ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Jeudi
11 mars 2021
Séance de 11 heures

Compte rendu n° 39

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. le professeur Thibault Douville, professeur des universités, directeur du master Droit du numérique à l'Université Caen Normandie

La séance est ouverte à 11 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons M. le professeur Thibault Douville, professeur des universités en droit privé et directeur du master Droit du numérique à l'Université Caen Normandie.

Cette audition porte sur les aspects juridiques de la souveraineté numérique, s'agissant notamment de la protection des données personnelles. Plusieurs décisions sont intervenues à ce sujet ces derniers mois – la plus importante étant la décision *Schrems* II, rendue par la Cour de justice de l'Union européenne (CJUE) le 16 juillet 2020. Celle-ci invalide le *Privacy Shield*, c'est-à-dire la décision de la Commission européenne permettant le transfert de données par des entreprises européennes vers des pays tiers. Cette décision a suscité des doutes chez nombre d'acteurs, même si une recommandation du Comité européen à la protection des données est intervenue, depuis, pour préciser de quelle façon les entreprises pourraient, elles-mêmes, évaluer le cadre juridique externe afin de poursuivre correctement leurs transferts de données. Nous souhaiterons vous entendre également à propos des autres initiatives européennes en cours.

M. Philippe Latombe, rapporteur. Je souhaite vous questionner sur trois points en particulier.

Je souhaite d'abord vous interroger sur la définition de la souveraineté numérique. Ce sujet fait l'objet d'une attention croissante de la part des pouvoirs publics depuis la crise sanitaire. Au cours de nos auditions, nous avons eu l'occasion de recueillir plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. J'aimerais donc savoir comment vous appréhendez ce concept, en votre qualité de juriste, et quelle définition vous pouvez lui donner.

Ma deuxième interrogation concerne la décision *Schrems* II prise par la CJUE le 16 juillet 2020. De nombreux acteurs auditionnés, depuis le début des travaux de notre mission d'information, nous ont indiqué que cette décision avait créé beaucoup d'incertitudes. Le Health Data Hub a mandaté un cabinet d'expertise juridique pour en mesurer la portée exacte en ce qui concerne ses propres activités. J'aimerais donc que vous nous présentiez ses conséquences en droit et votre interprétation de sa portée.

Quelles sont les conséquences, pour la France, de l'arrêt de la CJUE du 2 mars 2021 concernant l'affaire *Prokuratuur*, dont les acteurs estiment qu'il pourrait poser des difficultés pour la bonne marche des procédures judiciaires françaises.

J'aimerais enfin aborder avec vous les différents projets de régulation du numérique et des données qui occupent l'actualité européenne ces derniers mois. Je pense en particulier au *Digital Services Act (DSA)*, au *Digital Market Act (DMA)* et au *Data Governance Act (DGA)*. Pensez-vous que ces initiatives s'orientent dans le bon sens ? Avez-vous des remarques ou des points d'alerte à nous communiquer sur ces projets qui n'ont pas encore fait l'objet du processus de trilogue ?

Pr Thibault Douville, professeur des universités, directeur du master Droit du numérique à l'Université Caen Normandie. La souveraineté numérique est un concept émergent en droit. Il ne fait pas l'objet, pour l'instant, d'une définition juridique. Comment la définir par référence au concept classique de souveraineté ? La souveraineté désigne le caractère suprême d'une puissance qui n'est soumise à aucune autre. Trois caractéristiques sont généralement mises en avant pour préciser sa définition. On s'attache tout d'abord au titulaire de celle-ci – qui est souverain ? On s'attache ensuite aux prérogatives mises en œuvre – quelle est la puissance souveraine ? On considère enfin la souveraineté comme une qualité constitutive de l'État : elle permet de distinguer l'État des autres organisations. Ce concept est donc étroitement dépendant d'une logique territoriale, qui pose difficulté dans l'environnement numérique.

Comment définir la souveraineté dans l'environnement numérique ? La souveraineté comme expression d'une puissance souveraine – c'est-à-dire la possibilité d'adopter des normes et de les faire appliquer dans l'environnement numérique – est un aspect admis de la souveraineté. De ce point de vue, l'État exerce une souveraineté sur l'espace numérique par les dispositions qu'il adopte, sous réserve des difficultés liées à la compétence territoriale.

La souveraineté numérique est, dans l'ordre externe, la capacité de l'État à demeurer indépendant. Ce deuxième aspect de la souveraineté numérique complète le premier : il existe, d'une part, l'aptitude à émettre des normes dans l'environnement numérique, et, d'autre part, son autonomie stratégique dans l'environnement numérique.

À mon sens, ces deux aspects permettent de définir la souveraineté numérique : elle recouvre un aspect normatif et un aspect lié à l'autonomie stratégique – économique, juridique et technologique. Ces deux aspects rejoignent, d'une certaine manière, la distinction classique entre la souveraineté interne et la souveraineté externe.

Le terme de souveraineté numérique n'est généralement pas admis en droit, pour une raison assez simple : Internet repose sur une logique initialement libertarienne. Ce réseau pourrait donc se passer d'État. Cette approche trouve son fondement dans la déclaration d'indépendance du cyberespace de 1996. Elle est aujourd'hui remise en cause par les acteurs d'Internet, puisque nous assistons à un mouvement de privatisation de ce réseau. L'émergence d'acteurs importants comme les géants du web américains – Google, Apple, Facebook, Amazon et Microsoft (GAFAM) – et chinois – Baidu, Alibaba, Tencent, Xiaomi (BATX) – met en exergue l'idée selon laquelle les États deviennent des colonies numériques. Il est vrai que la souveraineté réelle de l'État interroge, dès lors que des acteurs maîtrisent des données, émettent une monnaie, contrôlent les paiements, maîtrisent les places de marché, contrôlent la liberté d'expression en ligne et proposent des solutions d'identité numérique. Les différents modes d'expression de l'État sont ainsi petit à petit « mangés » par ces acteurs.

Il existe une production législative très importante pour encadrer le numérique, depuis une dizaine d'années, à l'initiative de l'Union européenne. Nous faisons face à un empilement très important de textes qui apportent des dispositions en matière de services de confiance, de protection des données personnelles et non personnelles, de protection des équilibres économiques. Nous assistons à une densification normative pour encadrer le numérique. Je ne suis pas persuadé que les réponses à ces enjeux soient nécessairement toujours juridiques. Il y a, à mon sens, un vrai problème de politiques publiques en matière de souveraineté numérique.

J’en veux pour exemple l’identité numérique, qui traduit l’aptitude des États à exercer leur souveraineté numérique. Elle constitue une clé pour transformer les services publics et pour développer la confiance dans les services en ligne. Du point de vue de l'État, ce service se développe très lentement avec France Connect Plus, qui n’est pas encore notifié à la Commission et qui n’est pas encore interopérable – alors même que des acteurs privés prétendent proposer des solutions en la matière, comme Facebook avec ID Connect. L'État a pourtant naturellement vocation à proposer une solution d’identification électronique à ses citoyens, et ainsi favoriser l’émergence d’un socle de confiance en ligne et réaffirmer sa place dans l’environnement numérique.

La souveraineté numérique s’exprime au-delà du droit par des moyens suffisants, comme les effectifs de la Commission nationale de l'informatique et des libertés (CNIL) ou de la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS). Il existe une vraie question d’investissement humain et technique, ainsi qu’une nécessité d’investissement dans la recherche de technologies innovantes. Cela constitue de vraies difficultés pour les États, qui doivent investir suffisamment dans l’innovation pour conserver une longueur d’avance par rapport aux acteurs privés.

