PETIT GUIDE

pour comprendre

L'INFORMATIQUE

sans se prendre la tête

33 notions expliquées avec des images simples

Le glossaire du Guide de Souveraineté Numérique



Vague 0 : comprendre le vocabulaire

en 33 notions

Gabriel Ananda gabriel.ananda@mailo.com

Version 1.5

11 novembre 2026

CC BY SA

Sommaire

Partie 1 : Les bases de l'informatique....3
1. L'ordinateur (ou "PC") – Computer....3
2. Le système d'exploitation – Operating System (OS)....4
3. Le logiciel (ou application) – Software / App....5
4. Différence entre Internet et le Web – Internet vs World Wide Web....5
5. Navigateur web – Web browser....6
6. Moteur de recherche – Search engine....6
7. Logiciel propriétaire – Proprietary software....7
8. Logiciel libre / Open Source – Free software / Open Source....8
9. Les pièges des "gratuits" en ligne....9
10. Pourquoi tant de mots différents ? (récap des bases)....9
Partie 2 : Notions complémentaires (pour aller plus loin)....10
11. Le cloud (ou "nuage") – Cloud....10
12. Le chiffrement (ou cryptage) – Encryption....12
13. La donnée – Data....13
14. L'adresse IP – IP address....13
15. Le pare-feu – Firewall....14
16. Le cookie (ou témoin de connexion) – Cookie....14
17. Le VPN – Virtual Private Network (VPN)....15
18. Le serveur – Server....16
19. Le client (informatique) – Client....17
20. Le protocole (informatique) – Protocol....17
21. Les permissions (ou droits d'accès) – Permissions / Access rights....18
22. La base de données – Database....19
23. Le mot de passe et l'authentification – Password & Authentication....20
24. Le DNS (Domain Name System) – DNS....21
25. La sauvegarde – Backup....22
26. L'antivirus et les logiciels malveillants – Antivirus & Malware....23
27. L'intelligence artificielle (IA) – Artificial Intelligence (AI)....24
28. L'hameçonnage – Phishing....25
29. Les objets connectés – Internet of Things (IoT)....26
30. L'alias de courriel – Email alias....27
31. La fuite de données – Data breach....27
32. Le NFC (le « sans contact ») – Near Field Communication (NFC)....28
33. OpenPGP (chiffrer et signer) – OpenPGP....29
34. Le Fédivers (réseau fédéré, instance) – Fediverse....30
35. La mise à jour (correctif, fin de support) – Software update....31
36. Le format ouvert et le verrou numérique (DRM) – Open format and DRM....32
Partie 3 : Récapitulatif général....33
Tableau des 36 notions....33
La phrase à retenir absolument....36
Trois petits conseils pour commencer....36

Partie 1 : Les bases de l'informatique

Vous utilisez un ordinateur, un téléphone ou une tablette sans vraiment savoir ce qui se passe dedans ? C'est tout à fait normal. Ce guide a été écrit pour vous : il ne suppose aucun savoir préalable.

Nous allons voir ensemble, pas à pas, les grandes pièces du puzzle informatique : d'abord les bases (ordinateur, logiciel, navigateur...), puis des notions un peu plus techniques (cloud, chiffrement, IP, pare-feu, etc.). Tout est expliqué avec des mots simples, sans jargon inutile.

---

1. L'ordinateur (ou "PC") – Computer

C'est quoi ?

Un ordinateur est une machine physique – ce que vous pouvez toucher. Il contient un écran (parfois séparé), un clavier, une souris, et une "tour" ou un bloc principal.

L'image à garder en tête : un ordinateur, c'est comme une maison vide. Elle a des murs, des pièces, des prises électriques... mais elle ne fait rien toute seule. Il faut l'habiter et la meubler.

Le terme "PC" vient de "Personal Computer" (ordinateur personnel). On l'utilise souvent pour parler des ordinateurs fonctionnant avec Windows, mais techniquement un Mac (Apple) ou un ordinateur sous Linux sont aussi des PC.

À retenir : l'ordinateur = la machine en métal, plastique et circuits électroniques.

---

2. Le système d'exploitation – Operating System (OS)

C'est quoi ?

Le système d'exploitation (OS = Operating System) est le "chef d'orchestre" de la machine. C'est lui qui :

•démarre l'ordinateur,
•gère ce qui s'affiche à l'écran,
•permet d'ouvrir et fermer des logiciels,
•fait le lien entre vous (vos clics) et les composants électroniques.

L'image : si l'ordinateur est une maison vide, le système d'exploitation est l'ensemble des règles de base qui font fonctionner cette maison : électricité, plomberie, portes qui s'ouvrent... Sans lui, la maison n'est qu'un tas de matériaux inertes.

Les plus connus :

•**Windows** (Microsoft) → le plus répandu sur les ordinateurs personnels.
•**macOS** (Apple) → celui des Mac.
•**Linux** → un système gratuit, plus discret mais très utilisé (souvent sans que vous le sachiez, dans les serveurs, les téléphones Android, les box internet...).
•**iOS** (Apple) → celui des iPhone / iPad.
•**Android** (Google) → celui de la plupart des téléphones et tablettes non-Apple. Il existe aussi des versions d'Android sans Google, comme /e/OS ou GrapheneOS.

À retenir : le système d'exploitation est le premier logiciel qui se lance quand vous allumez votre machine. Il rend l'ordinateur utilisable.

3. Le logiciel (ou application) – Software / App

C'est quoi ?

Un logiciel est un programme qui fait quelque chose de précis : écrire une lettre, calculer un budget, naviguer sur Internet, regarder une vidéo, jouer...

L'image : dans notre maison (ordinateur), les logiciels sont les meubles et appareils : une table pour écrire, un frigo pour stocker, une télé pour regarder des films. La maison vide ne sert à rien ; une fois meublée, elle devient utile.

Différents noms : on dit aussi "application" (surtout sur téléphone), "programme", "app". C'est la même idée.

Exemples de logiciels :

•Pour écrire un texte → Word, LibreOffice Writer, Pages, Bloc-notes.
•Pour naviguer sur le web → Firefox, Chrome, Edge, Safari.
•Pour regarder une photo → la visionneuse d'images intégrée.

À retenir : un ordinateur sans logiciel ne sert à rien. Le système d'exploitation lui-même est un logiciel un peu particulier.

---

4. Différence entre Internet et le Web – Internet vs World Wide Web

•**Internet** est le réseau physique mondial : des câbles sous-marins, des fibres optiques, des routeurs, des antennes 4G/5G, des serveurs, etc. C'est l'infrastructure matérielle qui permet aux ordinateurs de communiquer entre eux (comme le réseau routier).

