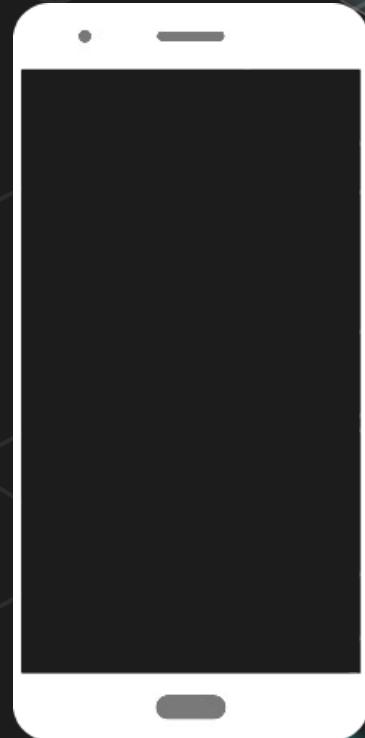


Smartphones & Surveillance

Identifier les menaces et
limiter les risques



Deux familles de surveillance

COMMERCIALE

ÉTATIQUE

Surveillance Commerciale

MOTIVATIONS

- Exploiter des données à des fins commerciales
- Revendre à des annonceurs ou à des assurances
- Entraîner des modèles de langage (IA)

ACTEURS



Surveillance Étatique

MOTIVATIONS

- Assurer sa sécurité intérieure
- Participer à la guerre économique (cf Alstom)
- Maintenir l'ordre sur son territoire

ACTEURS



Surveillance Étatique Généralisée

HISTORIQUE

- Débute en 1946 (accord *UKUSA*)
- Post 11 septembre 2001 : moyens décuplés
- Révélations d'Edward Snowden en 2013



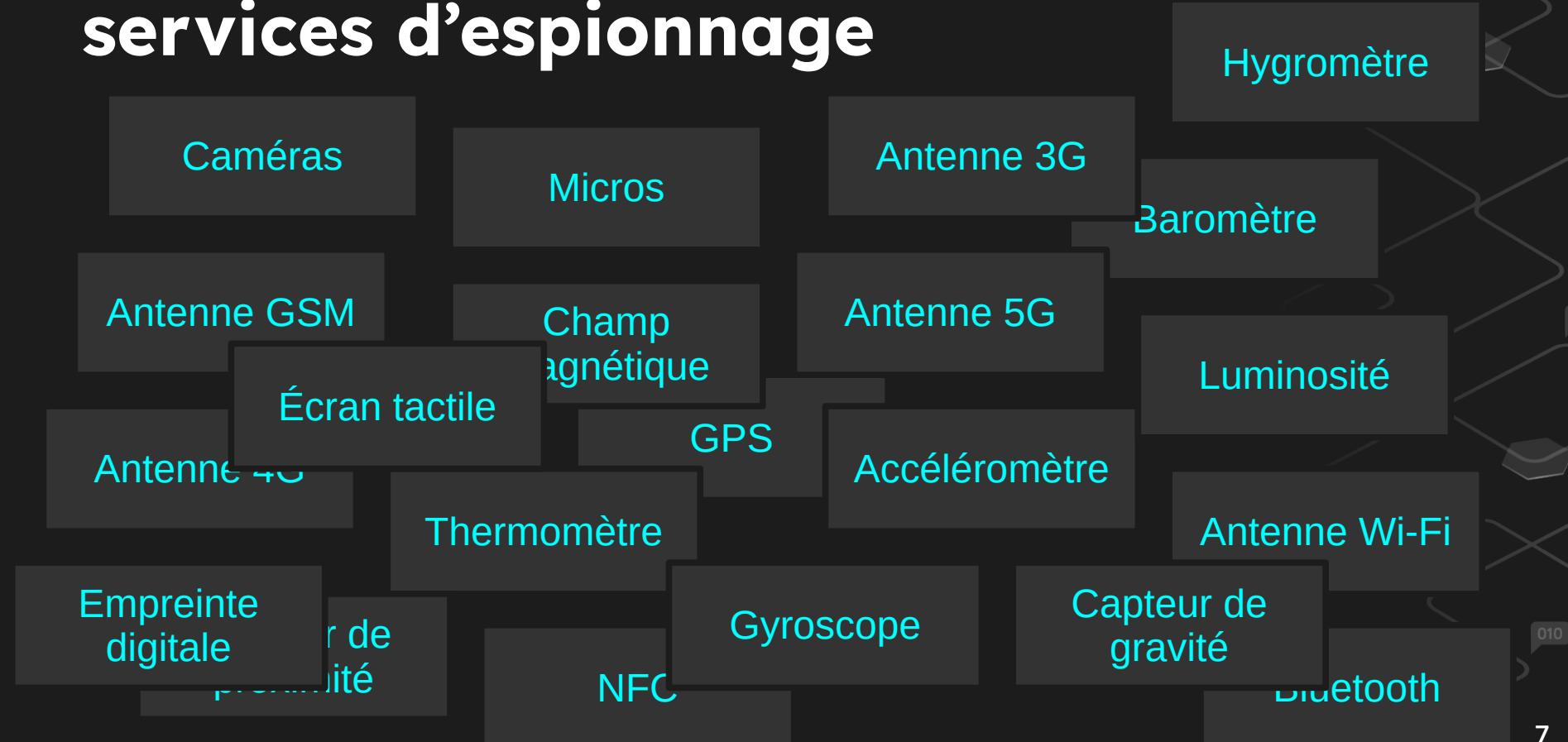
Surveillance Étatique

MATÉRIALISATION

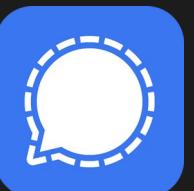
- Caméras de surveillance
- Accès à des serveurs
- Interception de communications
- Infiltration de smartphones

