L'UNION EUROPÉENNE ET LE NUMÉRIQUE

Sécuriser ses données

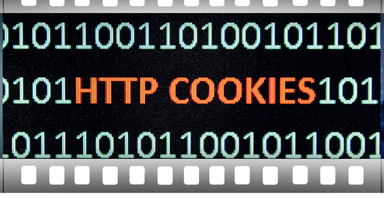
faire des choix éclairés



Quelles traces laisse-t-on en ligne ?

Le terme "donnée personnelle" désigne toute information qui peut identifier directement ou indirectement un individu, comme un nom, un numéro de téléphone ou une adresse IP. Les "données sensibles", telles que les opinions politiques ou la santé, bénéficient d'une protection renforcée en raison des risques que leur diffusion pourrait présenter.

Pour répondre à ces enjeux, l'UE a adopté le Règlement général sur la protection des données (**RGPD**). Ce texte majeur, entré en vigueur en 2018, protège la vie privée en obligeant les entreprises à être transparentes sur l'utilisation des données et à obtenir un consentement éclairé. Le RGPD confère également le droit de consulter, de corriger ou de supprimer ses données : une action concrète pour un numérique plus respectueux des citoyens et de leurs libertés.

Si c'est gratuit, vous êtes le produit !

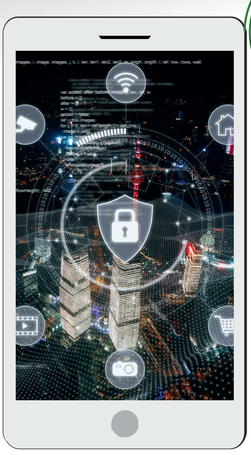
Les réseaux sociaux, moteurs de recherche et applications sont souvent gratuits en apparence mais ils se financent, en réalité, grâce à nos données. En utilisant ces plateformes, on "paie" avec notre attention et nos données, savamment analysées par des algorithmes : elles vendent ensuite des espaces publicitaires ciblés à des entreprises. C'est ce qu'on appelle le modèle économique du "marché biface" : les utilisateurs d'un côté, les annonceurs de l'autre.

contenus réalisés avec la contribution de Diane Dubreuil, Corentin Fourrier et Jules Pintaud, étudiants du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté
Europe Direct
Université Marie & Louis Pasteur
UFR SJEPG Sciences juridiques économiques politiques et de gestion

Protection des données

garder le contrôle



Piliers juridiques

L'UE a fait de la protection des données personnelles un pilier de sa régulation numérique.

Depuis l'entrée en vigueur du Règlement général sur la protection des données (**RGPD**) en 2018, chaque citoyen dispose de droits clairs : accès, rectification, effacement, limitation, portabilité et opposition.
Ces droits rendent aux individus le contrôle sur leurs informations, qu'elles soient ordinaires ou sensibles, comme la santé ou les opinions politiques. Toutefois, par facilité ou manque de clarté, bon nombre d'usagers en ligne laissent de nombreuses traces et données sans le vouloir.

Le Digital Services Act (**DSA**) vise à réguler les plateformes en ligne pour lutter contre les contenus illégaux et la désinformation, en protégeant les droits fondamentaux des utilisateurs.

Le Digital Markets Act (**DMA**) a pour objectif d'empêcher les grandes plateformes numériques d'abuser de leur position dominante sur le marché, afin de garantir une concurrence équitable pour les autres entreprises.

Des enjeux multiples

La collecte massive de données se fait souvent sans transparence ni consentement éclairé. On clique "accepter les cookies" sans imaginer les effets et conséquences.

Il existe plusieurs enjeux majeurs liés à l'exploitation des données :

- économiques

Les GAFAM dominent le marché. Ils font d'énormes profits en exploitant nos données tout en mettant en place des stratégies d'évitement fiscal. Cela crée une concurrence déloyale vis-à-vis d'acteurs européens, plus petits, qui ne peuvent pas rivaliser. En outre, cela rend l'Europe dépendante technologiquement des États-Unis.

