FONDATION ROBERT SCHUMAN

POLICY PAPER

Question d'Europe
n°484
17 Septembre 2018

Ce que révèle le modèle européen de protection des données personnelles

Constance Bommelaer de Leusse
Lucien Castex

Des centaines de **millions** de personnes utilisent désormais Internet au quotidien avec des usages multiples : achats, banque en ligne, réseaux sociaux, etc. Ils échangent à cette occasion un nombre exponentiel de données dont certaines revêtent un caractère éminemment personnel. Les risques associés sont également croissants et ce dans un large spectre allant du traitement non autorisé de données, à la fraude ou encore la manipulation de l'opinion publique qui met en danger les démocraties modernes. Pour l'ensemble de ces raisons, la protection de la vie privée et des données personnelles est devenue une priorité européenne. Un marché unique du numérique n'émergera pas sans un sentiment de confiance des usagers.

I UNE PROTECTION REFLÉTANT UNE AMBITION EUROPÉENNE

La protection des données personnelles est rapidement devenue une question centrale en France et en Europe. Ce droit est formalisé dès 1978 en France avec la loi dite informatique et libertés, en 1981 avec la Convention 108 du Conseil de l'Europe, puis en 1995 avec l'adoption d'une première directive européenne. Elle constitue un droit inscrit dans la Charte des droits fondamentaux de l'Union européenne. Depuis le 25 mai 2018, l'applicabilité du règlement général sur la protection des données (RGPD) permet d'adapter cette protection aux dernières évolutions technologiques.

Décriée par d'autres forces régionales l'accusant de palier son manque d'innovation par le protectionnisme réglementaire, l'Europe n'hésite pas à se démarquer par ses choix qui peuvent trouver une justification autre qu'économique.

En effet, le modèle de protection de la vie privée européenne reflète une certaine vision de l'Homme et de la société. L'Union européenne entend porter une politique des données centrée sur l'humain. Elle s'adonne ainsi à un exercice d'équilibre permanent entre la recherche de l'innovation et la protection des citoyens. Le partage de compétence entre ce qui relève des autorités nationales, européennes et extra-européennes relève aussi d'un jeu subtil.

En effet, si l'Internet présente un caractère transnational, la localisation des données et l'échange de données personnelles entre Etats est géographique par nature, ce qui soulève des questions de souveraineté numérique. Le standard européen de protection associé à la circulation de données personnelles est régulièrement mis à l'épreuve. En témoigne l'invalidation de l'accord Safe Harbor entre l'Union européenne et les Etats-Unis par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield en octobre 2017.

Les tensions entre régions du monde se reflètent également sous forme d'un phénomène de compétition réglementaire. Les autorités européennes souhaitent en effet protéger leurs citoyens tout en étendant leur influence économique. Conscients que l'Afrique et l'Amérique Latine s'inspirent traditionnellement de leur exemple, elles espèrent qu'ils adopteront des règles compatibles pour demeurer des partenaires privilégiés.

Cependant, les forces régionales s'organisent et préparent leurs propres instruments juridiques. Tel est le cas des Etats-Unis notamment avec le projet de « Cloud Act », soit le Clarifying Lawful Overseas Use of Data Act, qui concerne l'accès aux données stockées à l'étranger, texte extraterritorial qui porte un risque d'ingérence. La Chine a d'ores et déjà fait le choix de l'imperméabilité à toute influence réglementaire en limitant sa dépendance numérique. Le pays opère en cercle fermé, accueillant un nombre limité d'opérateurs étrangers avec des obligations de localisation des données sur le sol chinois.

Dans un tel contexte, un risque de fragmentation de l'espace numérique est à craindre. Certains services basés sur d'autres continents peuvent devenir indisponibles car ils ne respectent pas la réglementation du pays de l'usager. Avec cette tendance, le mythe d'un monde interconnecté, support d'une économie globalisée, est peut-être en train de toucher à sa fin.

II LE CHOIX D'UNE PROTECTION RENFORCÉE ET EXHAUSTIVE

• De la protection du citoyen européen à la protection de ses données

Dès 1995, l'Union européenne a mis en place un cadre juridique via la **directive 95/46/CE** sur « la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ».

La Commission européenne souhaitait ainsi mettre en place un cadre uniforme de protection favorisant la circulation des données personnelles résultant de l'ouverture des frontières. Selon les mots de Viviane Reding en 2002, l'objectif était de « donner un coup d'accélérateur à l'économie européenne ». L'esprit du texte visait à protéger des risques qui accompagnent le développement des usages et la consolidation des services en ligne, sans étouffer les opportunités que représente ce formidable marché.