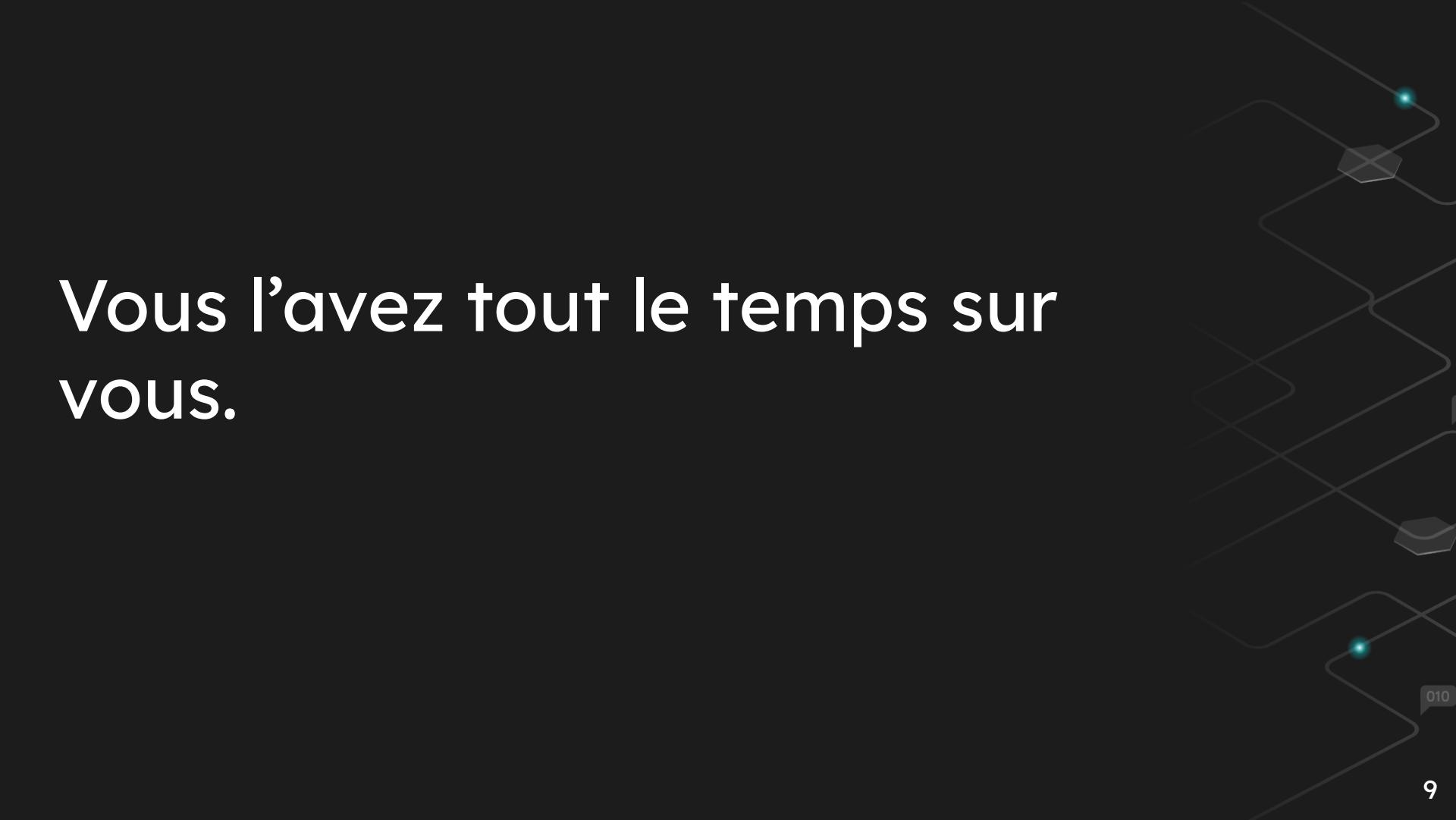


Le smartphone, parfait allié des services d'espionnage



Le smartphone, parfait allié des services d'espionnage



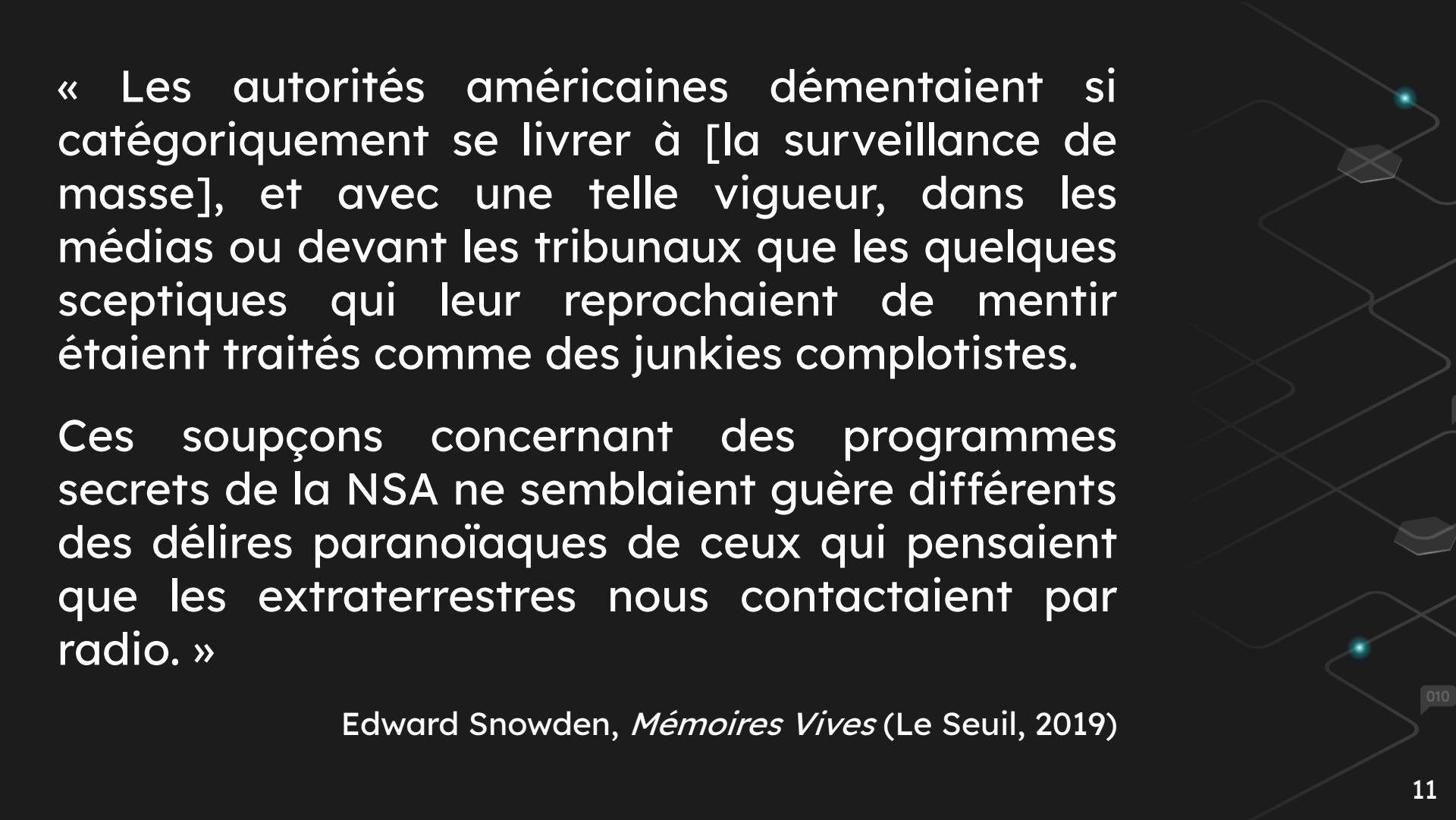


**Vous l'avez tout le temps sur
vous.**

Surveillance de masse, illégale ?

Le programme de surveillance de la NSA révélé par Snowden était illegal.





« Les autorités américaines démentaient si catégoriquement se livrer à [la surveillance de masse], et avec une telle vigueur, dans les médias ou devant les tribunaux que les quelques sceptiques qui leur reprochaient de mentir étaient traités comme des junkies complotistes.