•**Le web** (World Wide Web) est l'un des services qui utilise Internet. Ce sont les pages web, les sites, les liens hypertexte, les vidéos YouTube, etc. Il fonctionne sur le protocole HTTP/HTTPS (comme les voitures qui roulent sur les routes).

Métaphore simple :

•Internet = **les routes** (le réseau physique)
•Le web = **les voitures, les camions, les vélos** (les services qui circulent)

D'autres services utilisent aussi Internet sans passer par le web : les emails (SMTP), le transfert de fichiers (FTP), le jeu en ligne, la visioconférence, etc.

---

5. Navigateur web – Web browser

C'est quoi ?

Le navigateur est un logiciel spécialisé pour aller sur Internet. C'est la "porte d'entrée" du web. Vous l'utilisez pour visiter des sites (YouTube, Wikipédia, vos emails en ligne...).

L'image : si Internet est un océan gigantesque avec des millions d'îles (les sites web), le navigateur est votre bateau. Selon le bateau, la traversée est plus ou moins agréable, plus ou moins rapide, plus ou moins sécurisée.

Les principaux navigateurs :

•Firefox (indépendant, open source)
•Chrome (Google – très répandu)
•Edge (Microsoft)
•Safari (Apple)
•Brave, Vivaldi, etc.

À retenir : le navigateur, ce n'est PAS Internet. C'est l'outil pour y accéder. Sans navigateur, vous ne pouvez pas voir de site web.

6. Moteur de recherche – Search engine

C'est quoi ?

Le moteur de recherche est un site web qui vous aide à trouver d'autres sites web. Vous tapez des mots, il vous renvoie une liste de réponses.

L'image : dans l'océan Internet, le navigateur est le bateau ; le moteur de recherche est le sonar ou le GPS qui repère où se trouvent les îles (sites) dont vous avez besoin.

Les principaux moteurs :

•Google (très majoritaire, mais il vous trace et collecte vos données)
•Bing (Microsoft)
•DuckDuckGo (ne vous trace pas, sans publicité ciblée)
•Qwant (français, plus respectueux)

Ne pas confondre :

•Le **navigateur** = le logiciel (Firefox, Chrome)
•Le **moteur de recherche** = le site dans lequel vous tapez votre question (Google, DuckDuckGo)

Vous pouvez utiliser n'importe quel moteur dans n'importe quel navigateur.

---

7. Logiciel propriétaire – Proprietary software

C'est quoi ?

Un logiciel propriétaire est un logiciel dont on ne peut pas voir le code secret (les instructions précises qui le composent). Comme une recette de cuisine cachée par le cuisinier. Vous avez le droit de l'utiliser (souvent en payant), mais vous ne pouvez pas le modifier, ni le partager librement, ni savoir exactement ce qu'il fait dans votre dos.

L'image : vous achetez une voiture dont le capot est soudé. Elle roule très bien, mais vous ne pouvez pas réparer vous-même un petit problème, ni comprendre pourquoi elle émet parfois des signaux bizarres.

Exemples :

•Windows (Microsoft)
•Microsoft Office (Word, Excel, PowerPoint)
•Adobe Photoshop
•Google Chrome (oui, même s'il est gratuit, il est propriétaire : c'est Google qui décide de ce qu'il contient)

À retenir : avec un logiciel propriétaire, vous êtes "client". Vous n'avez aucun contrôle dessus.

---

8. Logiciel libre / Open Source – Free software / Open Source

C'est quoi ?

Un logiciel libre (ou "open source") est un logiciel dont le code source est public. N'importe qui peut le lire, le modifier, l'améliorer, le copier, le partager. C'est comme une recette de cuisine affichée dans la cuisine du restaurant.

L'image : vous avez une voiture dont le capot s'ouvre, avec le manuel de réparation fourni. Vous ou un mécanicien de confiance pouvez la réparer, l'améliorer, ou même construire une voiture similaire pour votre voisin.

Ce que ça change concrètement :

•Souvent gratuit (pas toujours, mais la plupart du temps)
•Pas de piège : personne ne peut cacher un espion ou une publicité intrusive dans un logiciel libre, car des milliers de gens peuvent vérifier
•Pas d'abonnement surprise : vous restez propriétaire de ce que vous faites
•Communauté : des bénévoles ou des entreprises peuvent améliorer le logiciel sans attendre l'accord d'un grand éditeur

Exemples :

•LibreOffice (alternative gratuite à Microsoft Office)
•Firefox (navigateur)
•GIMP (dessin, retouche photo, alternative à Photoshop)
•VLC (lecteur vidéo)
•Linux (système d'exploitation)
•Nextcloud, Cryptpad, Framadate

À retenir : "libre" ne veut pas dire forcément "gratuit" (même si c'est souvent le cas), mais "respectueux de vos libertés". Vous pouvez utiliser, étudier, modifier et partager le logiciel. Attention : un logiciel dont le code est seulement « consultable » n'est pas forcément libre, s'il est interdit de le modifier ou de le partager.

---

9. Les pièges des "gratuits" en ligne

Pourquoi certains services gratuits (Google, Gmail, Facebook, Doodle, etc.) peuvent poser problème ?

•**Vous n'êtes pas le client, vous êtes le produit** – Le service est gratuit parce que l'entreprise gagne de l'argent en collectant vos données (vos centres d'intérêt, vos habitudes, vos contacts, parfois vos messages) pour les revendre sous forme de publicité ciblée.
•**Les logiciels propriétaires peuvent faire ce qu'ils veulent** – Puisque vous ne pouvez pas voir leur code, vous ne savez pas réellement ce qu'ils collectent, ni où vos données partent.

À l'inverse, un logiciel libre ou un service libre (comme Framadate ou Cryptpad) ne peut pas cacher de collecte douteuse, car tout le monde peut inspecter son fonctionnement.

---

10. Pourquoi tant de mots différents ? (récap des bases)

Terme (français)	Terme (anglais)	Traduction simple	Exemple
Ordinateur / PC	Computer	La machine physique	Un Dell, un MacBook, un Asus
Système d'exploitation	Operating System (OS)	Le chef d'orchestre qui fait tourner la machine	Windows, macOS, Linux
Logiciel / Application	Software / App	Programme qui fait une tâche précise	Word, VLC, Firefox
Navigateur	Web browser	Logiciel pour aller sur Internet	Firefox, Chrome, Edge
Moteur de recherche	Search engine	Site web qui trouve d'autres sites	Google, DuckDuckGo
Logiciel propriétaire	Proprietary software	Code secret, non modifiable	Windows, Microsoft Office
Logiciel libre / Open Source	Free / Open Source software	Code public, modifiable, partageable	LibreOffice, Firefox, Linux

---

Partie 2 : Notions complémentaires (pour aller plus loin)

Maintenant que vous connaissez les bases, voici d'autres termes que vous rencontrerez fréquemment, avec le même style simple.

