Numérique et droit

Enjeux juridiques et cybersécurité

Antoine Touzain

Professeur agrégé de droit privé
Université Rouen Normandie — CUREJ

Numérique · Données · Cybersécurité

Université Populaire de Poissy

Plan de l'intervention

Introduction — Le numérique dans nos vies

I. **Le numérique dans nos vies quotidiennes**

Un monde transformé, des risques nouveaux

II. **Nos données personnelles et le droit**

RGPD, vie privée, réseaux sociaux, IA

III. **La menace cyber : identifier les risques**

Phishing, rançongiciels, escroqueries en ligne

IV. **Se protéger et faire valoir ses droits**

Conseils pratiques, recours, acteurs clés

Internet : 50 ans de révolution

5,4 Mds

d'internautes
dans le monde

85 %

des Français
en ligne

6h30

passées par jour
sur les écrans

Source : We Are Social / DataReportal 2024

Le numérique : au cœur de nos vies

Des usages qui ont transformé chaque aspect du quotidien

Ce que nous faisons en ligne tous les jours

- Communiquer : e-mails, WhatsApp, Signal, SMS
- S'informer : presse en ligne, réseaux sociaux, YouTube
- Gérer sa banque, ses impôts, sa santé (Mon Espace Santé)
- Acheter : Amazon, Leboncoin, billetterie en ligne
- Se divertir : streaming, jeux, musique

➜ Chaque usage laisse des traces numériques

De 7 à 77 ans

Une médaille à deux faces

✅ Avantages

- Accès à l'information
- Lien social renforcé
- Services publics simplifiés
- Commerce facilité
- Télémédecine

⚠️ Risques

- Escroqueries en ligne
- Vol de données
- Cyberharcèlement
- Dépendance numérique
- Désinformation / IA

Opportunité ou menace ?

Le droit à la conquête du numérique

Une législation en effervescence depuis 20 ans

Pourquoi légiférer sur le numérique ?

- Protéger les individus contre les abus
- Réguler les géants du web (GAFAM)
- Garantir la concurrence équitable
- Assurer la cybersécurité des États et des entreprises

Une réglementation essentiellement européenne

- RGPD (2018) — données personnelles
- DSA (2022) — contenus illicites en ligne
- DMA (2022) — régulation des plateformes
- AIA (2024) — intelligence artificielle

Le cadre européen

Penser par les risques

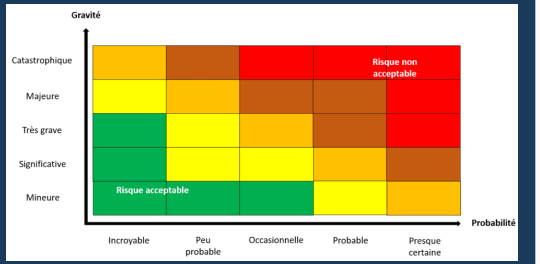
L'approche juridique moderne face au numérique

Le droit contemporain ne se contente plus de réparer après coup : il anticipe et prévient les risques.

Cartographie des risques numériques

- Risques économiques : destruction d'emplois, concentration des marchés
- Risques démocratiques : désinformation, manipulation électorale
- Risques sociaux : cyberharcèlement, exclusion numérique
- Risques sanitaires : addiction, données de santé
- Risques cyber : atteintes aux systèmes et aux données

L'équilibre entre liberté et sécurité est au cœur de toute régulation du numérique.



Cartographier pour anticiper

Les cinq familles de risques numériques

Une taxonomie pour comprendre les menaces

Les risques numériques ne se classent en cinq grandes familles :

- Risque de piratage
- Risque cyber généré : votre activité crée un danger pour d'autres (faille de sécurité)
- Risque algorithmique subi : une IA vous discrimine ou vous refuse un service
- Risque algorithmique généré : vous utilisez une IA qui cause un préjudice à autrui
- Risque d'infrastructure : panne, dépendance aux câbles sous-marins, cloud centralisé

Chaque famille appelle un régime juridique distinct — le droit doit s'adapter à cette diversité.

Cinq familles, un cadre d'analyse

L'asymétrie d'information dans le numérique

Le déséquilibre fondamental entre utilisateurs et plateformes

L'un des plus grands défis juridiques du numérique est l'asymétrie d'information : les géants du web en savent beaucoup plus sur vous que vous n'en savez sur eux.