Ces soupçons concernant des programmes secrets de la NSA ne semblaient guère différents des délires paranoïaques de ceux qui pensaient que les extraterrestres nous contactaient par radio. »

Edward Snowden, *Mémoires Vives* (Le Seuil, 2019)

La NSA recueille-t-elle des données concernant des centaines de millions d'américains ?

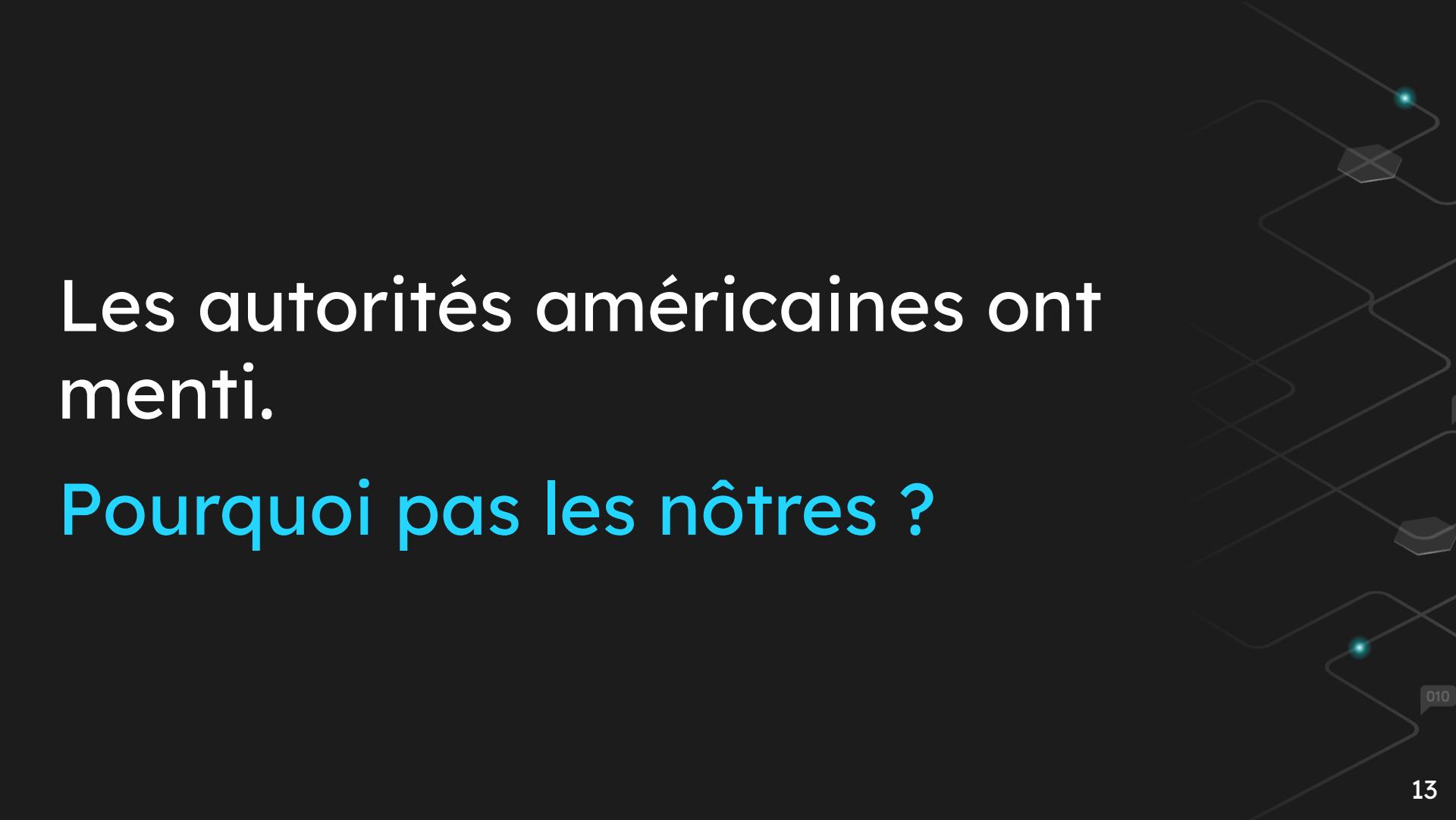


Non
Monsieur

James Clapper (Directeur du Renseignement National) mentant lors d'une audition au Sénat en 2013

Source : Laura Poitras, *Citizen Four*, 18:10

010



Les autorités américaines ont menti.

