Colloque Privacy Symposium 2024, Venise, Italie

Discours de Marie-Laure Denis, Présidente de la CNIL

Lundi 10 juin 2024

Seul le prononcé fait foi

Monsieur le Président, cher Sébastien ZIEGLER,
Madame la Présidente du Comité européen de la protection des données, chère Anu TALUS,
Monsieur le Président de la Garante, cher Pasquale STANZIONE,
Maître, chère Shirin EBADI,
Mesdames, Messieurs,

Je suis heureuse d'être parmi vous aujourd'hui et de pouvoir contribuer aux travaux de cet événement majeur que constitue le Privacy symposium.

Je remercie Sébastien ZIEGLER pour son invitation et l'opportunité qui m'est ainsi donnée d'échanger avec des acteurs de la protection des données venant du monde entier.

Ici à Venise, je veux saluer les actions menées par la Garante, autorité italienne de protection des données, et son Président, Pasquale STANZIONE.

Je tiens également à remercier Anu TALUS, pour son implication en tant que Présidente du CEPD.

Je veux enfin rendre hommage à Shirin EBADI, magistrate et avocate, et à qui a été décerné le prix Nobel de la paix (2003) pour récompenser son investissement en faveur de la démocratie et des droits humains.

Le développement du numérique et l'émergence d'un espace d'interaction permanent représente une évolution majeure. Cette transformation a modifié l'ensemble des activités humaines, faisant du numérique un élément essentiel du processus de mondialisation. Ce nouvel espace, en constante évolution, produit nécessairement un effet sur les droits humains, justifiant une attention particulière afin que les innovations qu'il porte servent nos valeurs démocratiques.

À cet égard, la question de la protection de la vie privée revêt une importance accrue dans ce nouvel environnement dans lequel les frontières sont abolies et où la donnée, personnelle ou non, circule constamment.

Plus le cybermonde se développe, plus il devient un enjeu de pouvoir, en étant à la fois une opportunité de promotion des libertés fondamentales mais aussi de manipulation et de contrôle des populations.

Depuis les années 70 et l'émergence de l'informatique, la collecte massive de données voit converger les intérêts des grandes entreprises du numérique et des gouvernements.
Les entreprises, pour asseoir un modèle publicitaire, les gouvernements, pour assurer la sécurité et/ou le contrôle des citoyens. Dans les deux cas l'ambition est la même : prédire les comportements.

Ainsi, s'il est fréquent d'indiquer que l'information c'est le pouvoir, je suis convaincue que, désormais, à l'ère numérique, le pouvoir c'est la donnée.

À chaque instant, des millions d'individus laissent des traces de leur activité numérique. Elles permettent de cerner leurs goûts et leurs centres d'intérêts. Mais aussi, plus souvent qu'on ne le pense, leurs convictions politiques ou religieuses, leurs relations amicales, leurs déplacements ainsi que leur état de santé.

C'est pourquoi, dans cet environnement, le respect de la vie privée joue un rôle essentiel.

À l'ère numérique, la protection des données personnelles des citoyens, est le terreau d'autres libertés.

Afin d'illustrer mon propos, je vous propose d'examiner la question des interactions entre la vie privée et la démocratie sous trois angles, d'abord celui du droit de vote, ensuite celui de la liberté de circulation et, enfin, celui de l'exercice de la liberté d'expression dans l'espace numérique.

1. Pour Abraham Lincoln, *« La démocratie est le gouvernement du peuple, par le peuple, pour le peuple »*.

Le citoyen se trouve au cœur du système démocratique et, pour exprimer ses choix lors d'élections, il doit pouvoir disposer d'une information objective pour prendre une décision éclairée. Mais, en tant qu'internaute, il s'expose à ce que ses données personnelles soit collectées et exploitées, sans son consentement, dans le but de l'influencer à l'approche d'une élection et de fausser les résultats du vote.

L'affaire Cambridge Analytica, révélée en 2018, a démontré les risques que pouvaient représenter, le recours à des pratiques opaques de traitement de données à caractère personnel qui aboutissaient, au ciblage politique des internautes, ouvrant la porte à la manipulation de l'opinion et à l'ingérence de puissances étrangères.

Dans le prolongement de ce scandale, le RGPD a renforcé la protection des données des citoyens et les pouvoirs des autorités de protection, y compris, en matière de prospection politique. La numérisation des campagnes politiques s'est accompagnée d'une prise de conscience aigüe, par les électeurs, de l'utilisation faite par les partis et les candidats de leurs données. Néanmoins, les citoyens restent vulnérables C'est un enjeu à la fois pour préserver la confiance des citoyens et pour protéger la vie démocratique.

Les autorités nationales, et en particulier les autorités de protection des données personnelles, ont donc un rôle à jouer pour protéger le processus démocratique électoral en s'assurant de l'effectivité du droit qu'ont les citoyens de recevoir des informations objectives, ouvertes et pluralistes.

