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
25 mars 2021
Séance de 9 heures 30

Compte rendu n° 46

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, *rapporteur*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL)

La séance est ouverte à 9 heures 30.

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous accueillons aujourd'hui M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL), accompagné de Mme Manon de Fallois, juriste au service de la santé et de M. Etienne Maury, juriste au service des affaires européennes et internationales.

La CNIL est une autorité administrative indépendante, créée par la loi Informatique et Libertés du 6 janvier 1978. Elle compte deux cent quinze agents et son collège est composé de dix-huit membres parmi lesquels quatre parlementaires.

La CNIL a pour mission de veiller à la protection des données personnelles contenues dans les fichiers informatiques ou papier, aussi bien publics que privés. Elle rend, en conséquence, un certain nombre d'avis et peut prendre des décisions de sanction en cas de non-respect du cadre juridique. Elle se situe donc au cœur des enjeux de notre mission d'information.

Nous souhaitons avant tout vous entendre sur trois sujets.

En prmier lieu, comment la CNIL se positionne-t-elle vis-à-vis de la souveraineté numérique ? Ce concept comprend de nombreuses définitions et déclinaisons, qui renvoient essentiellement, d'un point de vue juridique, à la capacité des pouvoirs publics à imposer le respect du cadre de régulation existant dans la sphère numérique, afin de protéger les droits et les libertés des citoyens.

Comment envisagez-vous votre action, dans un contexte marqué par le caractère évolutif des technologies numériques et un cadre juridique en mouvement, comme le montrent les différentes initiatives de régulation engagées au niveau européen ?

Nous souhaitons également échanger sur la façon dont les CNIL européennes coopèrent face aux pratiques de certains acteurs comme les GAFAM, qui déjouent largement les frontières nationales.

Notre deuxième questionnement porte sur les conséquences des récentes décisions de la Cour de justice de l'Union européenne (CJUE) sur la protection des données.

Notre mission d'information s'intéresse aux données de santé, dont l'exploitation est à la fois pleine de promesses, en termes d'innovation, et pleine de risques, raison pour laquelle elle est strictement encadrée en droit.

Nous aimerions savoir comment la CNIL se positionne sur ce sujet, notamment vis-à-vis des plateformes de données de santé et de la situation plus spécifique du Health Data Hub.

Nous nous interrogeons également sur les conséquences de la décision *Schrems* II, qui a invalidé le *Privacy Shield*, car il crérait une situation juridique insécure pour les entreprises, qui pouvaient transférer leurs données vers des pays tiers, en particulier les États-Unis.

Nous souhaiterions savoir quel regard vous portez à ce sujet et vous entendre sur les enjeux d'extra-territorialité du droit américain, le *Cloud Act* ou le *Foreign Intelligence Surveillance Act (FISA).*

Enfin, nous aimerions échanger sur les évolutions souhaitables ou nécessaires pour la CNIL dans ce contexte mouvant. Nous savons qu'elle souhaite intégrer davantage les problématiques de cybersécurité, qui est l'une de ses priorités en matière de contrôle en 2021. Le projet de loi 4D pourrait aussi renforcer l'effectivité du pouvoir de sanction de l'autorité en proposant une procédure simplifiée dans ce domaine.

Identifiez-vous d'autres évolutions souhaitables pour renforcer votre capacité d'agir en faveur de la protection des données, des droits et des libertés des citoyens dans le domaine du numérique ?

M. Gwendal Le Grand, secrétaire général adjoint de la Commission nationale de l'informatique et des libertés (CNIL). Mmes et MM. les députés, Mmes et MM, je suis très honoré d'avoir l'occasion de m'exprimer devant votre mission d'information et je vous remercie, au nom de la CNIL, pour votre invitation.

Je suis accompagné de M. Etienne Maury, qui travaille au service des affaires internationales et européennes, et de Mme Manon de Fallois, qui travaille au service de la santé.

La souveraineté numérique est devenue, en quelques années, un sujet politique majeur et décisif. Depuis sa création, il y a plus de quarante ans, la CNIL a observé comment les innovations technologiques ont progressivement envahi les espaces de la vie privée et de la vie en collectivité, au travail comme dans les entreprises ou les services publics. Le numérique a même modifié la perception de nos frontières, des valeurs de nos sociétés et de notre équilibre économique.

Cette difficulté nécessite de repenser le concept de souveraineté nationale et européenne pour faire face à deux principaux enjeux.

Le premier enjeu est lié à la capacité des États à appliquer leurs normes. En effet, rien de ce qui définit la puissance publique (un territoire, des frontières, des règles) ne fonctionnent en ligne, car Internet n'est pas un lieu, mais un lien dans lequel s'effectue d'innombrables traitements et transferts internationaux de données. La singularité de la révolution numérique tient d'ailleurs au fait que les gisements de données ne se tarissent pas avec le temps. L'usage de données génère de la valeur par leur recoupement, leur agrégation et leur mise en relation.

Le deuxième enjeu est celui de l'éthique. Le *« solutionisme technologique »* proposé par de multiples acteurs, qui se confrontent sur des marchés, est une tendance forte, qui pourrait nous conduire à subir des choix d'organisation de la vie en société. Le risque réside dans le fait que ces choix soient *in fine* opérés à notre insu, en dehors des circuits démocratiques traditionnels, et que les nations n'aient plus la capacité d'opérer des choix collectifs.

L'État est mis au défi dans toutes ses facettes d'expert, de stratège, de législateur, de régulateur et de pouvoir exécutif. Face à ce défi, l'intervention de la puissance doit se recomposer autour de leviers robustes, que je vous propose d'explorer au travers du prisme de la CNIL.

Je reviendrai rapidement sur la genèse du Règlement général sur la protection des données (RGPD) et la structuration de la souveraineté numérique, avant de présenter un bilan européen de la protection des données. Je terminerai sur les axes prioritaires à renforcer pour que la CNIL soit à la hauteur des enjeux dans un monde post-Covid. Mon propos répondra ainsi à la plupart de vos questions.

S'il existait un ADN du numérique à l'échelle française ou européenne, il s'agirait de placer la personne humaine au centre de la régulation. Celle-ci a évolué afin de répondre à des défis politiques, économiques et géopolitiques.