- politiques :

Qui décide des règles ? Les géants du numérique ou les institutions démocratiques ? L'UE a montré qu'elle souhaite réguler le marché numérique et poser un cadre éthique afin notamment d'éviter les manipulations électorales. Avec les lois-cadres telles que le **DSA**, **DMA** et l'**IA Act**, le marché européen se veut plus éthique, transparent et respectueux des citoyens.

contenus réalisés avec la contribution de Mathilde Daguet, Pauline Grossmann et Manon Jurdzinski, étudiantes du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté
Europe Direct
Université Marie & Louis Pasteur
UFR SJEPG Sciences juridiques économiques politiques et de gestion

Intelligence artificielle

entre innovation et régulation

L'UE premier régulateur au monde

Le Règlement sur l'IA (**AI Act**) est le texte européen majeur pour encadrer le développement, la commercialisation et l'utilisation de l'intelligence artificielle en Europe.
Son objectif est de protéger les droits fondamentaux des citoyens et de prévenir les risques potentiels, tels que les discriminations ou les atteintes à la vie privée.
Le règlement classe les systèmes d'IA en quatre niveaux de risque, allant du risque inacceptable (interdit) au risque minimal, qui ne requiert pas d'exigences particulières.

Propriété intellectuelle

Le règlement européen répond également aux défis soulevés par l'IA en matière de contrefaçon et de cybersécurité.
Certaines IA sont entraînées sur des œuvres protégées par le droit d'auteur, ce qui peut mener à la production de créations illégales car la frontière est mince entre "inspiration" et "plagiat".

Le règlement sur l'IA oblige les entreprises à être transparentes sur les données utilisées. Il vise aussi à contrer les utilisations malveillantes de l'IA par les cybercriminels, notamment pour la création de "deepfakes" (fausses vidéos réalistes) ou des campagnes de "phishing" (rançon) sophistiquées.
Le règlement européen renforce les exigences de cybersécurité pour les systèmes à haut risque afin de bloquer ces dérives (voir le panneau sur le sujet).

Limiter les risques

La responsabilité du contrôle est partagée entre deux niveaux :

- niveau européen : l'AI Office, au sein de la Commission européenne supervise l'application de l'AI Act, surtout pour les systèmes d'IA transfrontaliers ou à usage général. Il coordonne la coopération entre États membres, publie des lignes directrices, élabore des codes de conduite et apporte une expertise technique.

- niveau national : les autorités de surveillance désignées par chaque État membre (la CNIL en France) contrôlent la conformité des systèmes d'IA sur leur territoire (audits, inspections, sanctions).

contenus réalisés avec la contribution de Chloé Hardhuin-Verdet, Amina Mihoub et Adeline Tito, étudiantes du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté
Europe Direct
Université Marie & Louis Pasteur
UFR SJEPG Sciences juridiques économiques politiques et de gestion

L'UNION EUROPÉENNE ET LE NUMÉRIQUE

Cyber sécurité

enjeu de souveraineté

Une responsabilité partagée

Les cyberattaques représentent une menace sérieuse pour les infrastructures critiques, qu'il s'agisse des hôpitaux, des réseaux d'énergie ou des services bancaires.
Pour y faire face, la cybersécurité est devenue une priorité pour l'UE : elle agit en votant des normes qui s'appliquent directement dans les États membres, les règlements, ou que chaque pays doit adapter à sa propre législation, les directives.

En 2024, l'Agence européenne pour la cybersécurité a recensé 11 079 cyberattaques.

Un cadre juridique évolutif

La directive **NIS1**, adoptée le en 2016 et transposée en 2018, fut la première législation européenne sur la cybersécurité. Elle visait à renforcer la résilience face aux cyber-menaces et à protéger les infrastructures critiques comme l'énergie, la santé ou les transports. Son champ d'application couvrait principalement les Opérateurs de Services Essentiels (OSE) et les Fournisseurs de Services Numériques (FNS). La directive NIS 1 a été abrogée fin 2024, laissant place à NIS2.