---

11. Le cloud (ou "nuage") – Cloud

C'est quoi ?

Le cloud, c'est le fait de stocker vos fichiers sur des serveurs distants (des ordinateurs puissants quelque part sur la planète) au lieu de les garder uniquement sur votre disque dur. Vous y accédez via Internet.

L'image : au lieu de garder vos photos dans un album chez vous, vous les mettez dans un coffre sécurisé chez un voisin – mais vous pouvez les voir, les modifier, les partager depuis n'importe où, avec un mot de passe.

Exemples : Google Drive, iCloud (Apple), OneDrive (Microsoft), Dropbox, pCloud, Nextcloud.

À savoir : Le cloud est pratique, mais vos fichiers sont physiquement sur les ordinateurs d'une entreprise. Avec un cloud "libre" (Nextcloud auto-hébergé), vous gardez le contrôle. Avec Google Drive, vos fichiers peuvent être analysés.

Les trois localisations possibles pour vos données :

Type	Description
Disque dur local	Fichiers uniquement sur l'ordinateur connecté. Pas besoin d'Internet. Pas accessibles depuis d'autres appareils sans copie manuelle.
Cloud auto-hébergé (Nextcloud, Seafile)	Fichiers sur un serveur personnel chez vous. Accès depuis n'importe quel appareil. Synchronisation automatique. **Vous contrôlez physiquement vos données.**
Cloud non auto-hébergé (Google Drive, iCloud, OneDrive)	Fichiers sur les serveurs d'une entreprise tierce. Accès depuis n'importe où. **Vous ne contrôlez pas vos données** : l'entreprise peut les analyser, les utiliser pour

Type	Description
	ses IA, et les autorités américaines peuvent les réquisitionner (Cloud Act).

Métaphore simple :

•Disque dur local = **votre portefeuille physique** (vous l'avez sur vous, mais difficile à partager)
•Cloud auto-hébergé = **votre bibliothèque personnelle chez vous** (vous contrôlez tout)
•Cloud non auto-hébergé = **un casier chez un gardien** (pratique, mais le gardien a un double des clés)

En résumé : Le cloud auto-hébergé vous donne la commodité du cloud avec la souveraineté du stockage local. Le cloud non auto-hébergé vous donne la commodité mais vous perdez le contrôle.

---

12. Le chiffrement (ou cryptage) – Encryption

C'est quoi ?

Le chiffrement, c'est l'action de brouiller un message (ou un fichier) pour qu'il devienne illisible sans une clé secrète.

L'image : vous écrivez une lettre, puis vous la transformez avec un code secret. Même si quelqu'un l'intercepte en chemin, il ne verra qu'un charabia incompréhensible. Seule la personne qui possède la clé peut la "déchiffrer" et lire le vrai message.

Où on le trouve :

•Dans les navigateurs (le petit cadenas dans la barre d'adresse)
•Dans les messageries (Signal, WhatsApp, Telegram en mode "chiffré")

•Dans les VPN (comme Proton VPN)
•Dans les mots de passe (stockés chiffrés)

Chiffrement de bout en bout - **end-to-end-encryption** : les données sont chiffrées sur l'appareil de l'émetteur et ne sont déchiffrées que sur l'appareil du destinataire. **Même l'entreprise qui transmet le message ne peut pas le lire.**

Métaphore : vous mettez une lettre dans une enveloppe scellée, vous l'envoyez par la poste, et seul le destinataire a la clé pour l'ouvrir. Le facteur (l'entreprise) ne sait pas ce qu'il y a dedans.

Exemples : Signal, WhatsApp (dans les discussions normales), Proton Mail (entre utilisateurs Proton), SimpleX.

Ce que ce n'est pas : le chiffrement "standard" (comme le cadenas HTTPS) protège la liaison entre vous et le serveur, mais le serveur peut lire vos données. Le chiffrement de bout en bout protège vos données **même du serveur**.

---

13. La donnée – Data

C'est quoi ?

Une donnée, c'est une information brute, isolée, avant d'être interprétée. Par exemple : "25/03/1990" est une donnée. "Alice a 34 ans" est une information construite à partir de cette donnée.

L'image : les données sont comme des grains de sable. Chaque grain ne veut rien dire tout seul. Mais quand on les rassemble (date, nom, âge, adresse), on obtient une plage – c'est l'information utile.

Exemples de données : votre âge, votre adresse IP, l'heure de votre connexion, le modèle de votre téléphone, votre historique de recherche...

À savoir : Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) collectent massivement vos données pour les revendre ou pour entraîner leurs intelligences artificielles.

---

14. L'adresse IP – IP address

C'est quoi ?

Une adresse IP (Internet Protocol) est un numéro d'identification unique attribué à votre appareil (ordinateur, téléphone, box internet) quand il se connecte à Internet. C'est comme une plaque d'immatriculation.

L'image : sur Internet, chaque machine doit avoir une adresse pour que les informations sachent où aller. L'adresse IP, c'est comme le numéro de votre maison sur une rue : sans lui, le facteur (les données) ne sait pas où livrer.

Ce qu'elle révèle :

•Votre localisation approximative (souvent la ville, parfois le quartier)
•Votre fournisseur d'accès (Orange, SFR, Free...)

Pourquoi c'est important : Un site web peut voir votre adresse IP. Un VPN la masque (il la remplace par celle du serveur VPN).

---

15. Le pare-feu – Firewall

C'est quoi ?

Un pare-feu est un filtre qui surveille tout ce qui entre et sort de votre ordinateur ou de votre réseau. Il bloque automatiquement ce qui semble dangereux.

L'image : c'est le videur à l'entrée d'une discothèque. Il vérifie qui entre et qui sort. Si quelqu'un a l'air louche (un virus, une tentative d'intrusion), il le refuse.

Exemples :

•Le pare-feu intégré à Windows (Windows Defender Firewall)
•Le pare-feu de votre box internet
•Un pare-feu logiciel tiers

À retenir : Un pare-feu ne détecte pas forcément les virus (c'est le rôle de l'antivirus). Il surveille les connexions (qui parle à qui).

---

16. Le cookie (ou témoin de connexion) – Cookie

C'est quoi ?

Un cookie est un petit fichier qu'un site web dépose sur votre ordinateur pour se souvenir de vous. Il peut retenir votre connexion, votre panier d'achat, vos préférences de langue...

L'image : c'est comme un post-it que le site vous colle sur l'épaule. Quand vous revenez, il lit le post-it : "Ah, c'est Alice. Elle parlait français. Elle avait mis des chaussures dans son panier."