S'agissant des défis politiques, l'article premier de la loi Informatique et Libertés de 1978, qui a donné naissance à la CNIL, pose le principe selon lequel l'informatique doit être au service de chaque citoyen et ne porter atteinte ni à une entité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques. Quarante ans plus tard, cet article premier constitue toujours une boussole.

La loi Informatique et Libertés a également imposé quatre types de nouveaux droits citoyens : les droits d'information, d'opposition, d'accès et de rectification.

À partir des années 1990, des défis économiques surviennent. Avec l'explosion d'Internet, l'Europe se dote d'une directive en 1995, qui reprend les principes de la loi Informatique et Libertés. En 2002, une directive dite *« on Privacy »* (Vie privée et communication électronique) reconnaît la spécificité du secteur des communications électroniques. Depuis, le contexte économique a beaucoup évolué, avec les GAFAM qui sont devenues hégémoniques et de nombreuses avancées technologiques, comme les objets connectés, les techniques de profilage, de surveillance, les outils de contrôle, les algorithmes et le développement des cyberattaques, qui nourrissent la conscience collective de devoir revoir à la hausse le niveau de protection des données personnelles. Les révélations d'Edward Snowden aux débuts des années 2010 en sont le symbole.

Dans ce contexte, la directive a évolué le 25 mai 2018 en Règlement général sur la protection des données (RGPD), qui s'articule autour de cinq axes majeurs.

Le premier axe est le renforcement quantitatif et qualitatif du droit des personnes, une meilleure explication de la loi Informatique et Libertés, l'apparition de nouveaux droits, comme le droit à l'oubli, le droit à la portabilité et la possibilité de mener des actions de groupe.

Le deuxième axe est la responsabilisation de l'ensemble des acteurs de traitement de données, publiques et privées, sur la base de principes de minimisation de la collecte, de limitation de la durée de conservation et d'obligation de sécurité pour garantir à tout moment le respect du Règlement.

Le RGPD est d'ailleurs fondé sur la notion de risques présentés par les traitements, tant en volume qu'en sensibilité des données. En clair, plus l'acteur est important dans l'écosystème numérique, plus ses obligations et ses responsabilités sont nombreuses

Le troisième axe s'inscrit en contrepartie du précédent, par le renforcement du pouvoir de sanction administrative des différentes CNIL au niveau européen. Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial d'une entreprise, l'option majeure étant appliquée. La gamme des sanctions est également élargie.

Le quatrième axe est la mise en place d'un nouveau modèle de gouvernance de la régulation, inédit au niveau européen, au travers d'un guichet unique pour les entreprises et d'un guichet unique pour les citoyens. Si l'entreprise n'a qu'un seul interlocuteur, les décisions qui la concernent sont prises selon des principes de consensus et de coopération entre les différentes autorités nationales, afin de prononcer une décision applicable harmonisée à l'échelle européenne. En cas de désaccord entre les autorités, le nouveau Comité européen de la protection des données (CEPD), c'est-à-dire le groupe des CNIL européennes, arbitrera et prendra une décision contraignante vis-à-vis de l'autorité de l'établissement principal.

Le cinquième axe est le RGPD, qui a constitué une première étape décisive dans la souveraineté numérique, grâce à son principe de libre circulation des données sur l'ensemble du territoire de l'Union et son principe inédit d'extra-territorialité, selon lequel il s'applique à tous les acteurs dès lors qu'un organisme cible des citoyens européens. Il ne s'agit pas, pour l'Europe, de se livrer à du protectionnisme, mais d'affirmer un modèle de régulation fondé sur la défense du droit des personnes, héritée de la philosophie humaniste des droits de l'Homme, en vue de générer la confiance indispensable à la réussite de cette politique publique.

En outre, toutes les études récentes montrent une profonde aspiration de maîtrise des personnes sur leurs données. Ainsi, 87 % des Français se déclarent sensibles à la protection des données.

S'agissant des défis d'ordre stratégique, plusieurs modèles de régulation fondamentalement différents s'affrontent à l'échelle mondiale. Le RGPD est devenu un instrument de *soft power* de diplomatie. Nous constatons un avant et un après 25 mai 2018 au niveau mondial. Des pays ont procédé à la mise à jour de leur cadre national en matière de protection des données, afin de continuer à commercer avec l'Europe. Tel est le cas de la Suisse, du Japon, de la Corée du Sud, du Bénin ou de l'Australie. Des processus législatifs sont en cours dans d'autres pays comme la Tunisie ou le Burkina Faso. Des États ont, pour la première fois, adopté un cadre juridique général de protection des données personnelles comparable au RGPD dans ses principales dispositions. Tel est le cas de la Californie avec le *California Consumer Privacy Act (CCPA)* adopté en octobre 2018 et entré en application le 1er janvier 2020. Le Brésil a adopté son règlement en 2019. En Inde, la Cour suprême a consacré, en 2017, le droit à la protection de la vie privée comme un droit fondamental. Un projet de loi est en discussion au parlement.

En tout état de cause, le RGPD est un des rares textes dont nous parlons encore trois ans après son adoption, ce qui démontre que les échanges de données personnelles sont au cœur de toutes les discussions politiques au niveau international, au même titre que les règles en matière de concurrence ou de commerce.

Trois ans après la mise en œuvre du RGPD, quel bilan l'Europe peut-elle tirer ?

À l'échelle de la France, la CNIL en a véritablement constaté l'effet. Les citoyens se saisissent de leurs droits lorsque ceux-ci leur sont mieux expliqués. En 2019 et en 2020, nous

avons reçu environ 14 000 plaintes, ce qui représente une augmentation de 27 % par rapport à 2018, qui était déjà une année record.

En 2020, la crise sanitaire a fait émerger de nombreux enjeux. Les visites sur le site de la CNIL ont augmenté de 18 % en un an, ce qui témoigne de l'intérêt des citoyens pour ces questions au regard de l'actualité récente. Nous comptons aujourd'hui plus de 24 000 délégués à la protection des données, qui représentent plus de 72 000 organismes. Nous avons reçu près de 6 500 notifications de violation de données personnelles depuis 2018 et près de 1 200 dossiers en 2018, 2 300 en 2019 et plus de 3 000 dossiers en 2020. Ces dossiers permettent à la CNIL d'orienter son action de conseil et de répression et de mieux jouer son rôle dans l'écosystème de la cybersécurité.

