisation électrotechnique (Cenelec) - a rejoint l'AFNOR.

normalisation soient **définies en lien avec les pouvoirs publics**. L'Union européenne doit assumer son **rôle stratégique** en la matière. La définition de priorités à échéance régulière est en effet un outil permettant, *in fine*, de faire converger les acteurs européens de la normalisation vers une solution commune dont l'influence au niveau international serait plus importante que si cette solution n'était retenue que par quelques États membres. C'est ainsi que la Commission européenne définit un **programme annuel de travail** en matière de normalisation européenne[1]. S'agissant du numérique et des objets connectés, elle a adopté une **communication relative à la normalisation en matière de technologies de l'information et de la communication[2]**, qui établit comme domaines prioritaires : l'informatique en nuage, **l'internet des objets**, les réseaux 5G, la cybersécurité et les données. Il revient aux organismes de normalisation des États membres de définir leurs priorités d'action conformément à celles déterminées dans ces programmes.

Par ailleurs, comme l'ensemble des États membres, l'Union européenne peut également favoriser l'investissement des acteurs industriels nationaux à travers l'apport d'un **soutien financier** à la participation aux organismes de normalisation. En mars dernier, la Commission a lancé le **projet StandICT.eu**[3], qui a précisément pour objectif de renforcer la présence européenne dans les activités de standardisation du numérique à l'échelle internationale. D'ici à 2020, des appels à candidatures seront lancés dans ce cadre tous les deux mois en vue de distribuer des aides forfaitaires à des projets de standardisation portés par des universitaires ou des entreprises. Le montant des aides s'étalera de 1 000 euros à 3 000 euros pour la participation à un évènement ponctuel, et s'élèvera jusqu'à 8 000 euros pour des projets sur douze mois.

c) De nombreux travaux de normalisation en cours concernent les objets connectés

L'internet des objets suscite des **réflexions dédiées** au sein des organismes de normalisation. Au niveau international, le comité technique ISO/IEC JTC 1/SC 41 « Internet des objets et technologies connexes » établit des projets de normes portant principalement sur les définitions de l'internet des objets et les réseaux de capteurs[4]. Au niveau européen, la Commission européenne a lancé, en 2015, l'*« Alliance for Internet of Things Innovation »* (AIOTI). L'ETSI participe à des coopérations entre organismes

---

[1] En application de l'article 8 du règlement européen sur la normalisation. Le dernier exemple en date est la communication du 25 août 2017 de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions relative au programme de travail annuel de l'Union en matière de normalisation européenne pour 2018.

[2] Communication du 19 avril 2016 de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions relative aux priorités pour la normalisation en matière de TIC dans le marché unique numérique.

[3] https://standict.eu/content/open-calls

[4] https://www.iso.org/fr/committee/6483279/x/catalogue/

internationaux de normalisation en matière de télécommunications, comme le projet « OneM2M » dédié à la normalisation des services liés aux équipements de communication de machine à machine. L'Association française de normalisation (AFNOR) a, de son côté, créé début 2016 la Commission Nationale sur l'internet des objets (CN IoT) pour défendre les enjeux français lors des travaux internationaux menés par l'ISO. Mentionnons également, en dehors des instances de normalisation, la LoRa Alliance, qui réunit des opérateurs européens et mondiaux pour travailler à plus de standardisation dans le domaine de l'internet des objets.

De très nombreuses autres initiatives **en lien avec les objets connectés** ont été lancées. En matière de cybersécurité, on peut mentionner les structures de travail suivantes : ISO/TC 121/AG « Compréhension des vulnérabilités et des menaces en matière de cybersécurité », CEN/CLC/JTC 13 « Cybersécurité et protection des données », et AFNOR/CN 27 SSI « Sécurité des systèmes d'information ». En matière de protection des données à caractère personnel, plusieurs structures intéressent directement les objets connectés : ISO/IEC/JTC1/SC 31 « Automatic identification and data capture techniques », CEN/TC 225 – « Codes à barres », et AFNOR/CN 31 « RFID, codes à barres et autres techniques d'identification automatique des objets ».

II. LA PROPOSITION DE RÉSOLUTION EUROPÉENNE

A. LES ORIENTATIONS DE LA PROPOSITION DE RÉSOLUTION EUROPÉENNE

Se fondant sur la nécessité pour l'Europe d'assurer sa souveraineté dans le monde numérique alors que l'internet des objets va s'imposer dans la vie des Européens, la proposition de résolution dresse un constat juste et présente des demandes exigeantes.

L'auteure estime en effet, de longue date, que l'Union doit assurer sa souveraineté si elle ne veut pas être une « colonie » du monde numérique. Afin de promouvoir cette souveraineté, elle doit s'appuyer sur un projet industriel pour développer son propre internet des objets et assurer la protection des consommateurs européens et de leurs données.

En outre, la proposition relève à juste titre que les questions qui se posent aujourd'hui en matière de protection des données et les risques identifiés en termes de cybersécurité vont se multiplier avec l'essor des objets connectés. Elle appelle donc à une prise de conscience sur le sujet et propose plusieurs actions pour y faire face.

La proposition de résolution formule trois demandes principales : un dispositif de certification des objets connectés défini au niveau européen ; l'obligation de localisation et de traitement des données à caractère personnel sur le territoire européen ; une plus grande participation de l'Union européenne dans la normalisation en matière numérique et particulièrement en ce qui concerne l'internet des objets.

1. La demande d'un nouvel outil réglementaire européen pour la certification des objets connectés

Afin de garantir un niveau élevé de protection des consommateurs européens, la proposition de résolution demande *« l'adoption d'un outil réglementaire de reconnaissance et d'autorisation des objets connectés à destination des consommateurs prenant la forme d'une certification »*, celle-ci devant garantir *« un haut niveau de protection et de sécurité pour les données personnelles »*.

S'agissant des exigences minimales qui pourraient être posées par le cadre européen, la proposition de résolution mentionne quatre points :

– un « droit au silence des puces », autrement dit la possibilité de désactiver partiellement ou totalement l'objet connecté ;

– l'obligation de rendre possibles les mises à jour de sécurité pour tout objet connecté à destination des consommateurs – dans la mesure où, aujourd'hui, de nombreux objets connectés ne sont pas susceptibles de faire l'objet d'une mise à jour ;

– des exigences accrues pour les objets permettant la collecte de données particulièrement sensibles, notamment à travers l'usage de technologies cryptographiques ;

– une conformité au RGPD, et notamment au droit de rectification, d'effacement et d'opposition au traitement des données personnelles.

2. L'obligation de localisation des données personnelles sur le territoire de l'Union

Afin, d'une part, de garantir la protection des citoyens et, d'autre part, de permettre le développement des industries numériques qui se nourrissent de données à caractère personnel, la proposition de résolution demande « *que soit introduite une obligation de localisation et de traitement des données personnelles des consommateurs européens sur le territoire de l'Union* ».