Les bons cookies : vous permettent de rester connecté sans retaper votre mot de passe à chaque page.

Les mauvais cookies (traqueurs) : des cookies déposés par des régies publicitaires pour suivre vos visites d'un site à l'autre et établir votre profil d'intérêts (ciblage publicitaire).

En résumé : Tous les cookies ne sont pas malveillants. Mais les cookies tiers (ceux déposés par une autre société que le site que vous visitez) sont souvent utilisés pour vous pister.

---

17. Le VPN – Virtual Private Network (VPN)

C'est quoi ?

Un VPN est un **tunnel chiffré** entre votre appareil (ordinateur, téléphone) et un serveur distant. Tout votre trafic Internet passe par ce tunnel.

Ce que ça fait :

•**Masque votre adresse IP** : les sites web voient l'IP du serveur VPN, pas la vôtre.
•**Chiffre vos données** : votre fournisseur d'accès Internet (Orange, Free, etc.) ne voit pas quels sites vous visitez (il voit seulement que vous utilisez un VPN).
•**Protège sur les réseaux WiFi publics** (café, aéroport, gare) : personne sur le même réseau ne peut espionner votre navigation.

Métaphore simple :

•Internet sans VPN = une **carte postale** : tout le monde peut la lire (facteur, postiers, voisins).
•Internet avec VPN = une **enveloppe scellée** : seul le destinataire peut l'ouvrir.

Ce qu'un VPN ne fait pas :

•Il ne vous rend pas complètement anonyme (le fournisseur VPN peut théoriquement vous identifier si vous payez par carte bancaire).

•Il ne bloque pas les publicités ou les traqueurs (c'est le rôle d'un bloqueur comme uBlock Origin).
•Il ne vous protège pas si vous donnez vous-même vos identifiants sur un site de phishing.

Cas d'usage typiques :

•Se connecter à un réseau professionnel depuis l'extérieur.
•Protéger ses données sur un WiFi public.
•Contourner la censure géographique (certains sites ou services bloqués dans un pays).
•Cacher sa navigation à son FAI (pour une raison légitime ou non).

---

18. Le serveur – Server

C'est quoi ?

Un serveur est un ordinateur très puissant qui reste allumé en permanence et qui fournit des services à d'autres ordinateurs (les "clients").

L'image : dans un restaurant, le serveur (humain) apporte la nourriture aux tables. En informatique, le serveur (machine) envoie des pages web, des emails, des fichiers à ceux qui les demandent.

Exemples :

•Le serveur de Google : quand vous tapez une recherche, c'est lui qui vous renvoie les résultats
•Le serveur de YouTube : il héberge les vidéos
•Votre box internet contient aussi des petits serveurs (serveur DHCP, serveur DNS local)

À retenir : Votre ordinateur personnel peut devenir un serveur (si vous installez un logiciel serveur) mais ce n'est pas son usage courant.

19. Le client (informatique) – Client

C'est quoi ?

En informatique, un "client" est un logiciel (ou un appareil) qui demande un service à un serveur.

L'image : dans le restaurant, vous êtes le client : vous commandez, le serveur vous apporte. Votre navigateur (Firefox, Chrome) est un client : il demande une page web au serveur.

Exemples de clients :

•Navigateur web (client du serveur web)
•Client email (Thunderbird, Outlook, l'application mail de votre téléphone)
•Client VPN (l'application Proton VPN sur votre PC)

À retenir : La plupart des logiciels que vous utilisez sont des "clients" : ils parlent à des serveurs quelque part.

---

20. Le protocole (informatique) – Protocol

C'est quoi ?

Un protocole informatique est un ensemble de règles que deux machines s'engagent à suivre pour communiquer correctement.

L'image : quand deux personnes se parlent, elles suivent des règles implicites : l'une parle, l'autre écoute, on utilise des mots compris par les deux. Les protocoles en informatique, c'est la même chose, mais pour les machines.

Exemples :

•**HTTP / HTTPS** (le protocole pour naviguer sur le web) – c'est le langage entre votre navigateur et le site web
•**SMTP** (pour envoyer des emails)
•**DNS** (résoudre les noms de domaine – transformer google.com en adresse IP)
•**WireGuard / OpenVPN** (protocoles chiffrés pour les VPN)
•**CalDAV / CardDAV** (synchroniser agenda et contacts entre vos appareils, chez le fournisseur de votre choix)

À savoir : Le "S" de HTTPS signifie "Secured" (sécurisé). Si un site est en `https://`, les échanges sont chiffrés (vous voyez le petit cadenas). Si c'est `http://` (sans S), tout s'échange en clair → vulnérable.

---

21. Les permissions (ou droits d'accès) – Permissions / Access rights

C'est quoi ?

Les permissions sont des règles qui disent qui peut faire quoi avec un fichier, un dossier ou une fonction d'un logiciel.

L'image : dans une maison, certaines pièces sont privées (chambre), d'autres sont publiques (salon). Les permissions, c'est votre plan de la maison : "Moi, je peux tout. Les enfants peuvent accéder à la cuisine mais pas au bureau. Les invités, seulement le salon."

Exemples de permissions :

•**Lecture** (voir le contenu)
•**Écriture** (modifier, supprimer, ajouter)
•**Exécution** (lancer un programme)

Où on les trouve :

•Sur les fichiers (un document en "lecture seule")
•Sur un serveur (qui a le droit d'administrer, qui peut juste écouter)
•Sur votre téléphone (une application a-t-elle le droit d'utiliser le micro, la caméra, la localisation, vos contacts ?)

À retenir : Un administrateur (ou "admin") est quelqu'un qui a toutes les permissions (ou plus que les autres).

---

22. La base de données – Database

C'est quoi ?

Une base de données est une collection organisée d'informations, rangée pour pouvoir être retrouvée rapidement. C'est comme une immense bibliothèque, mais version numérique.

L'image : imaginez un classeur immense avec des milliers de fiches classées par ordre alphabétique, par catégorie, avec des index. La base de données, c'est ce classeur, sauf qu'il est dans l'ordinateur et qu'on peut poser des questions ultra-rapides.

Exemples :

•Votre répertoire téléphonique (noms, numéros)
•Le catalogue d'Amazon
•Votre liste de vidéos YouTube vues récemment
•Un fichier Excel peut être une base de données simple (mais limitée)

À savoir : La plupart des sites web que vous utilisez reposent sur une base de données (membres, articles, commentaires, commandes...).

---

23. Le mot de passe et l'authentification – Password & Authentication

C'est quoi ?

Un mot de passe est une clé secrète que vous utilisez pour prouver que vous êtes bien vous. C'est comme une clé de maison : seule la personne qui la possède peut ouvrir la porte. L'authentification, c'est le processus global qui vérifie votre identité : "C'est bien toi ?"

