ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

– Table ronde, ouverte à la presse, sur la protection des données personnelles réunissant :

- Mme Nataliia Bielova, directrice de recherche au centre Inria de l'université Côte d'Azur ;

- M. Julien Rossi, maître de conférences en sciences de l'information et de la communication à l'UFR Culture et communication et au Centre d'études sur les médias, les technologies et l'internationalisation (Cémti) de l'université Paris 8. 2

– Présences en réunion 18

Mercredi
1er avril 2026
Séance de 15 heures

Compte rendu n° 16

SESSION ORDINAIRE DE 2025-2026

Présidence de Mme Sophie-Laurence Roy, *Vice-présidente de la commission*

ASSEMBLÉE NATIONALE

La séance est ouverte à quinze heures.

Mme Sophie-Laurence Roy, présidente. Mes chers collègues, nous poursuivons les auditions de notre commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Le président de la commission d'enquête, Philippe Latombe, vous prie d'excuser son absence, j'assurerai la présidence de cette séance.

Nous recevons aujourd'hui Mme Nataliia Bielova, directrice de recherche au centre Inria de l'université Côte d'Azur et M. Julien Rossi, maître de conférences en sciences de l'information et de la communication à l'université Paris 8. Mme Bielova s'exprimera en anglais et ses propos feront l'objet d'une interprétation simultanée.

Madame, monsieur, vos travaux portent sur la protection de la vie privée en ligne. Quels sont en particulier les risques liés à la collecte massive par les *big tech* de données sur les citoyens ?

Je vous remercie de nous déclarer au préalable tout autre intérêt public ou privé de nature à influencer vos déclarations. Avant de vous céder la parole, je rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission de prêter le serment de dire la vérité, toute la vérité, rien que la vérité. Je vous invite donc à lever la main droite et à dire : « *Je le jure* ».

(Mme Bielova et M. Rossi prêtent serment).

Mme Nataliia Bielova, directrice de recherche au centre Inria de l'université Côte d'Azur. Je vous remercie pour votre invitation. Spécialisée en protection des données sur le web, je travaille depuis 2016 sur les technologies de *web tracking*, sur la conformité ainsi que sur les « *dark patterns* » ou « designs trompeurs » en français. Il s'agit d'interfaces qui influencent les utilisateurs et les conduisent à prendre des décisions contraires à leurs intérêts, par exemple en partageant davantage de données personnelles que ce qu'ils souhaiteraient réellement.

Je suis spécialiste en informatique et je dispose d'une expertise approfondie du règlement général sur la protection des données (RGPD) et de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (directive-ePrivacy), ainsi que de la manière dont ces textes s'appliquent concrètement au *web tracking*.

Ma contribution de ce jour à votre commission repose sur des données probantes, issues de parutions scientifiques internationales revues par des pairs, issues des sciences informatiques et du droit. Je travaille sur les obligations juridiques en matière de consentement et sur les méthodes techniques permettant d'auditer la conformité juridique. Lors de mon intervention, je me concentrerai sur des conclusions tirées de ma propre recherche et j'indiquerai explicitement lorsque je ferai référence à des résultats provenant d'autres sources.

En premier lieu, nous faisons aujourd'hui face à un déploiement à grande échelle des technologies de *tracking* ou de traçage sur internet. Un site web habituel contient en moyenne des dizaines de traceurs, autorisant la création de profils extrêmement fins et détaillés concernant les intérêts des utilisateurs. Il existe ainsi des taxonomies décrivant plus d'un millier

de segments, ce qui correspond à des données très détaillées permettant, par exemple, d'inférer les revenus d'un foyer. Il faut également mentionner des programmes logiciels, notamment des bibliothèques JavaScript, qui transmettent ces données à de grandes plateformes comme les réseaux sociaux et permettent leur rapprochement avec d'autres données déjà disponibles sur ces plateformes.

Nous sommes ainsi en présence d'informations très sensibles. Les utilisateurs peuvent être facilement manipulés ou discriminés sur la base de ces profils extrêmement précis, par exemple par le refus d'accès à certains services, à des offres d'emploi, ou encore par la proposition de prix différenciés pour des prêts, y compris des prêts immobiliers. Il existe donc des risques importants associés à ces profils d'une grande granularité.

En ce qui concerne les origines de cette collecte de données, nous avons observé que cette forme de surveillance est étroitement liée à l'écosystème publicitaire, notamment à travers la transmission de données à des dizaines d'entreprises en quelques millisecondes. Ce que l'on observe aujourd'hui est un système plus vaste de chaînes d'inclusion, dans lequel de nombreuses entreprises intègrent et dépendent des services des autres. D'un point de vue technique, cette situation est liée à la nature dynamique du contenu web. Des composantes peuvent être chargées par des bibliothèques JavaScript à l'insu de l'opérateur du site web, ce qui permet l'introduction de traceurs cachés. Le phénomène de traçage est ainsi profondément intégré à cet écosystème.

Par exemple, un service fournissant une carte à un site web peut inclure des cookies liés à une entreprise publicitaire, sans que l'utilisateur du site puisse réellement les éliminer. S'agissant des technologies spécifiques utilisées pour le traçage en ligne massif, l'industrie s'est historiquement appuyée sur les cookies tiers, qui permettent la constitution de profils utilisateurs à partir des sites visités. Ces cookies sont aujourd'hui plus difficiles à analyser, leur finalité est souvent peu claire et ils sont étroitement intégrés aux fonctionnalités centrales du contenu web.

Nos recherches montrent que certains cookies peuvent réapparaître même après avoir été supprimés par l'utilisateur. En parallèle, le secteur se tourne vers des techniques encore plus opaques, telles que le traçage de serveurs ou de données personnelles comme les identifiants liés aux adresses e-mail et aux numéros de téléphone, techniquement beaucoup plus difficiles à détecter. En conséquence, les opérateurs de sites web rencontrent de grandes difficultés à contrôler l'ensemble des types de traçage présents sur leurs propres sites. Ils ne savent pas précisément qui collecte les données des utilisateurs, à quelles fins, ni dans quelles conditions.

Par ailleurs, ces opérateurs ne disposent pas toujours des compétences nécessaires pour auditer leurs propres sites web et ignorent souvent les solutions techniques existantes sur le marché. Il existe certes des outils capables de scanner un site et de détecter les cookies et les traceurs, mais ces solutions ne suivent pas systématiquement l'évolution rapide des technologies de *tracking* et ne détectent pas l'ensemble des outils de traçage. Les sites web demeurent ainsi porteurs de traceurs et sont, de fait, non conformes à la législation.

Sur le plan juridique, le RGPD et la directive ePrivacy visent à encadrer ces pratiques à travers le consentement de l'utilisateur et différentes obligations imposées aux opérateurs de sites web. Toutefois, de nombreux problèmes de conformité subsistent. Obtenir un consentement pleinement éclairé est presque impossible en raison de la complexité des chaînes d'inclusion dans cet écosystème. Il n'est pas rare de voir des demandes de consentement mentionner plus de 500 entreprises susceptibles de collecter des données sur un même site web.