Cette question apparaît régulièrement dans le débat public. Elle concerne tout autant la souveraineté de l'Union européenne que l'intérêt économique d'exploiter les données de 500 millions d'Européens. Au Sénat, lors de l'examen de la loi pour une République numérique, un amendement du groupe CRCE poursuivant une logique similaire avait été adopté[1]. Il ne fut finalement pas retenu dans le texte adopté. Dans le rapport précité sur l'intelligence artificielle que Cédric Villani vient de rendre au Gouvernement, notre collègue député appelle avec force au maintien et au traitement des données européennes en Europe. D'autres voix ont également appelé en ce sens.

3. Une implication plus importante de l'Union européenne en matière de normalisation internationale

Afin de soutenir le développement d'une offre européenne en matière d'objets connectés, alors que « *les technologies de l'internet des objets sont encore massivement conçues et développées sur deux continents autres que l'Europe* », la proposition de résolution demande :

– « *que la politique commerciale de l'Union inclue la normalisation et la standardisation en matière numérique* » (alinéa 28) ;

– « *que l'Union européenne développe sa présence dans les enceintes internationales d'élaboration des normes et des standards de sécurité en matière numérique, et particulièrement l'internet des objets* » (alinéa 29).

Cette orientation rejoint celle de la résolution européenne adoptée le 30 juin 2015 par notre Assemblée, sur proposition de Catherine Morin-Desailly, pour une stratégie européenne du numérique globale,

[1] *http://www.senat.fr/amendements/2015-2016/535/Amdt_473.html*

offensive et ambitieuse[1], qui insistait *« sur l'enjeu pour l'Union européenne d'être présente et impliquée dans les enceintes techniques internationales où s'élaborent les normes et protocoles qui dessinent l'avenir »*.

B. LA POSITION DU RAPPORTEUR

Votre rapporteur partage pleinement la position de l'auteure de la proposition de résolution en ce qui concerne la nécessité pour l'Union européenne de se doter d'une véritable politique industrielle pour les objets connectés. Il constate que, lors de la réunion du Conseil compétitivité du 12 mars 2018, les États membres ont réitéré leur appel à une stratégie industrielle globale pour 2030 et au-delà, et ont fait de l'internet des objets un objectif stratégique pour l'avenir :

« Pour fonctionner dans une économie de la donnée, les entreprises doivent continuellement mettre l'accent sur le développement innovant et suivre les tendances d'avenir essentielles que sont notamment l'internet des objets, l'intelligence artificielle, la robotique, les mégadonnées et les plateformes, les systèmes connectés autonomes, la 5G, l'impression 3D, la normalisation, la sécurité des TIC et la chaine des blocs »[2].

Le Conseil a également insisté sur le fait que dans la mesure où les données deviennent un facteur nouveau de compétitivité, il convient de développer dans l'Union le stockage des données, l'informatique en nuage ainsi que des capacités de traitement de haute performance, afin d'assurer un niveau ambitieux de cybersécurité, de protection des données et des services des technologies de l'information et de la communication fiables.

Au regard de la proposition de résolution, ces orientations sont satisfaisantes et appuient l'ambition de l'auteure de la résolution soutenue par votre rapporteur. Il convient, en complément, de mesurer si le cadre juridique européen permet, en l'état, de concrétiser cette ambition.

1. Un haut niveau de protection des données à caractère personnel et de sécurité informatique ne passe pas dans l'immédiat par un nouveau règlement propre aux objets connectés

Le recueil et le traitement des données à caractère personnel par les objets connectés ou à partir de ceux-ci sont soumis au respect du RGPD applicable de plein droit à compter du 25 mai prochain.

Dès lors, les objets connectés doivent garantir la licéité, la loyauté et la transparence du traitement des données à caractère personnel, le respect

---

[1] *Sénat, Résolution européenne du 30 juin 2015 pour une stratégie européenne du numérique globale, offensive et ambitieuse.*

[2] *Conclusions du Conseil compétitivité du 12 mars 2018.*

des finalités du traitement de ces données – finalités qui sont elles-mêmes encadrées –, et préserver l'intégrité et la confidentialité des données.

Le RGPD reconnaît en outre des droits aux personnes concernées, droits que celles-ci doivent pouvoir exercer effectivement : le recueil du consentement exprès et informé de l'intéressé préalablement à la collecte, au traitement et à l'utilisation de ses données à caractère personnel, droit d'accès à leurs données personnelles, de rectification, droit à l'effacement des données (« droit à l'oubli »), droit à la limitation du traitement et droit à la portabilité des données.

Compte tenu de la nature, de la portée et de la finalité du traitement de ces données, ainsi que des risques associés dont la probabilité et la gravité sont variables, les responsables des traitements de données à caractère personnel doivent mettre en œuvre des mesures techniques et organisationnelles pour garantir le respect de la finalité des traitements et la confidentialité des données (art. 25).

Dès lors, il n'est pas nécessaire de prévoir un nouveau cadre législatif au niveau européen mais bien plutôt de mettre en œuvre des mesures propres à assurer un niveau de sécurité approprié, en recourant notamment aux techniques énumérées par le RGPD (art. 32), dont le chiffrement des données.

À cet égard, les codes de conduite et le processus de certification volontaire approuvé prévu par le RGPD (art. 40 à 43), qui font intervenir les secteurs d'activité concernés, les organismes de normalisation et des organismes de certification accrédités, doivent jouer tout leur rôle. Les acteurs européens doivent être pleinement actifs au niveau national, comme au niveau européen et dans les enceintes internationales.

Par ailleurs, le projet de règlement sur la cybersécurité, s'il est adopté, pourrait entrer en vigueur dans un an environ. De nouveaux schémas de sécurité seraient adoptés dans ce cadre, notamment en ce qui concerne l'informatique en nuage, au cœur du développement de l'internet des objets.

C'est pourquoi **votre rapporteur estime que tant l'entrée en vigueur du RGPD que l'adoption de la proposition de règlement sur la cybersécurité vont apporter un encadrement réglementaire satisfaisant à ce stade des objets connectés**. Il n'est donc pas souhaitable d'appeler à de nouvelles règles propres au secteur. Au demeurant, avant d'envisager un nouveau règlement spécifique, il conviendrait de mesurer l'impact du nouveau cadre réglementaire sur les objets connectés. On peut également objecter qu'un cadre réglementaire stable est plus favorable à l'activité des entreprises. Ainsi, pour faciliter le développement d'une industrie numérique en Europe, il importe de ne pas modifier les règles trop souvent.