Pourquoi c'est un problème juridique

- Vous ne savez pas ce qu'on fait de vos données → consentement biaisé
- Vous ne pouvez pas évaluer le risque cyber des services que vous utilisez
- Les algorithmes décident pour vous sans que vous compreniez pourquoi
- Les conditions générales sont illisibles → le « consentement » est une fiction

➜ Le RGPD et le DSA tentent de rétablir cet équilibre par la transparence obligatoire

Rétablir l'équilibre

I.

Le numérique dans nos vies quotidiennes

Des usages transformés, une société connectée

A. Les GAFAM et l'écosystème numérique

B. Nos traces numériques invisibles

C. Les réseaux sociaux et nos données

Les géants du numérique

Cinq entreprises qui structurent notre vie connectée

Entreprise	Services	Vos données utilisées
Google	Recherche, Maps, Gmail, YouTube	*Recherches, localisation, e-mails*
Apple	iPhone, App Store, iCloud	*Contacts, photos, paiements*
Meta	Facebook, Instagram, WhatsApp	*Réseau social, messageries*
Amazon	E-commerce, Alexa, Prime Video	*Achats, voix, habitudes*
Microsoft	Windows, Office, Teams, LinkedIn	*Travail, e-mails professionnels*

L'écosystème numérique mondial

Nos traces numériques

Chaque clic raconte une histoire

Ce que vous laissez sans le savoir

- Votre adresse IP — votre identité sur internet
- Vos cookies : préférences, historique de navigation
- Vos métadonnées : quand, depuis où, avec qui vous communiquez
- Votre géolocalisation : déplacements et habitudes
- Vos données de santé : applications, montres connectées

➜ Un profil publicitaire très précis peut être construit

- *Cas Target (2012) : la chaîne avait su qu'une cliente était enceinte avant sa propre famille… et avant la cliente elle-même !*

Votre portrait numérique invisible

Les réseaux sociaux et nos données

Quand le service est gratuit, le produit c'est vous

Le modèle économique

- Facebook, Instagram, TikTok : gratuits en apparence
- Revenus réels : la publicité ciblée grâce à vos données
- Plus vous êtes actif, plus vous êtes rentable

Histoire retracée dans S. Zuboff, *The Age of Surveillance Capitalism*, 2019.

Les risques spécifiques

- Surexposition de votre vie privée (photos, opinions, localisation)
- Harcèlement et arnaques via les messages privés
- Faux profils — usurpation d'identité
- Manipulation par les algorithmes (bulle de filtre)

Omniprésence des réseaux sociaux

II.

Nos données personnelles et le droit

RGPD, vie privée, intelligence artificielle

A. Qu'est-ce qu'une donnée personnelle ?

B. Le RGPD et vos droits concrets

C. La CNIL : votre protecteur

D. L'intelligence artificielle et les deepfakes

Qu'est-ce qu'une donnée personnelle ?

Une définition large qui nous concerne tous

Toute information permettant d'identifier directement ou indirectement une personne physique.

Exemples concrets

- Nom, prénom, adresse postale → identification directe
- Numéro de téléphone, e-mail → identification directe
- Adresse IP, cookie → identification indirecte
- Photo, empreinte digitale, voix → données biométriques
- Dossier médical, résultats d'analyses → données sensibles

→ Données sensibles = protection renforcée (santé, religion, opinions politiques)

Toute info qui vous identifie

Le RGPD : votre bouclier européen

Règlement Général sur la Protection des Données — 2018

Les grands principes

- Consentement : vous devez accepter explicitement la collecte
- Finalité : les données ne servent qu'à l'usage déclaré
- Minimisation : on ne collecte que ce qui est nécessaire
- Sécurité : l'entreprise doit protéger vos données

Vos droits concrets

- Droit d'accès — savoir ce qu'on détient sur vous
- Droit de rectification — corriger des données erronées
- Droit à l'effacement — « droit à l'oubli »
- Droit à la portabilité — récupérer vos données

En vigueur dans toute l'Union européenne

Comment exercer vos droits RGPD ?