L’arrêt *Schrems* II est un arrêt fondamental en droit des données à caractère personnel. Cet arrêt était inattendu du point de vue de sa solution, car le contentieux qui a amené à l’arrêt *Schrems* II ne portait pas sur la validité de la décision d’adéquation *Privacy Shield*, mais sur le recours à des clauses contractuelles-types par Facebook pour transférer des données aux États-Unis.

Le contentieux ayant donné lieu aux arrêts *Schrems* I et II est assez ancien. L’autorité irlandaise de protection des données, amenée à se prononcer, a formulé, par deux fois, des questions préjudicielles qui ont conduit la Cour de justice à rendre un arrêt. Dans le cas de *Schrems* II, à l’occasion de l’appréciation de la validité des clauses contractuelles-types pour le transfert des données, la Cour de justice a jugé nécessaire de se prononcer sur la décision d’adéquation du *Privacy Shield*. Pour qu’un transfert de données à caractère personnel puisse avoir lieu d’Europe vers un pays tiers ou vers une organisation internationale, il faut s’appuyer sur une base juridique (comme une décision d’adéquation) permettant d’obtenir des garanties équivalentes à ce qui existe en droit de l’Union pour la protection des données, ou à défaut, sur des mécanismes beaucoup plus simples comme le consentement à un traitement de données pour des transferts ponctuels.

Dans l’arrêt *Schrems*, la Cour de justice a été amenée à apprécier la validité de la décision d’adéquation sur le point de savoir si les États-Unis présentaient ou non un niveau de protection des données équivalent à celui offert par le droit de l’Union. Elle a estimé que les États-Unis n’offraient pas cette protection équivalente. Elle s’est appuyée sur la protection du droit au respect de la vie privée garanti par l’article 7 de la Charte des droits fondamentaux, la protection du droit au respect des données à caractère personnel et son régime exprimé à l’article 8 de la Charte des droits fondamentaux et enfin, sur l’article 47 de la Charte des droits fondamentaux qui consacre le droit à un recours juridictionnel au titre des droits protégés par cette Charte.

Partant, la Cour de justice a été amenée à mettre en œuvre le contrôle habituel de proportionnalité. Elle s’est intéressée au but poursuivi par la législation américaine, à la nécessité de ce but et à la proportionnalité dans l’atteinte portée aux droits garantis par la Charte. À l’issue de cette analyse, la Cour de justice a estimé que la protection des données aux États-Unis ne présentait pas un niveau de garantie suffisant, car les personnes concernées

ne bénéficient ni de droits effectifs et opposables, ni d'un droit à un recours juridictionnel. Elle a également jugé que le médiateur mis en place par les États-Unis, en tant qu'autorité chargée de protéger les données à caractère personnel des citoyens européens, ne présentait pas de garantie d'indépendance et ne disposait pas d'un pouvoir permettant d'adopter des dispositions contraignantes en matière de protection des données.

Par ce raisonnement, la Cour de justice a donné des indications importantes sur la manière d'apprécier le niveau de garantie équivalent présenté par une législation étrangère. Cela est important, car ce critère permet d'apprécier la validité d'une décision d'adéquation ou le caractère adéquat du recours à des garanties complémentaires, en l'absence d'une décision d'adéquation, comme des clauses contractuelles types ou des règles d'entreprise contraignantes. En rendant cet arrêt *Schrems*, la Cour de justice a donc donné la méthode : elle a précisé le niveau de protection des données requis en droit de l'Union, et donc requis d'un État tiers pour qu'une décision d'adéquation soit adoptée ou pour que des garanties appropriées soit adoptées pour compenser la différence de niveau de protection.

Pour les États-Unis, le recours à des clauses contractuelles-types ne permet pas de compenser la différence de niveau de protection, car celles-ci ne sont pas opposables à l'État américain et elles ne permettent pas, en elles-mêmes, d'accorder un recours juridictionnel aux citoyens européens, ni d'instituer une autorité de contrôle indépendante. En conséquence de cette décision, le transfert de données à caractère personnel vers les États-Unis est impossible. La législation américaine qui prévoit le contrôle et le stockage généralisé des données à caractère personnel transitant par les États-Unis rend difficilement possible l'adoption d'une nouvelle décision d'adéquation ou le recours à d'autres garanties appropriées. Le transfert des données vers les États-Unis est donc aujourd'hui prohibé. Le fait de procéder à un transfert de données entraîne une non-conformité au droit de l'Union, ce qui, en France, constitue une infraction pénale.

Cela cause un cataclysme dans les activités économiques. 65% de l'offre *cloud* est offerte par Amazon, dont une partie des serveurs se situe aux États-Unis. Dans le cas du Health Data Hub, Microsoft stocke des données en Europe, mais on sait que des opérations sur les données sont, pour partie, conduites grâce à un transfert temporaire *via* des serveurs américains. Ces situations causent potentiellement une non-conformité au droit de l'Union à la suite de l'arrêt *Schrems* II.

M. Philippe Latombe, rapporteur. Quelles sont les conséquences de cet arrêt pour les structures des entreprises ou des administrations qui utilisent des *clouds* américains ? Pour le Health Data Hub, le Conseil d'État a accordé à l'État un délai complémentaire au motif que les clés de chiffrement sont propriété de l'organisation qui collecte les données, qui est de droit européen. Il a été par ailleurs exigé, par contrat, que les données soient hébergées dans des serveurs en Europe. Est-ce suffisant aujourd'hui ?

Pr Thibault Douville. La conséquence de principe de cet arrêt est que la décision d'adéquation ne peut plus servir de fondement juridique pour le transfert de données à caractère personnel. Nécessairement, un autre fondement juridique doit être retenu pour procéder à ce transfert. Puisque la décision d'adéquation est invalidée, des fondements juridiques doivent présenter des garanties appropriées permettant de compenser la différence de niveau de protection. Il est ainsi admis qu'un transfert peut intervenir vers un pays tiers dans l'hypothèse où des mesures complémentaires sont adoptées. Le chiffrement des données constitue un exemple de mesure complémentaire pouvant être adoptée pour assurer une protection des données à caractère personnel de niveau équivalent. D'autres moyens existent,

comme une pseudonymisation ou à une anonymisation des données. Si des mesures complémentaires peuvent être adoptées pour compenser la différence de niveau de protection, encore faut-il que ces mesures soient effectives. Le chiffrement des données est un moyen intéressant pour lever l'obstacle au transfert des données.

M. Philippe Latombe, rapporteur. Lors d'une précédente audition, IBM nous a expliqué ne pas être soumis au *Cloud Act* et n'avoir aucun problème d'extraterritorialité : IBM France est une filiale d'IBM Corporation, mais il s'agit d'une société de droit français qui n'est, à ce titre, pas soumise aux règles extraterritoriales américaines. Le fait, pour une société de droit européen, d'entretenir un lien capitalistique majoritaire avec une société américaine assujettit-il la société à la réglementation américaine ? Si tel n'était pas le cas, le fait d'utiliser des algorithmes ou des solutions informatiques propriétés de la maison-mère aux États-Unis, assujettit-il la société à la réglementation américaine ?

Pr Thibault Douville. Je ne suis absolument pas spécialiste du *Cloud Act*, et par conséquent je me permettrais de ne pas répondre à votre question. Je procèderai à une vérification et vous apporterai une réponse écrite par la suite.