L'image : vous arrivez à votre immeuble. Pour entrer, vous avez besoin de votre clé (le mot de passe). Mais pour plus de sécurité, il y a un deuxième verrou (l'authentification à deux facteurs, ou 2FA) : par exemple, un code envoyé par SMS sur votre téléphone. Sans les deux, vous ne pouvez pas entrer.

Les trois facteurs possibles (ce que vous pouvez utiliser pour prouver votre identité) :

•**Quelque chose que vous savez** : votre mot de passe, un code PIN.
•**Quelque chose que vous possédez** : votre téléphone (qui reçoit un code), une clé physique (YubiKey).
•**Quelque chose que vous êtes** : votre empreinte digitale, votre visage (reconnaissance faciale).

Exemples :

•Se connecter à votre boîte email = mot de passe (facteur 1)
•Ajouter un code reçu par SMS = deuxième facteur (2FA)
•Déverrouiller votre téléphone avec votre empreinte = facteur biométrique

Pourquoi c'est important :

•Un mot de passe seul peut être volé (piratage de site, tentative de deviner, etc.)
•Avec la double authentification (2FA), même si un pirate a votre mot de passe, il ne peut pas se connecter car il n'a pas votre téléphone (ou votre clé).

À retenir : Ne réutilisez jamais le même mot de passe sur plusieurs sites, et choisissez-en d'au moins 12 caractères. Si un site est piraté, vos autres comptes restent protégés. Utilisez un gestionnaire de mots de passe libre (KeePassXC, Proton Pass, Bitwarden...) pour générer et stocker des mots de passe uniques et complexes.

---

24. Le DNS (Domain Name System) – DNS

C'est quoi ?

Le DNS (Domain Name System) est l'annuaire téléphonique d'Internet. Il transforme les noms de domaine que vous tapez (comme `google.com` ou `lemonde.fr`) en adresses IP (des séries de chiffres du style `172.217.168.46`) que les ordinateurs comprennent.

L'image : vous voulez appeler votre ami. Vous ne connaissez pas son numéro de téléphone par cœur. Vous cherchez son nom dans l'annuaire (ou sur votre téléphone), et l'annuaire vous donne le numéro. Le DNS, c'est le même principe : votre navigateur demande "Où est `google.com` ?" et le DNS répond "Voici son adresse IP : `172.217.168.46`".

Ce qui se passe quand vous tapez une adresse web :

1.Vous tapez `www.lemonde.fr` dans votre navigateur.
2.Votre ordinateur envoie une requête à un serveur DNS.
3.Le serveur DNS répond avec l'adresse IP du site (ex: `192.0.2.45`).
4.Votre navigateur peut alors se connecter au serveur du site.

Pourquoi c'est important :

•Les ordinateurs ne comprennent que les nombres (les adresses IP). Les noms de domaine sont faits pour nous, les humains.
•Sans DNS, vous devriez retenir des adresses comme `192.0.2.45` au lieu de `lemonde.fr`.
•Votre fournisseur d'accès (Orange, Free, etc.) utilise son propre serveur DNS. Il peut voir tous les sites que vous visitez. C'est pourquoi des serveurs DNS alternatifs comme Quad9 (`9.9.9.9`, fondation suisse à but non lucratif, celui que recommandent nos fiches) ou Cloudflare (`1.1.1.1`) existent : ils respectent mieux votre vie privée.

À retenir : Le DNS est "l'annuaire téléphonique d'Internet". Si vous changez de serveur DNS (par exemple vers Quad9, `9.9.9.9`), vous pouvez gagner en confidentialité et parfois en rapidité.

---

25. La sauvegarde – Backup

C'est quoi ?

Une sauvegarde (ou "backup") est une copie de vos fichiers importants (photos, documents, mots de passe, etc.) stockée dans un endroit différent de l'original. Si l'original est perdu, vous pouvez le restaurer grâce à la copie.

L'image : vous avez une photo de famille précieuse. Vous en faites deux tirages : un dans votre portefeuille, l'autre dans un coffre chez vos parents. Si vous perdez votre portefeuille, vous pouvez récupérer la photo chez vos parents. La sauvegarde, c'est cette deuxième copie.

Les trois grands types de sauvegarde :

Type	Exemple	Avantage	Inconvénient
Locale	Disque dur externe, clé USB	Rapide, pas d'Internet	Peut être détruite en même temps que l'original (incendie, vol)
Cloud non auto-	Google Drive,	Accessible partout,	Vos données sont chez une

Type	Exemple	Avantage	Inconvénient
hébergé	iCloud, OneDrive	automatique	entreprise tierce
Cloud auto-hébergé	Nextcloud, Syncthing	Contrôle total, pas de surveillance	Nécessite un peu de technique

La règle d'or : la méthode 3-2-1

•**3** copies de vos données (1 originale + 2 sauvegardes)
•**2** supports différents (ex: disque dur externe + cloud)
•**1** copie hors site (chez un proche, ou dans un cloud)

Pourquoi c'est important :

•Les disques durs tombent en panne (c'est une question de "quand", pas de "si").
•Les ransomwares (logiciels malveillants) chiffrent vos fichiers et demandent une rançon. Une sauvegarde non connectée vous permet de tout restaurer sans payer.
•Le vol, l'incendie, l'inondation ou simplement une mauvaise manipulation (suppression accidentelle) peuvent arriver.

À retenir : Si vous n'avez qu'une seule copie de vos photos et documents, ils n'existent qu'à un seul endroit. C'est risqué. Une sauvegarde régulière (automatique de préférence) vous évite des catastrophes.

---

26. L'antivirus et les logiciels malveillants – Antivirus & Malware

C'est quoi ?

Un **malware** (contraction de "malicious software") est un logiciel conçu pour nuire : espionner, endommager, voler des données, ou prendre le contrôle de votre ordinateur. Un **antivirus** est un logiciel qui détecte et supprime les malwares.

L'image : imaginez que votre maison est un ordinateur. Un malware, c'est un cambrioleur qui entre discrètement. L'antivirus, c'est votre système d'alarme + un chien de garde : il détecte l'intrusion, sonne, et peut neutraliser l'intrus.

Les types de malwares les plus courants :

Type	Ce qu'il fait	Exemple
Virus	Se propage d'un fichier à l'autre comme une maladie	Attaché à un document ou un programme
Ransomware	Chiffre vos fichiers et demande une rançon (souvent en cryptomonnaie)	WannaCry, Ryuk
Spyware	Espionne vos activités (frappes au clavier, mots de passe)	Keyloggers
Trojan (cheval de Troie)	Se fait passer pour un logiciel légitime pour entrer	Fausse mise à jour Flash
Adware	Affiche des publicités intempestives	Pop-ups incessants

Comment les malwares arrivent sur votre ordinateur ?