A l'heure actuelle, la disponibilité du Cloud alliée au traitement massif des données et à la puissance de l'intelligence artificielle permet une utilisation toujours plus fine des données et l'émergence de services plus personnalisés. En même temps, les consommateurs et citoyens ont une conscience accrue des risques encourus. Avec les scandales de Wikileaks ou de Cambridge Analytica comme les révélations du lanceur d'alerte Edouard Snowden, ils comprennent que la surveillance dont ils peuvent faire l'objet ne vise pas seulement des fins commerciales mais aussi politiques.

• La reconnaissance d'un droit fondamental

Le droit à la protection des données personnelles et le droit à la vie privée sont affirmés comme deux droits à part entière. Le second postule ce que l'on appelle souvent « un droit à être laissé tranquille ». Ainsi en France, l'article 9 du Code civil énonce que « chacun a droit au respect de sa vie privée ». Il s'y adjoint une protection pénale du secret des correspondances qui s'applique de manière transversale de la lettre missive au courrier électronique.

Le premier, le droit à la protection des données personnelles, vise toutes les données relatives à une personne physique, identifiée ou identifiable. Ce sont les noms et prénoms mais aussi une vidéo ou une adresse IP sur internet. Le traitement de telles données est réglementé comme toute opération de collecte, d'enregistrement, d'organisation, d'adaptation, de conservation, d'interconnexion ou encore de destruction de ces données.

Depuis 2009, la protection des données personnelles est un droit fondamental dans l'Union européenne. C'est alors que se dessinent les contours d'un nouveau cadre juridique qui s'applique désormais depuis le 25 mai 2018, le RGPD. Les négociations autour de ce règlement se sont étalées sur quatre ans de janvier 2012 au 14 avril 2016 et ont débouché sur une réforme globale du cadre juridique de la protection des données personnelles. Une période transitoire d'applicabilité de deux ans a été l'occasion de sensibiliser et de responsabiliser les citoyens européens comme les responsables de traitement et leurs sous-traitants.

Ce règlement, qui remplace la directive de 1995, est complété d'une **directive** relative à la protection des données à caractère personnel dans le cadre des activités policières et judiciaires. Le rôle des régulateurs, nationaux comme la CNIL en France, et du Comité européen de la protection des données (CEPD) qui vient remplacer le groupe de travail de l'article 29 au niveau de l'Union, est étendu. Une coopération renforcée entre les régulateurs nationaux et européen est en effet essentielle à une application cohérente et prospective du RGPD.

• Ce qui change avec le RGPD

Le RGPD impose de recueillir le consentement libre, informé et positif des utilisateurs et pose les principes fondamentaux de licéité, de loyauté et de transparence des traitements. Les principes clefs de la directive de 1995 sont perpétués : du droit à l'information sur l'utilisation

des données personnelles collectées au droit d'opposition et aux droits d'accès ou de rectification. Le responsable de traitement doit également notifier toute fuite de données et prendre en compte la protection des données personnelles dès la conception d'un nouveau service. Il doit se montrer le protecteur par défaut. Ainsi, il ne saurait y avoir de cases pré-cochées sur un site web ni de consentement tacite à continuer la navigation.

Les possibilités de désanonymisation, les ensembles intriqués de données personnelles et de données non-personnelles, comme le développement des capacités d'identification indirectes, imposent une conception prospective de la protection des données. Le RGPD propose ainsi une approche basée sur le risque qui suppose d'évaluer l'impact d'un traitement de données personnelles et d'adapter la sanction d'un manquement à la gravité de la violation.

Par ailleurs, la capacité à agir des citoyens pour leur permettre de reprendre la main sur leurs données est renforcée. Les sanctions administratives sont largement étendues ainsi que les pouvoirs des régulateurs.

L'article 80 du RGPD introduit un nouveau mécanisme européen d'action de groupe pour faire cesser tout manquement en matière de protection des données. Il précise que les Etats membres peuvent en droit national permettre à des associations d'exercer ce droit au nom des personnes concernées.

L'article 82, ensemble avec le considérant 146, prévoit que le responsable du traitement ou le sous-traitant doit réparer tout dommage résultant de la violation du règlement qui leur serait imputable, les personnes concernées devant recevoir « une réparation complète et effective pour le dommage subi », qu'il soit matériel ou moral. Cette imbrication entre le droit national et le droit européen fait la richesse du RGPD. C'est en effet aux Etats membres d'opter ou non pour un tel droit à réparation. C'est d'ailleurs le choix qu'a fait la France dans **sa loi d'adaptation du 20 juin 2018**.