S'agissant de l'utilisation des moyens, toute la difficulté est de savoir comment ces moyens sont utilisés. Si des moyens de traitement de données sont utilisés dans le *cloud* et que ceux-ci supposent un transfert de données vers des serveurs hébergés aux États-Unis, la question se pose à la fois du transfert des données à caractère personnel vers un pays tiers et de l'application du *Cloud Act.*

Dans l'hypothèse du traitement des données dans le *cloud*, la question du maintien des mesures complémentaires, par exemple du déchiffrement des données, peut se poser. À cette occasion, la non-conformité au Règlement général sur la protection des données (RGPD) peut réapparaître, puisque les mesures complémentaires de protection des données seront levées pour un temps déterminé.

M. Philippe Latombe, rapporteur. La CJUE connaît une actualité forte sur ces sujets. L'arrêt *Prokuratuur* fait suite aux arrêts *Tele2* et *La quadrature du Net* suite à une question préjudicielle du Conseil d'État sur le stockage des métadonnées. Quels sont les impacts de ces arrêts sur le droit français ?

Pr Thibault Douville. Cette dynamique jurisprudentielle trouve son origine dans la directive européenne de mars 2006 sur la conservation des données de communications électroniques. Cette directive est intéressante car elle prévoit la conservation généralisée d'un certain nombre de données liées aux communications électroniques, qu'il s'agisse de données d'identification des utilisateurs ou de métadonnées. C'est ce qui est en cause dans la législation interne, notamment les dispositions du code des postes et des télécommunications électroniques et du code de la sécurité intérieure.

La Cour de justice a invalidé la décision de 2006 dans son arrêt *Digital rights* en affirmant l'interdiction du stockage et de la conservation généralisée de l'ensemble des données de connexion. Ce stockage et cette conservation sont, selon la Cour, disproportionnés par rapport aux buts poursuivis. Dès 2014, la Cour de justice mettait en avant l'ingérence dans le droit au respect de la vie privée et le non-respect des données à caractère personnel. Elle mettait en avant l'idée selon laquelle le texte n'opérait aucune différenciation entre les différents objectifs poursuivis par le législateur : la conservation des données était

déconnectée du but poursuivi, soit de prévention d'atteinte à la sécurité publique ou de lutte contre la criminalité grave.

Postérieurement à l'invalidation de cette décision de 2006, la Cour de justice s'est à nouveau prononcée sur la question, cette fois au sujet de dispositions nationales par l'arrêt *Tele2* puis par l'arrêt *La quadrature du Net*, en reprenant des solutions similaires et en apportant des précisions quant à ces arrêts antérieurs. Elle mettait notamment en avant une échelle de mesures pouvant être adoptées selon le but poursuivi : lutte contre le terrorisme, lutte contre la criminalité grave ou protection de la sécurité publique. En fonction du but poursuivi, les mesures de conservation des données varient : elles peuvent être des mesures de conservation généralisée mais temporaire, des mesures de conservation ciblée et temporaire, des mesures de conservation uniquement des données d'identification des utilisateurs. Les solutions apportées par les différents arrêts ne sont qu'une application de l'exigence de proportionnalité entre la protection des données, d'une part, et le but poursuivi, d'autre part.

En l'état, les dispositions internes sont remises en cause et supposent une réécriture. Cette réécriture ne me semble pas impossible : elle suppose de tenir compte du but poursuivi, qui varie en fonction de la gravité de l'infraction en cause.

Le récent arrêt *Prokuratuur* possède tout de même une spécificité. La Cour de justice se prononçait cette fois sur l'hypothèse dans laquelle des infractions peu graves auraient été commises – il s'agissait de vols pour des montants relativement réduits. Pour identifier l'auteur de ces vols, une juridiction estonienne avait permis la collecte et la conservation de l'ensemble des données concernant l'auteur des vols. La Cour de justice a considéré que la conservation généralisée des données de l'utilisateur permettait de dresser un profil de la vie privée de l'individu et était, là encore, disproportionnée par rapport au but poursuivi. La Cour de justice rappelle donc sa jurisprudence antérieure et la nécessité de cantonner les mesures de collecte et de conservation des données à la criminalité grave et à des menaces graves contre la sécurité publique. Cela n'interdit pas forcément l'ensemble des mesures de collecte ou de conservation des données, dès lors qu'elles sont ciblées et qu'elles ne permettent pas de dresser un portrait de la vie privée de l'individu. La portée donnée à la solution de cet arrêt est peut-être excessive : la Cour de justice n'interdit pas des mesures ciblées de conservation ou d'accès aux données mais la communication de données doit être limitée dans son étendue temporelle et matérielle.

Ces arrêts, depuis *Tele2* jusqu'au récent arrêt de mars 2021, viennent mettre en œuvre l'exigence de proportionnalité. Le législateur n'est pas interdit de mettre en place des mesures de conservation de données, mais ces mesures doivent être proportionnées par rapport au but poursuivi. Dès lors, il est étonnant que le législateur interne n'ait pas mis en œuvre l'exigence de proportionnalité en droit interne dès l'arrêt *Tele2*. Il aurait pu prévoir, par exemple, de rendre possible la conservation de l'ensemble des données d'identité des utilisateurs, de limiter la conservation de l'activité de l'utilisateur à certaines circonstances de lutte contre la criminalité grave et d'instituer un régime à paliers, selon la gravité des infractions ou du but de prévention.

M. Philippe Latombe, rapporteur. Au-delà des données personnelles, l'arrêt *Prokuratuur* questionne-t-il l'indépendance de la procédure ? L'arrêt de la Cour de justice indique que le ministère public ne présentait pas les garanties d'indépendance nécessaires pour demander la communication de ces informations. Est-ce un élément nouveau dont il faut tirer des conséquences ?

Pr Thibault Douville. Oui, cela est un élément nouveau. La Cour de justice ne s'était pas prononcée sur cet aspect dans les arrêts précédents. Sur le fondement de l'article 15 de la directive 2002-58, la Cour de justice s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale. Elle pose l'exigence de l'intervention d'un juge indépendant pour autoriser l'accès aux données, le ministère public ne remplissant pas, dans le cas estonien, les conditions suffisantes d'indépendance. Cela est certainement également applicable au droit français : je pourrais imaginer que l'on confie la mission d'autoriser l'accès aux données au juge des libertés et de la détention, en raison de l'atteinte aux droits et libertés que cet accès va entraîner.

M. Philippe Latombe, rapporteur. Cela veut-il dire que cette décision serait également applicable au juge d'instruction en France ?

Pr Thibault Douville. Oui. Deux aspects ressortent de l'arrêt : la Cour de justice distingue bien, d'une part, l'autorité de poursuite et, d'autre part, la mission d'instruction. Ni l'un ni l'autre ne pourrait se voir confier cette prérogative, qui serait laissée à un tiers. Ce tiers pourrait être le juge des libertés et de la détention en France, qui présente les garanties d'indépendance requises pour adopter une mesure attentatoire au droit au respect de la vie privée ainsi qu'à la liberté d'expression, puisque les données recueillies au titre de la criminalité grave permettent de dresser un profil complet de la personne concernée.

M. Philippe Latombe, rapporteur. Quel impact peut avoir cet arrêt sur nos procédures en cours ? Le Conseil d'État a saisi la CJUE d'une question préjudicielle. Dans un mémoire, le gouvernement a fait état d'une inapplicabilité de la décision de la CJUE pour des raisons constitutionnelles. Qu'en pensez-vous ?