En ce qui concerne la répression, la CNIL conduit environ 300 contrôles formels chaque année. Le nombre de mesures correctrices est en constante hausse. Après une période d'actions pédagogiques en 2018, la CNIL a prononcé une quinzaine de sanctions en 2020 (contre huit sanctions en 2019) pour un montant cumulé d'environ 139 millions d'euros.

À l'échelle européenne, la mise en œuvre de nouveaux modèles est clairement enclenchée, avec plus de 1 500 cas transfrontaliers identifiés, 550 procédures de guichet unique lancées avec nos homologues et plus de 190 décisions finales adoptées en application du mécanisme de coopération et de cohérence.

Fin 2020, une première décision contraignante a arbitré un différend entre l'autorité irlandaise et les autorités européennes concernant Twitter. Le CEPD a également ajouté une vingtaine de lignes directrices précisant le RGPD sur des notions essentielles, comme son champ d'application territorial, le ciblage des utilisations sur les réseaux sociaux ou le *privacy by* design – la protection des données dès la conception – contribuant ainsi à une véritable doctrine européenne en la matière.

À ce jour, la CNIL a prononcé plus de 550 sanctions représentant plus de 300 millions d'euros d'amendes.

Le RGPD a passé le test de la crise sanitaire, en évitant le détournement d'usage des données sensibles tout en se montrant suffisamment souple pour permettre aux États membres de traiter et de partager ce type d'informations dans un contexte exceptionnel.

Ces fondements posés, quels sont les axes prioritaires des années à venir pour renforcer la souveraineté numérique ? Ces axes relèvent de trois domaines : la cybersécurité, la politique industrielle et le cadre législatif européen.

Concernant la cybersécurité, il ne se passe pas un jour sans que ne nous soit signalée une attaque ciblant les réseaux de grands organismes publics ou privés, y compris ceux ayant des moyens financiers importants ou menant des activités particulièrement critiques.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a traité plus de 200 attaques en 2020 contre 50 en 2019. La plupart du temps, ces attaques prennent la forme de rançongiciels, qui paralysent le système d'information et demandent le paiement d'une rançon pour récupérer l'accès aux données. Ces attaques sont la première cause de recherche et d'assistance auprès du site cybermalveillance.gouv.fr.

La CNIL reçoit des notifications de violation de données. Elle vérifie la sécurité et accompagne les personnes et les PME, tandis que l'ANSSI traite plutôt de grandes failles ou d'actions particulièrement malveillantes.

Le deuxième levier d'action consiste à déployer une politique volontariste pour faire émerger les champions européens du numérique. Le respect de la vie privée et l'intégration du principe de *privacy by design* sont de véritables avantages concurrentiels pour les acteurs européens qui sauront s'en saisir, car ils répondent aux aspirations actuelles des consommateurs. La sécurité du *cloud* en est un bon exemple. En dépit de l'échec des premiers *clouds* souverains, la France défend une solution nationale ou européenne pour abriter les données sensibles et favoriser l'émergence d'un marché de confiance, en ajustant des offres déjà matures pour les mettre en conformité avec les standards de protection des données et de transparence des contrats. La CNIL entend suivre et accompagner ces initiatives, qui offrent une alternative viable aux géants du c*loud*, tant pour le fournisseur que pour le client.

Un exemple stratégique est l'hébergement des données de santé, qui doit être transféré sous deux ans vers une solution française ou européenne relevant exclusivement de la juridiction de l'Union européenne. Pour la CNIL, ce délai garantit un juste équilibre entre la préservation du droit à la protection des données personnelles et l'objectif de favoriser la recherche et l'innovation dans le domaine de la santé.

Le troisième levier d'action est la préservation de notre ordre juridique européen. La question du transfert des données est devenue prégnante en 2020 et plusieurs décisions législatives d'envergure ont été prises.

L'arrêt *Schrems* II, rendu le 16 juillet 2020 par la Cour de justice de l'Union européenne, a tout d'abord invalidé le bouclier de protection de données, le *Privacy Shield,* qui permettrait le transfert de données vers les États-Unis sans formalité supplémentaire. Le CEPD, le groupe des CNIL européennes, et la CNIL se sont emparés de cette décision, afin d'en tirer toutes les conséquences.

La Commission européenne a annoncé, fin 2020, sa stratégie de régulation de l'écosystème numérique européen. Le *Digital Market Act (DMA)* pose le principe de régulation économique en présentant un certain nombre d'adhérences avec le RGPD en matière d'obligations, d'interopérabilité des données, de transparence des traitements et de consentement explicite des consommateurs pour la mutualisation des données.

Le *Digital Services Act (DSA)* concerne la responsabilité des plateformes face à la souveraineté de l'État.

Le *Data Governance Act* (*DGA)* vise, quant à lui, à définir un cadre européen pour la réutilisation et le partage des données, qu'elles soient personnelles ou non. Ce texte ambitieux constitue le socle d'une future économie européenne de la donnée.

Pour conclure, le contexte actuel offre un alignement assez inédit des intérêts entre notre modèle de gouvernance de la donnée et notre politique industrielle. Il est essentiel que nous parvenions collectivement à nous en saisir pour mener une politique ambitieuse de souveraineté numérique européenne. Le RGPD est un facteur clé de cette ambition.

Je me tiens maintenant à votre disposition pour répondre à vos questions.

M. Philippe Latombe, rapporteur. Nos questions sont nombreuses.

Dans les récents arrêts *Schrems* de la Cour de justice européenne et la jurisprudence *Tele2 Sverige* et *Prokuratuu*r, il y a quelques semaines, qu'est-il autorisé et interdit aujourd'hui ? Les addendas ou les spécificités techniques sont-ils suffisants pour assurer la protection des données lorsque nous utilisons les *clouds* étrangers des GAFAM ? Quelle est la portée de l'extra-territorialité américaine réelle sur les filiales de ces grands groupes en Europe ?

Nous avons interrogé IBM, qui nous a répondu que les jurisprudences *Schrems* ne lui sont pas applicables en raison de ses filiales en France relevant du droit français. À la même question, Google et Amazon nous ont répondu, la semaine passée, que ces jurisprudences leur étaient évidemment applicables, malgré leurs filiales irlandaises.

Quelle est la position de la CNIL sur les données personnelles classiques et les données personnelles sensibles ? Cette demande émane aussi des entreprises, qui ne savent plus où elles en sont.