Pourquoi pas les nôtres ?



Point à retenir n°1

Ne comptez pas sur la loi pour vous protéger.

Pour garantir votre droit à la vie privée dans vos activités numériques, vous devez de rendre sa violation **techniquement** impossible.



Conséquence

Pédocriminalité : l'outil « Chat Control », qui scanne vos messageries, fait polémique

L'UE pourrait adopter ce dispositif qui vise à lutter contre les abus sexuels sur enfants en ligne. Mais un risque d'atteinte « excessive » à la vie privée est pointé.



Publié le 12/10/2025 à 10h30

« Chat Control » : le projet de surveillance des messages abandonné

La mesure prévoyait d'imposer aux éditeurs de messagerie de scanner les conversations privées de leurs utilisateurs pour lutter contre les abus sexuels sur mineurs. Cela avait notamment été dénoncé par l'Allemagne.

Le Monde
Publié le 31 octobre 2025 à 10h05, modifié le 31 octobre 2025 à 10h05 - 0 Lecture 1 min

PIRE DE LA SÉCURITÉ DU NET

TRIBUNE

« Chat Control » :
enfants, ou surveiller

Le contrôle généralisé et automatisé de toutes les conversations privées n'est pas une bonne idée. Or, pour le député LFI de Paris, c'est ce qu'il faut faire pour lutter contre les abus sexuels sur mineurs.

Soutenue par plusieurs associations de protection de l'enfance, elle prévoyait d'obliger les plates-formes de messagerie en ligne à détecter et signaler de tels contenus dans des discussions privées.

Par Le Parisien avec AFP
Le 30 octobre 2025 à 17h28

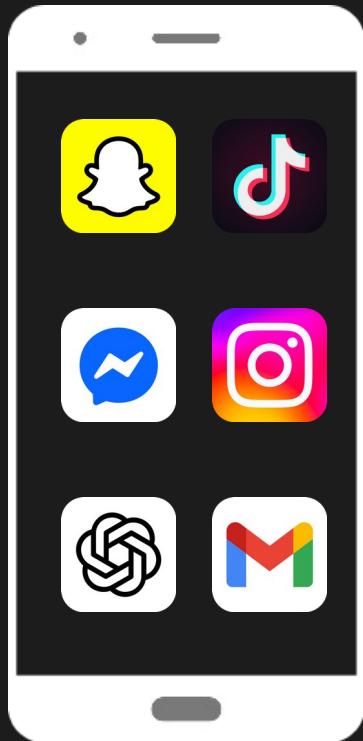
NON-SUJET

Marche arrière sur le
scan des messages

« Technique impossible » ?

Comment renforcer la sécurité de son téléphone ?

Fonctionnement d'un smartphone



RESSOURCES

RAM
(mémoire)

Processeur

Capteurs

Stockage

Analogie



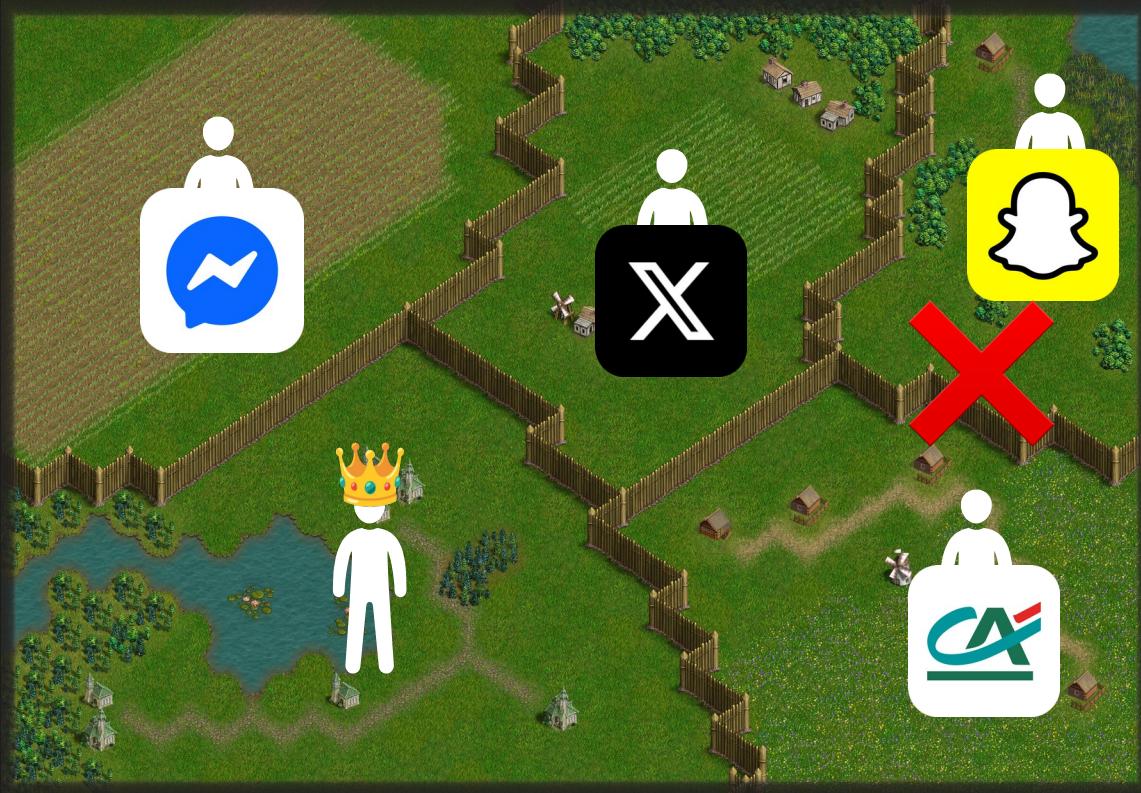
Je suis propriétaire
de toutes les
ressources