De fait, il est irréaliste d'informer pleinement l'utilisateur de l'existence de toutes ces entreprises et de leurs pratiques de collecte.

Le RGPD interdit en outre le recours aux *dark patterns*, c'est-à-dire aux interfaces trompeuses qui incitent l'utilisateur à partager plus de données qu'il ne le souhaite. En outre, les fournisseurs de plateformes de gestion du consentement opèrent des choix précis de *design*, notamment en matière de couleurs mettant en valeur certains boutons, de placement des options ou de taille de police, dans le but de maximiser la probabilité que l'utilisateur consente au traçage. Le bouton de refus peut ainsi être rendu moins visible ou moins accessible.

De nombreuses recherches montrent que ces *dark patterns* influencent effectivement les décisions des utilisateurs. Nous avons mesuré leur impact sur le processus décisionnel de plus de 4 000 utilisateurs en France et avons conclu que ces interfaces trompeuses modifient significativement la probabilité de consentement. Nous avons également observé un effet d'exposition : des utilisateurs ayant déjà été confrontés à des *dark patterns* sont plus enclins à cliquer sur « Accepter » par la suite. De nombreux fournisseurs proposent par ailleurs des bandeaux de consentement avec des paramètres par défaut favorables au traçage. Or, nous connaissons bien la force de ces choix par défaut.

Un autre problème apparaît après l'interface de recueil du consentement. Une fois le choix effectué, le consentement est stocké sous la forme d'un signal dans le navigateur, signal qui doit être partagé avec l'ensemble des entreprises collectant les données afin d'assurer le respect des préférences de l'utilisateur. Or, ces signaux n'atteignent pas toutes les entreprises impliquées dans le traçage. Les opérateurs de sites web sont censés superviser cette chaîne complexe et garantir la transmission correcte du consentement, ce qui est extrêmement difficile en pratique.

En conclusion, le système actuel de *web tracking* se caractérise par des chaînes d'entreprises complexes, des technologies de traçage en évolution permanente et des opérateurs de sites web qui peinent à assurer la conformité. En définitive, ils ne sont pas en mesure de garantir le respect effectif des droits fondamentaux en matière de vie privée. Les utilisateurs finaux ne disposent pas d'un contrôle réel sur leurs données personnelles.

Mme Sophie-Laurence Roy, présidente. Je vous remercie. À vous écouter, on a le sentiment qu'une masse d'entreprises espionnent les informations que chacun d'entre nous peut laisser traîner à chaque fois qu'il visite un site. Quelle est la finalité de ce traçage ? Quels en sont les dangers pour les Français ?

Mme Nataliia Bielova. Il existe effectivement des dizaines d'entreprises présentes sur la toile et, lorsqu'on observe plus finement leurs pratiques, on constate que les traceurs n'utilisent pas tous les mêmes schémas. Je ne dispose pas de chiffres exhaustifs, mais la complexité vient du fait que, lorsque les utilisateurs consultent des sites internet, ces derniers intègrent une multitude de services dont ils ont besoin pour fonctionner. Par exemple, lorsqu'un opérateur souhaite savoir combien d'utilisateurs consultent son site, d'où ils viennent ou comment ils interagissent avec le contenu, il a recours à des services spécialisés.

Ces services sont, dans la majorité des cas, fournis par des entreprises étrangères, ce qui implique que les données soient transmises à l'étranger, vers les serveurs distants de ces sociétés. S'agissant du risque ou du danger, je ne peux m'exprimer que sur la taille potentielle des profils constitués. Le *tracking* est aujourd'hui présent sur environ 90 % du web, d'après les études existantes. On peut donc imaginer l'ampleur des profils ainsi créés et le volume de

données agrégées. Je ne dispose pas d'informations précises sur la taille exacte de ces profils, car cet aspect n'a pas encore été pleinement étudié, mais nous pouvons en observer la présence, la prévalence et les types de données susceptibles d'être collectées.

Ces données incluent, par exemple, les sites consultés par l'utilisateur, mais aussi des informations beaucoup plus fines, comme les endroits où il clique, la manière dont il déplace ou dirige sa souris, ou la façon dont il interagit avec une page. Je ne peux donc pas fournir une réponse chiffrée sur la taille des profils, mais leur granularité est manifeste.

Mme Sophie-Laurence Roy, présidente. À quoi cela leur sert-il ? Quel est le véritable danger pour nous ?

Mme Nataliia Bielova. Le risque principal réside dans la réutilisation de ces données à des fins très diverses. D'un point de vue extérieur, celui du chercheur, il est difficile de savoir précisément ce qu'en font les entreprises. Or ces profils peuvent contenir des informations extrêmement sensibles sur la santé ou les centres d'intérêt. Nous avons par exemple mené une étude sur des sites de santé et constaté que la majorité d'entre eux utilisent des *trackers*. Ainsi, consulter un site médical ou un site lié à des informations politiques conduit à un enregistrement. Cette précision extrême interpelle.

Mme Sophie-Laurence Roy, présidente. Je cède la parole à M. Rossi, pour un propos liminaire.

M. Julien Rossi, maître de conférences en sciences de l'information et de la communication. Je vous remercie pour votre invitation de ce jour. Les profonds bouleversements que connaît le système international construit dans les décennies ayant suivi la chute du mur de Berlin soulèvent aujourd'hui de nouvelles interrogations dans de nombreux domaines de la vie publique. Les politiques en matière de numérique n'y échappent pas. Votre commission examine précisément les dépendances structurelles et les vulnérabilités systémiques du secteur numérique, ainsi que les risques que ces dépendances, devenues de véritables vulnérabilités dans le contexte actuel, font peser sur l'indépendance de la France.

Vous avez jugé utile de m'interroger sur ces questions, et je m'efforcerai d'y répondre de la manière la plus exhaustive possible, tout en demeurant, à l'instar de ma collègue, aussi précis que possible et en m'abstenant de toute spéculation. Je m'appuierai sur des travaux scientifiques aboutis et publiés, qu'il s'agisse des miens ou de ceux de collègues, que je serai amené à citer. Il pourra toutefois m'arriver, en fonction des questions posées, de formuler des observations ou des hypothèses encore en cours de vérification, mais toujours fondés sur l'expérience des terrains et les objets de recherche qui structurent mon parcours universitaire, dont l'étude des rapports entre informatique et libertés, et plus largement la protection des données, constitue le fil directeur.

Le développement de l'informatique a soulevé des interrogations quant à ses effets sur les libertés publiques dès ses débuts. Les travaux de recherche, notamment ceux de Michel Atten, montrent que des informaticiens américains s'interrogeaient déjà, dans les années 1950, sur les conséquences du traitement informatisé de données personnelles, en particulier dans le cadre de l'informatisation du recensement. Dès 1966, la Chambre des représentants des États-Unis créait la première commission d'enquête parlementaire au monde consacrée à ce sujet. La France n'était pas très loin derrière : le Conseil d'État publiait en 1970 un rapport sur les conséquences du développement de l'informatique sur les libertés publiques et sur les décisions administratives, tandis que le Land de Hesse adoptait la même année la première loi

de protection des données, la Datenschutzgesetz. La Suède a suivi en 1973, puis la France en 1978 avec l'adoption de la loi informatique et libertés.