M. Gwendal Le Grand. Un avis sur la mise en œuvre de l'arrêt *Schrems* a été publié assez rapidement par le Comité des CNIL européennes pour consultation publique. Nous travaillons aujourd'hui sur sa version définitive. La CNIL et le CEPD ont également rédigé des questions fréquentes pour répondre aux entreprises.

Cette décision *Schrems* est cruciale sur trois plans. La Cour a reconnu la validité des clauses contractuelles-types de la Commission européenne comme outil de transfert. Elle a toutefois précisé que pour recourir à cet outil, il appartient à l'exportateur des données de vérifier que la législation applicable à ce transfert dans le pays tiers de destination n'aboutit pas à affaiblir le niveau de protection des données. À défaut, des mesures supplémentaires doivent être prises pour protéger les données. Enfin, la Cour a invalidé la décision concernant le bouclier de protection des données.

Le CEPD a publié des recommandations. Une consultation publique a été ouverte jusqu'en début d'année. Leur mise à jour est en cours pour tenir compte des nombreux commentaires reçus.

Concernant la question de l'accès aux données par les autorités américaines, l'une des premières questions à se poser pour déterminer si l'entité est sujette à l'extra-territorialité du droit américain est de savoir si la garde, la possession ou le contrôle des données concernées relèvent d'une société soumise au droit américain. Selon le *Cloud Act*, un responsable de traitement ou un fournisseur de communications électroniques ou de services informatiques distants, dont les traitements sont soumis au RGPD, pourrait devoir répondre à un mandat des autorités américaines en vertu du *Cloud Act*. Un sous-traitant de responsable de traitement américain, établi dans l'Union européenne, peut être destinataire d'un mandat des autorités américaines pour les données qu'il sous-traite.

La section 702 du *FISA* n'apporte pas de précision sur la portée extraterritoriale des ordres à produire, mais elle ne restreint pas ces demandes aux seules données stockées sur le territoire américain, ce qui implique un possible accès à des informations en dehors du territoire américain. Il n'y a donc pas de doute sur le caractère extraterritorial des acquisitions et des interceptions fondées sur l'*Executive Order* 12333.

L'utilisation des logiciels et de solutions techniques brevetés par des sociétés américaines n'est pas déterminante de la possibilité pour les autorités américaines de

contraindre des sociétés à divulguer des données, dès lors que ces solutions sont utilisées par des responsables de traitements qui ne sont pas soumis à la juridiction américaine. Il suffit de s'assurer que ces solutions techniques ne permettent pas un accès aux données par le biais de portes dérobées, intégrées par des développeurs à la demande des autorités américaines, notamment en application de la section 702 du *FISA*.

M. Philippe Latombe, rapporteur. Concrètement, Watson, un logiciel d'intelligence artificielle d'aide aux commerciaux, qui a accès aux bases de données pour préparer les réponses aux consultations des clients, est breveté par IBM Corp aux États-Unis et mis à la disposition de l'ensemble de ses filiales dans le monde. Watson constitue-t-il une porte d'extra-territorialité en Europe pour les États-Unis ? Watson est-il soumis au *Cloud Act* et éventuellement à la section 702 du *FISA* ?

M. Gwendal Le Grand. Pour répondre précisément, nous devrions observer la mise en œuvre de ce logiciel. D'une manière générale, si Watson est une solution logicielle mise en œuvre par un responsable de traitement européen non soumis à la législation américaine, la réponse est négative.

En revanche, si Watson traite de données par lui-même, la réponse est affirmative. Il convient de définir précisément la nature du logiciel et s'il est mis en œuvre, sans transfert de données, dans des systèmes informatiques d'une société européenne ou si des données sont adressées à l'intelligence artificielle de serveurs pouvant se situer aux États-Unis.

M. Philippe Latombe, rapporteur. Quelles sont les conséquences de l'arrêt *Schrems* appliqué aux données de santé ? Sur une sollicitation du Conseil d'État, vous avez émis un avis en faveur de migrations vers un *cloud* souverain, alors même que le Health Data Hub (HDH) applique les clauses contractuelles-types et des addenda signés avec Microsoft, sous couvert d'une localisation en Europe et d'une clé de chiffrement à laquelle Microsoft n'a pas accès.

M. Gwendal Le Grand. L'avis du Conseil d'État sur ce cas est très intéressant et il confirme l'analyse de la CNIL. Il convient de distinguer la question des transferts et le traitement des données par une société susceptible de recevoir des requêtes de la part des autorités américaines. Le Conseil d'État estime qu'il existe un risque d'accès par les autorités américaines, y compris en l'absence de transfert de données, du fait de la loi d'extra-territorialité américaine. De nombreux échanges ont ainsi porté sur la nécessité d'assurer un hébergement des données de santé, qui sont particulièrement sensibles, afin de garantir l'absence de risque d'accès par les autorités américaines.

M. Philippe Latombe, rapporteur. J'en déduis que cette décision serait applicable à d'autres données et d'autres systèmes utilisés par l'État et la sphère publique. Nous pouvons citer les *smart cities*, dans lesquelles une municipalité placerait les données des citoyens pour calculer le coût de la cantine ou de l'EHPAD.

M. Gwendal Le Grand. Le HDH concerne normalement un large volume de données particulièrement sensibles. Le raisonnement sur les possibilités d'accès par les autorités américaines du fait que le HDH est hébergé par un prestataire américain peut effectivement être appliqué à d'autres systèmes d'information.

M. Philippe Latombe, rapporteur. Le Conseil d'État a été saisi à propos de Doctolib. Considérez-vous également que les données de prise de rendez-vous pour la vaccination contre la Covid ne sont pas des données de santé ?

M. Gwendal Le Grand. Le Conseil d'État estime que la gestion des prises de rendez-vous, assurée par trois sociétés, dont Doctolib, et le fait d'être prioritaire pour la vaccination ne sont pas des données de santé. AWS et Doctolib ont conclu un addendum définissant une procédure précise en cas de demande d'accès aux données par une autorité publique. Cette procédure prévoit notamment la contestation de toute demande générale ou ne respectant pas la réglementation européenne. Ces sociétés ont, par ailleurs, mis en place un certain nombre de mesures techniques, dont un système de chiffrement fondé sur un tiers de confiance basé en France.