Je redistribue à
chacun selon ses
besoins



Analogie

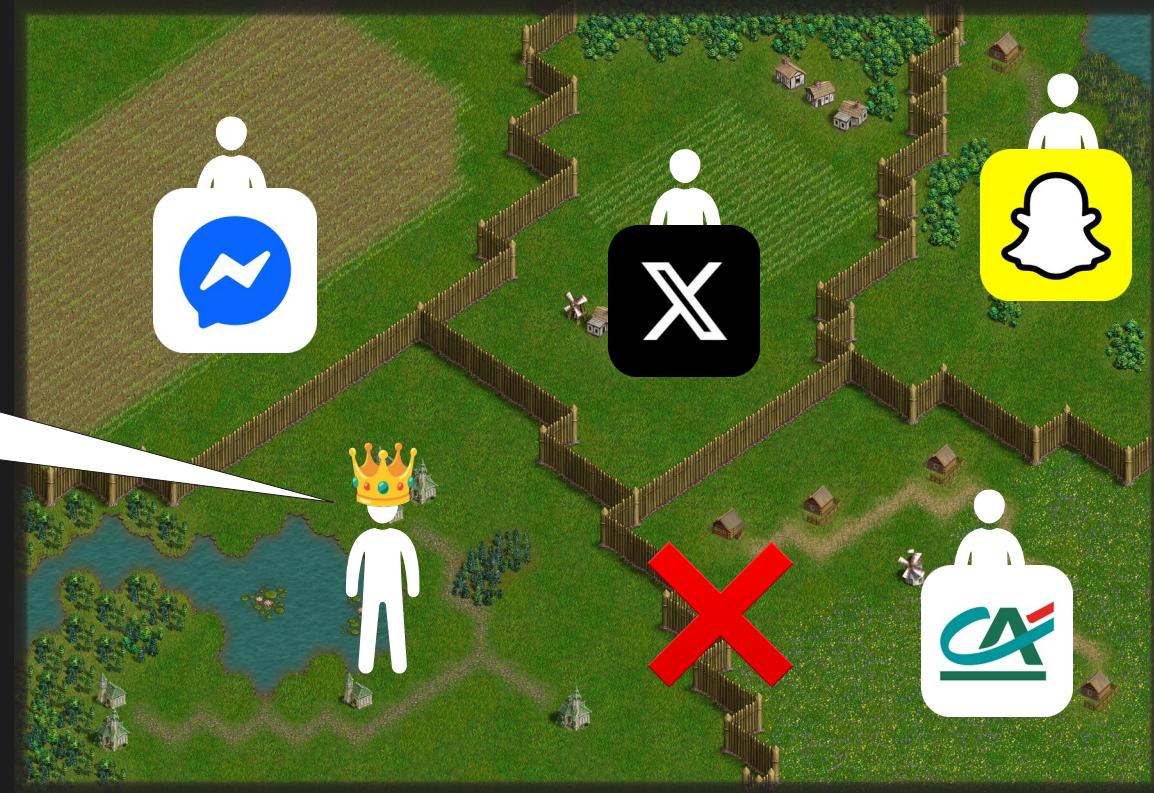
On veut à tout prix éviter que quelqu'un accède à un territoire qui n'est pas le sien



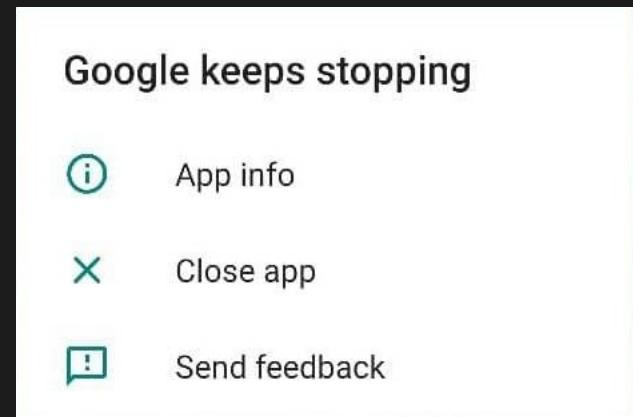
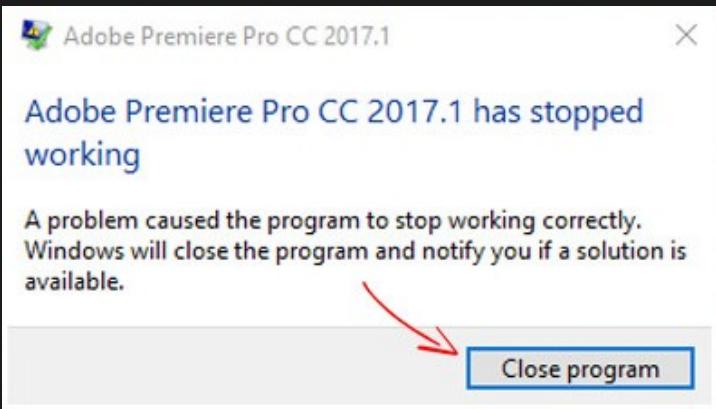
Analogie

On veut **à tout prix**
éviter que quelqu'un
accède à un territoire
qui n'est pas le sien

Je surveille et
j'interviens en cas
d'action illégale



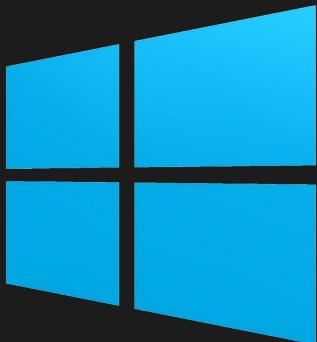
Analogie



Analogie



= Système d'exploitation (OS)





Point à retenir n°2

**Les smartphones et ordinateurs
sont orchestrés un peu comme une
dictature communiste.**

Le système d'exploitation s'approprie les ressources de l'appareil et les redistribue aux applications selon leurs besoins.