Cette loi française contenait déjà, sous une forme que l'on peut considérer comme préfigurant les débats actuels sur l'intelligence artificielle, un principe d'encadrement de la décision automatisée. Ce principe, aujourd'hui repris à l'article 22 du RGPD, pose l'interdiction de la prise de décision fondée exclusivement sur un traitement automatisé, sous réserve de certaines exceptions. La protection des données, contrairement à ce que son intitulé pourrait laisser penser, ne protège pas les données en tant que telles, mais les personnes, qu'elles soient citoyennes ou non, car il s'agit d'un domaine relevant des droits fondamentaux. Elle vise à prévenir toute atteinte à la personne résultant d'un traitement frauduleux ou négligent d'informations la concernant.

Rien de tout cela n'est véritablement nouveau. Contrairement à l'idée répandue selon laquelle le droit serait condamné à courir perpétuellement derrière les progrès technologiques, la relative stabilité des règles du droit des données personnelles démontre qu'il n'existe aucune fatalité en la matière. L'essentiel des principes applicables aujourd'hui a été élaboré dès les années 1970, notamment au Conseil de l'Europe et à l'OCDE, puis complété par la directive européenne de 1995 et, plus récemment, par le RGPD. Pour autant, le monde a profondément changé depuis cette époque. Internet n'est plus un projet de recherche excluant les usages commerciaux, comme ce fut le cas jusqu'au début des années 1990, mais un espace public transnational comptant près de six milliards d'internautes, rendu possible par une infrastructure devenue omniprésente.

Je rejoins à cet égard le constat formulé par Luciano Floridi dans *The Onlife Manifesto*, selon lequel la distinction entre vie en ligne et vie hors ligne n'a plus véritablement de sens. Il y a encore quinze ans, être en ligne relevait d'un choix ; aujourd'hui, c'est une obligation de fait, et presque une obligation en droit. L'accès aux services publics s'effectue de plus en plus par voie numérique, du fait de la dématérialisation, parfois au mépris de la jurisprudence du Conseil d'État reconnaissant, dans certaines circonstances, un droit à une alternative hors ligne. Or, le marché du numérique présente des tendances monopolistiques marquées. La liberté de choix d'un fournisseur de matériel ou de logiciel est, en pratique, fortement limitée pour l'individu.

Dès lors que l'accès à un service public peut être subordonné à l'acceptation des conditions d'utilisation d'un service numérique incontournable, souvent développé hors de l'Union européenne (UE), la vulnérabilité de l'individu face aux choix technologiques rejoint des enjeux de souveraineté régalienne. Il suffit par exemple de penser à FranceConnect+, qui implique en pratique la possession d'un smartphone fonctionnant sous iOS ou Android, devenus *de facto* des contrôleurs d'accès à l'identité civile et aux services publics.

Un autre changement majeur réside dans la montée en puissance de ce que Shoshana Zuboff a qualifié de « capitalisme de surveillance », fondé sur la promesse de prédire et de contrôler les comportements à partir des traces numériques. Les prémices de cette économie existaient avant l'informatique contemporaine, mais elles ont pris une ampleur considérable. Aujourd'hui, les principales capitalisations boursières reposent sur la valorisation des données et sur les technologies d'intelligence artificielle.

Dans ce contexte, le droit des données personnelles fait l'objet de critiques récurrentes, notamment en raison de son recours aux mécanismes d'autodétermination informationnelle et au consentement comme base légale du traitement. Le RGPD définit pourtant de manière très

exigeante les conditions de validité du consentement, notamment à l'article 4, paragraphe 1. À défaut, le consentement est invalide et ne peut fonder un traitement. Mais ce modèle peut se révéler illusoire lorsque l'individu ne peut raisonnablement refuser de participer à un système sociotechnique dont dépend son insertion sociale et économique. Il ne peut, par ses seuls choix individuels, échapper au capitalisme de surveillance.

Dans ce contexte, bien que le RGPD comporte une dimension structurelle, notamment par le rôle confié aux autorités de contrôle et aux juges, l'individu demeure relativement peu protégé face aux mécanismes décrits préalablement par ma collègue. Le droit des données personnelles offre certes au juge et au régulateur une panoplie d'outils d'intervention, mais la littérature académique souligne un déficit d'application du droit, profitant aux acteurs qui ne s'y conforment pas. Pour les personnes concernées, les recours demeurent souvent longs et complexes.

Le législateur européen a entendu conférer de nouveaux droits pour les plaintes en matière de protection des données qui impliquent les autorités de contrôle de plusieurs États membres de l'Union européenne. Ces nouveaux droits entreront en application en 2027, mais les personnes qui saisiront l'autorité compétente sur leur territoire – par exemple la Commission nationale de l'informatique et des libertés (Cnil) en France – d'affaires purement nationales, ne bénéficieront pas de ces nouveautés procédurales introduites par le droit de l'Union européenne pour les affaires transfrontières.

Parallèlement, certains acteurs économiques dénoncent une inflation normative depuis une quinzaine d'années, ainsi qu'une multiplication des autorités de régulation, susceptibles de créer des conflits de compétences et, paradoxalement, d'affaiblir l'effectivité du droit. Ces critiques sont reprises par le rapport Draghi et la Commission européenne a présenté, le 19 novembre 2025, une proposition « Omnibus numérique » visant à maintenir un haut niveau de protection des droits fondamentaux tout en simplifiant le droit applicable aux acteurs économiques. Des travaux de recherche récents, notamment ceux menés sous la direction de Margo Bernelin au CNRS, montrent toutefois que ces propositions risquent d'affaiblir substantiellement les garanties existantes, tout en portant atteinte à la compétitivité des entreprises européennes.

En 1992 déjà, la Commission européenne avait dû revoir en profondeur sa première proposition de directive sur la protection des données, et la directive adoptée en 1995 a ensuite démontré son efficacité pendant plus d'une décennie.

Mme Sophie-Laurence Roy, présidente. Comment vivre sans donner accès à ses données, qui sont pourtant aujourd'hui incontournables pour pouvoir accéder à de très nombreux services essentiels ? Je pense notamment à FranceConnect+, dont vous avez déjà fait mention.

M. Julien Rossi. Dans le droit des données à caractère personnel, il n'existe pas toujours un droit d'opposition ou un droit de refuser. Par exemple, il n'est pas possible de refuser que notre banque vérifie que nous ne soyons pas en train de préparer un virement vers une organisation terroriste, car la loi l'impose pour des motifs d'intérêt public. Dans de nombreux autres cas de figure, en revanche, nous sommes censés disposer soit de la faculté de refuser notre consentement, soit de celle de nous opposer ultérieurement au traitement.