La directive **NIS2** vise à renforcer la cybersécurité en élargissant son champ d'application et en distinguant les entités *essentielles* (énergie, transports, eau, santé, espace...) des entités *importantes* (gestion des déchets, alimentation, accès numériques...). En France, ces entités sont placées sous le contrôle de l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**).

Le Digital Operational Resilience Act (**DORA**) en 2022 et le Cybersecurity Act en 2019 complètent l'arsenal juridique européen.

Des dispositifs de coordination

- ENISA (Agence européenne pour la cybersécurité) : organe central qui apporte expertise, formation, tests et soutien aux États membres, tout en coordonnant la gestion de crises.
- CSIRTs Network : réseau européen des équipes nationales d'intervention en cas d'incident informatique, qui coopèrent et partagent des informations techniques.
- EU-CyCLONe (European Cyber Crises Liaison Organisation Network) : structure créée avec NIS 2 pour coordonner la réponse politique et stratégique lors des cyber-incidents majeurs.
- Cyber Solidarity Act (2023) : texte qui prévoit la mise en place d'un réseau européen de centres de cybersécurité, un système d'alerte précoce et une réserve européenne de cybersécurité mobilisable en cas de crise.
- Mécanisme de réaction d'urgence : possibilité pour la Commission de soutenir directement un État membre attaqué, grâce à des moyens techniques et financiers communs.

contenus réalisés avec la contribution de Kasaï Ngangue, Ariane Sounda Poba et Lorraine Thomassin, étudiantes du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté
Europe Direct
Université Marie & Louis Pasteur
UFR SJEPG Sciences juridiques économiques politiques et de gestion

Climat & numérique

quelle compatibilité ?

Progrès & responsabilité

L'UE a pris conscience que le numérique, moteur d'innovation et de compétitivité, représente aussi un défi écologique majeur. Elle agit pour concilier transition numérique et durabilité.

Plusieurs directives traduisent cet engagement :

- Le principe du « **pollueur-payeur** » (directive 2004/35/CE) responsabilise les industriels.
- La directive sur **l'écoconception** (2009/125/CE) impose des appareils moins énergivores, tandis que la directive DEEE (2012/19/UE) fixe des règles strictes de recyclage des équipements électroniques.
- L'Europe innove aussi par des mesures concrètes, comme l'**unification des chargeurs** (directive 2022/2380/UE) qui réduit les déchets liés aux câbles et adaptateurs.

Au coeur du Pacte vert

Le Pacte vert pour l'Europe fixe un cap clair : atteindre la neutralité climatique d'ici 2050. Dans ce cadre, l'UE agit sur le cloud et les infrastructures numériques, en imposant une déclaration obligatoire de la consommation énergétique des *data centers*, en promouvant l'*edge computing* (traitement local des données) et en fixant des normes de sobriété.

L'UE soutient aussi la recherche et les projets collectifs pour un numérique plus responsable, comme **OCRE**, qui favorise l'accès à un *cloud* durable pour la recherche.

L'UE se positionne ainsi comme pionnière d'un numérique à la fois innovant et respectueux de la planète.

Des impacts significatifs

Contrairement à l'idée reçue qu'il est "propre" et "immatériel", le secteur numérique a un impact écologique bien réel et croissant. Les technologies numériques représentent près de 10 % de notre consommation d'énergie et près de 4 % de nos émissions de gaz à effet de serre.
L'impact environnemental du numérique provient majoritairement de la production de nos smartphones, ordinateurs, composants électroménagers, voitures, etc. (78 % de cette empreinte).
À cela s'ajoutent les coûts cachés : l'extraction de métaux rares détruit des écosystèmes à des milliers de kilomètres de notre continent et 150 000 tonnes de déchets électroniques sont exportées illégalement chaque année hors de l'UE.