Toutefois, votre rapporteur partage avec l'auteure de la proposition de résolution l'exigence qu'un haut niveau de protection soit

mis en place dans le cadre évoqué. C'est le sens des modifications qu'il propose d'apporter aux alinéas 21 à 25 de la proposition de résolution

2. La question de la localisation des données appelle un examen approfondi

La localisation des données a une portée symbolique forte et peut paraître facilement comprise par l'opinion publique. Mais les auditions menées par votre rapporteur laissent à penser qu'elle ne sera pas suffisante si elle ne s'accompagne pas d'autres exigences de sécurisation, comme la confidentialité et la traçabilité ou encore l'anonymisation ou le chiffrement.

La sauvegarde des données amène aussi à s'interroger sur la portée de l'obligation. On peut très bien supposer que, concernant des données sensibles, une sauvegarde soit faite et stockée dans un lieu différent pour la prémunir d'attaques physiques ou virtuelles. L'obligation s'appliquerait-elle aussi au double des données ? Ou, au contraire, ne serait-il pas judicieux de sauvegarder ces copies ailleurs qu'en Europe ?

De plus, il n'est pas certain qu'un environnement réglementaire plus exigeant que celui d'autres régions du monde sera plus favorable aux entreprises européennes pour développer l'internet des objets. En outre, pour analyser les masses de données (on évoque actuellement plusieurs centaines de milliards de données par jour !), il faut disposer de capacités techniques suffisantes comme des outils d'intelligence artificielle ou des ordinateurs à haute performance. Or, ce n'est pas le cas de l'Europe actuellement. La mesure, en elle-même, pourrait donc s'avérer contreproductive.

On peut également ajouter que **les règles actuelles n'empêchent pas de favoriser une localisation de certaines données sensibles sur le territoire européen, voir national**. C'est particulièrement le cas des documents et données numériques des collectivités territoriales, qui relèvent du régime juridique des archives publiques et sont considérés comme un trésor national. À ce titre, ils ne peuvent sortir du territoire douanier national. Une solution d'archivage de ces données en nuage ne peut être mise en place qu'à la condition que celle-ci prévoit une localisation physique des données sur le sol français. On parle de « cloud souverain ».

C'est aussi le cas de mesures visant à attribuer un label à un prestataire de service d'informatique en nuage. L'Agence nationale de sécurité des services d'information, l'ANSSI, a ainsi créé un référentiel d'exigences applicables à des solutions d'informatique en nuage, le *cloud*, appelé SecNumCloud. Pour répondre aux exigences de l'ANSSI et voir le service qu'il propose recueillir une validation de niveau dit « essentiel », le professionnel doit s'engager à stocker et à traiter les données du client au sein de l'Union européenne. En outre, les opérations d'administration et de supervision du service doivent être réalisées depuis l'Union européenne. On

peut constater l'effet vertueux d'une telle mesure. Pour obtenir la labellisation par l'ANSSI, le professionnel de l'informatique en nuage doit donc maintenir les données de ses clients dans l'Union européenne. Le label est un gage de sécurité pour le client et les données sont maintenues sur le territoire européen, sans qu'il soit besoin d'un nouveau règlement.

Cependant, il convient de rappeler que le droit de l'internet est en construction permanente et concerne un objet en évolution constante. **L'Union européenne ne peut totalement exclure le principe d'une obligation générale de localisation des données à caractère personnel sur le territoire européen,** ainsi que les conditions de leur sécurisation. La question se posera aussi pour les données à caractère non personnel qui constituent, elles aussi, un enjeu.

C'est la raison pour laquelle **l'opportunité de cette localisation doit être étudiée de manière approfondie afin d'en mesurer toutes les conséquences, tant juridiques qu'économiques et techniques**. Une telle étude devrait s'appuyer sur l'examen de l'accord d'adéquation avec les États-Unis, *Privacy Shield*, dont les résultats devraient être connus en septembre prochain, et au regard des évolutions législatives récentes aux États-Unis.

Le *Cloud Act* américain :
l'extraterritorialité des lois face à la localisation des données

Le législateur américain vient de voter une loi (promulguée le 23 mars 2018) sur la surveillance des données à caractère personnel dans le nuage : le *Cloud Act*, pour *Clarifying Lawful Overseas Use of Data Act*.

Ce texte permet aux services de police et de surveillance américains, qu'ils soient fédéraux ou locaux, de contraindre les fournisseurs de services américains, par mandat ou assignation, à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers. Ainsi, la loi donne un cadre légal à la saisie par des agences gouvernementales ou des forces de police d'e-mails, de documents et de communications électroniques localisés dans des *datacenters* de sociétés américaines situés hors du sol américain. Autrement dit, le nouveau texte permet aux forces de l'ordre américaines d'obtenir les données personnelles d'un individu sans que celui-ci en soit informé, ni que son pays de résidence ne le soit, ni même que le pays où sont stockées ces données ne le soit.

En échange, le texte prévoit une forme de réciprocité : les autorités étrangères pourraient avoir accès aux données stockées aux États-Unis, et en dehors des règles concernant le droit américain des données à caractère personnel.

Ces mesures nouvelles ont été adoptées suite au refus de la société Microsoft de livrer aux autorités américaines des données relevant de comptes gérés par elle et stockées en Irlande. Le Gouvernement américain, estimant que son pouvoir d'enquête était entravé, avait porté l'affaire devant la Cour suprême.

Il est encore tôt pour mesurer la portée exacte du nouveau texte de loi américain. Pour certains, il apporte une sécurité juridique, pour d'autres il constitue une atteinte aux libertés. Il n'en demeure pas moins qu'il constitue une application extraterritoriale du droit américain.

Il convient de rappeler que le RGPD prévoit que les règles protégeant les données à caractère personnel des Européens s'appliquent même en-dehors du territoire de l'Union. Les deux textes pourraient entrer en conflit. En outre, de telles mesures mènent en exergue les limites d'une localisation géographique des données à l'ère numérique, à la fois comme moyen de protection contre des intrusions ou de l'espionnage et comme limite à la garantie juridique que les États doivent à leurs citoyens.

3. La normalisation : poursuivre les actions engagées en vue d'accroître l'influence des acteurs européens de la normalisation au niveau international et appeler les acteurs français à se mobiliser

Votre **rapporteur partage l'idée selon laquelle les acteurs européens de la normalisation doivent renforcer leur influence au niveau international**, particulièrement en matière numérique et, plus spécifiquement, concernant l'internet des objets. C'est pourquoi il propose de ne **modifier qu'à la marge la proposition de résolution à ce sujet**.