Le système d'exploitation représente l'autorité de l'État, les applications, le peuple.

À Savoir

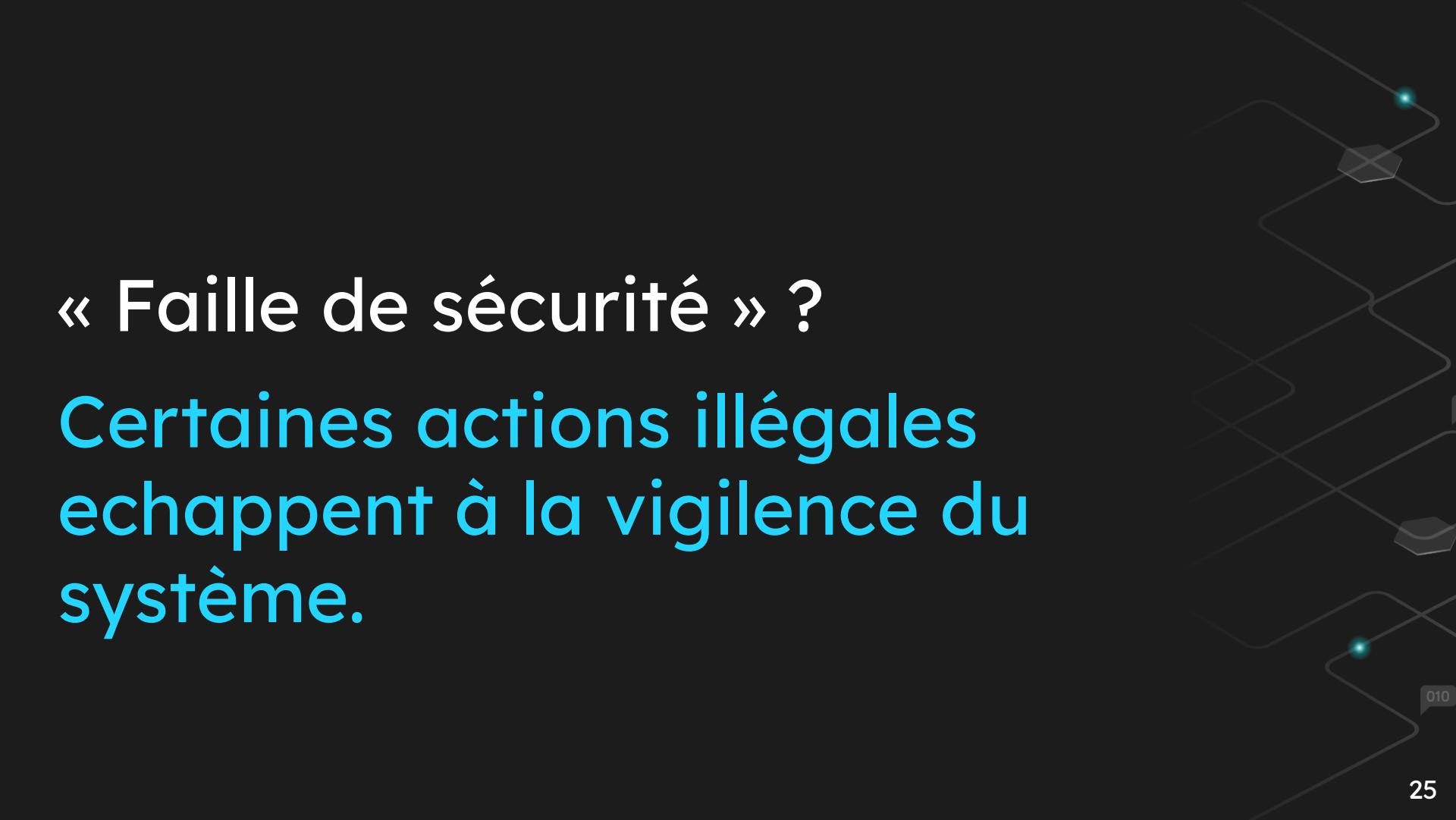
Toutes les applications tentent d'effectuer des actions « illégales ».