Au final, le RGPD met en place un régime équilibré, associant cybersécurité et protection des données. Toutefois, un bilan nuancé impose de souligner le coût économique de sa mise en œuvre, en particulier pour les PME. Par ailleurs, la marge de manœuvre laissée aux États membres soulève la question de la parfaite compatibilité des pratiques de protection des données à travers l'Europe. Dans un futur proche, il serait notamment utile de circonscrire la notion subjective d'intérêt légitime du responsable de traitement, l'une des bases juridiques de traitement sans consentement. Les modalités de mise en œuvre du devoir d'information du responsable de traitement devront également être clarifiées. Gageons que les lignes directrices du CEPD viendront, dans la suite du G29 (le groupe des CNIL européennes), préciser ces notions.

• Des données des communications électroniques

Ce cadre juridique ne serait pas complet sans la prise en compte des communications électroniques. Lex specialis du RGPD, un projet de règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques est actuellement débattu et doit venir remplacer la **directive 2002/58/CE**.

En visant la protection de la confidentialité des « communications électroniques », il vise toutes les communications : traditionnelles mais aussi électroniques (OTT avec Skype ou encore WhatsApp), quelle que soit la technologie utilisée. En l'état du texte, le projet de règlement s'appliquerait aux cookies, aux métadonnées comme à la communication de machine à machine.

Le projet de texte vise à harmoniser les différentes législations nationales relatives aux communications électroniques dans l'Union européenne afin de les rendre conformes au RGPD. Il reflète une volonté claire de redonner confiance aux internautes européens en favorisant des pratiques respectueuses de leurs données. C'est ainsi un équilibre difficile à négocier entre des droits fondamentaux (limitation des tracking-walls, nécessité d'un opt-in préalable, etc.) et le modèle économique de nombreux services numériques, en particulier celui de la publicité ciblée. C'est là tout l'enjeu de créer un marché unique du numérique équilibré pour plus de 500 millions de citoyens.

Le texte devrait promouvoir le principe du consentement préalable avec, là encore, la nécessité de limiter les

exceptions, en particulier de l'intérêt légitime et des traitements ultérieurs. Certaines questions restent toutefois en suspens et mériteraient d'être clarifiées. En effet, ne faudrait-il pas durcir les paramètres de confidentialité des navigateurs web et autres logiciels permettant les communications électroniques ? Ou encore améliorer les concepts de protection par défaut et de protection dès la conception, tout en laissant la possibilité d'un paramétrage fin, par exemple site par site ? Et enfin, ne faudrait-il pas imposer des standards comme le « Do Not Track » ?

III LE RÔLE DE LA FRANCE ET LES ENJEUX À VENIR

La France a joué un rôle moteur dans l'évolution récente du cadre de la protection européenne des données personnelles. Des initiatives, comme « Data For Good » ou encore la tenue en novembre prochain à Paris du Forum des Nations unies sur la gouvernance de l'Internet (**FGI**), témoignent de ses ambitions en la matière.

Le 26 juillet dernier, le gouvernement a lancé des **états généraux** des nouvelles régulations numériques sous la forme d'une concertation menée dans le cadre du Conseil national du numérique (CNNum) et associant les parties prenantes : société civile, différents régulateurs, administration, etc. Ces états généraux doivent permettre de consolider, d'ici début 2019, la position de la France sur la régulation numérique. L'objectif est « de promouvoir un numérique libre, ouvert, interopérable et innovant, au service du progrès humain et de l'émancipation des femmes et des hommes par l'éducation, le travail et le plein exercice de leurs libertés fondamentales ».

L'occasion de ces états généraux pourrait être saisie pour questionner le modèle économique de l'Internet, notamment sous l'angle des pratiques concurrentielles. S'il s'avère qu'un nombre limité d'acteurs abusent de leur position dominante sur le marché pour s'adonner à des pratiques peu respectueuses de la vie privée, de nouvelles normes pourraient s'imposer. Cela pourrait alors motiver la France à demander la révision de la directive e-commerce adoptée en juin 2000.

En tout état de cause, l'activisme dont fait preuve la France s'inscrit ainsi dans la stratégie numérique européenne.

En avril dernier, la Commission européenne présentait son **approche** pour lutter contre la désinformation en ligne et missionnait en juin un groupe d'experts de haut niveau sur l'Intelligence artificielle (IA) pour piloter le travail de l'Alliance européenne de l'IA. La protection des données, notamment des données personnelles, devrait être centrale dans ce nouveau dispositif. Il s'appuiera sur des principes de limitation de la collecte et de la durée de conservation.

Avec l'arrivée massive dans les foyers européens des **objets connectés**, la montée en puissance de l'apprentissage automatique et de l'échange de machine à machine, ces principes de protection devraient continuer de démontrer leur pertinence dans les années à venir.

Constance Bommelaer de Leusse
Directrice des politiques publiques, ISOC Monde

Lucien Castex
Chercheur, Université Sorbonne Nouvelle, Secrétaire Général, ISOC France

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN