100
QUESTIONS/RÉPONSES

LE BON USAGE DU NUMÉRIQUE

Comment s'en servir, pour soi et pour les autres

Audrey Damiens
Jimmy Bordarie
Anne-Laure Sweiker

ellipses

L'ÉTHIQUE NUMÉRIQUE

1 Qu'est-ce que le numérique ?

La société contemporaine est assez largement numérisée : tout ou presque, du personnel, au professionnel en passant par la citoyenneté – au sens des services publics, ou encore de l'administration – passe par le numérique aujourd'hui.

■ Définitions du numérique

Le numérique est rentré dans notre vocabulaire depuis de nombreuses années déjà. Mais de quoi parle-t-on exactement ? Initialement, le terme « numérique » renvoie au nombre. Ainsi, le numérique correspond à une partie des mathématiques, de la physique et des sciences cognitives. Y est ajouté, et c'est évidemment la partie la plus évidente dans l'utilisation quotidienne du terme « numérique », l'informatique, celle-ci étant à l'origine une branche des mathématiques, et fonctionnant par une logique numérique binaire. Tel qu'on l'entend aujourd'hui, son périmètre est cependant bien plus large : robotique, intelligence artificielle, les réseaux et l'ensemble des logiciels, ressources, équipements…

Le numérique modifie grandement notre environnement social et culturel. Il inquiète autant qu'il donne certains espoirs d'avancées, d'améliorations. Pour certains, c'est même devenu le principal espace de nos actions. Certains auteurs parlent alors de culture numérique, ou de fait social total en ce qu'il change l'ensemble de la société.

■ Numérique ou digital ?

Étymologiquement, le terme « digital » renvoie à ce qui se rapporte au doigt : les empreintes digitales sont celles que l'on a au bout des doigts ! À s'en tenir à l'étymologie, le terme « digital » ne devrait être utilisé que pour les technologies numériques qui utilisent le doigt pour fonctionner, comme les smartphones et leurs applications ou encore les ordinateurs tactiles. L'utilisation du terme « digital » pour désigner l'ensemble du numérique est donc, du point de vue de la langue, erroné. Il s'agirait d'un anglicisme, le terme *digital* étant plus large en anglais qu'en français. L'Académie française lutte contre la confusion depuis longtemps déjà. Officiellement, le législateur a même publié au journal

officiel du 9 mars 2021 une liste du vocabulaire de l'informatique tel qu'il devrait être utilisé, et le terme « numérique » apparaît comme la traduction unique du terme anglais *digital*.

Pour certains, la différence est ailleurs. Elle se situerait plutôt du côté du point de vue. Ainsi, le numérique renverrait aux technologies de base, comme un smartphone et les applications que l'on peut y trouver. Digital aurait trait à ses usages et aux phénomènes qui y sont liés, comme le marketing digital qui empruntent les canaux numériques, ou encore l'utilisation par un adolescent, par exemple, de son smartphone au quotidien.

Dans le langage courant, numérique et digital sont toutefois souvent utilisés sans distinction, comme synonymes qu'ils ne sont pourtant pas malgré leurs liens indéniables.

2 Qu'est-ce que l'éthique numérique ?

Le numérique inquiète autant qu'il donne certains espoirs. Certaines pratiques non éthiques sont considérablement amplifiées, comme la propagation de rumeurs. Le numérique est donc un espace particulier qui renouvelle les questions éthiques classiques, l'éthique étant un questionnement sur ses actions, et les (re)met sur le devant de la scène. L'éthique numérique est dès lors une réflexion qui a une grande importance dans nos sociétés actuelles.

■ Les deux voies possibles de l'éthique numérique

La première voie possible consiste à appliquer les principes éthiques classiques au contexte du numérique. Il n'existe pas une liste définie de principes à appliquer, l'éthique est plus un questionnement. Mais certains reviennent souvent : l'autonomie, la bienveillance, la non-malfaisance, la justice, l'intégrité, la responsabilité… Il s'agira alors de réfléchir aux conséquences spécifiques de l'utilisation du numérique au regard de ceux-ci : c'est l'éthique de l'usage.