•Pièce jointe douteuse dans un email (phishing)
•Téléchargement depuis un site non officiel
•Clé USB infectée
•Faille de sécurité dans un logiciel non mis à jour

Ce que fait (et ne fait pas) un antivirus :

•✅ Détecte et bloque la plupart des malwares connus
•✅ Analyse les fichiers téléchargés
•❌ Ne vous protège pas contre les mots de passe faibles ou la double authentification mal configurée
•❌ Ne remplace pas un pare-feu (§15) : l'antivirus cherche les virus, le pare-feu surveille les connexions

Quel antivirus choisir ?

•Sur **Windows** : Windows Defender (déjà installé, gratuit, suffisant) – évitez les antivirus payants qui ralentissent la machine.
•Sur **macOS** : la protection intégrée est correcte (mais pas invulnérable).
•Sur **Linux** : peu de virus, mais des malwares existent (soyez vigilant sur ce que vous installez).

À retenir : Le meilleur antivirus, c'est vous-même. Ne cliquez pas sur des liens suspects. Ne téléchargez que depuis des sources officielles. Faites vos mises à jour. Et ayez une sauvegarde (§25) au cas où.

---

27. L'intelligence artificielle (IA) – *Artificial Intelligence (AI)*

C'est quoi ?

Une intelligence artificielle est un programme entraîné sur d'immenses quantités de textes, d'images ou de sons, pour produire à son tour des réponses, des textes ou des images. Les plus connues sont les **assistants conversationnels** : ChatGPT (OpenAI), Gemini (Google), Copilot (Microsoft), Claude (Anthropic), Vibe (Mistral, France)…

L'image : un perroquet très savant qui aurait lu toute une bibliothèque. Il répond vite et avec aplomb, souvent juste, mais il ne comprend pas vraiment ce qu'il dit, et il lui arrive d'inventer.

Ce qu'il faut savoir :

•Vos questions partent sur les **serveurs de l'entreprise**, où elles peuvent être conservées, relues et servir à entraîner le modèle, selon vos réglages.
•Une **IA locale** (installée sur votre ordinateur, comme Jan ou Ollama) fonctionne sans Internet : rien ne sort de chez vous. Pour le quotidien, préférez un assistant européen (Lumo, Euria, Vibe) à ceux des géants américains.
•Une IA peut se tromper avec assurance (on parle d'**hallucinations**) : vérifiez tout ce qui compte (santé, argent, droit).

•Beaucoup d'assistants ont une **mémoire** : ils retiennent ce que vous leur dites d'une conversation à l'autre.

À retenir : n'écrivez à un assistant en ligne que ce que vous accepteriez d'envoyer sur une carte postale. L'IA propose, vous décidez.

---

28. L'hameçonnage – *Phishing*

C'est quoi ?

L'hameçonnage est une arnaque : quelqu'un se fait passer pour un organisme de confiance (banque, impôts, Ameli, livreur, opérateur...) par courriel, SMS ou téléphone, pour vous pousser à **cliquer sur un lien**, **donner un mot de passe**, un **code reçu par SMS** ou vos **coordonnées bancaires**.

L'image : un pêcheur lance un hameçon garni d'un appât appétissant (« colis en attente », « remboursement », « compte bloqué ») et attend que le poisson morde.

Les signes qui doivent alerter :

•Un ton **urgent** ou menaçant (« dernier avis », « sous 24 heures »).
•Un lien qui ne mène **pas au site officiel**.
•Une demande de **mot de passe** ou de **code reçu par SMS**.
•Attention : avec l'IA, les faux messages sont désormais **sans fautes** et très crédibles.

Les bons réflexes : ne cliquez pas, et ouvrez vous-même le site ou l'application officiels. Transférez les SMS frauduleux au **33700** (gratuit). Si vous êtes victime, rendez-vous sur **17cyber.gouv.fr**. Signalez les courriels douteux sur **signal-spam.fr** et les faux sites sur **phishing-initiative.fr**.

À retenir : votre banque ne vous demandera **jamais** votre mot de passe ni un code reçu par SMS, ni par téléphone, ni par courriel.

---

29. Les objets connectés – *Internet of Things (IoT)*

C'est quoi ?

Ce sont des objets du quotidien reliés à Internet : téléviseur, enceinte avec assistant vocal, caméra, babyphone, ampoule, prise, thermostat, montre, voiture, jouet…

L'image : autant de petites fenêtres ouvertes sur votre maison. Elles sont pratiques pour regarder dehors, mais on peut aussi s'en servir pour regarder dedans.

Ce qu'ils peuvent faire :

•**Collecter** : ce que vous regardez à la télévision, votre voix, vos heures de présence et d'absence.
•**Être piratés** s'ils gardent leur mot de passe d'usine ou ne reçoivent plus de mises à jour.
•**Servir de porte d'entrée** vers les autres appareils de votre réseau.

Les bons réflexes : changer le mot de passe par défaut, faire les mises à jour, désactiver ce qui ne sert pas (par exemple la « reconnaissance des contenus » du téléviseur), et les connecter au **Wi-Fi invité** de votre box.

À retenir : un objet « intelligent » est d'abord un petit ordinateur. Il se règle et se met à jour comme un ordinateur.

---

30. L'alias de courriel – *Email alias*

C'est quoi ?

Un alias est une **adresse e-mail supplémentaire**, sans boîte à elle, qui **transfère** les messages vers votre vraie boîte. On en crée une différente pour chaque site.

L'image : une boîte aux lettres relais. Le facteur y dépose le courrier, et il est apporté chez vous. Si une boîte se remplit de prospectus, vous la fermez, sans déménager.

Exemples : SimpleLogin, Proton Pass, addy.io, Firefox Relay.

Ce que ça change :

•Les sites ne connaissent **jamais votre vraie adresse**.
•Un alias qui reçoit du spam se **désactive en un clic**.
•Vous savez **quel site** a revendu ou laissé fuir votre adresse.

À retenir : un alias par site marchand ou newsletter ; gardez votre vraie adresse pour la banque, l'administration et vos proches.

---

31. La fuite de données – *Data breach*

C'est quoi ?

Une fuite de données, c'est quand des informations personnelles gardées par une organisation (opérateur, administration, mutuelle, site marchand…) sont **volées ou exposées** à des personnes qui n'auraient jamais dû y accéder.

L'image : le coffre du gardien (§11) a été cambriolé. Ce n'est pas votre faute, mais vos affaires circulent désormais entre de mauvaises mains.