À la lumière de ce nouvel arrêt, les procédures en cours seraient-elles susceptibles d'être remises en cause ? Quelles mesures correctives faut-il donc prendre ?

Pr Thibault Douville. Je répondrai d'abord à l'argument de l'identité constitutionnelle de la France comme moyen d'échapper à cette jurisprudence et plus largement au régime applicable à la protection de la vie privée dans le cadre des communications électroniques. L'identité constitutionnelle de la France est une notion assez récente, découverte par le Conseil constitutionnel au début des années 2000. À l'occasion de la transposition en droit interne d'une directive communautaire, le Conseil constitutionnel a estimé, par une décision en date du 27 juillet 2006, que s'il n'appartenait qu'au juge communautaire de contrôler le respect de cette directive et des compétences définies par les traités, il a précisé que la directive pourrait faire l'objet d'un contrôle dans l'hypothèse où elle irait à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France. Plus tôt, dans une décision du 10 juin 2004, le Conseil constitutionnel avait évoqué l'idée de l'identité nationale inhérente aux structures fondamentales et politiques constitutionnelles de la France.

Cette notion pose un problème de définition. Nous avons bien du mal à identifier le contenu de l'identité constitutionnelle de la France : la langue, l'unicité du peuple, la laïcité peuvent naturellement en faire partie. La procédure pénale et la conservation des données à fins de prévention des infractions ou de lutte contre la criminalité relèvent-elles de l'identité constitutionnelle ? Doit-on considérer que l'exercice de la souveraineté pour garantir la sûreté publique est rattaché à l'identité constitutionnelle de la France ?

À mon sens, cela n'est pas le cas, pour deux raisons au moins. Tout d'abord, les dispositions relatives à la protection des données de communications électroniques font l'objet d'une européanisation depuis bientôt vingt ans. L'État français applique cette législation, sans avoir jusqu'à présent invoqué l'identité constitutionnelle de la France. Ensuite, du point de vue du droit de l'Union européenne, l'invocation de l'identité constitutionnelle de la France permettrait d'échapper à l'application du droit de l'Union. Cet élément pose question. Un certain nombre de matières ne relèvent pas du champ du droit de l'Union, comme par exemple la défense nationale. La lutte contre les infractions ou la criminalité, en revanche, fait l'objet d'une européanisation. J'ai du mal à imaginer, dans ce contexte, en quoi les dispositions internes en matière de procédure pénale et de conservation des données présentent une spécificité française. Enfin, la France sert de modèle et invoquer l'identité constitutionnelle nationale pour échapper à l'application de ces dispositions conduirait d'autres États à tirer parti de l'argument.

Je note un point important : pourquoi le droit de l'Union européenne et le RGPD ont-ils vocation à s'appliquer ? Le droit de l'Union s'applique car sont visées, à chaque fois, des exigences de conservation de données qui s'imposent aux acteurs des traitements de données. C'est dans ce contexte que la Cour de justice a été amenée à se prononcer. J'ai du mal à concevoir que la législation interne pourrait être considérée comme distinctive par rapport au droit des autres États ou au droit de l'Union, et permettrait de justifier une forme d'exemption. Le Conseil constitutionnel n'a par ailleurs pas donné de définition générale de la notion d'identité constitutionnelle de la France, ce qui laisse la question en suspens.

Je répondrai maintenant à votre question sur les changements induits par cet arrêt en ce qui concerne la procédure pénale. L'arrêt *Prokoratuur* a une incidence en droit pénal interne, notamment du point de vue des actes d'instruction ou bien des actes d'enquête hors instruction. Pour l'instant, le juge des libertés et de la détention n'a pas vocation à autoriser la conservation ou l'accès aux données : un travail de réécriture serait donc à opérer de ce point de vue.

M. Philippe Latombe, rapporteur. Quelles seraient les conséquences d'une éventuelle acceptation par le Conseil d'État de l'argument de l'identité constitutionnelle de la France pour écarter le droit de l'Union ? Un de vos collègues professeur de droit a évoqué le risque de « balkanisation » du droit européen. Est-ce le vrai risque ?

Pr Thibault Douville. Il est évident qu'il existe un risque de balkanisation : suivre une telle approche peut conduire les autres États à adopter le même argument pour s'écarter du droit de l'Union, avec des champs d'application qui peuvent être variables. Pourquoi ne pas répliquer l'argument dans d'autres domaines ?

Il existe également un risque de conflit entre les juges. La Cour de justice pourrait tout à fait être amenée à se prononcer sur la position du Conseil d'État et à considérer que le droit de l'Union a vocation à s'appliquer à ces dispositions concernant la conservation et l'accès aux données de connexion. Cela créerait un problème de conciliation des positions entre l'ordre interne et l'ordre communautaire. Le fait d'évoquer l'argument de l'identité constitutionnelle de la France en la matière est absolument inédit.

Le sujet pourrait également être traité à l'occasion de la révision de la directive qui constitue le futur Règlement *e-privacy*. Il serait possible d'introduire directement dans le Règlement *e-privacy* un certain nombre de dispositions prévoyant la conservation de données de connexion à certaines conditions et dans certains buts de prévention du terrorisme ou de

lutte contre la criminalité grave, ce qui permettrait de donner un socle européen à ces dispositions. La Cour de justice pourrait tout à fait être amenée à contrôler la validité de ce texte à l'aune de la Charte des droits fondamentaux et il ne faudrait donc pas que ce texte présente de disproportion. L'exigence de proportionnalité conduit à raisonner en escalier : plus l'on descend des marches de gravité, moins les données qui peuvent être conservées sont importantes.

M. Philippe Latombe, rapporteur. Cela nous permet d'échanger sur les trois projets de directives en cours. Selon vous, ces directives sont-elles bien calibrées et atteignent-elles leur but ?

Pr Thibault Douville. La proposition de règlement *DSA*, qui constitue une réforme de la directive sur le commerce électronique et le statut des intermédiaires techniques, est très intéressante. Tout en maintenant l'acquis communautaire en matière d'intermédiaires techniques (c'est-à-dire le principe d'irresponsabilité pour les hébergeurs et les fournisseurs d'accès à Internet), la proposition pose un cadre juridique, à plusieurs niveaux, en ce qui concerne la modération du contenu. Le texte s'applique aux prestataires de services intermédiaires, puis aux prestataires de services intermédiaires ayant la qualité de plateforme en ligne, puis aux grandes plateformes en ligne, avec des obligations différentes pour chaque sous-qualification.

Le *DSA* propose d'instituer un régime de modération des contenus par les plateformes en ligne. Son apport est très intéressant puisqu'il vise, à la fois, à lutter contre certains contenus illégaux ou illicites par rapport aux conditions générales d'utilisation des services et à garantir la liberté d'expression. Nous savons que l'équilibre est difficile à trouver. Le *DSA* propose un mécanisme intéressant, alliant des exigences concernant les notifications et les instructions de communication de données par les autorités compétentes, d'une part, et des mécanismes de recours interne, de règlement des différends, d'évaluation des risques systémiques présentés par les grandes plateformes en ligne quant à la liberté d'expression, d'autre part.

Certains aspects de ce mécanisme peuvent néanmoins poser difficulté. Le premier aspect problématique est politique : la régulation des contenus va d'abord peser sur des acteurs privés, la modération relèvant des plateformes. L'institution d'une autorité de contrôle indépendante – le Conseil supérieur de l'audiovisuel (CSA) pour la France – est une proposition intéressante, mais elle s'inscrit dans une logique de régulation.