La seconde consiste à développer des principes éthiques spécifiques au numérique ou à reconsidérer complètement les normes habituelles, comme la transparence ou le droit au respect de la vie privée et le droit à l'image, sous le prisme du numérique. Le numérique vient créer des dilemmes éthiques qui lui sont propres, et qui ne relèvent pas seulement des conséquences de son utilisation. Il n'y aurait alors pas forcément que des utilisations bonnes ou mauvaises à partir de technologies neutres, mais des technologies en elles-mêmes porteuses de questionnements éthiques qui doivent attirer l'attention. Dans la lignée, l'éthique ne devrait pas être envisagée *a posteriori*, mais *a priori*, lors de la conception même des nouvelles technologies : c'est l'éthique de la conception.

■ Les grands domaines de l'éthique numérique

Les réflexions d'éthique numérique peuvent être regroupées en trois domaines.

Le premier est celui de la protection des données personnelles. Lorsque vous utilisez des services numériques, des données personnelles sont souvent demandées ou récupérées malgré vous pour être réutilisées,

notamment à des fins commerciales. C'est une question éthique dans la mesure où les utilisateurs n'ont plus forcément la main, sans toujours le savoir, sur leurs données (voir questions 4 à 18).

Le deuxième domaine est celui de la protection de l'environnement et des aspects écologiques du numérique. L'utilisation de l'Internet représenterait 3 à 4 % d'émission de gaz à effets de serre dans le monde (rapport de l'ADEME – Agence de l'environnement et de la maîtrise de l'énergie – et de l'ARCEP – Autorité de régulation des communications électroniques, des postes et de la distribution de la presse – de janvier 2023). Le numérique et l'Internet polluent, et une réflexion éthique sur ce point est nécessaire (voir questions 98 à 100).

Le troisième domaine est celui de l'intelligence artificielle qu'elle soit générative (par exemple, *ChatGPT*) ou non (par exemple, *Google Lens* qui permet de faire une recherche à partir d'une photo). Son développement contemporain rapide met en avant de nombreux questionnements éthiques (voir questions 45 à 74).

Ces trois domaines ne sont pas cloisonnés, et des questionnements éthiques peuvent surgir à la croisée de plusieurs. Pour ne prendre qu'un exemple, les premières plaintes en France auprès de la CNIL (Commission nationale de l'informatique et des libertés, voir question 18) à propos de *ChatGPT* le sont à propos de la protection des données personnelles, mêlant ainsi l'éthique de l'intelligence artificielle à l'éthique numérique relative à la protection des données. D'autres questionnements éthiques, spécifiques à certains domaines numériques, peuvent également éclore çà et là.

3 Qu'est-ce que le comité consultatif national d'éthique du numérique ?

À l'image du Comité consultatif national d'éthique pour les sciences de la vie et de la santé (CCNE), créé en 1983, juste après la naissance du premier « bébé-éprouvette », la France s'est récemment dotée d'un Comité consultatif national d'éthique du numérique (CCNEN).

■ Naissance du comité

Initialement, l'émergence de questions d'éthique du numérique a conduit, en 2019, à ce qu'un Comité national pilote d'éthique du numérique (CNPEN) soit constitué sous l'égide du CCNE pour une durée de deux ans. Ce Comité était composé d'un directeur, Claude Kirchner, de 26 membres bénévoles spécialistes du numérique, dont cinq membres du CCNE. Il était organisé à partir de groupes de travail destinés à préparer des avis rendus par le Comité après saisine par une institution ou une autorité ou autosaisine, ou à constituer un observatoire de thématiques émergentes ou en évolution. Il a notamment produit neuf avis (sur les voitures autonomes, le diagnostic médical et l'intelligence artificielle, ou encore les agents conversationnels par exemple), un manifeste pour une éthique du numérique, et deux ouvrages.

Déjà renouvelé, le Président de la République a annoncé sa pérennisation en tant qu'organisme indépendant dans un discours en 2023. Sa création officielle a été actée dans un décret en date du 23 mai 2024, complété par un décret du 25 février 2025. Il prend le nom de Comité consultatif national d'éthique du numérique.

■ Organisation et missions du Comité

Le Comité est constitué d'un Président et de 20 membres. Le Président a été nommé par le décret de 2025 : Claude Kirchner poursuit ainsi les fonctions qu'il exerçait dans le Comité pilote. Les 20 autres membres sont des membres des juridictions supérieures françaises (Conseil d'État et Cour de cassation), des personnalités spécialistes nommées par les différents ministères concernés (numérique, sécurité intérieure, recherche, santé…), des scientifiques appartenant à des institutions nationales (Académie des Sciences, CNRS, France Université…), des

personnalités spécialistes membres des comités nationaux proches (CCNE, Commission nationale de l'informatique et des libertés, et Conseil national du numérique) et enfin des représentants de la société civile. Les premières nominations ont eu lieu en septembre 2025. On y retrouve ainsi des personnalités telles qu'Alexei Grinbaum, Yannick Meneceur, ou encore Célia Zolynski pour n'en citer que quelques uns.