Selon les acteurs de la normalisation, l'influence d'un pays au sein des organisations internationales se mesure essentiellement aux **places occupées par des experts représentant les intérêts du pays en question dans les instances de travail propres à chaque organisation internationale**. Auditionnés par votre rapporteur, les représentants de l'Association française de normalisation (AFNOR) ont, par exemple, souligné, d'une part, l'investissement du Gouvernement chinois dans la normalisation, qui en fait un élément de sa politique industrielle, d'autre part, l'influence toujours prégnante de l'Allemagne, tant au niveau européen que mondial. Si l'investissement des États membres et de leurs entreprises dans le processus de normalisation est donc d'une intensité diverse au sein de l'Union européenne, une **mobilisation accrue de l'ensemble des acteurs européens est souhaitable**. Cela concourrait sans aucun doute au **développement d'une industrie européenne** forte en ces domaines, là où l'Europe accuse déjà un retard non négligeable.

L'influence des Européens dans les organismes internationaux de normalisation est d'autant plus cruciale que, comme l'AFNOR l'a indiqué à votre rapporteur, **seules 10 % des normes publiées dans la collection française ont une origine exclusivement française**, le reste étant d'origine européenne ou internationale.

a) Renforcer la présence des acteurs européens dans les organismes internationaux de normalisation en matière de sécurité numérique et d'internet des objets

Comme précisé plus haut, les organismes internationaux de normalisation reposent sur le principe selon lequel chaque membre dispose d'une voix, et les États y sont représentés par les organismes nationaux de normalisation qu'ils peuvent subventionner, mais qui sont composés de professionnels, et pas d'administrations publiques.

En conséquence, les États membres de l'Union européenne apparaissent plus forts en disposant chacun d'une représentation dans ces organismes, plutôt qu'en étant représentés par l'Union européenne.

C'est pourquoi **votre rapporteur propose de substituer, à l'alinéa 29, à la mention selon laquelle l'Union européenne doit renforcer sa présence** dans les organismes internationaux de normalisation, **celle selon laquelle ce sont les acteurs européens du secteur qui doivent, avec le soutien de l'Union européenne et de ses États membres, renforcer leur présence** dans les enceintes internationales d'élaboration des normes de sécurité en matière numérique, et particulièrement d'internet des objets.

b) Appeler les acteurs français de l'internet des objets à se mobiliser en ce sens

Les auditions menées par votre rapporteur ont également souligné le **manque d'investissement des acteurs français dans la normalisation**. Ce constat avait également été dressé par notre collègue Elisabeth Lamure, dans son rapport précité sur la normalisation. C'est pourquoi votre rapporteur propose d'insérer, dans la proposition de résolution, un **alinéa 30**, qui **appelle tant les entreprises que les administrations publiques à se mobiliser pour assurer leur présence dans les organismes européens et internationaux de normalisation**.

4. La politique commerciale de l'Union : promouvoir des normes exigeantes en matière numérique

Le système de normalisation ne fait pas partie de la politique commerciale des États, qui s'entend comme l'ensemble des moyens dont dispose un État pour orienter les flux d'échanges avec un pays étranger.

C'est pourquoi votre rapporteur propose la modification de l'alinéa 28 dans un sens plus cohérent avec la notion de politique commerciale : **la proposition de résolution appelle l'Union à promouvoir, dans la conduite de sa politique commerciale, des normes – tant professionnelles que réglementaires – exigeantes dans le secteur numérique**, notamment en matière de sécurité des systèmes d'information et de protection des données à caractère personnel. Au demeurant, le

numérique étant de plus en plus présent dans les accords commerciaux, cette orientation de principe apparaît nécessaire[1].

5. Renforcer les moyens de contrôle en France

Les auditions menées par votre rapporteur ont montré que face aux évolutions juridiques et aux enjeux, notre pays ne dispose pas de suffisamment de moyens d'action et de contrôle.

À titre d'exemple, le rapport annuel de la CNIL fait état, pour 2017, de l'adoption de 2 964 autorisations de transfert de données en dehors de l'Union européenne, adoptées dans cadre total de 4 124 décisions et délibérations. Or, la commission ne dispose que d'un effectif limité, 198 personnes.

On sait d'ores et déjà que l'entrée en application du RGPD va augmenter la charge de travail de la CNIL.

L'essor de l'internet des objets – et de l'intelligence artificielle – va multiplier les questions relatives à la protection des données à caractère personnel dans les années à venir. Notre pays doit prendre la pleine mesure de ces défis et adapter les moyens de notre contrôleur national en conséquence. C'est le sens de l'alinéa 34 proposé par votre rapporteur.

[1] *Voir, sur ce sujet, le rapport précité de l'Inspection générale des finances et du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies intitulé « Accord plurilatéral sur le commerce des services et partenariat transatlantique pour le commerce et l'investissement : enjeux numériques des négociations ».*

EXAMEN EN COMMISSION

La commission des affaires européennes s'est réunie le jeudi 12 avril 2018 pour l'examen du présent rapport. À l'issue de la présentation faite par le rapporteur M. André Gattolin, le débat suivant s'est engagé :

M. Jean Bizet. – Je retiens que le souci principal, c'est le haut niveau de sécurité. On voit bien qu'au XXIe siècle, celui qui possède l'information et qui peut la transgresser détient une arme. Je l'avais constaté en ce qui concerne la propriété intellectuelle sur les semences.

Le deuxième point, c'est que l'Europe doit être plus présente dans l'élaboration des normes internationales. C'est vrai dans d'autres secteurs, c'est vrai aussi pour le numérique.

Et c'est vrai que nous sommes carencés en ce qui concerne les superordinateurs. Je crois que notre pays en a quatre, mais ils sont d'une ancienne génération. Et leurs capacités sont près de dix mille fois inférieures à celles dont disposent les États-Unis et la Chine.

Quant aux hommes et aux femmes de très grande qualité que nous avons en Europe et particulièrement en France, si on ne les rémunère pas suffisamment, ils s'en vont.

M. Jean-Marie Janssens, rapporteur pour la commission des affaires économiques. – Monsieur le Président, Mes chers collègues, je souhaite d'abord remercier le président Bizet et la présidente Sophie Primas, qui ont souhaité que nous travaillions ensemble sur ce sujet. Ce travail a été effectué en commun en vue de simplifier le processus d'élaboration de la résolution et de travailler plus efficacement.

C'est donc avec plaisir, et un grand intérêt, que j'ai participé, avec le rapporteur André Gattolin, aux auditions. Ces auditions, d'une grande qualité, nous ont permis de nous forger une opinion sur les sujets évoqués par la proposition de résolution.

Contrairement à mon collègue, je suis plutôt néophyte sur le sujet des objets connectés. Les auditions ont néanmoins été l'occasion pour moi de prendre conscience que ce sujet comporte des enjeux d'une importance capitale. Ceux-ci sont d'abord d'ordre économique – je pense à la normalisation. Ils sont également d'ordre politique – je pense à la cybersécurité et à la protection des données à caractère personnel. Le sujet est donc relativement complexe, car il se situe au croisement de nombreuses législations. Notre collègue Catherine Morin-Desailly, présidente de la commission de la culture, a raison de nous alerter, car ces objets connectés vont inonder nos vies, et il convient que le cadre applicable soit

suffisamment protecteur des citoyens et favorise le développement d'une industrie européenne de l'internet des objets.