La question concerne en réalité les conséquences pratiques de leur mise en œuvre. Ma collègue Nataliia Bielova a notamment étudié ce qui se produit lorsque l'on clique sur « Je

refuse » sur un bandeau cookie. Si je ne me trompe pas, cela fonctionne parfois, mais pas toujours. C'est alors que se pose la question des limites de ce qu'un individu peut effectivement faire. Certes, il est possible de refuser d'utiliser un service qui conditionne son accès au consentement, mais lorsque l'accès à un service public devient subordonné à cette acceptation, le droit peut finalement s'avérer impuissant, la personne concernée risquant de se voir privée de services dont elle a besoin.

Mme Sophie-Laurence Roy, présidente. Dans certains cas, nous sommes face à un droit qui feint de nous protéger, mais demeure impuissant.

M. Julien Rossi. Je serai moins pessimiste quant à la faculté du droit. Le droit a, en réalité, exercé une influence tangible à la fois sur l'environnement technique et sur les comportements des acteurs, qu'ils soient publics ou privés, qui collectent et traitent des données personnelles. Il existe une grande diversité de situations intermédiaires entre une conformité parfaite aux exigences juridiques et un mépris total de la loi.

Un exemple récent me permet de l'illustrer. Ce matin même, au CNRS, des collègues de l'université de Neuchâtel ont présenté leurs recherches portant sur les tribulations de chauffeurs VTC et de livreurs travaillant pour des plateformes numériques lorsqu'ils cherchent à accéder aux données personnelles que ces plateformes traitent à leur sujet. L'objectif est notamment de pouvoir faire valoir un certain nombre de droits, ou encore d'établir, le cas échéant, l'existence d'un lien de subordination.

Ces travaux, dirigés par Jessica Pidoux, montrent que le droit fournit néanmoins des outils qui ont permis, *in fine*, à un certain nombre de personnes d'accéder à leur dossier personnel. Dans certains cas, cela a nécessité le dépôt de plaintes, notamment une plainte dirigée contre une entreprise de VTC, qui a conduit à une amende prononcée il y a quelques années aux Pays-Bas.

Nous sommes donc clairement dans une situation intermédiaire, située entre une conformité idéale et une absence totale de respect du droit. Le droit n'est pas impuissant. La question centrale demeure celle de son effectivité. Il s'agit de savoir si le droit est réellement appliqué et s'il est aisé de le faire respecter en cas d'infraction ou de soupçon d'infraction. C'est sans doute à ce niveau que résident aujourd'hui les principales difficultés.

Mme Cyrielle Chatelain, rapporteure de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Les données dont vous parlez sont normalement captées de manière anonymisée, c'est-à-dire qu'on a rarement le nom, le prénom, l'adresse de manière stockée. Pouvez-vous revenir sur la distinction entre une donnée personnelle et une donnée anonymisée ? En quoi une donnée anonymisée permet malgré tout d'obtenir un grand nombre d'informations à caractère personnel, comme le lieu d'habitation, les centres d'intérêt ; par exemple ?

Mme Nataliia Bielova. Lorsqu'on évoque la collecte massive de données sur le web et les technologies de suivi ou de traçage, il faut d'abord raisonner à partir des identifiants uniques attribués à chaque navigateur ou à chaque individu. En pratique, par exemple, j'ai des identifiants uniques placés par des entreprises dans mon navigateur, identifiants qui sont différents de ceux qu'une entreprise va placer dans vos navigateurs, sur vos téléphones, sur vos ordinateurs, sur vos réseaux sociaux, sur vos téléphones ou sur vos ordinateurs. Ces identifiants uniques, *a priori*, ne contiennent pas d'informations directement liées à mon nom. En ce sens,

ils ne sont pas immédiatement connectés à mon identité civile, mais ils sont rattachés à l'appareil et au navigateur que j'utilise. Les données associées à cet identifiant deviennent ainsi les miennes de manière unique.

À chaque visite d'un site web, une requête est envoyée à l'entreprise qui détient cet identifiant. Celle-ci reçoit alors l'information et peut constater que la personne dissimulée derrière cet identifiant s'est rendue sur tel site web ou a recherché telle ou telle information. Les données sont donc très personnelles, directement liées à mon parcours et à mon expérience en ligne, même si mon nom n'apparaît pas explicitement.

Il existe toutefois un risque majeur. Ces identifiants uniques peuvent être très facilement reliés à des informations personnelles. Un cas typique est celui d'un traceur qui me suit sur le web et qui, à un moment donné, fusionne mon profil avec celui que je possède sur un réseau social. En quelques millisecondes, l'identifiant est alors associé à mon nom et à mon prénom. Ce risque est bien réel et ne doit pas être sous-estimé.

Enfin, pour compléter, d'autres techniques sont aujourd'hui proposées par l'industrie publicitaire, notamment en réaction aux annonces récentes de certaines *big tech* visant à bloquer certaines méthodes comme les cookies tiers. Le secteur semble évoluer et met en avant des solutions fondées sur des adresses e-mail « hachées », qui sont, de fait, beaucoup plus étroitement liées aux identités des individus.

M. Julien Rossi. La proposition Omnibus numérique de la Commission européenne envisage de redéfinir la notion de données à caractère personnel, afin d'en exclure les données dites pseudonymes. Cette évolution fait l'objet de débats importants et, surtout, du point de vue des recherches que nous menons, elle risque de réduire le champ d'application du droit des données personnelles d'une manière problématique, en empêchant de prendre en compte certaines situations pourtant particulièrement sensibles.

Pour simplifier, cette redéfinition pourrait conduire à ignorer des jeux de données qui, bien que ne comportant ni le nom de la personne, ni son adresse, ni son numéro de téléphone, ni son adresse IP, restent hautement révélateurs. Prenons l'exemple de données composées uniquement de points de géolocalisation horodatés. Si l'on sait qu'une personne passe 90 % de ses nuits dans un lieu donné, 90 % de ses horaires ouvrés dans un autre lieu donné, et une part significative de ses dimanches matin, ou de ses vendredis, dans un lieu de culte précis, il devient relativement aisé de reconstituer un fichier d'individus classés par religion.

Dans ce cas, il ne s'agit formellement que de données pseudonymes, puisque le nom de la personne n'apparaît pas. Néanmoins, un tel jeu de données peut faire courir un risque réel, y compris physique, aux personnes concernées, notamment dans des contextes de tensions religieuses. C'est pour cette raison que certains collègues, en particulier Szilvia Lestyán, évoquent le phénomène d'« *anonymity washing* », ou blanchiment par l'anonymisation, afin de souligner que des données présentées comme anonymes ou pseudonymes peuvent malgré tout faire courir un risque aux personnes concernées.

Mme Cyrielle Chatelain, rapporteure. En quoi cette proposition Omnibus numérique pourrait-elle fragiliser la compétitivité pourtant mise en avant par la Commission européenne ? Le RGPD, en dépit de ses failles, s'est imposé comme un standard international. Dégrader notre niveau d'exigence peut-il engendrer un impact sur la compétitivité ?