Les possibilités de le saisir sont très larges. Il peut l'être directement par le Président de la République, le Premier ministre, le président de l'Assemblée nationale, le président du Sénat ou un membre du Gouvernement, ainsi que par un établissement d'enseignement supérieur, un établissement public ou une fondation reconnue d'utilité publique (à condition d'être en lien avec la recherche ou le numérique). Mais le comité peut également s'autosaisir soit directement (questions posées par l'un ou plusieurs de ses membres), soit après avoir été interrogé par toute personne. Aussi, il est permis à tout citoyen de soulever des questions d'éthique du numérique auprès du CCNEN afin qu'il se prononce.

Aux termes du décret, la mission du CCNEN est « de donner des avis sur les questions d'éthique soulevées par les avancées des sciences, technologies, usages et innovations dans le domaine du numérique, et de leurs potentiels impacts, notamment sociaux, économiques, environnementaux ou éducatifs ». À cette fin, il formule des recommandations, des avis, organise des débats ou ateliers ou encore échange sur les questions avec les autorités étrangères.

ÉTHIQUE NUMÉRIQUE ET DONNÉES PERSONNELLES

4 Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) est un règlement de l'Union européenne entré en application le 25 mai 2018 qui a pour objectif la protection des données à caractère personnel (DCP). Il est constitué de 11 chapitres, et recense 99 articles qui définissent les principes, droits, obligations et mécanismes relatifs au traitement de ces DCP. Il remplace la directive 95/46/CE de 1995 qui était jusqu'alors en vigueur.

■ Objectifs généraux du RGPD

En renforçant les droits des personnes concernant leurs DCP, le RGPD vise à donner plus de contrôle et un pouvoir décisionnel aux personnes afin notamment de répondre aux nouveaux enjeux que pose le numérique avec l'avènement du Big Data (traduit par « données massives » correspondant à un ensemble de données trop volumineux et complexe pour les applications traditionnelles de traitement), de l'intelligence artificielle et des réseaux sociaux par exemple. Ainsi une personne peut désormais récupérer ses données et être informée de ce qui en est fait, en demander l'effacement et retirer son consentement à ce qu'elles soient traitées (voir questions 10 à 15).

En responsabilisant l'ensemble des acteurs, le RGPD implique une responsabilité proactive des acteurs traitant des données en leur imposant la mise en place de règles strictes, dont elles doivent pouvoir attester et démontrer leur mise en place. Parmi ces règles, nous pouvons citer la tenue d'un registre des traitements, la réalisation d'analyses d'impact pour les traitements sensibles, l'application d'un principe de respect de la vie privée dès la conception et par défaut, et dans certains cas, la nomination d'un délégué à la protection des données (DPO).

En harmonisant les règles dans l'Union européenne, le RGPD devient un cadre juridique appliqué dans les 27 pays de l'Union permettant de créer un espace numérique unifié et sécurisé qui facilite notamment les activités transfrontalières et réduit les coûts en simplifiant les démarches pour les entreprises européennes et internationales.

En favorisant la confiance en une économie numérique, le RGPD permet notamment un avantage concurrentiel grâce à la protection des DCP. Ainsi, l'objectif est double : d'une part, renforcer l'innovation et l'investissement tout en favorisant l'adoption de pratiques éthiques concernant l'usage de services numériques, et d'autre part éviter certaines dérives.

■ Principes fondamentaux du RGPD

L'article 5 (1) du RGPD énonce six principes fondamentaux relatifs au traitement des DCP qui doivent être (1) « traitées de manière licite, loyale et transparente », (2) « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités », (3) « adéquates, pertinentes et limitées à ce qui est nécessaire », (4) « exactes et, si nécessaire, tenues à jour », (5) « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » et (6) « traitées de façon à garantir une sécurité appropriée des données à caractère personnel ».