Le Conseil d'État a conclu que le niveau de protection des données ne pouvait pas être considéré comme manifestement insuffisant au regard du risque de violation du RGPD.

M. Philippe Latombe, rapporteur. Ma question était de savoir ce que le Conseil d'État considère comme une donnée de santé.

M. Gwendal Le Grand. Le Conseil d'État n'a pas expressément indiqué que les données relatives aux prises de rendez-vous ne sont pas des données de santé. Le communiqué de presse précise que le juge des référés du Conseil d'État relève que les données transmises à Doctolib dans la campagne de vaccination ne comprennent pas de motifs médicaux d'éligibilité à la vaccination, mais portent uniquement sur l'identité des personnes et la prise de rendez-vous. La définition d'une donnée de santé est donnée par l'article 4 du RGPD.

M. Philippe Latombe, rapporteur. Certains juristes considèrent que la décision du Conseil d'État n'est pas cohérente avec cette définition.

Vous avez récemment utilisé un procédé particulier pour sanctionner Google à propos des cookies au moyen d'un texte ancien, qui présente l'intérêt de ne pas entrer dans le champ de la régulation des CNIL européennes, dont le chef de file aurait été la CNIL irlandaise. Selon vous, celle-ci est-elle mal à l'aise vis-à-vis de grands groupes, qui se sont installés sur son territoire pour des raisons fiscales ? N'est-elle pas soumise à un conflit d'intérêts, qui l'empêche de sanctionner les GAFAM ?

M. Gwendal Le Grand. Fin décembre 2020, la formation restreinte de la CNIL a prononcé une sanction de 100 millions d'euros à l'encontre de Google LLC, Google Irlande et Amazon pour l'utilisation de cookies sur la base d'une législation largement appliquée. Cette directive de 2002 avait été révisée en 2009, puis en 2018 sous l'effet de la mise en application du RGPD. Cette législation n'est donc pas ancienne. Un accord a même été conclu récemment au Conseil pour qu'elle devienne un Règlement européen.

Cette directive traite notamment du stockage de cookies sur le terminal d'un utilisateur. Ce stockage doit faire l'objet d'une information et d'un consentement préalable. Cette directive est transposée en droit national dans tous les états membres. En France, la CNIL est chargée de contrôler l'application de cette règle et de sanctionner les éventuels manquements. Beaucoup d'actions ont d'ailleurs été engagées par la CNIL pour clarifier les règles en matière de dépôt de cookies. Des lignes directrices, qui ont d'ailleurs été attaquées

devant le Conseil d'État, et une recommandation ont été édictées. Les entreprises ont jusqu'à la fin du mois de mars 2021 pour se mettre en conformité.

La décision a été attaquée en référé par Google devant le Conseil d'État. Dans l'ordonnance du 4 mars 2021, le juge a rejeté la demande de suspension de l'exécution formulée par les sociétés Google LLC et Google Irlande d'une injonction prononcée par la formation restreinte des CNIL dans sa décision de décembre 2020.

Dans sa décision de référé, le Conseil d'Etat a confirmé que le mécanisme du guichet unique, institué par le RGPD, n'est pas applicable en matière de dépôt de cookies, dans la mesure où les règles qui le régissent sont prévues par la directive *ePrivacy*. L'autorité de protection des données nationales n'est, en effet, pas toujours compétente pour faire appliquer l'*ePrivacy*. L'autorité compétente peut être l'équivalent de l'ARCEP dans les autres pays européens. Il n'existe pas de coordination européenne dans les textes actuels. Seule une autorité nationale est compétente pour vérifier le respect de cette directive.

S'agissant de l'Irlande, l'organisme de régulation est face à un enjeu de crédibilité du modèle. Un certain nombre de décisions a déjà été pris pour activer tous les échelons du RGPD. Certains observateurs estiment que nous n'aboutissons pas suffisamment rapidement sur des projets de décisions irlandaises portant sur les acteurs majeurs de l'écosystème numérique. Certains estiment qu'il convient de changer les règles de gouvernance du RGPD.

Quant à elles, les autorités européennes pensent que le RGPD est un texte solide, qui mérite d'être conservé et accompagné dans son application, en renforçant la coopération entre les autorités et en leur donnant davantage de moyens. Si certains droits nationaux rendent difficile l'aboutissement à des décisions nationales, il appartient à la Commission européenne d'intervenir.

En tout état de cause, la CNIL souhaite renforcer l'efficacité de la coopération européenne en continuant à s'appuyer sur le RGPD, qui constitue une force de l'Europe dans toutes les négociations au niveau international. La CNIL contribue au renforcement de la coopération en utilisant tous les outils à sa disposition, comme les lignes directrices du CEPD sur la coopération européenne, qui clarifient les procédures, le RGPD ou les demandes d'assistance. En dernier recours, elle a la possibilité d'adopter des mesures d'urgence en cas d'atteinte grave au droit des personnes.

M. Philippe Latombe, rapporteur. De nombreux observateurs craignent l'existence d'un problème par rapport à la CNIL irlandaise et aux GAFAM, du fait de leur proximité et de l'intérêt économique que ces dernières représentent pour l'Irlande.

Les GAFAM ont l'habitude de faire de l'entrisme ou du lobbying. Le ressentez-vous à la CNIL ? D'autres CNIL européennes l'ont-elles évoqué ?

M. Gwendal Le Grand. Ces sociétés pratiquent évidemment du lobbying sur notre doctrine. Elles cherchent à participer aux consultations publiques, lors de la publication de lignes directrices par exemple, pour faire valoir leurs positions, mais les autorités de protection sont indépendantes dans la prise de leurs décisions. Les montants des sanctions sont d'ailleurs nettement plus élevés qu'avant 2018, puisque le plafond est passé de 150 000 euros à 3 millions d'euros, voire 4 % du chiffre d'affaires mondial d'une entreprise.

Il est essentiel d'assurer la solidité de nos décisions devant les juridictions, y compris pour l'Irlande. J'en veux pour preuve que nos décisions sont de plus en plus attaquées devant le Conseil d'État, voire la Cour de justice de l'Union européenne. Chacun respecte sa procédure nationale et peut être contraint par ses propres difficultés. La Commission européenne a aussi son rôle à jouer si des procédures nationales font obstacle à l'application du droit de l'Union européenne.