- hexagon Erreurs involontaires de la part des développeurs

Faille de sécurité

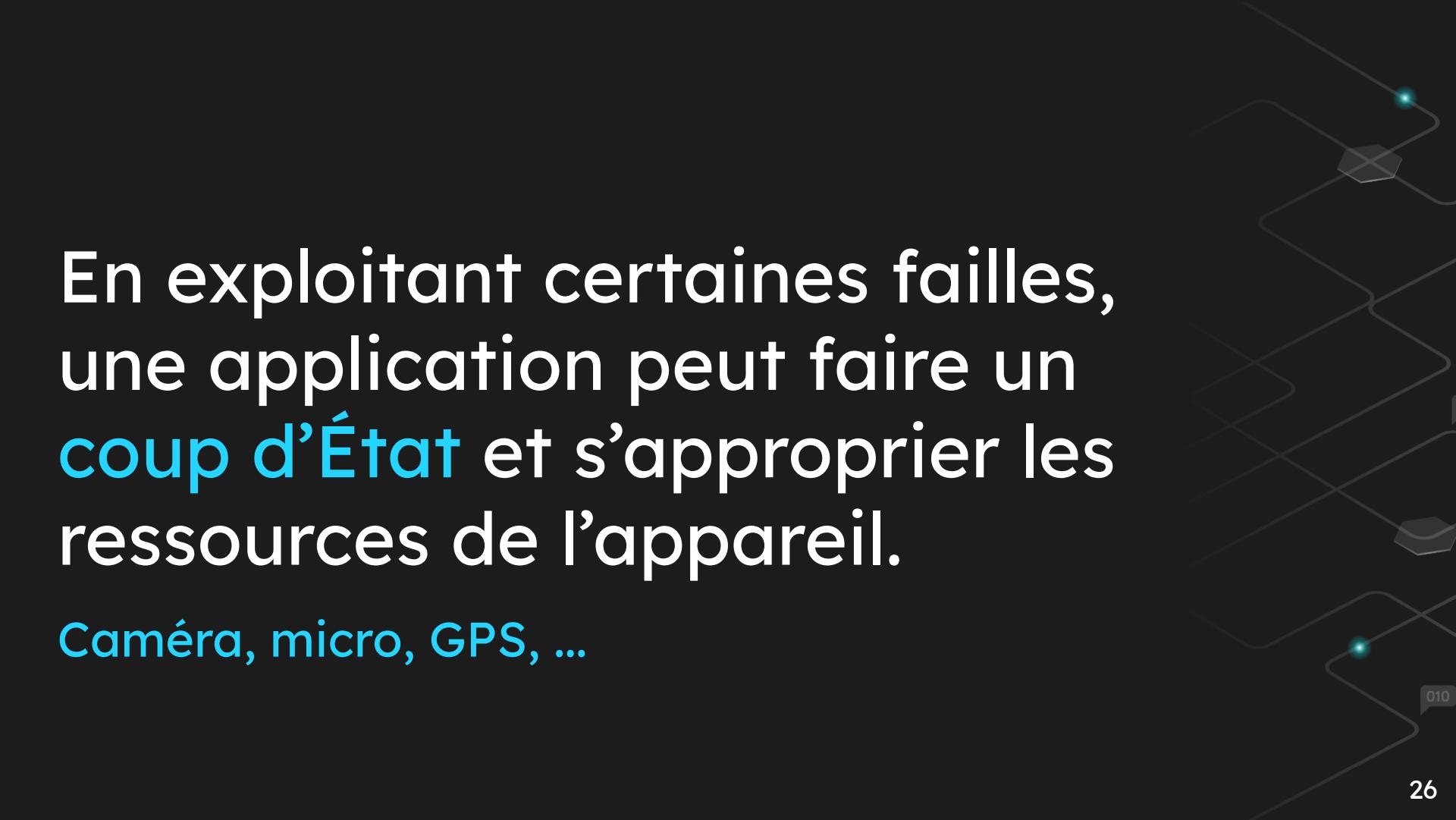
- hexagon Volontaire dans le but d'être exploité

Porte dérobée / « *backdoor* »



« Faille de sécurité » ?

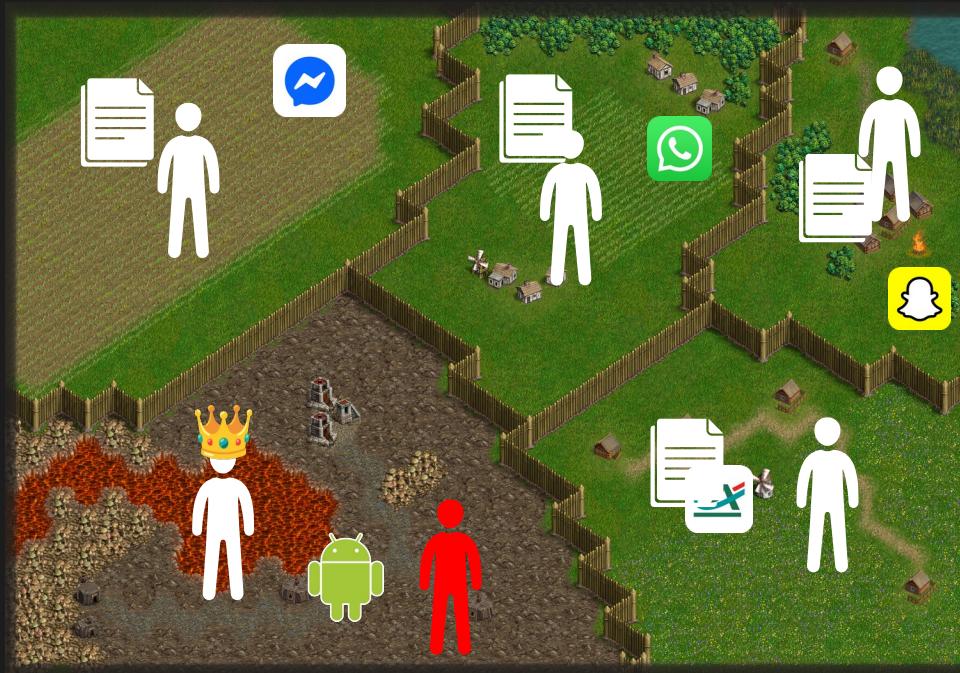
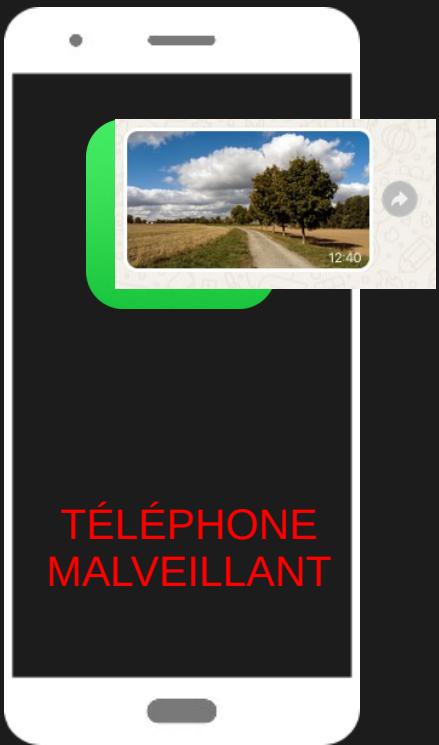
Certaines actions illégales
échappent à la vigilance du
système.



En exploitant certaines failles,
une application peut faire un
coup d'État et s'approprier les
ressources de l'appareil.

Caméra, micro, GPS, ...