L'article 5 (2) ajoute par ailleurs le principe de responsabilité et stipule que « le responsable du traitement est responsable du respect [des six principes mentionnés] et est en mesure de démontrer que celui-ci est respecté ». Il s'agit d'un principe juridique transversal, qui relève de l'obligation du responsable à prouver le respect des six principes fondamentaux. Cette exigence complémentaire permet d'éviter le caractère passif de la mise en conformité, et implique des actions en interne, visant la logique de responsabilité proactive évoquée dans le point précédent sur les objectifs généraux.

5 Qu'est-ce que l'identité numérique ?

L'identité numérique est l'ensemble des traces qu'un utilisateur peut laisser de lui-même dans ses activités numériques : pseudonymes, identifiants, cookies, adresse *IP* (numéro d'identification unique à chaque périphérique connecté à l'Internet), *tag*, commentaires, coordonnées bancaires, géolocalisation.

■ Une triple identité

On distingue d'abord une identité déclarée, relative aux informations que l'on saisit sur soi-même et qui semblent donc être les plus proches de l'identité réelle de la personne : identité civile, identifiant (email, souvent), mot de passe lors de la création d'un compte, ce que l'on dit de soi dans l'espace « profil » d'un réseau social. Plus les informations sont détaillées, plus l'identité sera différenciante. Cependant, la transparence avec cet être numérique n'est pas totale : on peut recourir au pseudonyme, plus ou moins proche de sa véritable identité ou d'une de ses passions, pour éviter de dévoiler son identité civile. On peut également segmenter ce que l'on souhaite livrer de soi-même, en divisant ses centres d'intérêt entre plusieurs plateformes. On peut se créer un avatar de toutes pièces, jouant avec la distance entre celui-ci et sa propre identité.

L'identité agissante recouvre les traces qu'on laisse par les activités numériques que l'on mène : commentaires, publications, achats, invitation à un groupe acceptée… Elle s'est développée avec le web 2.0 et définit l'individu par son comportement. L'espace numérique devient un terrain de pratiques, d'expériences, de mise en scène de soi, conduisant à une reconstruction de soi, par la multiplication des facettes que l'on peut donner à voir, voire à une projection d'un soi idéalisé, mis en scène par des photos et *stories* correspondant au modèle social auquel on aspire. Cette identité agissante se traduit aussi par la possibilité de se tester en tant qu'artiste, de rencontrer aisément un public dont le retour permettra de valider une nouvelle facette identitaire. L'activité validée par des inconnus conduit ainsi à enrichir l'identité déclarée, le récit que l'on peut faire de soi.

L'identité calculée est celle déterminée par le système informatique : elle recouvre des informations permettant de définir le temps passé sur un site, les pages lues, les liens cliqués, le nombre d'interactions sur un réseau social, la fréquence de connexion, les comportements d'achat, etc., et peut donc délivrer un portrait de navigation, d'habitudes, de l'usager. Ce sont ces données de navigation qui, après analyse et recoupement de toutes nos identités par rapport à des profils, permettent de personnaliser nos usages et d'adapter les recommandations des plateformes (voir questions 26 et 48).

■ Enjeux éthiques de l'identité numérique

L'identité numérique soulève la question de l'accès aux données personnelles et de leur utilisation (voir question 9). Mais elle interroge aussi la construction de soi dans un contexte où vie virtuelle et vie actuelle se chevauchent : par les éléments biographiques disséminés sur les plateformes, mais aussi parce qu'il est fréquent de retrouver en ligne ses proches, maintenir une présence hermétique dans des espaces virtuels est difficile. Varier les expressions de soi impliquera donc une sélection des publics pour se protéger de tout débordement de visibilité et éviter qu'un aspect de soi ne soit réutilisé contre soi sur un espace où il n'est pas censé être visible (voir question 20).

Enfin, l'identité numérique repose sur des traces, dont la longévité pose question. L'identité humaine évolue, et se voir rappeler ce que l'on a dit ou fait, parce que les données numériques en gardent une trace, peut engendrer une atteinte à l'estime de soi. Le droit à l'oubli apparaît alors comme une nécessité (voir questions 15 et 30).

6 Qu'est-ce qu'une donnée personnelle ?

Le numérique soulève souvent des questions relatives aux données personnelles – ou données à caractère personnel – lesquelles bénéficient d'une protection particulière. Elles sont au cœur du Règlement Général sur la Protection des Données (RGPD) (voir question 4). Pour comprendre les difficultés éthiques soulevées, il importe de savoir ce que sont les données personnelles, car chacun en laisse quotidiennement sur son passage, notamment sur des supports numériques.