Des démarches simples, des délais garantis

Étape 1 — Contacter le DPO de l'organisation

- *Chaque organisation traitant des données doit avoir un délégué à la protection des données*
- *Adresse : dpo@[organisation].fr ou formulaire sur le site web*

Étape 2 — Délai légal de réponse : 1 mois

- *Extensible à 3 mois si demande complexe (information obligatoire)*

Étape 3 — Si pas de réponse ou refus : saisir la CNIL

- *www.cnil.fr → rubrique « Vos droits » → « Plaintes » (service gratuit)*

Pour supprimer vos données Google : myaccount.google.com → Données et confidentialité → Supprimer vos données

Une demande écrite suffit

La CNIL : votre gendarme du numérique

Commission Nationale de l'Informatique et des Libertés — créée en 1978

Ce que fait la CNIL

- Surveille le respect du RGPD et de la loi Informatique et Libertés
- Sanctionne les entreprises en infraction
- Répond à vos plaintes (service totalement gratuit)

Amendes records prononcées en Europe

- Google : 150 millions € (CNIL, 2022) — cookies non conformes
- Amazon : 746 millions € au Luxembourg (2021)
- Meta : 1,2 milliard € en Irlande (2023) — transferts de données vers les USA

Pour toute question sur vos droits : www.cnil.fr — accessible à tous, gratuit.

CNIL.

Autorité indépendante

Les cookies : que se passe-t-il quand vous cliquez ?

Comprendre ces petits fichiers omniprésents

Un cookie, c'est quoi ?

Un petit fichier déposé sur votre appareil par un site web, qui mémorise vos préférences et vous reconnaît lors de votre prochaine visite.

Les types de cookies

- Cookies nécessaires : panier d'achat, connexion → autorisés sans consentement
- Cookies analytiques : mesure d'audience → consentement requis
- Cookies publicitaires : ciblage comportemental → consentement explicite obligatoire

→ Vous avez le droit de refuser tous les cookies non essentiels

Mémoriser pour mieux cibler

L'intelligence artificielle dans notre quotidien

De ChatGPT aux assistants vocaux, l'IA est partout

L'IA déjà dans votre vie

- Reconnaissance faciale pour déverrouiller votre téléphone
- Assistants vocaux : Siri, Alexa, Google Assistant
- Recommandations : Netflix, Spotify, Amazon
- ChatGPT, Gemini : génération de texte, images, vidéos

Les risques juridiques de l'IA

- Deepfakes : fausses vidéos pour escroquer ou nuire à la réputation
- Discrimination algorithmique : décisions automatisées biaisées
- Propriété intellectuelle : qui détient les créations de l'IA ?

Une révolution en cours

L'IA Act : le droit européen de l'IA

Premier cadre réglementaire mondial — 2024

Une approche par les risques

- IA à risque inacceptable → interdite (notation sociale, manipulation psychologique)
- IA à risque élevé → encadrée (recrutement, crédit, décisions judiciaires)
- IA à risque limité → obligation de transparence
- IA à risque minimal → libre (filtre anti-spam, jeux vidéo)

Vos droits face aux décisions automatisées

- Droit à une explication (pourquoi un algorithme vous a refusé)
- Droit à une intervention humaine
- Droit de contestation de la décision

Réguler sans brider l'innovation

Qui est responsable quand l'IA cause un dommage ?

La grande question juridique du XXIe siècle

Le problème fondamental

- Une voiture autonome renverse un piéton — qui paie ?
- Un algorithme bancaire refuse votre crédit à tort — qui est responsable ?
- Un diagnostic médical par IA se trompe — quelle indemnisation ?

Ce que dit le droit aujourd'hui

- Responsabilité du fait des choses (art. 1242 al. 1 C. civ.) : le gardien de l'IA
- Responsabilité du fait des produits défectueux : la directive européenne de 2024
- L'IA Act (2024) : obligations de transparence et de gestion des risques

> *« L'IA n'est pas une personne juridique — ce sont toujours des humains qui répondent de ses défaillances. »*

Un vide juridique en voie de comblement

L'IA : à la fois un risque et un outil

🤖 L'IA comme risque

- Discrimination algorithmique
- Deepfakes et désinformation
- Remplacement d'emplois
- Opacité des décisions automatisées
- Atteinte à la vie privée

🛠️ L'IA comme outil

- Détection de fraudes bancaires
- Diagnostic médical précoce
- Tarification des assurances
- Prévention des cyberattaques
- Accessibilité et traduction

Le droit doit encadrer les risques sans brider les bénéfices

Deepfakes et arnaques à l'IA

Quand on ne peut plus croire ce qu'on voit ou entend

Le deepfake : une fausse réalité convaincante

- Vidéo ou audio fabriqués par l'IA pour imiter une personne réelle
- Faux appel téléphonique du « PDG » demandant un virement urgent
- Faux messages vocaux de proches demandant de l'argent en urgence

Ce que dit le droit

- Usurpation d'identité numérique : délit pénal (art. 226-4-1 C. pén.)
- Atteinte à la réputation : responsabilité civile et pénale
- L'IA Act impose une signalétique obligatoire sur les contenus générés

Réflexe : en cas de doute sur un appel ou une vidéo, raccrochez et rappelez vous-même le numéro officiel.