Les data centers européens consomment environ 96 TWh par an, soit l'équivalent de la consommation électrique des Pays-Bas, de la Pologne, de l'Irlande et de la Roumanie réunis. D'ici à 2030, elle pourrait tripler, atteignant l'équivalent des besoins de 193 millions de personnes, soit 43 % de la population de l'UE

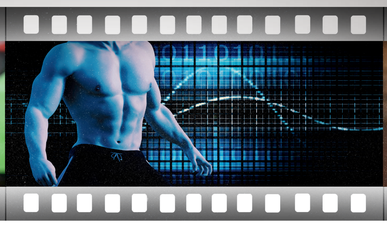
contenus réalisés avec la contribution de Inès Clausse, Léa Minesi et Erwan Ropers, étudiants du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté · Europe Direct · Université Marie & Louis Pasteur · UFR SJEPG Sciences juridiques économiques politiques et de gestion

L'UNION EUROPÉENNE ET LE NUMÉRIQUE

Sport & numérique

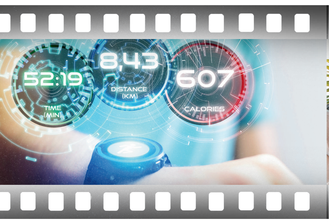
performance, suivi et protection des données

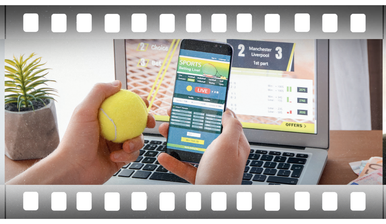




Encadrer les usages et les données

Dans le domaine sportif, l'UE encadre l'usage des données personnelles. Les performances des athlètes sont de plus en plus analysées via des objets connectés, collectant rythme cardiaque, sommeil ou analyses médicales. Grâce au **RGPD**, l'UE impose que seules les données strictement nécessaires soient utilisées, avec le consentement explicite des sportifs, afin de préserver leur vie privée tout en favorisant l'innovation dans l'entrainement. Ils conservent, comme chaque individu, un droit d'accès à leurs données, droit de rectification, droit à l'oubli, droit d'opposition.

L'encadrement européen s'applique aussi à la lutte antidopage. Les athlètes de haut niveau doivent déclarer leur localisation pour permettre des contrôles inopinés. Bien que cette pratique soit intrusive, la justice l'a validée au nom de l'équité sportive, en insistant sur les garanties de proportionnalité et de sécurité exigées par l'UE. Les données collectées sont conservées pour une durée limitée dans des bases sécurisées, conformément aux standards européens.






Prévenir les menaces dans le respect des libertés

Les Jeux olympiques de Paris 2024 ont révélé la vulnérabilité des données face aux cyberattaques. L'UE a renforcé la coopération entre États membres pour prévenir ces menaces, en encourageant l'usage de technologies sécurisées et la formation des acteurs. La cybersécurité devient une priorité européenne, au même titre que la sécurité physique des compétitions.

L'UE encadre l'expérimentation de nouvelles technologies de surveillance comme la reconnaissance faciale ou les caméras augmentées, utilisées temporairement pour sécuriser les grands événements. La loi française « JOP2024 », inscrite dans le cadre juridique européen, illustre cette volonté de concilier innovation, sécurité et protection des libertés fondamentales. L'UE s'affirme ainsi comme garante d'un équilibre entre sport, technologie et respect de la vie privée.

contenus réalisés avec la contribution de Sacha Kety, Aleyna Kocer et Manuel Mouly, étudiants du Master de droit du numérique- 3C de l'UFR SJEPG
crédits des illustrations : Canva

Maison de l'Europe Bourgogne-Franche-Comté
Europe Direct
Université Marie & Louis Pasteur
UFR SJEPG Sciences juridiques économiques politiques et de gestion