Elles sont définies à l'article 4 du RGPD de la façon suivante : « une donnée à caractère personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »

■ Reconnaître une donnée personnelle

Les données personnelles peuvent se référer à l'identité (tels que le nom, le prénom, la date de naissance, ou encore la photo d'identité), aux coordonnées (adresse postale, email ou numéro de téléphone), à la vie professionnelle (CV, intitulé de poste, évaluations, numéro de matricule), à la vie privée (situation familiale, habitudes de consommation), aux données de navigation (cookies, adresse IP, historique de recherche), aux données financières (relevés bancaires, RIB, numéro de carte bancaire) ou encore à des données considérées comme sensibles (voir question 7). Ainsi, si ces données sont souvent liées à la vie privée avec laquelle elles se recoupent fréquemment, les deux notions ne sont pas exactement synonymes.

Ces informations permettent alors d'identifier la personne soit directement avec une seule donnée (c'est le cas des données liées à l'identité, la photo), soit indirectement (c'est le cas lorsqu'on peut identifier la personne en croisant plusieurs données, comme le sexe et l'adresse). Notons que les données personnelles ne concernent que les personnes physiques, c'est-à-dire les êtres humains dotés de la personnalité juridique. Cela concerne donc les êtres humains nés vivants,

et toujours vivants. Par voie de conséquence, d'une part, les données d'identification d'une personne morale, telles qu'une société ou une association, ne sont pas considérées, en principe, comme des données personnelles. D'autre part, les données d'identification d'une personne physique décédée ne sont pas protégées par les mêmes mécanismes.

■ Pourquoi et comment protéger ses données personnelles ?

Protéger ses données personnelles permet de préserver sa vie privée. L'enjeu est d'autant plus important que ces données peuvent être utilisées à des fins frauduleuses, et les protéger permet d'éviter notamment l'usurpation d'identité ou le démarchage commercial excessif, à travers notamment la publicité ciblée (voir question 9).

Afin de les protéger, il existe plusieurs solutions, complémentaires et non exhaustives : faire attention à ce que l'on partage, vérifier les paramètres de confidentialité, utiliser des mots de passe robustes, éviter les connexions non sécurisées, faire attention aux démarches d'hameçonnage (technique de fraude pour voler des données personnelles en se faisant passer pour une entité de confiance), et mettre à jour régulièrement ses appareils numériques (voir question 10).

Une donnée à caractère personnel peut perdre son caractère personnel en cas d'anonymisation (voir question 12) ou après pseudonymisation à condition que le processus soit irréversible (voir question 13).

7 Qu'est-ce qu'une donnée sensible ?

Parmi les enjeux du numérique, la question des données sensibles est cruciale et fait l'objet d'une réglementation spécifique. Les données peuvent être de natures différentes, et recouvrir des informations dont le traitement, le stockage et l'analyse impliquent des précautions spécifiques. Aussi, en Europe, le Règlement Général sur la Protection des Données (voir question 4) assure la protection des personnes et de leurs données sensibles.

■ Identifier une donnée sensible

Une donnée sensible est une information personnelle relevant de la vie privée d'une personne. Le RGPD répertorie l'ensemble de ces données sensibles à l'article 9 : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques, données de santé et données relatives à l'orientation ou la vie sexuelle. Parmi les données biométriques strictement encadrées par le RGPD, nous pouvons mentionner les empreintes digitales, la reconnaissance faciale, l'empreinte vocale, l'iris et la rétine, les données ADN, etc.

D'autres données sensibles de type biométrique rentrent également dans ce cadre si elles sont utilisées à des fins d'identification. L'article 4 (14) rappelle que les données biométriques sont des « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique ». Cela concerne par exemple la dynamique de frappe au clavier, la dynamique de la signature et la reconnaissance de la démarche. De même, une photo, une vidéo ou la voix d'une personne ne sont pas considérées comme des données biométriques si elles ne sont pas utilisées pour identifier la personne, mais peuvent l'être si elles sont utilisées afin de la reconnaître.

Enfin, d'autres données peuvent être considérées comme particulièrement sensibles. En effet, c'est le cas des données financières du numéro de sécurité sociale, ou encore des données relatives aux

infractions ou condamnations pénales. Ces dernières sont mentionnées à l'article 10 et leur traitement doit se faire sous le contrôle de l'autorité publique.