Un point technique peut par ailleurs être bloquant : le recours à des traitements automatisés pour procéder à la modération des contenus. Le *DSA* prévoit une exigence de transparence. La question de la transparence algorithmique soulève une vraie difficulté. Ne faudrait-il pas mettre en place des tests plus poussés des algorithmes dans des situations déterminées, ou par rapport à des types de propos déterminés ? On avance souvent l'idée d'une forme d'analyse d'impact algorithmique, mais il n'est pas certain que cela soit suffisant.

L'internalisation du mécanisme de recours est intéressante – il s'agit d'un mécanisme de règlement interne des différends dans l'hypothèse de suppressions de comptes ou de contenus. Là encore, le règlement interne a vocation à être indépendant, mais relève de la sphère privée. Nous assistons à une forme de marginalisation du juge dans le cas des atteintes à la liberté d'expression et cela peut poser problème. Il est, de plus, proposé de mettre en place un mécanisme de règlement extra-judiciaire des différends, en cas d'insatisfaction quant à la décision de règlement interne adopté. Cet empilement de mécanismes n'est pas forcément

satisfaisant et risque d'être très long. Il peut être intéressant de maintenir une procédure judiciaire rapide pour qu'une juridiction se prononce sur un conflit lié à l'absence de modération d'un propos ou à la suppression d'un propos. La marginalisation du juge me surprend, avec la désignation du CSA comme autorité de contrôle. Le recours contre une décision du CSA relève du Conseil d'État et non du juge judiciaire, garant des libertés individuelles. En tant que juriste privatiste, cette décision m'interroge.

Le projet de loi renforçant le respect des principes de la République va à mon sens dans le bon sens, proposant une forme d'introduction anticipée du *DSA* : il permettra d'expérimenter par avance le système du *DSA* et de bénéficier d'un retour d'expérience qui pourra être intéressant lors des négociations sur le texte.

M. Philippe Latombe, rapporteur. Dans les futures négociations, les pays européens sont-ils d'accord sur les contenus qui seront soumis à cette réglementation ? Les pays européens ont-ils la même interprétation de ce qu'est la liberté d'expression ?

Pr Thibault Douville. C'est en effet une question centrale. Nous le voyons déjà en matière de droit au déréférencement et de droit à la protection des données personnelles. Les conceptions de la liberté d'expression varient. Les plateformes en ligne ont une interprétation autonome et globale de la liberté d'expression, qui répond à des critères différents des nôtres. Il n'est pas prévu que le *DSA* définisse une liste des propos illégaux. Au regard de l'état de son droit, chaque État membre va être amené à définir le caractère illicite de certains propos. Nous faisons donc face à un risque d'éclatement ou de fragmentation de la manière dont sera apprécié le caractère illicite de certains propos. Avec un mécanisme comme le *DSA* instituant la compétence du prestataire en la matière, il y a un risque que l'appréciation des propos varie en fonction des opérateurs.

M. Philippe Latombe, rapporteur. Le RGPD a mis en place un fonctionnement dans lequel toutes les autorités de contrôle nationales de type CNIL travaillent ensemble sous la direction d'un chef de file. Le *DSA*, lui, ne prévoit pas de tel mécanisme. Chaque pays conduira donc sa propre interprétation ?

Pr Thibault Douville. On peut imaginer une coopération entre les autorités de contrôle – cela est dans la logique de l'instrument. Mais effectivement, le texte ne prévoit pas de mécanisme instituant une autorité de contrôle chef de file avec un mécanisme de règlement des conflits entre autorités (dans le RGPD, ce rôle est confié au Comité européen). Il y a donc un vrai risque de fragmentation de la manière dont la liberté d'expression est appréciée dans l'Union européenne, ainsi qu'un risque de définition variable des contenus illicites, au sens des conditions générales d'utilisation des acteurs.

En revanche, il ne faut pas oublier que la Charte des droits fondamentaux promeut la liberté d'expression et garantit la protection de la vie privée et des données à caractère personnel. Les autorités nationales s'inspireront naturellement tant de la jurisprudence de la Cour de justice que de celle de la Cour européenne des droits de l'Homme. Cet acquis apportera quelques garanties dans la mise en œuvre de ces mécanismes.

M. Philippe Latombe, rapporteur. Les conditions générales d'utilisateurs ne sont pas spécifiquement visées dans le *DSA*. Ne devrions-nous pas récupérer de la souveraineté sur ce sujet ? Il s'agit de réglementations privées s'appliquant à l'ensemble des utilisateurs. Les États n'ont-ils pas le devoir de s'y intéresser et de les réguler ?

Pr Thibault Douville. Le *DSA* ne prévoit en effet pas l'encadrement des conditions générales d'utilisation, au-delà d'une exigence de transparence et de la nécessité de préserver la liberté d'expression – cela demeure très vague.

À titre individuel, les utilisateurs pourront toujours se prévaloir d'une atteinte à leur liberté d'expression résultant de l'application des conditions générales d'utilisation. On peut imaginer que certaines conditions générales d'utilisation prohibant certains propos soient contraires à la liberté d'expression : la clause pourrait alors être déclarée illicite car contraire à l'ordre public, et frappée de nullité partielle.

À titre plus général, est-il possible d'imaginer un mécanisme de contrôle des conditions générales d'utilisation ? On pourrait dresser un parallèle avec le mécanisme de contrôle des clauses abusives en droit de la consommation. Il pourrait être intéressant d'intégrer dans le *DSA* un mécanisme similaire de contrôle visant à encadrer ou à limiter la liberté d'expression sur les plateformes, afin de déterminer les frontières du licite et de l'illicite dans ces clauses. Cela est tout à fait imaginable. En la matière, le mécanisme de contrôle des clauses abusives est un bon exemple qu'il serait possible de dupliquer.

Le *DGA* constitue une proposition très intéressante qui vise à faciliter le partage des données. Le texte considère que les données constituent une infrastructure qu'il est possible et souhaitable de mobiliser pour différents usages et en vue de différentes finalités. Le *DGA* propose donc la mise en place de services de partage des données à travers les *data hubs*. La difficulté de ces plateformes est la confiance des utilisateurs, aussi bien ceux détenant les données que ceux qui pourraient les réutiliser, à la fois, quant aux jeux de données et à la protection du secret et aux finalités de la réutilisation. L'instrument européen cherche à répondre à cet enjeu de confiance. Il promeut certains services nouveaux, comme la mise à disposition de données à caractère personnel en faveur de réutilisateurs ou la mise en place de services de coopératives de données.

Au-delà de son affirmation de principe, très intéressante, beaucoup de questions se posent. Le partage des données demeure facultatif et volontaire. La question de la qualité des données partagées se pose : nous avons besoin d'un référentiel en matière de fraîcheur, de format, de contenu et des finalités de réutilisation des données. Les *data hubs* mis en place ne sont pas toujours une réussite : il demeure un écart entre l'affirmation politique et économique de la création d'un *data hub* et les réutilisations effectives de données. Il n'est pas certain, pour l'heure, que les *data hubs* aient trouvé leur public.