Synthèse — Vos données, vos droits

Ce qu'il faut retenir

Les acteurs qui vous protègent

- La CNIL (France) et ses équivalents dans chaque pays de l'UE
- Le DPO (délégué à la protection des données) de chaque organisation
- La justice civile et pénale

Vos réflexes en 3 points

- 1. Limitez ce que vous partagez en ligne
- 2. Lisez les politiques de confidentialité (les grandes lignes)
- 3. En cas de problème → CNIL, association de consommateurs, avocat

Les repères essentiels

III.

La menace cyber : identifier les risques

Phishing, rançongiciels, escroqueries en ligne

A. Qu'est-ce que le risque cyber ?

B. Les attaques contre les particuliers

C. Les attaques contre les organisations

D. La responsabilité juridique

Le risque cyber en chiffres

N°1

risque mondial
(Allianz 2024)

10 Md€

coût annuel
pour la France

385 000

plaintes cyber
en France (2023)

+65 %

hausse des
arcroqueries en ligne

Sources : ANSSI, Allianz Risk Barometer 2024, Ministère de l'Intérieur

Le risque cyber : de quoi parle-t-on ?

Une menace sur nos systèmes et nos données

Définition

Toute menace portant sur l'intégrité, la confidentialité ou la disponibilité de systèmes informatiques ou de données numériques.

Trois types d'atteinte

- Confidentialité : accès non autorisé à des données privées
- Intégrité : modification ou destruction de données
- Disponibilité : blocage d'un service (site hors ligne, système paralysé)

➜ Personne n'est à l'abri : particuliers, PME, hôpitaux, mairies, États

Systèmes et données en danger

L'hameçonnage (phishing)

L'arnaque numérique la plus répandue en France

Comment ça fonctionne ?

Un e-mail, SMS ou message imitant votre banque, La Poste, les impôts ou Ameli vous demande de cliquer sur un lien et de saisir vos identifiants.

Les signaux d'alerte

- Adresse expéditeur suspecte : ameli-sante@secure-fr.net
- Urgence exagérée : « Votre compte sera bloqué dans 24h »
- Fautes d'orthographe, mise en forme imparfaite
- Lien qui ne correspond pas exactement au site officiel

Règle d'or : votre banque, les impôts et Ameli ne vous demandent JAMAIS vos identifiants ou coordonnées bancaires par e-mail ou SMS.

La ligne jetée dans votre boîte mail

Les escroqueries ciblant les séniors

Des techniques de manipulation très sophistiquées

L'arnaque au faux conseiller bancaire

- Appel : « Des mouvements suspects ont été détectés sur votre compte »
- Demande de valider des opérations ou de communiquer des codes SMS
- Résultat : virement frauduleux depuis votre compte

Autres arnaques fréquentes

- Fausse assistance technique (Microsoft, Orange) : « Votre ordinateur est infecté »
- Arnaques aux sentiments : faux prétendants sur internet
- Faux remboursements Ameli, CAF ou impôts par SMS
- Arnaque au petit-fils : « Grand-mère, j'ai besoin d'argent en urgence »

L'arnaque commence souvent par un appel

Le rançongiciel (ransomware)

Vos fichiers pris en otage

Mécanisme de l'attaque

Un logiciel malveillant s'installe sur votre ordinateur, chiffre tous vos fichiers, et exige le paiement d'une rançon pour les débloquer.

Exemples réels

- Hôpital de Corbeil-Essonnes (2022) : 10 millions € demandés, 380 000 dossiers volés
- Mairie d'Annecy (2023) : services bloqués pendant plusieurs semaines
- Particuliers : photos de famille, documents personnels chiffrés

⚠️ **Ne JAMAIS payer la rançon : cela encourage les criminels sans garantie de récupération.**

Vos données verrouillées

L'usurpation d'identité numérique

Quand quelqu'un se fait passer pour vous en ligne

Comment cela se produit-il ?