Aussi, je confirme que je partage les conclusions que notre collègue André Gattolin vient de vous présenter. Nous souhaitons appuyer les demandes exigeantes mais pertinentes de Mme Morin-Desailly, même si quelques ajustements sont apparus nécessaires. Ceux-ci ont été parfaitement décrits par le rapporteur.

Merci, Monsieur le président, de m'avoir permis de vous donner mon sentiment en tant que rapporteur pour la commission des affaires économiques.

M. Jean-François Rapin. – Je voulais évoquer le problème des compteurs Linky. Sur le terrain, la situation est ambiguë. Pour les préfets aussi, car il y a de nombreuses contestations de la part de citoyens. Je voudrais savoir quels sont les travaux conduits par le Sénat sur le sujet et ce qui en a été conclu.

J'en parlais encore avec le préfet de mon département, qui ne comprend pas cet acharnement sur un dispositif censé améliorer la vie des gens et, à terme, permettre de faire des économies. Si on regarde, EDF nous demande déjà de transmettre nos informations ; sur la base du volontariat, pour nous aider à améliorer notre consommation. Linky, c'est un système d'abonnement.

Je demande une précision technique, même si je ne suis pas certain de l'avoir ce matin, mais c'est un sujet qui est sur la table depuis 2-3 ans.

Mme Sylvie Robert. – Merci au rapporteur et à Catherine Morin-Desailly, qui avait évoqué la question des objets connectés lors de la discussion sur la mise en œuvre du RGPD en France. Elle souhaitait que ces mots y soient inscrits mais elle a reçu une fin de non-recevoir. Pourtant, ce sujet est extrêmement important.

Je partage les conclusions de ce rapport et, singulièrement, la demande d'augmentation des moyens de la CNIL. Là aussi, nous l'avions demandé durant le débat sur la mise en œuvre du RGPD en droit français. Mais j'ai été très étonnée de la réponse du Gouvernement, qui s'est contenté de dire que ces moyens avaient été augmentés il y a quelques années et que, puisqu'on était passé à un système de mise en conformité, là ou avant il fallait une autorisation, la CNIL aurait moins de travail. On verra ce qu'il en sera dans le prochain projet de loi de finances, mais j'attire l'attention de nos collègues, car c'est une question très importante.

Par ailleurs, j'aimerais que la notion de consentement soit plus clairement mise en avant dans le texte, en insistant sur le fait que l'utilisateur peut à tout moment retirer son consentement. Les deux facettes « *in-in* et *in-out* » et leurs conséquences sont bien expliquées, mais sur le consentement, il faudrait être plus précis. C'est une notion très importante

en ce qui concerne les données à caractère personnel. Et si je partage la position du rapporteur sur les trois grands axes de la proposition de résolution, l'exigence du consentement me paraît devoir être renforcée dans le texte.

Mme Laurence Harribey. – Je remercie le rapporteur pour ce travail, qui s'ajoute à ceux déjà réalisés sur le sujet. Et je pense qu'on devrait les compiler, car on commence à avoir un corpus intéressant et, surtout, pertinent.

Sur le texte concernant la certification de cybersécurité, avec René Danési, nous sortons d'une série d'auditions. Le texte sur lequel nous avions émis un avis motivé de subsidiarité a été beaucoup retravaillé et notre position a été entendue. On se dirige vers une certification vers le haut, même si nous devons rester vigilants.

Ce qui a été dit sur la normalisation vaut aussi, en partie, pour la certification. Je soutiens une certification de cybersécurité européenne, mais je rappelle que les compétences sont dans les États. Il faut donc que l'Union accepte de travailler avec eux pour établir une certification de haut niveau qui lui permettra d'asseoir sa place à l'international.

Un texte propre aux objets connectés pourrait renforcer l'arsenal européen, mais il faudra s'assurer qu'il n'entre pas en contradiction avec le texte général sur la certification.

Sur la localisation des données, nous avons auditionné hier un représentant de Thales, qui était plutôt sceptique sur cette solution. Il évoquait plutôt le chiffrement comme une piste plus plausible. Dans vos auditions, avez-vous eu des éléments là-dessus ?

M. Pierre Ouzoulias. – Je voudrais à mon tour me féliciter de la qualité du travail effectué, notamment par la présidente de la commission de la culture, et rappeler la spécificité de cette commission sur les questions numériques. Je pense que la commission des affaires européennes et la commission de la culture, en lien avec les autres commissions, auront certainement à travailler ensemble sur ces questions à l'avenir.

Je retiens que les données à caractère personnel sont collectées très souvent sans notre consentement et permettent de façon très fine de restituer notre comportement social, voire politique. On sait que certains travaillent à un profilage fin des individus pour soit leur vendre des produits, soit orienter les campagnes électorales, par une programmation de l'orientation des votes.

Comme en matière sportive, j'estime qu'il n'y a pas de petit niveau de dopage : soit on respecte tous la même règle, soit on ne la respecte pas. Donc, en matière électorale, il est essentiel que certaines écuries ne disposent pas de moyens dont les autres seraient privées.

Je pense que notre Haute assemblée a un rôle essentiel à jouer dans la défense des libertés individuelles. Et nous sommes là au cœur du sujet, qui n'est pas un petit sujet. De par notre tradition, nous devons montrer que le Sénat a un rôle à jouer.

Je suis donc très favorable à ce rapport et il faut continuer dans cette direction.

M. Olivier Henno. – Je salue à mon tour la qualité du rapport et les propos du président sur l'arme détenue par celui qui possède l'information, qui me rappelle mon métier d'origine, le marketing direct. À l'époque, on croisait les mailings et on appelait ça le marketing discriminant. Évidemment les calculateurs étaient beaucoup moins puissants qu'aujourd'hui, mais c'est le même processus.

Je suis assez frappé par l'écart entre l'exigence que la CNIL peut avoir vis-à-vis des données stockées dans les mairies – qui est légitime, en soi – et l'exigence qu'elle a vis-à-vis des GAFA qui est encore trop faible. On le voit, tout tourne autour du consentement.

Quand on regarde l'audition de Mark Zuckerberg, le patron de Facebook, par le Congrès américain, on se dit : soit il est vraiment de bonne foi et c'est quelqu'un qui est à la tête d'une arme qu'il ne maîtrise pas, soit il est de mauvaise foi et il dissimule des choses et ne dit pas toute la vérité. Ce qui est frappant, c'est l'absence d'anticipation.