Je relève un constat final intéressant : les acteurs concurrents de l'État (les GAFAM et les BATX) collectent des données et les conservent pour améliorer leurs services et dégager de nouvelles connaissances. L'état du droit de l'Union, en revanche, ne va pas dans le sens d'une affirmation du partage des données. Par exemple, le Règlement européen *Platform to business* de 2019 vise à rétablir l'équilibre entre plateformes et entreprises utilisatrices et pose une exigence de transparence, quant au partage de données, en faveur des utilisateurs. On peut donc se poser la question de savoir si la simple mise en place d'un cadre de confiance pour le partage des données est suffisante afin de tirer parti des données collectées. Il pourrait être important également de diffuser une culture de la donnée à destination des acteurs économiques et des citoyens, afin de favoriser l'utilisation des données et de développer des solutions techniques qui permettent leur valorisation – celles-ci ne sont pas forcément disponibles actuellement.

Le texte est donc intéressant pour le cadre de confiance apporté, mais je ne suis pas certain qu'il réussira à atteindre son objectif qui est de favoriser la mise en place d'une économie de la donnée.

M. Philippe Latombe, rapporteur. Le texte ne réussira pas à atteindre son objectif car vous pensez qu'il n'apporte pas assez de confiance ?

Pr Thibault Douville. Cela n'est pas forcément dû à la confiance. L'instrument du *data hub* est intéressant, mais ce qui pose difficulté est de savoir pourquoi des détenteurs de données les mettraient à disposition de réutilisateurs. Dans quel but le feraient-ils ? Pourquoi des personnes mettraient-elles à disposition leurs données à caractère personnel ? Dans quel but le feraient-elles ? Il n'est pas certain que l'offre corresponde à la demande. Imaginons par exemple qu'un industriel récolte des données à l'occasion de sa production et qu'il cherche à les mettre à disposition d'autres acteurs. Quels autres acteurs seraient intéressés ? Il se pose un problème de correspondance entre collecteurs de données, d'une part, et réutilisateurs de données, d'autre part.

S'agissant de l'économie de la donnée, la plupart des transferts de données à caractère onéreux interviennent, aujourd'hui, dans le cas d'activités commerciales publicitaires. Il y a un alignement des intérêts des collecteurs de données et des réutilisateurs en la matière. Du point de vue industriel, cela est plus difficilement le cas. Je ne sais pas si mettre en place des plateformes de confiance, mettant en relation des collecteurs et des réutilisateurs, est la solution pour faciliter la réutilisation des données. Au-delà de l'instrument, se pose la question du marché : il existe un problème de marché et de circuit de la donnée.

M. Philippe Latombe, rapporteur. Quels sont les sujets juridiques auxquels nous devrions nous intéresser maintenant au regard des nouvelles technologies émergentes ? Je pense notamment à l'intelligence artificielle ou au quantique. En ce qui concerne l'intelligence artificielle, par exemple, des questions se posent sur la propriété intellectuelle d'algorithmes produits par l'intelligence artificielle. Devons-nous dès maintenant créer un cadre, ou devrons-nous nous adapter au fur et à mesure des avancées technologiques ?

Pr Thibault Douville. C'est une question fondamentale. Je me permettrai, pour débuter, un parallèle avec la *blockchain*. Il y a eu, en matière de *blockchain*, une volonté politique très forte de consacrer un cadre juridique, afin de favoriser l'émergence de la *blockchain* et de servir de modèle à l'échelle de l'Union européenne. Aujourd'hui, on se rend compte que le cadre mis en place a favorisé des initiatives, qui sont bloquées pour des raisons réglementaires, notamment de certifications. Nous avons assisté à un mouvement de mobilisation des énergies pour s'emparer de ces outils, et, aujourd'hui, un ralentissement en raison de contraintes réglementaires.

Le fait d'adopter des normes permet-il vraiment de faire émerger des initiatives et de prendre de l'avance ? Cela est vraiment discutable. Nous pouvons partir du principe que le premier cadre défini permet de servir de modèle, d'asseoir la confiance des utilisateurs et de favoriser l'investissement – cela est vrai : cela a été le cas pour l'utilisation de la *blockchain* en matière financière. Inversement, la mise en place d'un cadre juridique est un frein pour des acteurs qui sont encore à la recherche de solutions techniques.

L'intelligence artificielle reste, pour l'heure, des algorithmes sous maîtrise humaine. La question des créations peut trouver une réponse sur le fondement du droit actuel de la propriété intellectuelle ou par d'autres mécanismes contractuels. Je ne sais donc pas si la mise

en place d'un cadre juridique est le meilleur moyen d'encourager les initiatives en la matière. Il demeure cependant des questions importantes sur lesquelles le législateur pourrait se pencher, comme la mise en place d'un cadre pour l'audit des algorithmes ou la transparence des algorithmes. Cette question très intéressante n'est pas réglée et mériterait de l'être. S'il s'agit d'adopter un texte pour mettre en place des règles très générales sur l'intelligence artificielle, la question de la pertinence de ce cadre se pose.

En matière de souveraineté juridique, une question actuelle pose difficulté : il s'agit de l'identité numérique. Je ne comprends pas que nous ne disposions pas de moyens d'identification électronique, que l'État ne se réapproprie pas l'identité électronique, que l'identité numérique ne soit pas ouverte aux fournisseurs de services afin de favoriser son adoption, que l'on ne se saisisse pas de ce moyen pour opérer une transformation de l'État et des services publics permettant le déploiement de services de confiance, comme la signature électronique qualifiée, l'horodatage qualifié, la lettre recommandée électronique qualifiée – sous réserve évidemment de la protection des personnes exclues du numérique.

Parmi les actions concrètes immédiates, l'identité numérique est à mes yeux une clé de la transformation numérique de l'État et de la souveraineté de l'État. L'État est le détenteur naturel de l'identité de tous ses concitoyens : il a le monopole de l'émission des titres d'identité. Ce sujet est au croisement des dispositions législatives, réglementaires et de l'investissement public. Le déploiement d'une identité numérique étatique permettrait d'opérer une transformation de l'État en mettant le citoyen au cœur de la transmission de ses données entre administrations. Ceci apporterait aux citoyens une plus grande confiance dans le déploiement du numérique et permettrait de développer de nouvelles technologies : le recours au *deep* pour les services financiers, par exemple. Ce sujet est urgent à mes yeux.

Votre mission d'information s'intéresse principalement aux usages et aux services. Il pourrait être intéressant, pour le législateur, de s'intéresser à l'infrastructure. Il s'agit de se demander si l'infrastructure numérique n'a pas vocation à relever, dans une certaine mesure, de services publics. Cela concerne l'hébergement de données – avec des garanties d'indépendance, par exemple – et les réseaux. L'ouvrage récemment publié par Thibault Verbiest et Jonathan J. Attia, « *Un nouvel Internet est-il possible ?* » raisonne sur la couche de l'infrastructure. Il propose d'intégrer à la norme des protocoles Internet TCP/IP de nouvelles fonctionnalités d'identification, de certification de contenus, de transferts de données, qui permettraient à l'État et au citoyen de retrouver une certaine maîtrise sur leurs usages. Cette approche a été peu développée jusqu'à présent. Les directives européennes s'attachent davantage à réguler les usages ou le marché.

M. Philippe Latombe, rapporteur. Notre mission d'information ouvrira une séquence pour traiter du sujet de l'identité numérique. Mme Christine Hennion et M.Jean-Michel Mis ont déjà remis un rapport à ce sujet. Leurs recommandations n'ont pas été mises en œuvre.