M. Julien Rossi. Lorsque la Commission européenne a publié sa proposition au mois de novembre, nous avons constitué un réseau de chercheurs et de chercheuses issus de différentes disciplines, principalement le droit, l'informatique et les sciences sociales, coordonné par Margo Bernelin.

Nous nous sommes donné pour objectif d'analyser les propositions de la Commission européenne en conservant strictement les deux objectifs normatifs qu'elle a elle-même affichés. La Commission a en effet affirmé vouloir simplifier le cadre juridique tout en maintenant le même niveau de protection des données personnelles. Nous nous sommes donc interrogés sur la capacité réelle de ces propositions à atteindre cet objectif et, dans l'hypothèse où elles s'en révéleraient incapables, sur la possibilité de formuler des propositions alternatives plus pertinentes.

Je me limiterai à deux exemples. Le premier concerne la définition des données à caractère personnel. La Commission propose d'ajouter un paragraphe à l'article 4, paragraphe 1, du RGPD, selon lequel des données pseudonymes pour une entité pourraient être anonymes et sortir du cadre de la notion de données à caractère personnel. Cette proposition soulève plusieurs difficultés majeures. D'une part, la notion d'« entité » n'est pas définie dans le RGPD. D'autre part, le RGPD s'applique aux traitements de données à caractère personnel.

Dès lors qu'il existe un traitement de données à caractère personnel, le RGPD établit des droits pour les personnes concernées, notamment le droit à l'information, à la transparence, à l'accès, à la rectification, à l'opposition ou encore à l'effacement, ainsi que des obligations pour les responsables de traitement. Ces responsables sont les personnes physiques ou morales qui déterminent les finalités et les moyens du traitement, et non simplement celles qui ont matériellement accès aux données. Or, comme l'ont montré les travaux de collègues tels que René Mahieu, Nataliia Bielova ou Cristiana Santos, les traitements de données s'inscrivent très fréquemment dans des chaînes complexes de co-responsabilité.

On peut ainsi se trouver dans une situation où une PME française collabore avec une grande entreprise, qu'elle soit française ou étrangère, la nationalité étant indifférente au regard du droit des données. Cette grande entreprise peut affirmer qu'elle ne traite que des données pseudonymes et qu'elle n'est donc pas soumise au RGPD, tandis que la PME demeure responsable du traitement. En cas de violation des droits des personnes, la question de la répartition des responsabilités devient alors extrêmement floue. Or, la proposition de la Commission ne permet pas de trancher clairement cette difficulté.

Le second exemple concerne l'environnement international. L'Europe n'évolue pas en vase clos. Comme l'a montré Graham Greenleaf, plus de 170 pays dans le monde disposent aujourd'hui de législations en matière de protection des données personnelles. Dès lors, un affaiblissement des garanties offertes par le droit européen pourrait conduire des juridictions étrangères, par exemple au Brésil ou au Japon, à estimer que le niveau de protection en Europe n'est plus suffisant pour autoriser des transferts de données vers des acteurs européens. Jusqu'à présent, le RGPD fonctionnait *de facto* comme un étalon international, conférant aux entreprises européennes une présomption de conformité et, partant, un avantage compétitif.

Mme Nataliia Bielova. J'ai contribué au même document ; j'ai étudié la directive Omnibus numérique ainsi que les interactions entre le RGPD et la directive ePrivacy. Effectivement, il existe un risque d'affaiblissement de la protection individuelle, car la nouvelle proposition, notamment l'article 88 de l'Omnibus, pose un problème structurel. Elle conduit en effet à distinguer deux régimes distincts : d'une part, le RGPD, qui continuerait de s'appliquer

aux données personnelles, et d'autre part, la directive ePrivacy qui couvrirait les autres aspects, y compris l'aspect du terminal téléphonique, traité par une réglementation différente.

Cette dissociation est problématique, car elle segmente artificiellement des situations qui, dans la réalité technique, sont étroitement imbriquées. Il y a la question de l'utilisation des données, mais aussi celle des équipements par lesquels ces données sont collectées. S'agissant des exceptions prévues, je souhaite attirer votre attention sur l'une d'entre elles. L'Omnibus propose de dispenser de consentement certains traitements lorsqu'ils visent à mesurer l'audience, pour des services qualifiés d'analytique, utilisés par les propriétaires de sites internet afin de comprendre d'où proviennent leurs utilisateurs.

Le problème est qu'à l'heure actuelle, les utilisateurs ne comprennent généralement pas les conséquences techniques du recours à ces services. La proposition Omnibus semble considérer que ces pratiques auraient peu d'impact sur la vie privée et sur la collecte de données. Or, nos travaux montrent que certains de ces services collectent un volume considérable de données granulaires. Nous avons étudié l'un de ces services qui suit, de fait, chaque clic de souris, chaque mouvement, chaque interaction sur internet. Il apparaît que, bien souvent, le volume de données collectées est totalement disproportionné par rapport à la finalité affichée.

Nous estimons, en conséquence, que ces pratiques posent un problème d'autant plus grave qu'elles sont fréquemment combinées et fusionnées avec d'autres profils. Dans nos travaux antérieurs, nous avons observé des techniques de fusion permettant de relier deux identifiants distincts. Sur un échantillon de 9 000 sites étudiés, 40 % recouraient à ce type de méthode. Le projet actuel affaiblit donc, selon nous, la protection des données personnelles.

Enfin, la proposition Omnibus envisage d'ajouter un paragraphe supplémentaire à l'article 5.3. Celui-ci fait référence au traitement de données, mais la définition des données concernées demeure floue. Nous considérons que cette évolution risque de vider de son sens la directive de protection des données individuelles. J'ai d'autres préoccupations relatives au projet Omnibus, mais je m'arrêterai ici, sauf si vous souhaitez que je les développe.

Mme Cyrielle Chatelain, rapporteure. Nous sommes preneurs de toutes vos remarques concernant la directive Omnibus. Avez-vous identifié d'autres domaines que la publicité qui utilisent les données collectées sur les différents sites ?

Mme Nataliia Bielova. Je vais d'abord poursuivre sur l'Omnibus, dans la mesure où plusieurs préoccupations supplémentaires méritent d'être exposées. Je suis notamment préoccupée par les interfaces de recueil du consentement. L'Omnibus vise à réduire le nombre de demandes de consentement, au motif que les utilisateurs sont lassés de devoir répondre à ces sollicitations répétées. Il est vrai que cette approche peut, en apparence, alléger la charge cognitive qui pèse sur les utilisateurs. Toutefois, elle soulève des problèmes profonds liés à l'infrastructure même du web. Nous observons que l'article 88.4 propose un mécanisme permettant à l'utilisateur de refuser son consentement en un seul clic. Certes, cette possibilité constitue, sur le papier, une avancée, mais elle ne protège en rien les utilisateurs contre les interfaces trompeuses. Au contraire, elle peut les conduire à accepter sans réelle compréhension.