Il faudra travailler sur cette notion de consentement. Ce n'est pas parce qu'on accepte de partager des informations sur ses loisirs, ses voyages et ses vacances qu'on accepte de voir ses goûts décryptés pour savoir ce que sont ses opinions politiques, philosophiques ou recevoir n'importe quelle offre commerciale ciblée. Or, c'est exactement ce qui se passe !

Et je trouve qu'il y a deux poids- deux mesures dans l'exigence.

M. André Reichardt. – Je voudrais mettre l'accent sur le caractère équilibré de cette résolution, qui demande la mise en place rapide d'un haut niveau de certification au niveau européen au point 21 et qui, pour ce faire, demande l'implication plus forte des pays européens, dont le nôtre. Et la mobilisation de tous les acteurs sera nécessaire pour faire monter le niveau.

Et si on évoque le risque de surveillance par des entités non européennes, quid du risque de surveillance en Europe ?

Je m'interroge aussi sur l'obligation de localisation. Je ne suis pas convaincu qu'elle soit exempte de critiques.

M. André Gattolin. – Concernant les compteurs Linky, il ne s'agit pas de dire que les compteurs intelligents ne font pas sens. Je vous renvoie sur ce point au rapport de l'Office parlementaire des choix scientifiques et technologiques du 15 février 2018 sur les enjeux des compteurs communicants. En l'espèce, ce qui compte, c'est l'information et le

consentement des utilisateurs : on leur fait penser qu'on collecte leurs données pour qu'ils puissent mieux combattre leur consommation, alors qu'on va leur proposer de nouvelles offres marketing. Ce n'est pas le principe même des compteurs communicants qui est en jeu, mais l'usage qui en est fait.

Cela nous ramène à la notion de consentement. Pour certaines entreprises, l'acte d'achat vaut consentement. D'autres vous renvoient à la lecture de clauses écrites en tout petits caractères qu'on ne prend pas le temps de lire et c'est plutôt la question de l'information du consommateur qui est, à mon avis, en jeu. C'est un sujet complexe.

Sur le retrait du consentement, Catherine Morin-Desailly insiste sur un « droit au silence des puces ». L'idée est bonne, mais sa généralisation ne me paraît pas réaliste. Il y a des objets qui ne nécessitent pas ça. Il faut distinguer les objets « in-in » qui ne communiquent pas de données à l'extérieur et les objets « in-out », qui eux le font. C'est de ces derniers qu'on doit pouvoir se déconnecter. Mais, là encore, il faut distinguer : certaines données collectées peuvent être agrégées dans un objectif de santé ou de politique publiques. Par exemple, des données agrégées sur des logements plus ou moins insalubres dans un même espace permettraient de déterminer le meilleurs accès pour les forces d'intervention en cas d'incendie.

Et puis, il y aura des objets connectés, simples, qui auront une technologie peu développée et une durée de vie sûrement limitée. Et il faut quand même rappeler que, quand on achète un objet connecté, c'est justement parce qu'il l'est.

Tout comme Sylvie Robert et Pierre Ouzoulias, je suis favorable à des droits fondamentaux qui s'appliqueraient au numérique et soutiens aussi que notre Assemblée doit avoir un rôle éminent dans leur affirmation. Je suis plus réservé quant à leur généralisation à toutes les situations, car on se rend compte qu'on ne peut pas réglementer tous les aspects.

Je pense également qu'il ne faut pas négliger la régulation par la *soft law*, comme la certification et la normalisation qui impliquent les acteurs eux-mêmes. Les trois niveaux – national avec l'Afnor, européen et international avec les normes Iso – sont extrêmement importants.

Pour répondre à Sylvie Robert sur le fait d'inclure les termes « objets connectés » dans le projet de loi sur la protection des données, je signalerai que la CNIL nous a confirmé que, de fait, les objets connectés seront concernés par le RGPD, de portée plus large. En faire mention n'aurait rien apporté sur le plan juridique. Et sur le consentement, oui, il faut être plus clair.

Sur la différence d'exigence vis-à-vis des collectivités territoriales et des GAFA, je dirais qu'on essaie d'imposer des règles aux seconds, mais ce n'est pas facile. J'attire votre attention sur le RGPD, qui va quand même assez loin en imposant même des règles protégeant nos citoyens au-delà du

seul territoire européen. C'est la première fois que nous avons un texte qui créé de l'extraterritorialité, à l'image de ce que font les États-Unis avec le *Cloud Act* que j'ai évoqué.

Les sujets sont complexes et un texte entre tout juste en application : attendons déjà de voir comment cela se passe avant de proposer une nouvelle législation. Nous devons aussi être très attentifs à l'application du *Privacy Shield* signé avec les États-Unis. La Commission européenne doit présenter un rapport sur l'application de cet accord en septembre prochain. Nous en tirerons alors toutes les conséquences.

Concernant la rédaction de la résolution, nous proposons d'ajouter à la fin du point 21 : « *incluant notamment le libre consentement des personnes* ».

Mme Sylvie Robert. – Ça va dans le sens que je souhaitais, mais je voudrais qu'on indique qu'on peut retirer son consentement à tout moment.

M. André Gattolin. – Je ne crois pas qu'on pourra le faire pour tous les objets.

M. Jean Bizet, président. – Je comprends le point de vue de Sylvie Robert, dont je rappelle qu'elle siège à la CNIL. Je propose qu'on s'en tienne à la rédaction proposée en ce qui concerne la résolution, mais que le rapport explicite plus précisément ce point.

M. André Gattolin. – Je souhaiterais juste évoquer en complément la question de la territorialisation et du stockage des données. Certaines données ne sont pas uniques et nécessitent une sauvegarde. Un pays comme l'Estonie, qui craint une attaque d'un grand pays voisin, stocke ses données en Grande-Bretagne. Donc, j'attire votre attention sur les limites, voire le danger, de cette solution qui consisterait à garder toutes les données au même endroit. C'est pourquoi, je ne suis pas favorable à une localisation généralisée des données en Europe.