- Vol de vos identifiants par phishing ou fuite de données
- Création d'un faux profil à votre nom sur les réseaux sociaux
- Utilisation de vos coordonnées pour ouvrir des crédits à votre insu

Les conséquences

- Dettes contractées à votre nom
- Atteinte à votre réputation en ligne
- Blocage bancaire, fichage à la Banque de France

Ce que dit le droit

- Délit pénal — art. 226-4-1 C. pén. : jusqu'à 1 an et 15 000 € d'amende

Votre identité volée

Les organisations dans la ligne de mire

Entreprises, hôpitaux, mairies : personne n'est épargné

Pourquoi cibler les hôpitaux ?

- Des données très sensibles (dossiers médicaux) très prisées sur le dark web
- Des systèmes informatiques souvent anciens et insuffisamment sécurisés
- Pression maximale : arrêt des soins = danger vital pour les patients

L'impact sur les usagers

- Reports d'opérations, retour aux dossiers papier
- Vos données de santé revendues sur le « dark web »

CH de Corbeil-Essonnes (2022) : les dossiers médicaux de 380 000 patients publiés en ligne après refus de payer la rançon.

Les hôpitaux, cibles privilégiées

La cybercriminalité face à la justice pénale

Des infractions spécifiques, des peines sévères

Les principales infractions numériques

- Accès frauduleux à un système informatique : 2 ans / 60 000 €
- Entrave à un système (rançongiciel) : 5 ans / 150 000 €
- Escroquerie en ligne : 5 ans / 375 000 €
- Usurpation d'identité numérique : 1 an / 15 000 €

➜ Peines aggravées lorsque la victime est vulnérable (personne âgée, enfant)

Le Code pénal à l'ère numérique

La responsabilité civile face au risque cyber

Au-delà du pénal : réparer le préjudice des victimes

Qui doit indemniser les victimes d'une cyberattaque ?

- L'entreprise piratée qui n'avait pas sécurisé vos données (faute, art. 1240 C. civ.)
- Le sous-traitant informatique défaillant (responsabilité contractuelle)
- L'éditeur du logiciel vulnérable (produits défectueux, dir. 2024/2853)
- Le prestataire cloud (obligation de sécurité, RGPD art. 32)

➜ La chaîne de responsabilité est souvent complexe : plusieurs acteurs peuvent être tenus

Une chaîne de responsabilités

Les entreprises ont des obligations légales

Ce que la loi impose pour protéger vos données

Notification obligatoire en cas de fuite

- RGPD : toute violation déclarée à la CNIL sous 72 heures
- Si risque élevé pour vous → vous devez être personnellement informé

Devoir de sécurité

- Chiffrement des données, contrôle des accès, audits de sécurité réguliers

En cas de manquement

- Sanction CNIL : jusqu'à 4 % du chiffre d'affaires mondial
- Responsabilité civile : indemnisation des victimes

Obligations et sanctions

L'assurance face au risque cyber

Un marché en plein essor, des questions complexes

Le marché de l'assurance cyber en France

- 328 millions € de primes collectées en 2023 (AMRAE)
- Couverture : restauration informatique, pertes d'exploitation, communication de crise

Questions délicates

- Paiement de rançons assurable ? LOPMI 2023 : oui, sous conditions strictes
- Amendes CNIL assurables ? Non en principe (caractère dissuasif)
- Particuliers : vérifiez votre assurance habitation — protection numérique parfois incluse

Se prémunir financièrement

La loi LOPMI 2023 : naissance de l'assurance cyber

Un cadre légal pour l'indemnisation des victimes

Ce que change la loi du 24 janvier 2023

- Création de l'art. L. 12-10-1 du Code des assurances
- L'assurance cyber est désormais un produit légalement encadré

La condition controversée : porter plainte en 72 heures

- Couverture : pertes et dommages causés par une cyberattaque
- Pour être indemnisé, la victime doit déposer plainte dans les 72 heures
- Un délai très court qui peut piéger les victimes non averties
- Objectif : faciliter les enquêtes et lutter contre la cybercriminalité

Un cadre neuf, des questions ouvertes

Les rançons : payer ou ne pas payer ?

Le dilemme juridique et éthique de l'assurance des rançons

Le débat juridique

- La LOPMI 2023 autorise l'assurance du paiement des rançons
- Condition : dépôt de plainte dans les 72 heures suivant le paiement
- Avant 2023, la question était un vide juridique total

Les arguments opposés

- Pour l'assurance : la victime doit être indemnisée de sa perte
- Contre : payer les rançons finance la criminalité et encourage les attaques
- Le Lloyd's de Londres exclut désormais les cyberattaques étatiques (2023)

⚠️ **Les autorités (ANSSI, Europol) déconseillent formellement le paiement des rançons.**

Un dilemme sans réponse simple

IV.