M. Philippe Latombe, rapporteur. Une suite d'arrêts de la Cour de justice de l'Union européenne, *Tele2 Sverige* et *Prokuratuur*, est actuellement devant le Conseil d'État. Même si elle concerne essentiellement l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), quelles conséquences en tirez-vous à la CNIL ?

M. Gwendal Le Grand. La CNIL se charge de faire appliquer les décisions de la Cour, qui relèvent de son champ de compétences. Une décision a, par exemple, été prise sur le droit à l'oubli par la Cour de justice de l'Union européenne. La CNIL applique la jurisprudence de la Cour. Elle n'a pas de position à émettre sur les décisions de la Cour de justice de l'Union européenne. Elle n'a d'ailleurs pas produit d'écritures en observations.

Concernant les cas de conservation des données de connexion, nous pouvons relever la constance des arrêts de la Cour, qui s'est prononcée de façon cohérente à plusieurs reprises, à plusieurs années d'intervalle, sur des sujets similaires.

M. Philippe Latombe, rapporteur. Si le Conseil d'État confirme la décision de la Cour de justice de l'Union européenne, vous serez *in fine* chargé de vérifier l'application de l'arrêt.

M. Gwendal Le Grand. Bien sûr, nous sommes dans un État de droit, dans lequel le législateur détermine des règles, qui peuvent être attaquées de différentes manières. La CNIL est chargée de faire appliquer la législation, parfois éclairée par des décisions de la Cour de justice de l'Union européenne.

M. Philippe Latombe, rapporteur. Compte tenu du volume, ne craignez-vous pas une rapide augmentation de la charge de travail ? Si le Conseil d'État confirme la décision de la Cour de justice de l'Union européenne, un certain nombre de procédures judiciaires s'en trouveront affectées. Les personnes mises en cause dans ces procédures pourraient saisir la CNIL pour demander l'application de l'arrêt du Conseil d'État.

M. Gwendal Le Grand. Je ne peux pas anticiper cette situation, qui est conditionnée par de nombreuses questions.

D'une manière générale, la CNIL continue de demander des moyens supplémentaires pour exercer convenablement ses missions. Nous sommes aujourd'hui 225 agents. À la fin de l'année 2021, nous serons 245, alors que les Anglais comptent entre 600 et 700 agents. Selon la Commission européenne, la France présente le troisième plus mauvais ratio pour son nombre d'agents de la CNIL rapporté au nombre d'habitants. Nos missions sont extrêmement larges, car la problématique des données personnelles est commune à toute l'économie numérique. Il est donc essentiel que l'autorité soit suffisamment dotée pour protéger les droits fondamentaux des citoyens.

M. Philippe Latombe, rapporteur. Comment entrevoyez-vous la suite avec vos homologues anglais après le mois de juin 2021 ? Le RGPD continue à s'appliquer jusqu'à cette date, mais la Grande-Bretagne pourra ensuite modifier son système de protection des données, en se rapprochant, par exemple, du modèle américain.

M. Gwendal Le Grand. Un projet de décision d'adéquation est en cours de discussion entre l'Europe et le Royaume-Uni pour pouvoir continuer à transférer des données sans formalité. Le CEPD a été saisi du sujet et doit se prononcer prochainement.

À ce jour, les données peuvent continuer à transiter, même si le Royaume-Uni ne fait plus partie du CEPD et ne relève plus du guichet unique. Une période de transition a été aménagée dans l'attente de la mise en œuvre de cette décision d'adéquation.

M. Philippe Latombe, rapporteur. En France, la carte nationale d'identité électronique et l'identité numérique sont largement évoquées. La CNIL est évidemment à la pointe sur cette question. Elle a rendu des avis sur la carte nationale d'identité et le système des titres électroniques sécurisés (TES) il y a quelques jours. Comment jugez-vous l'état d'avancement de la France dans ce domaine par rapport aux autres pays européens ?

M. Gwendal Le Grand. L'identité électronique recouvre plusieurs sujets. Un Règlement européen impose aux États membres de déployer une carte d'identité électronique avant août 2021. Dans ce contexte, le décret TES a été modifié pour permettre à l'État de créer de nouvelles cartes d'identité intégrant un composant électronique, dans lequel se trouvent des données biométriques en application d'un Règlement européen.

La question de l'identité numérique est plus large. Le gouvernement a porté plusieurs initiatives telles que FranceConnect et Alicem, sur lesquelles la CNIL a été amenée à se prononcer. Des textes ont ensuite été publiés pour contrôler leur application.

Un certain nombre de critères sont importants par rapport à l'identité numérique. Premièrement, une personne n'a pas besoin d'avoir une identité unique en ligne. Dans le monde réel, elle peut interagir avec un certain nombre de personnes, qui n'ont pas besoin de connaître l'ensemble des données de son état civil pour lui faire confiance et réaliser des transactions avec elle.

Deuxièmement, il existe un certain nombre de principes en termes de protection des données. Il s'agit tout d'abord de se demander qui peut voir les transactions que la personne réalise avec un acteur du privé et quelle est la nature des données présentées lors d'une authentification. Par exemple, pour s'inscrire à la bibliothèque, une personne doit seulement prouver qu'elle habite la commune sans forcément donner l'ensemble des attributs de son identité. De la même manière, pour accéder à certains services, elle aura besoin de fournir une preuve d'âge sans pour autant décliner son identité complète.

Ces principes doivent être portés par les solutions d'identité électronique. La CNIL n'est bien sûr pas opposée à un renforcement de la sécurité en ligne, qui est essentielle pour protéger les données personnelles et prévenir les risques d'usurpation d'identité, mais les solutions d'identité électronique ne doivent pas aboutir à une identité numérique unique, quel que soit le service auquel la personne souhaite accéder. Le respect des règles du RGPD et de la Loi Informatique et Libertés est indispensable.

M. Philippe Latombe, rapporteur. Pensez-vous que l'État à une bonne connaissance et un respect correct du niveau de protection des données ?

M. Gwendal Le Grand. Cette question est extrêmement large. Dans un État de droit, les textes sont appliqués, après avis du Conseil d'État et de la CNIL. En outre, des autorités contrôlent les fichiers mis en place par l'État.