*

À l'issue du débat, la commission des affaires européennes a conclu, à l'unanimité, à l'adoption de la proposition de résolution modifiée dans le texte suivant :

PROPOSITION DE RÉSOLUTION EUROPÉENNE MODIFIÉE

① Le Sénat,

② Vu l'article 88 4 de la Constitution,

③ Vu les articles 3, 16, 26 et 114 du traité sur le fonctionnement de l'Union européenne,

④ Vu le règlement (UE) 2016/679 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, et abrogeant la directive 94/46/CE (règlement général sur la protection des données),

⑤ Vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union,

⑥ Vu la proposition de règlement COM(2017) 10 final concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») et la proposition de règlement COM(2017) 477 final relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n°526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité),

⑦ Vu le livre blanc conjoint du groupe consultatif Union européenne - République populaire de Chine sur l'internet des objets de janvier 2016, intitulé *« EU-China Joint White Paper on the Internet of Things »*,

⑧ Vu la communication COM(2016) 180 final de la Commission européenne au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions du 19 avril 2016 intitulée « Passage au numérique des entreprises européennes : tirer tous les avantages du marché unique numérique »,

⑨ Vu le document de travail SWD(2016) 110 final de la Commission européenne intitulé *« Advancing the internet of things in Europe »* assortissant la communication COM(2016) 180 final de la Commission européenne au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions du 19 avril 2016 précitée,

⑩ Vu le rapport d'information du Sénat « L'Union européenne, colonie du monde numérique ? » (n° 443, 2012-2013) – 20 mars 2013 – de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes,

⑪ Vu le rapport d'information du Sénat « L'Europe au secours de l'internet : démocratiser la gouvernance de l'internet en s'appuyant sur une ambition politique et industrielle européenne » (n° 696 tome I, 2013 2014) – 8 juillet 2014 – de Mme Catherine Morin-Desailly, fait au nom de la mission commune d'information sur la gouvernance mondiale d'internet,

⑫ Vu le rapport d'information de l'Assemblée nationale sur les objets connectés (n° 4362, quatorzième législature) – 10 janvier 2017 – de Mmes Corinne Erhel et Laure de La Raudière, fait au nom de la commission des affaires économiques,

⑬ Vu la résolution européenne n° 122 (2014-2015) pour une stratégie européenne du numérique globale, offensive et ambitieuse, devenue résolution du Sénat le 3 juin 2015,

⑭ Considérant que la souveraineté numérique constitue un enjeu politique majeur pour l'Union européenne,

⑮ Considérant qu'il ne sera possible de promouvoir cette souveraineté numérique qu'en développant un écosystème numérique industriel puissant et diversifié sur l'ensemble du territoire européen,

⑯ Considérant que la mise en œuvre d'un niveau élevé de protection des consommateurs en matière d'objets connectés favorisera l'émergence d'objets connectés conformes au droit et principes européens et qu'elle stimulera le développement d'une filière industrielle de l'internet des objets en Europe ainsi que l'utilisation d'objets connectés européens par les industries traditionnelles,

⑰ Considérant la part croissante que représente l'internet des objets dans la production de données à caractère personnel et dans la production des données issues des activités industrielles et commerciales des opérateurs économiques,

⑱ Considérant que le risque de surveillance, par des entités non européennes soumises à des régimes juridiques autorisant les intrusions gouvernementales dans leur système d'information en est de fait accru,

⑲ Considérant l'importance que revêt l'internet des objets dans le développement économique de l'Union, notamment par la mise en œuvre de nouvelles générations d'objets industriels connectés dans les secteurs stratégiques pour l'économie européenne que sont la santé, la maîtrise de l'énergie, la protection de l'environnement ou encore les transports,

⑳ Considérant que l'objectif de construction d'un marché unique doit être appuyé par une stratégie industrielle européenne audacieuse dans le domaine de l'internet des objets et que la mise en œuvre de cette politique passe à la fois par le développement de technologies qui répondent aux principes de protection des données et de sécurité des systèmes d'information, et par le soutien à l'édification d'un marché unique numérique porteur de croissance et acteur de l'économie numérique européenne,

㉑ Demande en conséquence la mise en place rapide d'une certification des objets connectés qui garantisse un haut niveau de sécurité informatique et de protection des données à caractère personnel, incluant notamment le libre consentement des personnes ;

㉒ Estime que ce haut niveau de protection doit notamment inclure :

㉓ –la possibilité d'une désactivation sélective ou totale de l'objet connecté ;

㉔ – la possibilité de mises à jour de sécurité ;

㉕ – l'usage de technologies cryptographiques pour la protection des données sensibles ;

㉖ Demande que soit considérée l'opportunité d'une obligation de localisation et de traitement des données à caractère personnel des consommateurs sur le territoire de l'Union européenne ;

㉗ Demande que l'Union européenne inclue dans la conduite de sa politique commerciale la promotion de normes exigeantes en matière numérique ;

㉘ Demande que les acteurs européens renforcent leur présence dans les enceintes internationales d'élaboration des normes et des standards de sécurité en matière numérique, et particulièrement l'internet des objets ;

㉙ Appelle les acteurs français de l'internet des objets à élaborer des normes au niveau national et européen pour les proposer ensuite dans ces enceintes ;

㉚ Demande le renforcement des moyens de la CNIL pour lui permettre de faire face à l'essor des objets connectés.

TABLEAU COMPARATIF

Texte de la proposition de résolution	Texte adopté par la commission
(1) Le Sénat,	*(1) Sans modification*
(2) Vu l'article 88-4 de la Constitution ;	*(2) Sans modification*
(3) Vus les articles 16, 26 et 114 du traité sur le fonctionnement de l'Union européenne,	*(3) Vu les articles 3, 16, 26 et 114 du traité sur le fonctionnement de l'Union européenne,*
(4) Vu le règlement (UE) 2016/679 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, et abrogeant la directive 94/46/CE (règlement général sur la protection des données),	*(4) Sans modification*
(5) Vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union,	*(5) Sans modification*
	(6) Vu la proposition de règlement COM(2017) 10 final concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») et la proposition de règlement COM(2017) 477 final relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n°526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité),
(6) Vu le livre blanc conjoint du groupe consultatif Union européenne - République populaire de Chine sur l'internet des objets de janvier 2016, intitulé *« EU-China Joint White Paper on the Internet of Things »*,	*(7) Sans modification*

(7) Vu la communication COM(2016) 180 final de la Commission européenne au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions du 19 avril 2016 intitulée « Passage au numérique des entreprises européennes : Tirer tous les avantages du marché unique numérique »,	*(8) Sans modification*
(8) Vu le document de travail SWD(2016) 110 final de la Commission européenne intitulé « *Advancing the internet of things in Europe* » assortissant la communication COM(2016) 180 final de la Commission européenne au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions du 19 avril 2016 précitée,	*(9) Sans modification*
(9) Vu le rapport d'information du Sénat « L'Union européenne, colonie du monde numérique ? » (n° 443, 2012-2013) – 20 mars 2013 – de Mme Catherine Morin-Desailly, fait au nom de la commission des affaires européennes,	*(10) Sans modification*
(10) Vu le rapport d'information du Sénat « L'Europe au secours de l'internet : démocratiser la gouvernance de l'internet en s'appuyant sur une ambition politique et industrielle européenne » (n° 696 tome I, 2013-2014) – 8 juillet 2014 – de Mme Catherine Morin-Desailly, fait au nom de la mission commune d'information sur la gouvernance mondiale d'internet,	*(11) Sans modification*
(11) Vu le rapport d'information de l'Assemblée nationale sur les objets connectés (n° 4362, quatorzième législature) – 10 janvier 2017 – de Mmes Corinne Erhel et Laure de La Raudière, fait au nom de la commission des affaires économiques,	*(12) Sans modification*
(12) Vu la résolution européenne n° 122 (2014-2015) pour une stratégie européenne du numérique globale, offensive et ambitieuse, devenue résolution du Sénat le 30 juin 2015,	*(13) Sans modification*
(13) Considérant que la souveraineté numérique constitue un enjeu politique majeur pour l'Union européenne,	*(14) Sans modification*