Ce rôle a encore été récemment renforcé par le règlement européen relatif à la transparence et au ciblage de la publicité à caractère politique adopté le 11 mars dernier et qui prévoit que la publicité politique devra désormais être clairement identifiée et reposer sur le consentement, ce qui facilitera nos contrôles.

À cet égard, en France, la CNIL se mobilise, à chaque période électorale, pour contrôler les traitements de données personnelles dans le cadre des opérations de prospection politique.

Tout d'abord, en amont de chaque élection, nous demandons à toutes les parties prenantes, notamment les groupes politiques, les candidats et les plateformes en lignes, de prendre en compte la protection des données personnelles dans leurs pratiques.

Nous leur transmettons des ressources pédagogiques pour appuyer leur mise en conformité et nous mettons également à disposition des citoyens des contenus en ligne pour les informer sur leurs droits.

Ensuite, à l'approche de l'élection, comme pour les élections européennes d'hier, la CNIL réactive un observatoire des élections qu'elle a initié en 2012.

Il s'agit d'une plateforme en ligne, exclusivement dédiée à recueillir les signalements des citoyens, en lien avec les traitements de données personnelles effectués pour les élections.

Lors des dernières élections présidentielle et législatives de 2022, la CNIL a ainsi reçu plus de 3000 signalements concernant des pratiques de prospection par appel téléphonique automatisé et SMS.

Ces signalements lui ont permis de conduire des investigations et d'adopter des mesures correctrices à l'encontre de certains candidats ou partis.

Pour les élections européennes, nous avons été particulièrement attentifs à l'impact de l'utilisation de l'intelligence artificielle dans les stratégies de communication politique, la

multiplication des hypertrucages et le recours au profilage et ciblage des électeurs par des algorithmes de recommandation.

Enfin, à côté des risques liés à la prospection et au ciblage politique, recours au vote électronique doit garantir que les solutions de recueil des votes répondent à un haut niveau de fiabilité et de sécurisation.

À défaut, en cas de dysfonctionnements, la sincérité et la fiabilité du vote sont remises en cause.

Pour ces raisons, la CNIL a jugé utile d'adopter, en 2019, une recommandation qui porte sur la sécurité de ces systèmes.

À ce jour, les travaux ainsi que les investigations que nous avons menés nous amènent à considérer que le vote électronique peut être envisagé pour des élections professionnelles, afin de faciliter l'organisation et le déroulement du scrutin.

En revanche, des risques importants nous semblent peser sur la sincérité du scrutin, comme le traçage des connexions, l'interception des messages et de possibles ingérences extérieures, lorsque de tels systèmes sont déployés pour des élections politique à échelle nationale

2. **Je voudrais maintenant évoquer : la liberté de circulation des personnes dans l'espace public**.

Les Etats, le plus souvent pour garantir la sécurité des citoyens, recourent à des technologies de surveillance qui, lorsqu'elles sont mal encadrées, peuvent aboutir à limiter la liberté de circulation.

Je pense, notamment, aux dispositifs de vidéoprotection qui, par leur omniprésence et leur intrusivité, font partie des systèmes comportant le plus de risques pour la vie privée.

En effet, les images captées et les données associées révèlent, où nous sommes, à quel moment, avec qui et ce que nous faisons. Les récentes évolutions technologiques viennent encore augmenter la masse des informations collectées : identification en temps réel par couplage à de la reconnaissance faciale ou analyse algorithmique des comportements.

Nous nous souvenons tous de l'affaire Snowden, en 2013, et l'indignation internationale qu'a causé la révélation publique des activités de surveillance massive, systématique et sans distinction, auxquelles se livraient les services de renseignement aux Etats-Unis et en Europe.

En France, la CNIL s'est prononcée à plusieurs reprises sur des dispositifs législatifs permettant d'accroitre le recours aux dispositifs vidéo, notamment sur la voie publique, qui est le lieu où s'exercent des libertés publiques comme le droit d'aller et venir, le droit de manifester ou l'accès à des lieux de cultes.

La CNIL a considéré qu'un débat sociétal était souhaitable autour de l'utilisation des nouvelles technologies vidéo, en particulier celles impliquant le recours aux algorithmes et à l'intelligence artificielle.

Le déploiement des caméras augmentées, a suscité un large débat, en France, dans le cadre de l'organisation des prochains Jeux olympiques et paralympiques de Paris (JOP) de cet été.

Les garanties prévues par la loi ont permis de limiter les risques d'atteinte aux données et à la vie privée des personnes et vont dans le sens des préconisations formulées par la CNIL.

La loi a ainsi encadré strictement le recours à la vidéosurveillance algorithmique pour 8 cas d'usage précis correspondant à des risques graves pour les personnes. Elle prévoit également que ces dispositifs sont expérimentaux, limités dans le temps et l'espace, ne procèdent pas au traitement de données biométriques et n'entraînent pas de décision automatique, une analyse humaine restant toujours nécessaire.

Pendant cette expérimentation, qui a débuté en septembre 2023 à l'occasion de l'organisation en France de la Coupe du monde de rugby et qui s'achèvera le 30 juin 2025, la CNIL procède à des contrôles sur le terrain, notamment pour vérifier le caractère nécessaire et proportionné de ces dispositifs.