Pr Thibault Douville. Ce rapport formulait d'excellentes propositions. Nous disposons de France Connect Plus et une notification à la Commission devrait en principe intervenir cet été. La question est vraiment celle de l'ouverture du système à des fournisseurs de services privés pour permettre au citoyen de s'en emparer. Une vraie communication doit être faite à ce sujet.

M. Philippe Latombe, rapporteur. En ce qui concerne la *blockchain*, vous avez évoqué la partie financière et la volonté marquée dans la loi relative à la croissance et la

transformation des entreprises, dite loi PACTE, d'avancer à ce sujet. La réglementation par décret a, par la suite, bloqué les intermédiaires financiers. Mais la *blockchain* permet aussi l'horodatage et l'inscription au registre. Certains pays sont très en avance et ont adopté des réglementations internes pour donner une force probante à la *blockchain*. Où en est la France et quelles mesures devons-nous adopter en urgence ?

Pr Thibault Douville. Un rapport et plusieurs propositions parlementaires sont intervenus à ce sujet. Votre collègue, M. Jean-Michel Mis, avait proposé, à l'occasion de la loi PACTE, d'introduire dans le code civil une disposition visant à donner une force probante aux enregistrements sur une *blockchain*.

Je formule à ce sujet plusieurs remarques. Le déploiement de la technologie de la *blockchain* demeure limité en dehors des cryptomonnaies ou des actifs numériques. Cela étonne, dès lors que la *blockchain* est connue et commence à être maîtrisée par tous. Du point de vue des usages, la *blockchain* pose la question de la conservation de l'information, de son intégrité et de sa datation. Elle ouvre la possibilité de la digitalisation de l'activité contractuelle par les *smart contracts*.

En ce qui concerne la force probante, la consécration d'une forme d'intégrité des données pourrait être intéressante. Le code civil permet d'ores et déjà d'utiliser une signature électronique avancée qui permet de garantir l'identité du signataire et de faire le lien entre la signature et l'acte. Il est possible à des prestataires de services de confiance de combiner leurs services avec des services de *blockchain* privés. La question de la consécration de la force probante sur des *blockchains* publiques se pose : elle pourrait être intéressante, au moins s'agissant d'une présomption quant à la datation de l'enregistrement et quant à l'intégrité de l'information, mais non une présomption quant à l'identité de celui ou celle ayant enregistré l'information – car cet élément ne peut pas faire l'objet d'un contrôle s'agissant d'une *blockchain* publique, sauf si un intermédiaire intervient pour délivrer des clés d'identification.

Il pourrait être intéressant de réfléchir à l'intégration d'un régime de *smart contracts*. L'autonomisation d'un certain nombre de contrats a vocation à intervenir, s'agissant des clauses contractuelles pouvant faire l'objet d'une mise en œuvre automatique, comme, par exemple, les conditions suspensives d'obtention d'un prêt. Le *smart contract* ne serait-il alors qu'une déclinaison de clauses contractuelles dans la *blockchain*, ou peut-on imaginer un contrat entièrement codé ? Cette seconde option poserait des questions de transparence, de compréhension par les parties et d'expression du consentement par les parties. Dans un premier temps, on pourrait imaginer la consécration de l'utilisation de *smart contracts*, c'est-à-dire d'exécution automatique de contrats sur une *blockchain*. Cela permettrait de lever un certain nombre d'incertitudes quant à l'inexécution éventuelle du contrat, mais pose, dans le même temps, des problèmes en ce qui concerne sa suspension éventuelle. Cela soulève beaucoup de questions qui mériteraient une vraie réflexion.

Le prochain congrès annuel des notaires aura pour thème l'homme, le numérique et le droit. Les notaires proposeront notamment un premier clausier de *smart contracts*, sur des opérations simples (conditions suspensives, terme d'un contrat, paiement d'une somme d'argent), qui ne requièrent pas d'information ou d'exécution extérieure de la part d'une personne. Cela pose une première brique de réflexion intéressante.

En France, en ce qui concerne les faits juridiques, un enregistrement sur une *blockchain* peut parfaitement être invoqué devant une juridiction, en vertu du principe de non-discrimination des documents électroniques instauré par le Règlement européen eIDAS. Une

révision du Règlement eIDAS est envisagée, notamment pour y intégrer les *blockchains*. Jusqu'à présent, le Règlement eIDAS traite de l'identification électronique et des services de confiance, qu'il envisage de manière centralisée. Il est envisagé d'intégrer la *blockchain* dans ce Règlement : cela poserait davantage de questions pour les *blockchains* publiques que pour les *blockchains* privées.

En France, contrairement à la Belgique, nous n'avons pas profité de l'adaptation du droit français au Règlement eIDAS pour intégrer un statut des prestataires de confiance ou des tiers de confiance numériques. Il pourrait être intéressant de le faire. J'en veux pour exemple la consécration du coffre-fort numérique comme service de confiance en France. Le pouvoir réglementaire n'a pas indiqué qui peut proposer un service de coffre-fort numérique et quel est son statut. Il pourrait être intéressant de consacrer un régime général, peut-être dans le code de commerce, de l'activité de services de confiance en ligne. Cette activité pourrait être entendue soit de manière restrictive (c'est-à-dire tous les services de confiance au sens du Règlement eIDAS ou ajoutés par le législateur interne), ou bien plus largement : le tiers de confiance pourrait être celui qui propose des services de confiance ou la certification d'information par voie électronique. Cela peut être intéressant à l'occasion du déploiement des *blockchain* qui proposent des services de conservation d'actifs numériques, en rattachant les prestataires de services d'actifs numériques à cette catégorie des tiers de confiance.

Cela ferait apparaître un acteur qui bénéficierait d'un statut sur lequel le législateur pourrait s'appuyer pour de nouveaux usages à consacrer par la suite : des garanties financières de responsabilité, de respect des données à caractère personnel, de cybersécurité, qui seraient variables selon la qualité du tiers de confiance. On pourrait par exemple imaginer que les notaires puissent être tiers de confiance pour la certification et l'authentification d'information. On pourrait également imaginer que les prestataires de services qualifiés au sens d'eIDAS bénéficient de ce statut pour les services donnés. Cela permettrait d'agréger un certain nombre d'acteurs sous une qualification unique. Le législateur pourrait ensuite consacrer de nouveaux services de confiance se rattachant à cette catégorie de tiers de confiance bénéficiant d'un régime unitaire.

M. Philippe Latombe, rapporteur. Vous ne préconisez pas de créer une profession juridique réglementée spécialisée ? D'autres pays européens l'ont fait.

Pr Thibault Douville. Derrière la notion de « confiance en ligne » se cache une multitude de services possibles. Il existe les services de confiance au sens classique, c'est-à-dire au sens du règlement eIDAS. La Poste, dans le cadre de la délivrance de moyens d'identification électroniques, exerce, elle aussi, une activité de confiance. Ce service de confiance de vérification d'identité n'est pas consacré par le législateur – il est rattaché à un référentiel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pour permettre le déploiement des *smart contracts*, les notaires pourraient eux aussi exercer une activité d'authentification d'information en ligne. Il serait donc intéressant de disposer d'un statut unique de prestataire de services de confiance, dont les titulaires pourraient être habilités à proposer un service d'authentification de documents, aussi bien que de vérification d'identité. Cette catégorie a vocation à être adaptable en fonction du service de confiance proposé par les différents professionnels.