Se protéger et faire valoir ses droits

Conseils pratiques, recours, acteurs clés

A. L'hygiène numérique au quotidien

B. Reconnaître et signaler une arnaque

C. Les recours en cas de victimisation

D. Les acteurs qui vous aident

L'hygiène numérique : les bons réflexes

Des gestes simples pour se protéger efficacement

Mots de passe

- 12 caractères minimum, mélange lettres / chiffres / symboles
- Un mot de passe différent par site (gestionnaire : Bitwarden, KeePass)
- Jamais votre date de naissance, prénom ou « 123456 »

Double authentification (2FA)

- Code envoyé par SMS ou application en plus du mot de passe
- À activer en priorité : banque, e-mail, réseaux sociaux

Mises à jour — toujours les accepter

- Elles corrigent les failles de sécurité exploitées par les pirates

La sécurité commence par vous

Protéger ses appareils et sa navigation

Ordinateur, téléphone, tablette : les bons outils

Sur votre ordinateur

- Antivirus : Windows Defender (inclus dans Windows) suffit s'il est à jour
- Sauvegarde régulière : disque dur externe ou cloud (OneDrive, iCloud)
- Ne cliquez jamais sur un lien suspect dans un e-mail

Sur votre smartphone

- Verrou par code PIN ou biométrie (empreinte digitale, visage)
- Téléchargez uniquement depuis l'App Store ou Play Store officiels
- Évitez les opérations bancaires sur le Wi-Fi public (café, hôtel, gare)

→ Sauvegardez vos photos : un rançongiciel peut tout effacer

Votre matériel, votre responsabilité

Reconnaître une arnaque en ligne

DANGER	On vous demande des informations bancaires ou un code SMS
DANGER	L'offre est « trop belle pour être vraie » (cadeau, gain miraculeux)
DANGER	On crée une urgence artificielle : « Agissez maintenant ! »
DANGER	L'expéditeur ou le numéro vous est inconnu
ATTENTION	Fautes d'orthographe ou mise en forme inhabituelle
ATTENTION	Le lien ne correspond pas exactement au site officiel

Méfiance = protection

Vous êtes victime : que faire ?

Les étapes à suivre immédiatement

Étape 1 — Agissez vite

- Bloquez votre carte bancaire : appelez le 0 892 705 705 (24h/24)
- Changez immédiatement vos mots de passe compromis
- Déconnectez l'appareil infecté d'internet

Étape 2 — Signalez

- Portez plainte : commissariat, gendarmerie ou sur masecurite.fr
- E-mails frauduleux : signal.spam.gouv.fr
- SMS suspects : transférez au 33700

➜ Conservez toutes les preuves : captures d'écran, e-mails, relevés bancaires

Des recours accessibles à tous

Faire valoir ses droits : les recours

Du signalement à l'indemnisation

Voies de recours

- Plainte pénale : commissariat ou gendarmerie (gratuit)
- *Délai de prescription : 6 ans pour les délits numériques*
- Procédure civile : tribunal judiciaire pour obtenir réparation
- *Aide juridictionnelle possible si ressources limitées*
- CNIL : en cas d'atteinte à vos données personnelles (gratuit)

L'indemnisation bancaire

- Assurance habitation : souvent couverte (à vérifier dans votre contrat)
- Si vous n'avez pas été « négligent » : remboursement de la banque sous 48h
- *Art. L. 133-18 Code monétaire et financier*

La justice accessible à tous

Les acteurs qui vous aident

Un écosystème de protection à votre disposition

Qui ?	Pour quoi ?	Contact
CNIL	Protection des données personnelles	*www.cnil.fr*
Cybermalveillance.gouv	Aide aux victimes d'actes malveillants	*cybermalveillance.gouv.fr*
ANSSI	Sécurité informatique, guides pratiques	*ssi.gouv.fr*
Police / Gendarmerie	Dépôt de plainte, enquête pénale	*17 ou en ligne*
Banque de France	Médiation bancaire, fichage abusif	*banque-france.fr*
UFC-Que Choisir	Conseil consommateurs, action en justice	*quechoisir.org*

Un réseau de soutien coordonné

Protéger ses proches

Enfants, petits-enfants, entourage vulnérable

Protéger les enfants en ligne

- Contrôle parental : outils intégrés dans Windows, iPhone et Android (gratuits)
- Parler ouvertement des risques (harcèlement, images inappropriées)
- Vérifier les paramètres de confidentialité de leurs comptes

Aider les aînés

- Expliquer les arnaques les plus fréquentes (faux conseillers, colis)
- Mettre en place des alertes SMS sur les comptes bancaires
- Désigner une personne de confiance qui peut intervenir rapidement

Les ateliers numériques en médiathèque et maison de quartier sont gratuits : n'hésitez pas à y emmener vos proches.