Les exemples sont nombreux. Cette nouvelle bannière à clic unique peut manipuler l'utilisateur par le jeu des couleurs, par la clarté apparente de certains boutons ou par la mise en avant visuelle de l'option d'acceptation. De fait, toute une présentation graphique peut être conçue pour orienter l'utilisateur vers l'acceptation, tandis que l'identification du bouton de

rejet devient complexe, peu visible ou contre-intuitive. Dans certains cas, le refus est associé à une perte de fonctionnalités, réelle ou supposée. Nos travaux ont montré que, bien souvent, l'utilisateur clique sur « Accepter » par crainte de ne pas pouvoir poursuivre la consultation du site.

Nous avons étudié environ 200 sites internet extrêmement populaires et analysé leurs interfaces, lesquelles, en théorie, devraient permettre aux utilisateurs de retirer un consentement précédemment donné. Or, nous avons constaté que de nombreux sites ne sont pas conformes, car cette possibilité de retrait n'apparaît pas de manière effective. Par ailleurs, l'Omnibus ne dit rien de ce qui se passe derrière l'interface de recueil du consentement. Des questions essentielles restent sans réponse : où ce consentement est-il stocké ? Peut-il être transmis à des tiers ? Il n'existe pas de pratiques harmonisées concernant le stockage ni le partage des consentements. Il devient dès lors extrêmement difficile de contrôler ces mécanismes et de les analyser. Tout cela signifie qu'il peut y avoir, en apparence, un respect de la législation, alors qu'en pratique, la situation est inverse.

Enfin, la proposition Omnibus, notamment à travers l'article 88 B-6, n'embrasse pas l'ensemble des hypothèses. Il ne faut pas oublier, par exemple, les télévisions intelligentes. Certaines chaînes de télévision fonctionnent désormais comme de véritables applications et intègrent des *trackers*. Or, aucun de ces outils n'est véritablement couvert par la réglementation envisagée, ce qui laisse subsister des angles morts importants.

M. Julien Rossi. Nos travaux sur l'Omnibus ont été publiés et je pourrai, si vous le souhaitez, vous transmettre de la documentation complémentaire. En revenant à votre question sur les autres domaines dans lesquels nous observons des traitements massifs de données à caractère personnel, il est en réalité difficile de les lister de manière exhaustive, car tout le monde traite des données personnelles, y compris avant même l'avènement de l'informatique moderne. Le RGPD s'applique d'ailleurs également aux fichiers manuels. Certains collègues évoquent l'existence d'un paradigme « dataïste », un mouvement de fond qui encourage la collecte systématique de données. Anaïs Théviot l'a étudié, par exemple, dans le contexte de la vie politique française.

Un domaine qui suscite aujourd'hui de nombreuses interrogations est celui de ce que l'on appelle l'intelligence artificielle. J'emploie volontairement cette expression avec prudence, car elle recouvre en réalité une grande diversité de techniques et de domaines d'application. La penser comme un bloc homogène empêche souvent d'appréhender les problèmes spécifiques propres à chaque usage. Néanmoins, pour l'entraînement de modèles, notamment dans le cadre des IA génératives, on observe une volonté marquée des acteurs de réutiliser des stocks de données à caractère personnel déjà disponibles. Cet aspect soulève immédiatement la question de la base légale du traitement, notion centrale du RGPD. S'agit-il du consentement éclairé de la personne concernée ou d'une autre finalité juridique ? L'Omnibus numérique tente d'apporter certaines réponses, mais celles-ci demeurent contestées.

Le problème sous-jacent à ces interrogations juridiques est que, jusqu'ici, la Cour de justice de l'Union européenne avait admis, dans son arrêt *Google Espagne* de 2014 consacré au droit au déréférencement, que l'indexation de données personnelles publiées sur des pages web publiques par un moteur de recherche pouvait se fonder sur l'intérêt légitime de l'opérateur. La Cour n'avait pas exigé que Google recueille le consentement libre et éclairé des personnes concernées à chaque indexation. Le corollaire de cette solution était le droit d'opposition, le fameux droit à l'oubli.

L'IA conversationnelle, en tant que nouveau mode d'accès à l'information en ligne, suscite toutefois de nouvelles interrogations. Les éditeurs de presse en ligne craignent ainsi un effondrement du trafic, dès lors que les utilisateurs obtiennent leurs réponses via une interface conversationnelle sans consulter directement les sites. Ces enjeux économiques sont nombreux, mais je ne m'y attarderai pas, n'étant pas économiste.

Un autre cas de figure mérite néanmoins d'être souligné. Un opérateur de réseau social a collecté, au fil des années, une quantité considérable de données personnelles pour des finalités liées au fonctionnement du service, par exemple permettre à des individus de partager des photographies de vacances avec leurs proches dans un cadre qu'ils pensent sécurisé. Cet opérateur peut être tenté de réutiliser ces données pour entraîner des algorithmes d'intelligence artificielle. Se pose alors, de nouveau, la question de la base légale de ce traitement, débat que l'on retrouve au cœur des discussions autour de l'Omnibus numérique.

Mme Sophie-Laurence Roy, présidente. L'intelligence artificielle ne finira-t-elle pas par tuer internet ?

M. Julien Rossi. Je ne saurais dire si elle relève de la spéculation ou si elle se confirmera, mais cette crainte existe bel et bien pour le web ouvert.

Mme Nataliia Bielova. La question des types d'applications et de sites web où les données des utilisateurs sont collectées mérite une attention particulière. On a souvent l'impression qu'un site de commerce en ligne est un contexte totalement anodin. Acheter une paire de chaussures ne semble, en soi, poser aucun problème. Or, le passage d'un contexte perçu comme neutre à un contexte hautement sensible peut être extrêmement rapide. Un exemple en cours aux États-Unis illustre cette réalité : une action collective vise un site de commerce en ligne spécialisé dans les *sex-toys*, dont les informations de navigation sont transmises à des services analytiques. Ce qui semblait anodin devient alors extrêmement problématique.

Les utilisateurs n'ont pas nécessairement conscience de ce basculement. Un autre exemple concerne les courtiers en données. En Californie, ces courtiers doivent être déclarés sur une plateforme publique. On en dénombre aujourd'hui 566, avec des indications sur les types de données détenues : données biométriques, orientation sexuelle, informations relatives à la santé reproductive, affiliation syndicale. Est également indiqué avec qui ces données sont partagées ou à qui elles sont vendues. Pour les chercheurs, disposer d'un annuaire équivalent en Europe serait essentiel afin de comprendre quelles entités collectent des données concernant les citoyens de l'Union européenne et à quel moment.

Mme Cyrielle Chatelain, rapporteure. Je souhaite à présent parler des outils qui permettent de garantir nos droits. Selon vous, la Cnil dispose-t-elle des moyens, y compris juridiques, adaptés pour faire face à l'ensemble de ces acteurs ? Faudrait-il confier en complément au Comité européen de la protection des données une compétence de sanction directe à l'égard des plus grands acteurs pour favoriser une application uniforme du RGPD ou de la directive ePrivacy ?

Par ailleurs, lors d'une audition tenue hier, a été évoqué l'enjeu des intermédiaires de données et ce que pourraient être des « *data trusts* ». Un tel outil pourrait-il être intéressant pour mieux faire valoir les droits, à tout le moins les droits attachés aux données, notamment aux données personnelles ?