En consacrant la notion de prestataire de services de confiance ou de tiers de confiance, on pourrait associer à cette qualification un ensemble d'obligations communes de transparence, de responsabilité, de certification. Cette qualification bénéficierait de l'ensemble de l'acquis interne et européen, tout en permettant d'ouvrir de nouveaux usages

par la suite. Un service de confiance d'authentification de documents est fondamental pour le déploiement des *blockchain* : il permettrait d'ajouter une présomption d'intégrité et de validité des informations enregistrées sur une chaîne de bloc. Nous avons besoin d'une catégorie.

M. Philippe Latombe, rapporteur. L'État travaille à sa numérisation et a besoin de plus en plus de données. Pour le contrôle fiscal par exemple, Bercy a souhaité pouvoir aspirer les données des réseaux sociaux. À l'occasion de l'examen du projet de loi sur la sécurité globale, la question du stockage des images filmées par les drones a également été débattue. Pensez-vous que l'État a aujourd'hui une suffisante culture de la donnée ?

Pr Thibault Douville. C'est une question difficile. Tout dépend des ministères et des services concernés. L'État mène une politique volontaire d'*open data* – c'est-à-dire d'ouverture des données – depuis bientôt vingt ans et cela commence à porter ses fruits. Un service public de la donnée a été créé et l'on constate aujourd'hui la mise à disposition d'un certain nombre de bases de données.

Votre question porte peut-être davantage sur les données que l'État collecte et traite dans ses activités. Ces données sont-elles valorisées et pourraient-elles l'être davantage ? Une récente initiative du ministère de la justice donne des clés de compréhension à ce sujet. Le décret DataJust de mars 2020 vise à mettre en place un traitement automatisé de données à caractère personnel. Un algorithme, établi à partir de décisions judiciaires, permet, par exemple, d'établir un barème d'indemnisations en matière de dommages corporels, de faire de la prospective et de l'analyse de moyens des juridictions, d'informer les justiciables concernant leurs droits et, potentiellement, l'indemnisation à laquelle ils peuvent prétendre. Cela favoriserait la mise en place de mécanismes de règlement extrajudiciaire des litiges. Cette initiative du ministère de la justice consiste à valoriser des données existantes, avec un objectif d'ordre à la fois opérationnel, prospectif, d'information et de pédagogie auprès des citoyens.

Ce modèle peut être dupliqué. La prospective et l'analyse de données peuvent, évidemment, être utiles à l'État – l'État le fait d'ailleurs déjà dans certains ministères et a vocation à le faire davantage. Cette initiative est également le moyen, pour l'État, de garder la main sur ses données et d'éviter que des acteurs privés ne s'en emparent. Les *legal tech*, par exemple, développent leurs activités sur des données judicaires : par son initiative, le ministère de la justice propose un service étatique et garde ainsi la main sur ses données. L'utilisation et la valorisation des données sont également un moyen de favoriser la confiance. La crise du COVID a montré que l'ouverture des données sanitaires était un très bon moyen de donner aux citoyens une prise sur l'évolution de la situation sanitaire. Plusieurs cas de réutilisation de données ouvertes par l'État ont ainsi été salués.

Les moyens posent problème dans la valorisation de la donnée. Nous en sommes toujours là. Nous avons créé le Health Data Hub ; il aurait été possible de prévoir une modernisation et une uniformisation des systèmes d'information des hôpitaux pour permettre une valorisation des données stockées localement, mais la difficulté est l'éclatement des suites logicielles utilisées dans les différents services des hôpitaux. En matière judiciaire, la même difficulté se pose : l'absence de rénovation du parc informatique et l'absence de matériel suffisant et à jour bloquent le développement de nouveaux usages. La mise à disposition de l'*open data* des données en matière judiciaire est aujourd'hui bloquée par la constitution de bases de données progressives. Nous sommes confrontés à un vrai problème d'investissement dans les politiques numériques, ainsi que de normalisation, d'uniformisation et de rénovation

numérique de l'État. Cela bloque un certain nombre d'initiatives que l'État pourrait lancer et cela est dommage.

M. Philippe Latombe, rapporteur. La culture de la protection de la donnée fait-elle partie de la culture de l'État, ou l'État doit-il l'acquérir ? Avez-vous des recommandations à partager en matière de protection des données ?

Pr Thibault Douville. L'État est actif en matière de protection des données. La loi de programmation militaire 2013-2019 a été, par exemple, la première à créer la catégorie des opérateurs d'importance vitale pour protéger les systèmes d'information et les données. L'État est par ailleurs actif par le cadre juridique mis en place, par exemple, concernant la sécurité des données de santé qui font l'objet d'un hébergement. Il existe une vraie politique étatique en matière de protection des données. De ce point de vue, il me semble que l'État est assez proactif, aussi bien en matière de protection des données que de cybersécurité.

Il est plus surprenant peut-être de constater la défiance que les citoyens peuvent entretenir à l'égard de l'État quant à la manière dont il traite les données et aux finalités poursuivies par ces traitements. Le projet Alicem en est un exemple concret : le traitement de données visait à permettre la création d'un moyen d'identification électronique sur un *smartphone*. Il a provoqué des réactions assez vives en raison des risques que le système poserait quant à la protection des données à caractère personnel, notamment en raison du stockage centralisé d'un certain nombre de données. L'État devrait peut-être mettre en œuvre une politique pour minimiser les données traitées afin de favoriser la confiance des citoyens. Était-il par exemple nécessaire, dans le projet Alicem, de prévoir un stockage centralisé des données à des fins d'authentification compte tenu des usages possibles du moyen d'identification électronique ? L'État devrait peut-être développer une politique de minimisation des données pour favoriser la confiance des citoyens. Il me semble que la quantité ou le volume des données traitées, par l'État, peut créer une difficulté pour les citoyens. La meilleure protection des données est la minimisation. La meilleure anticipation du risque cyber est la minimisation des données traitées.

La collecte massive des données génère un risque. Il est tout à fait possible de modifier, par voie réglementaire ou législative, la finalité de l'utilisation des données pour transformer l'objet du traitement. C'est en cela que le raisonnement sur la finalité du traitement n'est pas forcément satisfaisant à lui seul. Une mise en œuvre du principe de minimisation des données constitue une vraie protection complémentaire des droits et libertés. La minimisation constituait le principe de base du RGPD, et l'on se focalise aujourd'hui davantage sur les finalités poursuivies que sur la minimisation des données.

La transformation numérique de l'État est un point fondamental en ce qui concerne la souveraineté. La place de l'État dans l'environnement numérique a vocation à se renforcer : l'État est très présent hors numérique, mais quelle est sa place dans l'environnement numérique ? Il y a toute sa place. Pour cela, l'État a certainement vocation à remettre le citoyen au cœur de ses données et au cœur de son identité ainsi qu'à minimiser les données traitées, afin de redonner une certaine prise au citoyen sur l'activité de l'État en matière numérique et à lui redonner confiance. Il est aberrant que les citoyens aient, en France, davantage confiance en Facebook ou Google qu'en l'État pour traiter leurs données.

M. Philippe Latombe, rapporteur. Y a-t-il des sujets que nous n'avons pas abordés et que vous souhaitez évoquer ?

Pr Thibault Douville. Nous avons, je crois, couvert l'essentiel des questions. Je vous enverrai une réponse écrite sur le périmètre d'application du *Cloud Act* aux filiales d'entreprises américaines.

La séance est levée à 12 heures 50.

Membres présents ou excusés

Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du jeudi 11 mars 2021 à 11 heures

Présents. – MM. Philippe Latombe, Jean-Luc Warsmann

Excusées. – Mme Frédérique Dumas, Mme Nathalie Serre