Pendant la crise sanitaire, la CNIL a mené un travail spécifique pour accompagner à la fois les acteurs privés et les pouvoirs publics, en se prononçant sur SI-DEP, Contact Covid, le système d'information Vaccin Covid et à plusieurs reprises sur TousAntiCovid.

Courant 2020, la CNIL a ensuite réalisé une trentaine de contrôles sur les systèmes d'information mis en place par l'État dans la crise sanitaire. Elle doit donc avoir suffisamment de moyens pour être en mesure de répondre rapidement aux demandes, dans sa mission de conseil. Cet impératif s'est illustré pendant la crise sanitaire, période pendant laquelle elle a été extrêmement sollicitée pour se prononcer sur le recours au télétravail, les caméras de comptabilisation des masques, les drones, etc.

La CNIL fait face à des attentes fortes de la part des pouvoirs publics, du secteur privé et des parlementaires, qui ont besoin de connaître rapidement l'avis de la CNIL pour prendre position sur des questions souvent inédites.

La CNIL est une autorité dont l'indépendance est garantie par les textes et la constitution de la CNIL. Il lui arrive également de prendre des sanctions, y compris vis-à-vis d'acteurs du secteur public. Si ses moyens sont renforcés, elle pourra encore mieux exercer ses missions.

M. Philippe Latomb, rapporteur e. Votre pouvoir de sanction vis-à-vis de l'État est-il suffisant ? Je prends l'exemple des drones, sur lesquels vous avez eu une position très ferme vis-à-vis du ministère de l'Intérieur. Celui-ci continue toutefois à les utiliser, en vous renvoyant à votre simple pouvoir d'injonction. Vos pouvoirs de sanction ou d'interdiction doivent-ils être renforcés vis-à-vis de l'État ?

M. Gwendal Le Grand. Nous avons déjà d'importants pouvoirs de sanction. Notre priorité est de disposer de procédures de sanction simplifiées, notamment pour doter le président de la formation restreinte de la CNIL de nouvelles attributions dont l'exercice ne nécessite pas nécessairement l'intervention de l'ensemble du collège des sanctions. Cette configuration serait applicable aux seules affaires simples et de faible gravité et le montant des sanctions financières serait limité.

Aujourd'hui, toutes les affaires sont traitées avec le même niveau d'assurance juridique par la formation restreinte au complet.

Nous avons aussi, au-delà du pouvoir d'injonction, un poids sur le débat public. Les positions de la CNIL sont entendues et relayées. Ses positions peuvent d'ailleurs appuyer des recours devant les juridictions.

M. Philippe Latombe, rapporteur. Quelles sont, selon vous, les principales atteintes aux données ? Quelles sont les évolutions technologiques dont les atteintes en résultant pourraient vous donner le sentiment d'être désarmés ? Quelles évolutions législatives et réglementaires devraient être adoptées en urgence pour que vous puissiez continuer à exercer votre activité ? Je pense, par exemple, à l'intelligence artificielle.

M. Gwendal Le Grand. Nous avons identifié trois priorités en matière de contrôles en 2021 par rapport aux enjeux de protection des données : les cookies, la sécurité des données de santé et la cybersécurité.

Les cookies entrent dans le champ des lignes directrices, de la recommandation et des sanctions déjà évoquées. À compter de la publication des lignes directrices et de la recommandation en octobre 2020, nous avons donné aux entreprises un délai de six mois pour se mettre en conformité avec les nouvelles règles. Ce délai expire donc fin mars 2021. Dès lors, nous contrôlerons le respect de ces textes en matière de cookies.

Concernant la sécurité des données de santé, nous constatons le développement de systèmes d'information dans le domaine de la santé. Ils figuraient déjà dans notre programme de contrôle l'an dernier, mais ce dernier s'est décalé du fait de la crise sanitaire. Nous les avons donc à nouveau inscrits dans notre programme de contrôle. En pratique, nous menons des investigations sur les violations de données signalées à la CNIL et sur l'évaluation de la sécurité des établissements de santé et des laboratoires.

Enfin, s'agissant de la cybersécurité, nous nous attachons en particulier aux sites web, qui touchent le quotidien numérique des Français. L'objectif de nos contrôles est de monter le niveau de sécurité des sites web français les plus utilisés dans différents secteurs et relevant d'organismes de toutes tailles, publics comme privés. Nous portons une attention particulière aux formulaires de recueil de données à caractère personnel, à l'utilisation de la technologie « https » et au recours à des mots de passe suffisamment robustes.

Face à l'intelligence artificielle, nous ne sommes pas désarmés, mais cette technologie nécessite une meilleure interrégulation. En 2017, nous avons publié un rapport sur la façon de permettre à l'Homme de garder la main face aux algorithmes et à l'intelligence artificielle. Il est consultable sur le site de la CNIL. Il a fait suite à une série de débats engagés en 2017 et permet de dégager les principes applicables à l'intelligence artificielle, qui ont d'ailleurs été repris par divers forums de discussion au niveau européen et international.

Sur la reconnaissance faciale, la CNIL avait publié un rapport fin 2019, car cette technologie peut faire appel à l'intelligence artificielle.

L'une des spécificités de la CNIL est de posséder une expertise technique très pointue, qui lui permet de comprendre comment fonctionnent ces systèmes, afin d'être en mesure de les réguler correctement en appliquant, avec l'aide de ses juristes, des principes technologiquement neutres inscrits dans le RGPD.

M. Philippe Latombe, rapporteur. Le CSA a émis un avis indiquant que l'accès aux sites pour adultes, à caractère pornographique, ne peut pas être rendu uniquement possible en cochant une case pour certifier de sa majorité. Elle demande que soit trouvé un système robuste pour contrôler la majorité des personnes souhaitant y accéder.

Le CSA préconise un système de paiement avec une carte bancaire, même si en posséder une n'est pas forcément une preuve de la majorité. Les sites concernés ont lancé une grande consultation pour savoir ce que leurs utilisateurs accepteraient pour prouver leur majorité, depuis la photographie de la carte d'identité au moyen de la webcam jusqu'à l'obtention d'un numéro dans une institution publique. Toutes ces pistes portent atteinte à la protection des données personnelles. Avez-vous échangé avec le CSA ? Plus généralement,

quels sont vos rapports avec les autres autorités administratives, comme l'ARCEP, qui peuvent impacter les données ?