M. Julien Rossi. S’agissant des outils disponibles, il faut d’abord mentionner des instruments d’ordre individuel, comme le chiffrement ou d’autres techniques similaires, mais qui font peser une charge particulièrement importante sur l’individu. C’est d’ailleurs pour cette raison que le droit des données personnelles est fréquemment critiqué : on lui reproche d’être excessivement individualisé et, partant, illusoire, dans la mesure où le poids qu’il fait reposer sur les personnes concernées est trop élevé. En France, la Cnil représente le pilier de cette approche structurelle, qui existe également dans le droit des données personnelles.

Je ne saurais me prononcer sur l’adéquation des moyens financiers de la Cnil. Cependant, la panoplie juridique à sa disposition est relativement vaste et substantielle, avec l’avantage supplémentaire que nombre de ces règles existent depuis longtemps. En France, certaines remontent à la loi informatique et libertés de 1978, ce qui confère une certaine stabilité jurisprudentielle et une sécurité juridique non négligeable. Une difficulté fréquemment évoquée à propos de la Cnil tient toutefois au faible pourcentage de plaintes qui aboutissent à des sanctions. Il est cependant délicat de comparer les autorités de protection des données entre elles. L’autorité slovaque, par exemple, prononce proportionnellement davantage de sanctions que la Cnil, mais il est possible que ces autorités soient confrontées à des typologies d’affaires différentes.

Une autre difficulté soulignée par plusieurs collègues réside dans le manque de données comparatives concernant la durée moyenne des procédures d’une autorité à l’autre. Des recherches sont en cours pour tenter de définir des métriques permettant de comparer les autorités de protection des données. Dans ces travaux, la Cnil française n’est pas considérée comme particulièrement inactive, même si son taux de sanctions demeure relativement faible, ce qui n’est pas, en soi, l’unique indicateur pertinent. Cependant, nous constatons des délais parfois importants dans le traitement des plaintes. À cela s’ajoute une difficulté pratique : le parcours de dépôt d’une plainte auprès de la Cnil a évolué et apparaît aujourd’hui plus complexe qu’auparavant.

Dans ce contexte, une réflexion pourrait être engagée, notamment à l’approche de l’entrée en application du nouveau règlement européen harmonisant les procédures pour les plaintes impliquant plusieurs États membres. Il pourrait être envisagé de faire en sorte que les droits reconnus aux personnes dans les procédures paneuropéennes soient également garantis à celles qui saisissent la Cnil dans des affaires purement nationales, ne nécessitant pas de coopération européenne. Le transfert de l’ensemble des compétences à une autorité unique paneuropéenne relève, quant à lui, d’une appréciation politique. Du point de vue de la sociologie de l’action publique, cela impliquerait l’existence d’un point unique de décision, alors même qu’aujourd’hui les autorités nationales et européenne développent des approches distinctes et débattent entre elles au sein du Comité européen de la protection des données. Ces mécanismes de coopération favorisent la confrontation des points de vue et permettent, le cas échéant, un certain équilibre des influences. Une centralisation totale pourrait réduire cette pluralité d’approches.

Un dernier point mérite d’être mentionné, dans une perspective qui n’est pas accusatoire. Nos recherches, même lorsqu’elles adoptent un angle critique, ne visent pas à désigner des responsabilités individuelles ou à blâmer qui que ce soit. L’objectif consiste à comprendre les faits et les facteurs structurels qui compliquent l’effectivité du droit. Une hypothèse explicative des difficultés rencontrées par les autorités de protection des données tient, au moins en partie, à la capacité à recruter et à fidéliser des personnels disposant d’un très haut niveau de compétences techniques et juridiques nécessaires à l’instruction de dossiers complexes. Les autorités sont en effet soucieuses de rendre des décisions robustes, capables de

résister à un contrôle approfondi, notamment par le Conseil d'État. Il ne s'agit pas uniquement d'une question de moyens au sens strict, mais aussi de conditions de travail et de concurrence avec des secteurs où ces compétences sont très recherchées.

Mme Nataliia Bielova. Pour ma part, je souhaite attirer l'attention sur les divergences d'interprétation entre les États membres. Le droit est, en pratique, interprété de manière très différente. Dans nos travaux, nous avons analysé les lignes directrices nationales des régulateurs en matière de RGPD et de vie privée, en nous concentrant notamment sur les interfaces de recueil du consentement. Nous avons constaté que quatorze régulateurs européens ne s'accordent pas sur la manière dont le droit doit être appliqué concrètement. Certains exigent l'existence d'un bouton de rejet explicite, d'autres non. Les autorités divergent également sur la formulation de la finalité du traitement, pourtant essentielle pour permettre aux individus de comprendre l'usage de leurs données.

Les régulateurs ne s'accordent pas non plus sur les informations qui doivent apparaître dès la première interface, dans le bandeau de consentement, ni sur la formulation exacte des boutons d'acceptation ou de refus. Certains se contentent d'un simple « Refuser », tandis que d'autres imposent des formulations plus explicites. Cette hétérogénéité d'interprétation a une incidence directe sur le processus décisionnel des utilisateurs. Il apparaît dès lors nécessaire de renforcer l'harmonisation. Les lignes directrices européennes en matière de protection des données poursuivent cet objectif, mais leur mise en œuvre est difficile, car elles doivent concilier des positions nationales parfois très éloignées.

Un second point concerne l'évaluation à grande échelle des phénomènes que nous avons évoqués. La collecte de données est massive et ne peut être appréhendée en se limitant à l'analyse d'un site web isolé ; une telle approche est insuffisante. Les moyens des régulateurs nationaux ne relèvent pas de notre compétence d'analyse, mais, en tant que chercheurs, nous menons un travail analogue à notre échelle, en cherchant à comprendre ce qui se produit globalement. Cela suppose le développement d'outils capables de détecter automatiquement les traceurs et d'analyser les interfaces de recueil du consentement. C'est la seule manière de mesurer l'ampleur réelle du problème.

Pour y parvenir, il est indispensable de disposer d'obligations standardisées et transparentes concernant les technologies de traçage. Nous connaissons l'existence de ces technologies, mais il est souvent impossible de déterminer avec certitude les finalités exactes pour lesquelles elles sont utilisées, qu'il s'agisse de publicité ou d'autres usages. C'est pourquoi nous estimons qu'un renforcement des normes relatives au consentement est nécessaire afin de permettre une évaluation automatisée et à grande échelle de ces pratiques.

Mme Cyrielle Chatelain, rapporteure. Parmi les limites de l'Omnibus numérique, nous avons déjà évoqué le risque d'un affaiblissement des protections des données. Dans l'hypothèse où un tel affaiblissement interviendrait au niveau européen, quels seraient les outils dont les députés français disposeraient pour protéger, non pas les données en tant que telles, mais les personnes face aux effets que l'utilisation des données peut produire ? Je pense notamment aux atteintes à la vie privée, aux pratiques frauduleuses ou discriminatoires. Existe-t-il, dans différents corpus juridiques nationaux, des outils que des citoyens français pourraient mobiliser pour se protéger de violations de leurs droits liées à l'usage des données, indépendamment du RGPD ? Je pense par exemple pour la France au code pénal ou au code monétaire et financier. Enfin, quelles améliorations pourrions-nous envisager, en tant que législateur national ?