(14) Considérant qu'il ne sera possible de promouvoir cette souveraineté numérique qu'en développant un écosystème numérique industriel puissant et diversifié sur l'ensemble du territoire européen,	*(15) Sans modification*
	(16) Considérant que la mise en œuvre d'un niveau élevé de protection des consommateurs en matière d'objets connectés favorisera l'émergence d'objets connectés conformes au droit et principes européens et qu'elle stimulera le développement d'une filière industrielle de l'internet des objets en Europe ainsi que l'utilisation d'objets connectés européens par les industries traditionnelles,
(15) Considérant la part croissante que représente l'internet des objets dans la production de données à caractère personnel et dans la production des données issues des activités industrielles et commerciales des opérateurs économiques,	*(17) Sans modification*
	(18) Considérant que le risque de surveillance, par des entités non européennes soumises à des régimes juridiques autorisant les intrusions gouvernementales dans leur système d'information en est de fait accru ;
(16) Considérant le principe de protection des données personnelles porté par le règlement (UE) 2016/679 du 26 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la proposition de règlement COM(2017) 10 final concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques ») ainsi que les impératifs de sécurité des systèmes d'information,	*Supprimé*
(17) Considérant l'importance critique que revêt l'internet des objets dans le développement économique de l'Union, notamment par la mise en œuvre de nouvelles générations d'objets industriels connectés dans les secteurs critiques pour l'économie européenne que sont la santé, la maîtrise de l'énergie, la protection de l'environnement ou encore les transports,	*(19) Considérant l'importance que revêt l'internet des objets dans le développement économique de l'Union, notamment par la mise en œuvre de nouvelles générations d'objets industriels connectés dans les secteurs stratégiques pour l'économie européenne que sont la santé, la maîtrise de l'énergie, la protection de l'environnement ou encore les transports,*

(18) Considérant que l'objectif de construction d'un marché unique doit être appuyé par une stratégie industrielle européenne audacieuse dans le domaine de l'internet des objets et que la mise en œuvre de cette politique passe à la fois par le développement de technologies qui répondent aux principes de protection des données et de sécurité des systèmes d'information, et par le soutien à l'édification d'un marché unique numérique porteur de croissance et acteur de l'économie numérique européenne,	*(20) Sans modification*
(19) Considérant que le risque de surveillance, par des entités non européennes soumises à des régimes juridiques autorisant les intrusions gouvernementales dans leur système d'information est accru par le caractère sensible des données personnelles et par le caractère stratégique des données industrielles issues des objets connectés,	*Supprimé*
(20) Considérant que la mise en œuvre d'un niveau élevé de protection des consommateurs en matière d'objets connectés favorisera l'émergence d'objets connectés conformes au droit et principes européens et qu'elle stimulera le développement d'une filière industrielle de l'internet des objets en Europe ainsi que l'utilisation d'objets connectés européens par les industries traditionnelles,	*Supprimé*
(21) Demande en conséquence, l'adoption d'un outil réglementaire de reconnaissance et d'autorisation des objets connectés à destination des consommateurs prenant la forme d'une certification,	*(21) Demande en conséquence la mise en place rapide d'une certification des objets connectés qui garantisse un haut niveau de sécurité informatique et de protection des données à caractère personnel, incluant notamment le libre consentement des personnes ;*
(22) Demande que cette certification garantisse un haut niveau de protection et de sécurité pour les données personnelles, en imposant :	*(22) Estime que ce haut niveau de protection doit notamment inclure :*
(23) – la possibilité d'une désactivation sélective ou totale de l'objet connecté aux fins d'établir le refus de collecte de données en introduisant un « droit au silence des puces » ;	*(23) – la possibilité d'une désactivation sélective ou totale de l'objet connecté ;*
(24) – l'obligation de rendre possibles les mises à jour de sécurité pour tout objet connecté à destination des consommateurs ;	*(24) – la possibilité de mises à jour de sécurité ;*

(25) – la mise en œuvre de niveaux de sécurité plus exigeants pour les objets qui permettent la collecte de données de catégories particulières au sens de l'article 9 du règlement général sur la protection des données, en particulier l'usage de technologies cryptographiques ;	*(25) – l'usage de technologies cryptographiques pour la protection des données sensibles ;*
(26) – un niveau de protection des individus conforme aux dispositions du règlement général de protection des données personnelles, et notamment aux droits de rectification, d'effacement et d'opposition au traitement des données à caractère personnel ;	*Supprimé*
(27) Demande que soit introduite une obligation de localisation et de traitement des données personnelles des consommateurs européens sur le territoire de l'Union européenne ;	*(26) Demande que soit considérée l'opportunité d'une obligation de localisation et de traitement des données à caractère personnel des consommateurs sur le territoire de l'Union européenne ;*
(28) Demande que la politique commerciale de l'Union inclue la normalisation et la standardisation en matière numérique ;	*(27) Demande que l'Union européenne inclue dans la conduite de sa politique commerciale la promotion de normes exigeantes en matière numérique ;*
(29) Demande que l'Union européenne développe sa présence dans les enceintes internationales d'élaboration des normes et des standards de sécurité en matière numérique, et particulièrement l'internet des objets.	*(28) Demande que les acteurs européens renforcent leur présence dans les enceintes internationales d'élaboration des normes et des standards de sécurité en matière numérique, et particulièrement l'internet des objets ;*
	(29) Appelle les acteurs français de l'internet des objets à élaborer des normes au niveau national et européen pour les proposer ensuite dans ces enceintes ;
	(30) Demande le renforcement des moyens de la CNIL pour lui permettre de faire face à l'essor des objets connectés

LISTE DES PERSONNES AUDITIONNÉES

– Ministère de l'économie et des finances - Direction générale des entreprises :

M. Loïc DUFLOT, Sous-directeur des réseaux et usages numériques.

M. Olivier Rouxel, Chargé de mission RFID, Internet des objets, French Tech

– AFNOR :

Mme Nathalie LOCHET, Directrice de la communication.

M. Rémi REUSS, Responsable de projets Consommation - Collectivités territoriales - Innovation.

– Commission nationale de l'informatique et des libertés (CNIL) :

Mme Tiphaine HAVEL, Conseillère pour les questions institutionnelles et parlementaires.

M. Matthieu GRALL, Chef du service de l'expertise technologique

Mme Clémence SCOTTEZ, Cheffe du service des affaires économiques.