■ Pourquoi et comment sont traitées les données sensibles ?

Les données sensibles bénéficient d'un traitement spécifique pour éviter qu'elles ne soient utilisées à des fins malveillantes visant à nuire à la vie privée, la sécurité ou aux droits fondamentaux de la personne. C'est pourquoi le traitement des données sensibles est, par défaut, interdit, et que les exceptions qui peuvent être faites sont strictement encadrées par l'article 9 (2) du RGPD.

En effet, dans certaines situations, ces données peuvent être nécessaires. C'est le cas de la santé et de la médecine (raisons médicales, intérêts vitaux, médecine préventive), de la justice (exercice et défense des droits), du travail et de la sécurité et protection sociale (obligations légales spécifiques), du traitement par un organisme à but non lucratif ou rendue publique par la personne concernée, ou encore dans la recherche scientifique (mission d'intérêt public), et lorsque les données sensibles font l'objet d'un consentement explicite de la personne.

Dans tous les cas, le traitement des données sensibles doit respecter plusieurs principes, dont la minimisation des données et une application juste et proportionnée (voir, pour principes similaires, questions 63 et suivantes).

8 Que sont les cookies… à part des petits gâteaux ?

Aucune recette de cookies ici.

Selon le RGPD et la directive *ePrivacy*, « un cookie est une information déposée sur l'appareil terminal d'un utilisateur par un serveur, lors de sa visite sur un site web, dans le but de mémoriser certaines informations relatives à l'utilisation pour la durée de la session ou pour un temps plus long ». Il s'agit d'un fichier texte enregistré sur l'appareil numérique et qui peut contenir des informations telles que celles relatives à une session (par exemple le temps de connexion), aux préférences choisies (par exemple la langue) ou encore à des comportements en ligne.

Les cookies sont donc des données à caractère personnel (voir question 6) puisqu'elles permettent d'identifier une personne en fonction de ses préférences ou de ses comportements, et permettent de se souvenir de l'utilisateur d'une session à l'autre, ce qui implique donc qu'elles soient encadrées par le RGPD. Ce dernier rappelle que les personnes doivent être clairement informées sur les finalités des cookies, pouvoir les supprimer ou les modifier, et donner leur consentement pour tous les cookies non essentiels.

■ Les différents types de cookies et leur utilité

On peut les regrouper selon trois grandes catégories : (1) leur finalité, (2) leur durée de vie, ou (3) leur origine ; en sachant que les différents cookies peuvent se retrouver dans plusieurs catégories.

Dans la première catégorie (finalité), on retrouve les cookies techniques qui sont nécessaires au fonctionnement du site web consulté (seuls cookies de cette catégorie qui ne nécessitent pas de consentement), les cookies de préférence permettent de se souvenir des choix personnels, les cookies de mesure d'audience à visée analytique dont l'objectif est d'améliorer l'expérience et l'efficacité de l'expérience utilisateur, les cookies publicitaires à visée de ciblage et dont l'objectif est de pouvoir afficher des publicités ciblées et les cookies de réseaux sociaux qui permettent de suivre les utilisateurs et leur activité.

Dans la deuxième catégorie (durée de vie), on retrouve les cookies de session (qui ne nécessitent pas de consentement) dont la visée est de maintenir la session active et sont supprimés à la fermeture du

navigateur, et les cookies persistants (qui nécessitent généralement un consentement) dont la visée est de se souvenir des préférences et de l'activité de l'utilisateur (par exemple la langue ou les préférences de publicité) et sont conservés sur l'appareil numérique pendant une période définie pouvant aller jusqu'à plusieurs mois après la fermeture du navigateur.

Dans la troisième catégorie (origine), on retrouve les cookies propriétaires créés par le site web visité et permettant une navigation optimale (par exemple les paramètres de connexion ou de langue) et les cookies tiers qui sont installés par une autre entité et permettant un suivi et une analyse des habitudes et des comportements (par exemple les publicités ciblées).

■ Pourquoi et comment supprimer mes cookies ?

Si ce n'est pas en les mangeant que vous pouvez supprimer ces cookies, vous pouvez, malgré tout, les supprimer autrement.

C'est important parce que les supprimer vous permet de mieux contrôler vos informations personnelles. Par exemple, en révoquant votre consentement, vous pouvez mieux protéger votre vie privée et éviter le ciblage publicitaire, mais également améliorer la sécurité de vos appareils numériques et éviter notamment les conflits informatiques tout en optimisant les performances de votre navigateur.