Ce qui peut fuir, et ce que les escrocs en font :

•**Nom, e-mail, téléphone** → de faux messages très crédibles (§28).
•**Mot de passe** → la connexion à vos autres comptes, si vous l'avez réutilisé.
•**IBAN** → des tentatives de prélèvement.
•**Pièce d'identité, date de naissance** → l'usurpation de votre identité.

Les bons réflexes : vérifier si votre adresse figure dans une fuite sur **haveibeenpwned.com** ; changer d'abord le mot de passe de votre **messagerie**, puis celui du compte touché ; activer la **double authentification** (§23) ; surveiller vos relevés bancaires.

À savoir : en 2026, 45 % des Français disent avoir été prévenus d'une fuite de leurs données (baromètre Cybermalveillance.gouv.fr et Ipsos).

À retenir : un mot de passe différent par site limite les dégâts d'une fuite à un seul compte.

---

32. Le NFC (le « sans contact ») – *Near Field Communication (NFC)*

C'est quoi ?

Le NFC est une technologie radio qui permet à deux appareils d'échanger quelques informations quand on les **approche à quelques centimètres** l'un de l'autre, sans fil ni contact.

L'image : une poignée de main. Il faut être tout près pour se la serrer ; à un mètre, c'est impossible.

Exemples :

•**Payer sans contact** avec sa carte bancaire ou son téléphone.
•**Valider un titre de transport** ou un badge d'accès.
•**Présenter une clé de sécurité** au dos du téléphone pour se connecter ou signer un message (§23, §33).

Ce qu'il faut savoir :

•La portée est **très courte** : c'est ce qui rend le NFC assez sûr.

•Sur un téléphone, il s'active ou se désactive dans les **paramètres** (tapez « NFC » dans la loupe).
•Le lecteur se trouve en général **au dos du téléphone** ; une coque épaisse ou métallique peut le gêner.

À retenir : NFC = « sans contact ». Activez-le pour payer ou utiliser une clé de sécurité ; désactivez-le si vous ne vous en servez jamais.

---

33. OpenPGP (chiffrer et signer) – *OpenPGP*

C'est quoi ?

OpenPGP est une **norme ouverte**, libre d'utilisation, pour **chiffrer** (§12) et **signer** des messages et des fichiers. Elle vient de PGP (« Pretty Good Privacy »), créé en 1991. Chaque personne a une paire de clés : une **clé publique**, qu'on donne à tout le monde, et une **clé privée**, qu'on garde secrète.

L'image : vous distribuez des cadenas ouverts (la clé publique). N'importe qui peut fermer une boîte avec, mais vous seul avez la clé qui l'ouvre (la clé privée). Pour signer, c'est votre sceau personnel : tout le monde le reconnaît, personne ne peut l'imiter.

Ce que ça permet :

•**Chiffrer** : seul le destinataire peut lire le message.
•**Signer** : prouver que le message vient bien de vous et n'a pas été modifié.
•**Vérifier un téléchargement** : s'assurer qu'un logiciel vient bien de son auteur.

Exemples : GnuPG (GPG), Thunderbird (intégré), Proton Mail, et foodjis et foomms pour chiffrer ses SMS sur Android.

À savoir : la clé privée ne se partage jamais. Le plus sûr est de la garder sur une **clé de sécurité** physique, d'où elle ne sort jamais : il suffit alors de la présenter en NFC (§32) ou de la brancher.

À retenir : la clé publique, c'est le cadenas qu'on donne ; la clé privée, la clé qu'on garde. On chiffre avec la clé publique du destinataire, on signe avec sa propre clé privée.

---

34. Le Fédivers (réseau fédéré, instance) – *Fediverse*

C'est quoi ?

Le Fédivers (de « fédération » et « univers ») est un ensemble de réseaux sociaux et de services en ligne **indépendants** qui parlent la même langue : un protocole commun (§20). Chacun s'inscrit sur un serveur (§18) appelé **instance**, tenu par une association, une collectivité, une entreprise ou un particulier, et peut échanger avec les membres de toutes les autres instances.

L'image : le courrier électronique. Une adresse chez un fournisseur peut écrire à une adresse chez n'importe quel autre. Dans le Fédivers, c'est pareil : un compte sur un serveur associatif suit sans difficulté un compte hébergé ailleurs.

Exemples :

•**Mastodon** : messages courts, à la place de X (Twitter).
•**Pixelfed** : partage de photos, à la place d'Instagram.
•**PeerTube** : vidéos, à la place de YouTube.
•**Mobilizon** : événements et groupes, à la place des événements Facebook.

Ce qu'il faut savoir :

•Choisir son instance, c'est choisir **un hébergeur et ses règles** de modération ; on peut ensuite déménager.

•Pas de publicité ni d'algorithme imposé : le fil montre ce que vous suivez, dans l'ordre.
•Le mot « instance » sert aussi pour des services libres non fédérés (Jitsi Meet, Lufi) : c'est simplement un serveur qui fait tourner le logiciel.

À retenir : un réseau, beaucoup de serveurs. On choisit le sien, et on parle à tout le monde.

---

35. La mise à jour (correctif, fin de support) – *Software update*

C'est quoi ?

Une mise à jour est une nouvelle version d'un logiciel ou d'un système d'exploitation (§2). Elle apporte surtout des **correctifs de sécurité**, qui bouchent les failles découvertes, et parfois des nouveautés. Quand l'éditeur arrête d'en publier, le produit est en **fin de support**.

L'image : les rappels d'un constructeur automobile. Tant qu'il suit le modèle, il répare les défauts découverts. Quand il arrête, les défauts restent, et tout le monde les connaît.

Ce qu'il faut savoir :

•Une faille corrigée devient **publique** : les pirates s'en servent aussitôt contre les appareils pas à jour.
•Mettez à jour le système, le navigateur, les applications, et aussi la box et les objets connectés (§29).
•Avant une grosse mise à jour, faites une sauvegarde (§25).
•Installez vos logiciels depuis une **source officielle** (logithèque, magasin d'applications) : ils se mettent à jour tout seuls.
•Un appareil en fin de support n'est pas forcément perdu : un système libre (Linux Mint, /e/OS) peut prendre le relais.

À retenir : un appareil à jour est un appareil protégé. Un appareil en fin de support ne doit plus aller sur Internet sans solution de remplacement.

---

36. Le format ouvert et le verrou numérique (DRM) – *Open format and DRM*

C'est quoi ?

Un format de fichier est la façon dont les informations sont rangées dans un fichier (.odt, .docx, .epub, .jpg…). Un **format ouvert** est publié et utilisable par tous, sans autorisation : n'importe quel logiciel peut le lire, aujourd'hui comme dans vingt ans. Un **verrou numérique** (DRM, pour « Digital Rights Management ») va dans l'autre sens : il empêche d'ouvrir le fichier ailleurs que sur les appareils autorisés par le vendeur.