Ce que font les entreprises et l'État

Obligations légales de prévention

La directive NIS 2 (2022)

- Impose à des milliers d'entreprises françaises des mesures de sécurité
- Analyse des risques, formation des employés, gestion des incidents
- Sanctions : jusqu'à 10 millions € ou 2 % du chiffre d'affaires mondial

Ce que cela signifie pour vous

- Votre banque, assureur, mutuelle sont obligés de sécuriser vos données
- Votre employeur doit former ses salariés aux risques cyber
- Votre mairie et l'hôpital public sont progressivement inclus dans le dispositif

Une régulation de plus en plus exigeante

Le bouclier réglementaire européen

Pourquoi l'Europe réglemente autant le numérique

Une philosophie de protection

- L'Europe fait le choix de protéger les individus face aux géants du numérique
- Ce n'est pas un frein à l'innovation : c'est une gouvernance par les valeurs
- Les droits fondamentaux (vie privée, non-discrimination) guident chaque texte
- L'Europe est devenue l'exportatrice mondiale de normes numériques

Un arsenal juridique sans précédent

- RGPD (2018) — données personnelles
- DSA (2022) — contenus en ligne
- DMA (2022) — concurrence numérique
- NIS2 (2022) — cybersécurité
- AI Act (2024) — intelligence artificielle
- DORA (2025) — résilience financière numérique

L'Europe, puissance normative

NIS2, DORA, DSA, DMA : un arsenal coordonné

Chaque texte protège un aspect de votre vie numérique

Texte	Objet	Vous protège contre
NIS2	Cybersécurité des entreprises	*Pannes et piratages des services essentiels*
DORA	Résilience financière numérique	*Défaillances informatiques de votre banque*
DSA	Services numériques	*Contenus illicites, désinformation en ligne*
DMA	Marchés numériques	*Pratiques anticoncurrentielles des GAFAM*
AI Act	Intelligence artificielle	*Décisions automatisées abusives ou biaisées*

Un filet de sécurité européen

Le droit numérique de demain

Les grandes tendances à surveiller

Ce qui arrive en Europe

- Identité numérique européenne : un portefeuille unique (eIDAS 2)
- Règlement sur les données (Data Act) : plus de contrôle sur vos données
- Droit à la réparation numérique : lutte contre l'obsolescence programmée

Les grands débats

- Chiffrement vs. sécurité publique (accès des États aux messageries ?)
- Régulation de l'IA générative : qui est responsable des contenus créés ?
- Souveraineté numérique : où sont stockées vos données ?

Un chantier législatif permanent

La concentration des risques : un défi systémique

Quand tout repose sur les mêmes acteurs

Le numérique concentre les risques de manière inédite. Quand un seul acteur tombe, tout le monde est touché.

Les caractéristiques structurelles du risque numérique

- Corrélation des sinistres : une faille chez un hébergeur touche des millions de sites
- Concentration : 3 entreprises (AWS, Azure, Google Cloud) hébergent 65 % du web mondial
- Effet domino : la panne de CrowdStrike (2024) a paralysé des aéroports et des hôpitaux
- Asymétrie : l'utilisateur ne peut ni évaluer ni maîtriser ces risques

> *Le risque numérique est systémique : il ressemble davantage à une pandémie qu'à un accident de voiture.*

Un risque systémique mondial

Le low tech : une alternative juridique ?

Repenser notre rapport au numérique par le droit

Le mouvement low tech

- Questionner le tout-numérique : faut-il toujours plus de technologie ?
- Réduire l'empreinte environnementale du numérique (4 % des émissions mondiales de CO2)
- Favoriser des solutions simples, réparables, durables
- Un mouvement qui interroge aussi le droit

Les enjeux juridiques émergents

- Droit à la déconnexion et sobriété numérique
- Lutte contre l'obsolescence programmée (loi AGEC 2020)
- Droit à la réparation (directive européenne 2024)
- Souveraineté technologique : ne pas tout déléguer au cloud

Moins de tech, plus de droit ?