Pour ce faire, il suffit d'aller dans les paramètres de votre navigateur, trouver la section relative à la confidentialité et sécurité de la vie privée et identifier les éléments relatifs aux cookies en sélection l'option qui vous correspond.

9 Pourquoi mes données personnelles doivent-elles être protégées ?

Les données personnelles (y compris les données sensibles, voir questions 6 et 7), que chacun laisse constamment derrière lui tout au long de la journée (formulaire, données de connexion, cookies, localisation géographique…), encourent de nombreux risques.

■ La mercantilisation ou marchandisation des données

Les données personnelles sont devenues un produit, une marchandise très lucrative. On parle alors de mercantilisation ou marchandisation des données qui suscite des questions éthiques. Ces données vont être utilisées à des fins commerciales et marketing pour des publicités ciblées. En laissant des données sur un réseau social gratuit, par exemple, celui-ci va les réutiliser pour vous envoyer de la publicité ciblée c'est-à-dire adaptée à vos goûts et vos habitudes tels qu'ils ressortent de vos données, et donc semblant démontrer un besoin. Il peut également les revendre à des tiers qui en feront une utilisation similaire. Il est courant de dire que « quand c'est gratuit, c'est que c'est vous le produit ».

Certaines pratiques conduisent non pas à utiliser les données personnelles contre des services gratuits, sous couvert de consentement (voir question 14), mais à ce que les internautes vendent purement et simplement leurs données. C'est un procédé connu sous le nom de monétisation des données personnelles. La légalité de ce procédé interroge, car la vente des données implique que la personne n'ait plus du tout la main dessus en contradiction avec les droits protégés dans le RGPD auxquels on ne peut pas renoncer.

Si le RGPD tente de réguler et d'encadrer la protection des données personnelles dans ce contexte (voir question 4), la marchandisation des données n'est en elle-même pas strictement interdite. Elle suscite pourtant des problèmes éthiques, et les autorités, à l'image de la Commission nationale de l'informatique et des libertés (CNIL), redoublent de vigilance. Ces questions éthiques concernent d'une part les acteurs économiques en raison d'une distorsion de concurrence entre ceux qui y ont accès et les autres. Néanmoins, la protection des données pourra, à l'inverse, être utilisée comme argument marketing. Elles concernent d'autre part, et évidemment, les citoyens. La monétisation, par exemple,

risque de générer des inégalités entre ceux qui pourront payer pour accéder au service, et protéger leurs données, et ceux qui ne pourront pas, et se verront contraints d'accepter de vendre leurs données. La protection des données et de l'identité seront donc préservées pour certains, mais pas pour toutes et tous.

■ L'insécurité des données

Au-delà de devenir des marchandises, les données personnelles sont susceptibles d'être la cible de vol de données. Cela renvoie aux questions de sécurité numérique (voir question 84), et notamment aux questions de confidentialité et d'intégrité.

Or, ces données volées peuvent servir à des fins non éthiques, voire immorales ou illégales : usurpation d'identité, ingénierie sociale, atteinte à la réputation, utilisation des mots de passe pour accéder aux comptes, *deepfakes* (procédé développé avec l'intelligence artificielle consistant à modifier ou créer un enregistrement vidéo ou audio), etc.

Face à ces différents risques, le RGPD tente d'apporter des réponses, de même que l'éthique qui conduit à conseiller quelques bonnes pratiques de protection.

10 Comment peut-on protéger ses données ?

Au regard des risques encourus (voir question 9), la protection de ses données personnelles apparaît nécessaire.

■ L'évidence : la non-divulgation

L'évidence est de ne pas les divulguer. Cependant, la société dans laquelle nous vivons rend difficile une telle protection extrême. Nous laissons des traces numériques partout : les formulaires pour s'inscrire ou se connecter, les informations données, les données de connexion, les données de paiement, les données de localisation… (voir question 5).

Ainsi, la divulgation des données personnelles, et encore plus si elles sont sensibles, doit être évitée au maximum sur des réseaux publics ou inconnus. Ces réseaux sont souvent moins protégés, pour faciliter leur utilisation par tout le monde, ce qui est leur raison d'être. L'accès extérieur à vos données y est donc plus facile. De la même façon, la sagesse recommandera de ne pas divulguer d'informations trop personnelles (données bancaires, et même adresse email habituelle), et même d'éviter les sites marchands inconnus ou non sécurisés. Peuvent s'y cacher des systèmes de vol de données.