L'image : une recette écrite sur une fiche, que tout le monde peut lire et recopier, face à une recette enfermée dans un robot de cuisine qui ne la montre qu'à son propriétaire.

Exemples :

•**Formats ouverts** : ODT (LibreOffice), PDF, EPUB sans DRM, JPEG et PNG, MP3, FLAC et Ogg, CSV, Markdown.
•**Fichiers verrouillés ou enfermés** : livres Kindle, certaines musiques et vidéos achetées en ligne, données qu'on ne peut pas exporter d'un service.

Ce qu'il faut savoir :

•Un fichier dans un format ouvert vous appartient vraiment : vous pouvez changer de logiciel sans le perdre.
•Avec un DRM, vous achetez un **droit de lecture**, pas le fichier : il peut disparaître avec le compte.
•Avant de quitter un service, **exportez vos données** dans un format ouvert.

À retenir : préférez les formats ouverts et les fichiers sans verrou. Ce sont les seuls que vous êtes sûr de pouvoir relire demain.

Partie 3 : Récapitulatif général

Tableau des 36 notions

#	Terme (français)	Terme (anglais)	Paragraphe	Traduction simple
1	Ordinateur / PC	Computer	§1	Machine physique (ce qu'on touche)
2	Système d'exploitation	Operating System (OS)	§2	Chef d'orchestre qui fait tourner la machine
3	Logiciel / Application	Software / App	§3	Programme qui fait une tâche précise
4	Navigateur web	Web browser	§5	Logiciel pour aller sur Internet
5	Moteur de recherche	Search engine	§6	Site web qui trouve d'autres sites
6	Logiciel propriétaire	Proprietary software	§7	Code secret, non modifiable
7	Logiciel libre / Open Source	Free / Open Source software	§8	Code public, modifiable, partageable
8	Cloud	Cloud	§11	Stockage sur serveurs distants
9	Chiffrement (cryptage)	Encryption	§12	Brouillage d'un message pour le rendre illisible sans clé
10	Donnée	Data	§13	Information brute (ex : "25/03/1990")
11	Adresse IP	IP address	§14	Plaque d'immatriculation de

#	Terme (français)	Terme (anglais)	Paragraphe	Traduction simple
				l'appareil sur Internet
12	Pare-feu	Firewall	§15	Filtre / videur qui surveille les connexions
13	Cookie (témoin de connexion)	Cookie	§16	Petit fichier mémoire déposé par un site
14	VPN	Virtual Private Network (VPN)	§17	Tunnel chiffré qui masque votre IP et protège vos données
15	Serveur	Server	§18	Ordinateur puissant qui fournit des services
16	Client (informatique)	Client	§19	Logiciel qui demande un service à un serveur
17	Protocole (informatique)	Protocol	§20	Règles de communication entre machines
18	Permissions (droits d'accès)	Permissions / Access rights	§21	Règles qui disent qui peut faire quoi (lecture, écriture, exécution)
19	Base de données	Database	§22	Classement géant d'informations organisées
20	Internet	Internet	§4	Le réseau physique mondial (câbles, routeurs, antennes)
21	Web	World Wide Web (WWW)	§4	Service qui utilise Internet (pages web, sites, vidéos)
22	Mot de passe / authentification	Password & Authentication	§23	La clé qui prouve votre identité (mot de passe + double authentification)
23	DNS	Domain Name System (DNS)	§24	L'annuaire téléphonique d'Internet (transforme les noms de domaine en adresses IP)

#	Terme (français)	Terme (anglais)	Paragraphe	Traduction simple
24	Sauvegarde	Backup	§25	Copie de vos fichiers stockée ailleurs pour ne pas tout perdre
25	Antivirus / logiciel malveillant	Antivirus & Malware	§26	Logiciel malveillant (malware) et programme qui le détecte (antivirus)
26	Intelligence artificielle (IA)	Artificial Intelligence (AI)	§27	Programme entraîné sur d'immenses données, qui répond et rédige ; peut se tromper
27	Hameçonnage	Phishing	§28	Faux message d'un organisme de confiance pour voler codes et identifiants
28	Objets connectés	Internet of Things (IoT)	§29	Objets du quotidien reliés à Internet (téléviseur, enceinte, caméra…)
29	Alias de courriel	Email alias	§30	Adresse relais, une par site, qui transfère vers votre vraie boîte
30	Fuite de données	Data breach	§31	Vol ou exposition de données personnelles détenues par une organisation
31	NFC (sans contact)	Near Field Communication (NFC)	§32	Échange radio à quelques centimètres : paiement, badge, clé de sécurité
32	OpenPGP	OpenPGP	§33	Norme libre pour chiffrer et signer, avec une clé publique et une clé privée
33	Fédivers	Fediverse	§34	Réseaux indépendants qui communiquent entre eux : on choisit son instance, on parle à tous

#	Terme (français)	Terme (anglais)	Paragraphe	Traduction simple
34	Mise à jour	Software update	§35	Correctifs de sécurité ; un appareil en fin de support devient dangereux
35	Format ouvert et DRM	Open format and DRM	§36	Un format ouvert se lit partout ; un verrou numérique enferme le fichier chez le vendeur
36	(espace libre)	—	—	Pour une future notion

La phrase à retenir absolument

> **"Gratuit ne veut pas forcément dire éthique. Parfois, c'est vous le produit."**

Rappel : Un logiciel libre (comme Firefox, LibreOffice, VLC) est gratuit ET respectueux de votre vie privée. Il ne vous traque pas. Un service gratuit mais propriétaire (comme Gmail, Google Maps, Doodle) vit de vos données.

Trois petits conseils pour commencer

Si vous voulez vous éloigner des logiciels propriétaires sans devenir un expert :

1. **Navigateur** → passez de Chrome à **Firefox** (libre, simple, respectueux)
2. **Moteur de recherche** → remplacez Google par **DuckDuckGo** (même qualité, sans pistage)
3. **Suite bureautique** → remplacez Microsoft Office par **LibreOffice** (gratuit, fait la même chose)

Vous pouvez faire ces changements un par un, à votre rythme. Pas besoin de tout basculer d'un coup.

Fin du guide. Vous avez maintenant une vue d'ensemble claire des principaux objets et notions de l'informatique. Conservez ce document ou relisez certaines sections selon vos besoins. L'informatique n'est qu'un vocabulaire et des analogies : une fois que vous avez une bonne image mentale (la maison, la voiture, l'océan, le restaurant…), le reste s'enchaîne plus facilement.