M. Gwendal Le Grand. Nous échangeons régulièrement avec les autres autorités administratives indépendantes. La CNIL est également saisie par l'autorité de la concurrence. L'interrégulation est primordiale, car les données personnelles sont utilisées dans tous les secteurs. L'interrégulation prend d'ailleurs corps dans les projets de texte au niveau européen.

Pour répondre à la question de la vérification de l'âge, le micropaiement n'est pas forcément efficace. En outre, le principe du RGPD de minimisation des données doit être respecté. Ainsi, les traitements nécessaires à la vérification de l'âge doivent être proportionnés aux risques pour les personnes concernées, en l'occurrence, les enfants.

Pour avoir vu le questionnaire de ces sites, j'ai pu constater que certaines méthodes proposées peuvent effectivement paraître très intrusives à leurs utilisateurs.

M. Philippe Latombe, rapporteur. À partir de ces exemples, pourriez-vous émettre spontanément des recommandations sur la méthode à employer auprès du CSA ?

M. Gwendal Le Grand. La question de la méthode de vérification de l'âge est actuellement étudiée par un groupe de travail, car elle se pose également pour l'accès des mineurs à des sites de réseau social.

Ce sujet est également européen. Une mesure d'urgence a été prise par notre homologue italien envers Tik Tok en ce qui concerne la vérification de l'âge. Il a été demandé à Tik Tok de modifier un certain nombre de paramètres par défaut pour vérifier que les utilisateurs ont l'âge requis pour s'inscrire à ce réseau social.

Cette question est techniquement difficile et la réponse dépend du contexte. En outre, ce sujet est de niveau européen.

M. Philippe Latombe, rapporteur. Vous avez été saisi par France Digitale d'une demande concernant Apple. Nous avons le sentiment que les « vilaines » GAFAM sont porteuses de tous les maux et que la souveraineté numérique serait de s'en affranchir. Capitalisent-elles vraiment le plus de risques et le plus de conflits ou s'agit-il d'un effet de loupe ? Est-il si difficile de leur faire comprendre la protection des données à l'européenne ? Sommes-nous si irréprochables vis-à-vis de nos entreprises ?

Nous entendons parler des Chinois uniquement par rapport à Huawei, mais peu par rapport à leurs applications de places de marché et de réseau social, alors qu'elles sont similaires à celles des GAFAM.

M. Gwendal Le Grand. En tant que régulateur, nous adoptons une approche indifférenciée vis-à-vis des acteurs. Les GAFAM sont majoritaires, tant en volume de données traitées qu'en nombre de plaintes qui nous sont adressées, leurs services étant massivement utilisés par les citoyens français. Nous traitons également les problématiques d'acteurs non américains. Tik Tok, par exemple, intéresse également les autorités nationales et européennes.

Encore une fois, des moyens dont nous disposons dépend le champ que nous sommes capables de couvrir au niveau européen. Vos exemples montrent la diversité des sujets auxquels nous sommes confrontés au quotidien, alors que nous ne sommes que 225 agents.

M. Philippe Latombe, rapporteur. Y a-t-il une question que nous n'avons pas abordée ?

M. Gwendal Le Grand. Non, je pense avoir couvert les principaux points.

Nous avons parlé du HDH, du développement d'un *cloud* souverain. La période nous offre une opportunité assez unique d'alignement des intérêts de politique industrielle et de protection des données. Ces problématiques se rejoignent, car le développement d'un *cloud* souverain nous permettra de conserver la maîtrise de nos données, de relever le niveau d'indépendance au niveau européen et de renforcer le niveau de cybersécurité des entreprises. Il servira ainsi nos droits fondamentaux et la protection des données. Toutes les déclarations des décideurs politiques sur la politique industrielle, la protection des données et le plan de relance vont dans le sens d'un meilleur contrôle, par la France et par l'Europe, des données traitées dans les infrastructures informatiques.

Nous devons profiter de cet alignement d'intérêts pour collectivement nous atteler au développement de solutions nous permettant d'être plus efficaces et plus agiles dans un environnement cyber plus sécure.

M. Philippe Latombe, rapporteur. Merci pour le temps que vous nous avez consacré et pour vos réponses. Nous sommes preneurs de vos futures contributions si vous avancez sur la protection des données de santé et d'autres sujets d'actualité.

M. Gwendal Le Grand. Nous nous tenons à votre disposition pour vous fournir des informations complémentaires sur les décisions de la CNIL. Nous vous adresserons les réponses au questionnaire dans les prochains jours.

M. Philippe Latombe, rapporteur. Lors des auditions avec les chercheurs en santé, ils ont formulé un souhait d'une plus grande rapidité et d'une meilleure fluidité dans le traitement de leurs demandes d'accès au SNDS. Il serait intéressant de leur transmettre un mode d'emploi simplifié.

M. Gwendal Le Grand. Dans le domaine de la recherche en santé, de nombreuses procédures simplifiées existent. Dans la plupart des cas, il n'est pas nécessaire d'obtenir une autorisation de la CNIL, tant que la demande est déclarée conforme à la méthodologie de référence. Des instruments génériques fluidifient effectivement les traitements.

Dans le cas de la crise Covid, nous avons mis en place une procédure spécifique pour autoriser les recherches le plus rapidement possible. Plus de 90 % des recherches impliquant la personne humaine ont pu être mises en œuvre, sans avoir à constituer un dossier auprès de la CNIL, sous couvert de leur conformité à une méthodologie de référence. Par ailleurs, sur près de 50 % des dossiers, l'autorisation a été délivrée en moins de deux jours.

Je rappelle à ceux qui estiment que la CNIL se montre un peu trop tatillonne vis-à-vis des données de santé que les fuites de données ont des conséquences lourdes. Un fichier contenant les données de 500 000 patients de laboratoires a récemment été découvert libre d'accès sur Internet. Or le domaine de la santé est particulièrement sensible.

M. Philippe Latombe, rapporteur. Mon propos visait simplement à vous engager à rappeler les bonnes pratiques, pour que les chercheurs n'aient pas ce sentiment.

La séance est levée à 11 heures.

Membres présents ou excusés

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

Réunion du jeudi 25 mars 2021 à 9 heures 30

Présents. – Mme Danièle Hérin, Mme Amélia Lakrafi, MM. Philippe Latombe, Denis Masséglia, Jean-Luc Warsmann