■ La protection des accès

Reste à se protéger sur son réseau personnel et les sites reconnus. Car ces éléments ne confèrent pas une immunité. On renverra de façon générale aux conseils liés à la sécurité numérique (voir question 84). Ainsi, les mises à jour et autres mots de passe forts sont autant de moyens de protection.

D'autres conseils peuvent être ajoutés, propres à la confidentialité des données personnelles. Ainsi, le paramétrage des équipements, applications… est essentiel. Si cela peut paraître fastidieux, modifier les différentes options et paramètres afin de conserver la confidentialité de ce que vous divulguez est utile. Il en va de même de la double authentification de plus en plus proposée aujourd'hui (système où votre identité devra être confirmée après votre connexion via, par exemple, un code unique envoyé par SMS ou par email).

En complément : les droits permettant la protection des données personnelles

En complément de ces conseils pratiques usuels, le RGPD prévoit plusieurs droits qui permettent directement de conserver une certaine mainmise sur ses données, et ainsi les protéger. Le premier de ces droits est le droit d'opposition. Il ne s'agit pas ici de refuser dès le départ l'utilisation des données (voir sur ce point la question du consentement, question 14), mais dans un second temps, lorsque vous ne souhaitez plus que vos données figurent dans un fichier, de pouvoir demander que vos données ne soient plus utilisées. Il est nécessaire de justifier « des raisons tenant à votre situation particulière », sauf en cas de prospection commerciale. Dans cette hypothèse, aucune justification n'est nécessaire. Ce droit d'opposition se manifeste quotidiennement lorsqu'on se désabonne d'une newsletter (opposition à l'utilisation de l'adresse email) ou en refusant de figurer dans l'annuaire universel.

À ce droit d'opposition s'ajoute un droit de rectification. Il vous est permis de corriger des données fausses ou incomplètes qu'un organisme détient sur vous. Cela permet de conserver un certain contrôle de vos données, en limitant la possibilité de voir des informations erronées diffusées ou utilisées contre vous.

Enfin, le contrôle de vos données passe également par un droit à la portabilité de celles-ci. Ce droit vous permet d'obtenir une copie de vos données dans un format lisible par un système numérique afin de pouvoir les stocker ailleurs, ou les réutiliser dans un autre contexte.

11 Comment m'assurer que mes données sont protégées ?

Certaines des protections évoquées pour ses données personnelles impliquent un tiers, particulièrement l'organisme à qui l'on communique ces données. Comment, dans ce contexte, m'assurer que mes données sont protégées ? Ces vérifications pourront avoir lieu *a priori*, avant de communiquer les données, grâce au droit à l'information, mais aussi *a posteriori*, après avoir divulgué des données personnelles, avec le droit d'accès.

■ Le droit à l'information

Tout organisme qui collecte des données personnelles vous doit l'information, droit renforcé par le RGPD (voir question 4). Ce droit à l'information va surtout jouer avant que vous ne divulguiez vos données, et vous permettra de décider si vous souhaitez le faire ou non. Cela participe du consentement éclairé lorsque celui-ci est nécessaire (voir question 14), mais c'est aussi de manière générale un bon moyen de s'assurer que vos données seront protégées. Un défaut d'information, au contraire, est un signe qu'il y a un risque dans l'utilisation qui en sera faite. Pour la Commission nationale de l'informatique et des libertés (CNIL, voir question 18), « c'est le premier baromètre pour déterminer le degré de confiance à accorder à un organisme ».

Ce droit à l'information pourra prendre de multiples formes : mentions légales, politique de confidentialité, formulaire de consentement (sauf données anonymes), ou encore notices d'information sont autant de manières de prendre connaissance de ce qui sera fait de vos données. Ce faisant, l'organisme est transparent, et doit vous mettre en mesure d'accéder facilement et rapidement aux informations.

Ce droit d'information se poursuit tout au long de la relation. Aussi, au nom du droit à l'information, l'organisme doit nécessairement vous informer au cas où il a constaté une violation de vos données personnelles (par exemple, piratage des serveurs de l'organisme où sont stockées vos données) avec un risque grave pour vous. Il doit, dans le même temps, vous donner des conseils.