M. Julien Rossi. Nous n'avons pas encore analysé dans le détail cette question, dans la mesure où nous ne connaissons pas encore l'issue des trilogues, ni le contenu définitif du texte qui sera adopté. Néanmoins, quelques pistes exploratoires peuvent être envisagées. L'une d'entre elles consiste à se tourner vers le droit pénal, dans la mesure où le droit pénal ne relève pas pleinement de la compétence de l'Union européenne et où il existe, en France, depuis 1992, un droit pénal des données personnelles. Ce droit est toutefois très peu mobilisé en pratique et également très peu étudié.

Il s'agit pour nous d'un point d'attention important dans le cadre de la recherche, et cela fait partie de notre agenda scientifique que de réexaminer ce corpus juridique. La question se pose notamment de savoir s'il a été suffisamment mis à jour pour tenir compte des évolutions introduites par le RGPD, quelle en est la jurisprudence et comment il est appliqué concrètement. À ma connaissance, il existe très peu de travaux récents sur ce sujet, ce qui constitue un manque du côté de la communauté académique.

Cela peut néanmoins représenter une piste intéressante, d'autant plus que le droit français intègre dans son ordonnancement juridique les textes issus de l'Union européenne, mais également des conventions internationales. Parmi celles-ci figurent la convention 108 du Conseil de l'Europe et la convention 108 +, adoptée en 2018, qui n'est pas encore entrée en vigueur faute de ratifications suffisantes. Ce texte est particulièrement intéressant, dans la mesure où il est ouvert à la ratification de pays non européens et contribue ainsi à l'émergence d'un droit international des données personnelles.

Enfin, un dernier axe de réflexion consiste à interroger l'environnement numérique dans lequel nous évoluons à travers d'autres leviers de l'action publique. Il peut s'agir de la commande publique, des politiques de dématérialisation ou encore des investissements visant à créer davantage d'espace de choix pour les individus, en complément du cadre réglementaire. Il convient toutefois de rappeler que le RGPD, en tant que règlement, bénéficie de l'effet direct et ne peut faire l'objet de dérogations par le droit national, y compris par le biais du code monétaire et financier.

Mme Cyrielle Chatelain, rapporteure. Comme vous l'avez rappelé, il n'est plus pertinent aujourd'hui d'opposer une vie en ligne et une vie hors ligne. À partir de ce constat, il devient nécessaire de considérer que ce qui est interdit hors ligne doit l'être également en ligne. Or, on observe déjà le développement de pratiques qui interrogent fortement, et qui pourraient encore s'intensifier avec le recours à l'intelligence artificielle. Prenons l'exemple de l'achat de billets en ligne, dont le prix augmente à mesure que l'on se connecte à plusieurs reprises aux mêmes pages.

Avec l'IA, on peut aisément imaginer un système dans lequel une intelligence artificielle aurait accès à la fois à mes données de paiement, à ma carte bancaire, et à l'ensemble des données disponibles sur mon profil, pour en déduire mon niveau de revenu ou mes habitudes de consommation, afin d'adapter les prix en fonction de mon profil individuel. Il ne s'agit pas nécessairement de pratiques généralisées aujourd'hui, mais de scénarios plausibles à court terme. Or, ces pratiques relèveraient clairement de mécanismes discriminatoires.

De la même manière, nous avons déjà eu des débats sur certaines plateformes, comme Shein ou Temu, concernant la mise en ligne de produits à visée pédocriminelle, pratiques qui sont évidemment interdites. Dès lors, la question centrale est de savoir si nous disposons, pour ces pratiques en ligne manifestement illégales, d'outils juridiques suffisants. Si la pédocriminalité a fait l'objet d'un encadrement spécifique, la discrimination par les prix,

facilitée par l'exploitation des données et par l'IA, suscite aujourd'hui une inquiétude croissante.

M. Julien Rossi. L'article 5 du RGPD dispose clairement qu'un traitement de données à caractère personnel doit obéir à un principe de licéité. Si la finalité est illicite, le traitement lui-même devient illicite.

Mme Sophie-Laurence Roy, présidente. Se pose aussi ici la question de la protection du consommateur : un prix affiché ne devrait pas évoluer, par exemple en fonction de mon genre ou de mon âge.

M. Julien Rossi. Les discriminations interdites le demeurent, le code de la consommation continue à s'appliquer.

En revanche, le développement de l'IA agentique, notamment dans le domaine des paiements, nécessite davantage de recherche et de réflexion. L'industrie des paiements travaille déjà sur des standards techniques permettant à un agent d'intelligence artificielle de prendre des décisions d'achat pour le compte d'un individu. Par exemple, au lieu de rechercher un vol en définissant manuellement des critères précis, on pourrait formuler une instruction du type : « *Réserver le billet d'avion le moins cher pour passer une semaine à Tokyo au mois de juin, dans la grille de prix que je suis prêt à payer* ».

Ces mécanismes existent déjà à l'état de projets et appellent des recherches approfondies, y compris avec des économistes, afin d'en comprendre les conséquences micro- et macro-économiques, notamment en matière de fixation des prix, même si certaines sociétés proposent déjà de trouver automatiquement les offres les moins chères.

Mme Sophie-Laurence Roy, présidente. Il existe déjà des offres émanant de sociétés qui promettent de trouver le crédit le moins cher ou le voyage le moins onéreux, pour les particuliers.

M. Julien Rossi. Oui mais pour le moment, c'est toujours vous qui renseignez votre numéro de carte bancaire et qui cliquez sur le bouton de validation. Demain, un robot pourrait le faire pour vous, parce que vous lui avez donné mandat de négocier avec une autre IA le prix le moins cher.

Mme Nataliia Bielova. D'un point de vue technique, l'individualisation des prix a lieu de manière permanente, partout ; mais ces pratiques demeurent difficiles à identifier. En 2014, nous avons mené une étude spécifique, qui essayait de discerner le changement des prix des vols en fonction des cookies du navigateur et du profil enregistré dans le système. Nous avons constaté que les prix fluctuaient constamment : dans ce domaine, trop de facteurs contribuent au changement de prix. Dès lors, détecter ces discriminations dans un environnement en ligne est très complexe d'un point de vue technique : nous avons besoin d'hypothèses solides pour connaître les critères qui impactent le prix. À ce titre, une plus grande collaboration entre les chercheurs, les régulateurs et les juristes ne pourrait qu'être bénéfique.

Mme Sophie-Laurence Roy, présidente. Je vous remercie.

La séance s'achève à seize heures quarante.

Membres présents ou excusés

Présents. – M. Nicolas Bonnet, Mme Cyrielle Chatelain, Mme Sophie-Laurence Roy

Excusé. – M. Philippe Latombe