Sur ce dernier point, la CNIL estime que, d'une manière générale, la surveillance opérée par ces technologies réduit considérablement l'anonymat dont disposent les citoyens dans l'espace public et qu'il est nécessaire de fixer des lignes rouges, par exemple pour ne jamais utiliser ces caméras à des fins de « notation » des personnes.

3. **Je veux, pour finir, aborder la question de** la protection de la vie privée sur internet et ses enjeux dans une société démocratique.

Tout d'abord, je crois important de rappeler que l'anonymat en ligne n'existe pas, techniquement, et qu'on doit plutôt parler de pseudonymat, notamment pour les réseaux sociaux.

En effet, si l'utilisation des réseaux sociaux peut reposer sur l'usage par les utilisateurs de pseudonymes et de coordonnées fournies sur une base déclarative, il est possible, dans la plupart des cas, pour les autorités publiques, de retrouver l'identité des auteurs d'infraction à partir de leurs données de connexion.

Comme les autres autorités de protection des données, la CNIL est régulièrement interrogée sur sa position entre « sécurité » en ligne et « droit à l'anonymat », en particulier à la suite des campagnes de violence et de haine en ligne que connaît notre pays, comme beaucoup d'autres.

Des initiatives politiques, au niveau national ou européen, plaident pour que certains services, et notamment les réseaux sociaux, soient contraints de recueillir, au moment de la

création d'un compte, une copie d'un document d'identité pour pouvoir l'utiliser en cas d'infraction.

Dans l'espace numérique, comme dans le monde physique, il faut des règles pour encadrer et réguler les comportements. Plusieurs réglementations récentes permettent aujourd'hui de mieux lutter contre les contenus illicites publiés en ligne, en instaurant des mécanismes destinés à obtenir la suppression de ces contenus et l'identification de leurs auteurs.

Le DSA met en œuvre le principe selon lequel, ce qui est illégal hors ligne est illégal en ligne. Ces règles responsabilisent les plateformes numériques et permettent de lutter contre la diffusion de contenus illicites ou préjudiciables. L'objectif est de mieux protéger les internautes européens et leurs droits fondamentaux.

En France, une loi récente de mai 2024 prévoit de nouvelles sanctions pour condamner la haine en ligne et le cyberharcèlement. Elle introduit une peine pénale de bannissement des réseaux sociaux pour 6 mois. Ces dispositifs permettent de préserver le pseudonymat en ligne - et ainsi le droit à la liberté d'expression et à la vie privée - tout en permettant de lutter contre la publication de contenus illicites.

Le recours au pseudonymat en ligne doit donc demeurer une liberté fondamentale de l'utilisateur dans la mesure il constitue une composante essentielle de la protection de la liberté d'expression et du respect de la vie privée. Revenir sur cette possibilité pour toutes les utilisations des réseaux sociaux aurait, en revanche, un impact majeur, en réduisant la liberté d'expression, en rendant des personnes vulnérables en raison de leurs sujets d'intérêt en ligne, voire en facilitant leur discrimination.

À cela s'ajoute le fait que la plupart des grands acteurs du numérique ne sont pas européens. Renforcer l'identification en ligne en imposant la collecte de données d'identification robustes, voire de documents d'identité, soulève de sérieuses questions. Accepterions-nous que des puissances étrangères, via les acteurs économiques concernés, aient accès, de manière massive aux données de citoyens européens contenues dans les documents d'identité ? Prendrions-nous le risque d'usurpations d'identités qui peuvent résulter du piratage informatique de ces acteurs et de la réutilisation de nos données d'identité ? L'équilibre est délicat, et se façonne progressivement : il ne faut agir en cette matière qu'avec une grande prudence.

Il en va de même en ce qui concerne la tentation de s'attaquer au chiffrement de bout en bout de nos communications électroniques quelque soient les causes, parfois très légitimes, poursuivies. Il faut prendre garde qu'en affaiblissant la possibilité de communiquer de façon confidentielle, pour lutter contre tel ou tel type de délit ou de crime, on repousse parfois les délinquants vers d'autres canaux de communication tout en dégradant la situation du plus grand nombre et en portant atteinte à cette liberté de communication. Or j'aime à citer cette phrase souvent répétée dans la jurisprudence du Conseil constitutionnel français : « La liberté d'expression et de communication (…) est d'autant plus précieuse que son exercice est

une condition de la démocratie et l'une des garanties du respect des autres droits et libertés (v. par ex. CC, 4 avril 2019, n° 2019-780).

En conclusion, j'observe que la protection de la vie privée et la démocratie forment un couple en tension dans le monde numérique. Si nous n'assistons ni à la fin de la vie privée ni au déclin de nos démocraties, nous devons néanmoins avoir conscience que l'une et l'autre peuvent être menacées au gré des avancées technologiques.
La protection de la vie privée et la démocratie ont un destin intimement lié, l'une protégeant l'autre et vice versa. Il nous appartient à toutes et à tous de les défendre activement.

Je vous remercie.