L'humanisme juridique face au numérique

Le droit au service de l'humain, pas de la machine

Le fil rouge de la réglementation européenne

- Le droit numérique européen repose sur un postulat humaniste
- La technologie doit servir les individus, non l'inverse
- Chaque texte (RGPD, AI Act, DSA) place la personne au centre

Les grands principes en jeu

- Dignité humaine : pas de notation sociale, pas de manipulation
- Non-discrimination : les algorithmes ne doivent pas reproduire les biais
- Transparence : comprendre les décisions qui nous concernent
- Contrôle humain : un humain doit toujours pouvoir intervenir

La boussole humaniste

Vos droits numériques en 6 points

1 **Droit d'accès**

Savoir quelles données on détient sur vous

2 **Droit de rectification**

Corriger vos données erronées

3 **Droit à l'effacement**

Demander la suppression de vos données

4 **Droit à la portabilité**

Récupérer et transférer vos données

5 **Droit d'opposition**

Vous opposer à certains traitements

6 **Droit à l'explication**

Comprendre les décisions automatisées vous concernant

Ressources pratiques

Les sites et numéros à connaître absolument

Signalement

→ signal.spam.gouv.fr — signaler les e-mails frauduleux

→ 33700 — signaler un SMS suspect

→ internet-signalement.gouv.fr (PHAROS)

Aide aux victimes

→ cybermalveillance.gouv.fr — mise en relation avec des experts locaux

→ 0 892 705 705 — opposition carte bancaire (24h/24)

Vos droits

→ cnil.fr — plaintes et informations RGPD

→ service-public.fr — démarches officielles en ligne

Conseils

→ ssi.gouv.fr — guides de sécurité ANSSI (version grand public)

→ cybermalveillance.gouv.fr → kit sensibilisation (gratuit, imprimable)

À mettre dans vos favoris

Ma charte numérique personnelle

Mots de passe forts

12 car. min., 1 par site, gestionnaire

Double authentification

Activée sur banque, e-mail, réseaux

Mises à jour

Acceptées dès qu'elles arrivent

Sauvegardes régulières

Photos et docs sur disque externe

Vigilance arnaque

Vérifier l'expéditeur, jamais se presser

Porter plainte

Toujours si victime, conserver les preuves

🧠 Testez vos connaissances

Q1. Votre banque vous envoie un e-mail pour confirmer votre code secret. Que faites-vous ?

→ *Vous ne répondez JAMAIS. Appelez votre banque directement sur son numéro officiel.*

Q2. Un message vous dit que vous avez gagné un iPhone. Que faites-vous ?

→ *Vous supprimez sans cliquer : c'est une arnaque (phishing).*

Q3. Votre ordinateur est « bloqué » et affiche un message demandant de payer. Que faites-vous ?

→ *Vous ne payez pas. Vous allez sur Cybermalveillance.gouv.fr ou appelez un technicien.*

Questions — Réponses

Quelques situations fréquemment rencontrées

? Ma carte a été débitée sans mon accord. Que faire ?

Faites opposition immédiatement (0 892 705 705), puis contestez par écrit. La loi oblige la banque à rembourser si vous n'avez pas été négligent.

? J'ai donné mon numéro de sécurité sociale par téléphone. Est-ce grave ?

Oui. Prévenez votre CPAM, surveillez vos remboursements et signalez sur Signal.spam. Portez plainte si vous constatez une usurpation.

? Mon petit-fils m'a dit avoir besoin d'argent en urgence par message. Que faire ?

Rappeler le numéro habituel de votre petit-fils avant tout. L'arnaque « au grand-père » est très répandue. Ne jamais virer d'argent sans vérification orale.

Conclusion

Le numérique : une chance à saisir en connaissance de cause

- **Le numérique est entré dans toutes nos vies — avec des opportunités considérables.**
- Mais chaque usage laisse des traces et ouvre des vulnérabilités.
- Le droit vous protège : RGPD, CNIL et Code pénal sont de votre côté.
- La vigilance est votre meilleure protection — elle s'apprend et se partage.
- En cas de problème, vous n'êtes jamais seul : des acteurs publics existent.

Merci de votre attention

Antoine Touzain
Professeur agrégé de droit privé
Université Rouen Normandie — CUREJ

Université Populaire de Poissy

À retenir

- cybermalveillance.gouv.fr
- cnil.fr
- signal.spam.gouv.fr
- 33700 (SMS frauduleux)
- 0 892 705 705 (opposition CB)
- internet-signalement.gouv.fr

Toutes ces ressources sont gratuites et accessibles à tous.