Exemple d'exploitation



Téléphone cible de l'attaque

Logiciel espion Pegasus : l'enquête «tentaculaire» confiée à un juge d'instruction en France

L'enquête portera sur des infractions potentielles telles que l'atteinte à la vie privée ou l'utilisation frauduleuse de « systèmes de traitement automatisé de données », dont certains mis en œuvre par l'Etat.

Par Le Parisien avec AFP

Le 2 juillet 2022 à 13h02

« Pegasus est l'arme de cybersurveillance la plus puissante du marché » : les extraits du livre-enquête sur le logiciel espion

Les journalistes Laurent Richard et Sandrine Rigaud publient jeudi 14 septembre « Pegasus. Démocraties sous surveillance », aux éditions Robert Laffont. Un récit à deux voix de l'enquête qu'ils ont coordonnée, et à laquelle « Le Monde » a participé, sur le logiciel qui a permis d'espionner journalistes, militants des droits humains ou responsables politiques.

Par Laurent Richard et Sandrine Rigaud

Publié le 12 septembre 2023 à 05h00, modifié le 12 septembre 2023 à 12h00 · ⏲ Lecture 8 min.



Point à retenir n°3

**La sécurité des applications
dépend de la sécurité du système
d'exploitation.**

Si le système est corrompu, les données
d'applications sécurisées peuvent être
interceptées (et modifiées) avant d'être
chiffrées.



« Il n'y a pas d'application qui garantisse une confidentialité à 100 % de vos échanges. »

Nicolas Lerner, directeur de la DGSE, France Inter, 10 novembre 2025

Comment se protéger ?

Contre les failles de sécurité introduites
involontairement ...



Point à retenir n°4

Effectuez systématiquement les mises à jour de votre système et de vos applications.

Les développeurs corrigent régulièrement de nombreuses failles de sécurité.

Une faille corrigée ne peut plus être exploitée contre vous.

Important

Mises à jour de sécurité fournies pendant une durée **déterminée** selon les modèles !

Les vieux téléphones ne sont plus mis à jour !

Vérifier sur Android :

Paramètres > À propos du téléphone > Version d'Android > Mise à jour de sécurité Android

Important

clubic

30% des smartphones Android sont obsolètes et vulnérables avec 1 milliard de victimes potentielles



Par [Guillaume Belfiore](#), rédacteur en chef adjoint.

Publié le 29 décembre 2025 à 11h02



26

+ 100 failles corrigées en décembre 2025

Bulletin sur la sécurité d'Android – Décembre 2025



Publié le 1er décembre 2025 | Mis à jour le 17 décembre 2025

010

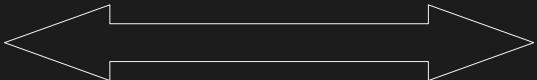
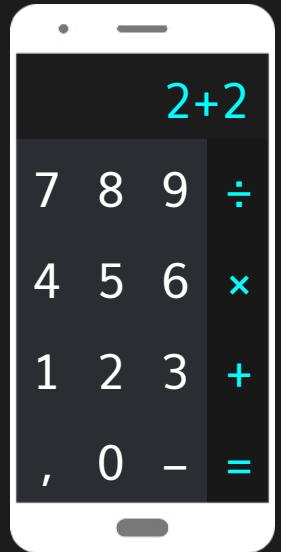
34

Comment se protéger ?

Contre les portes dérobées ...

Prévenir les portes dérobées

Hypothèse : les portes dérobées sont relativement **visibles** dans le code source des applications.





Il est difficile et donc peu rentable de cacher une porte dérobée dans une application dont le **code source est public**.

De telles applications sont dites « open source ».



Point à retenir n°5



**Open source n'implique
pas sécurisé !**

Ce n'est qu'une garantie de transparence.

Systèmes d'exploitation open source

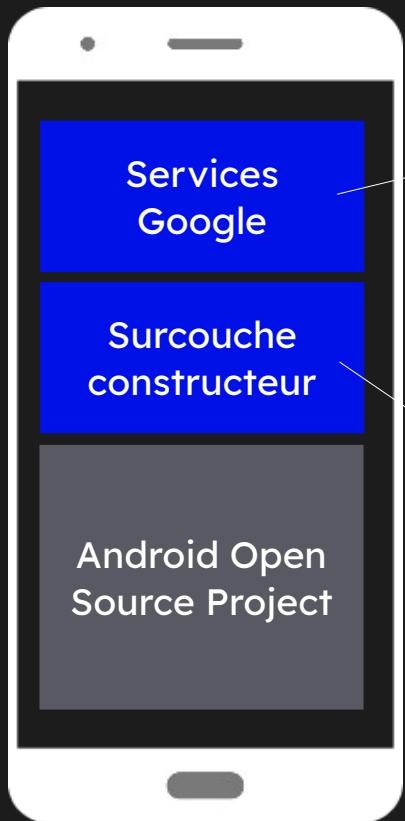


Partiellement open source



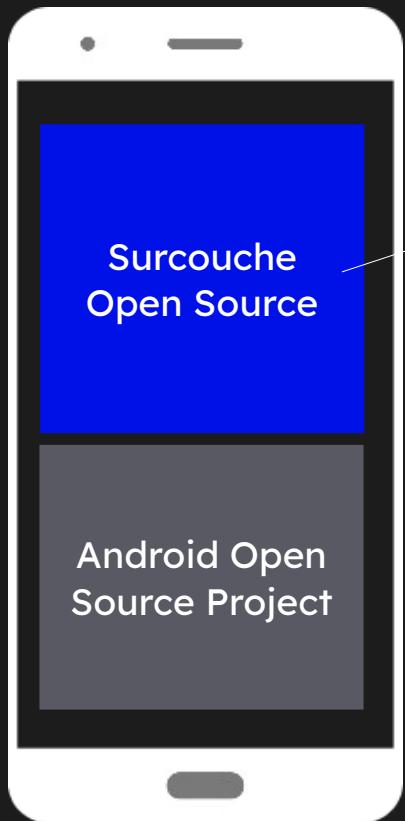
Non open source

Android, partiellement open source

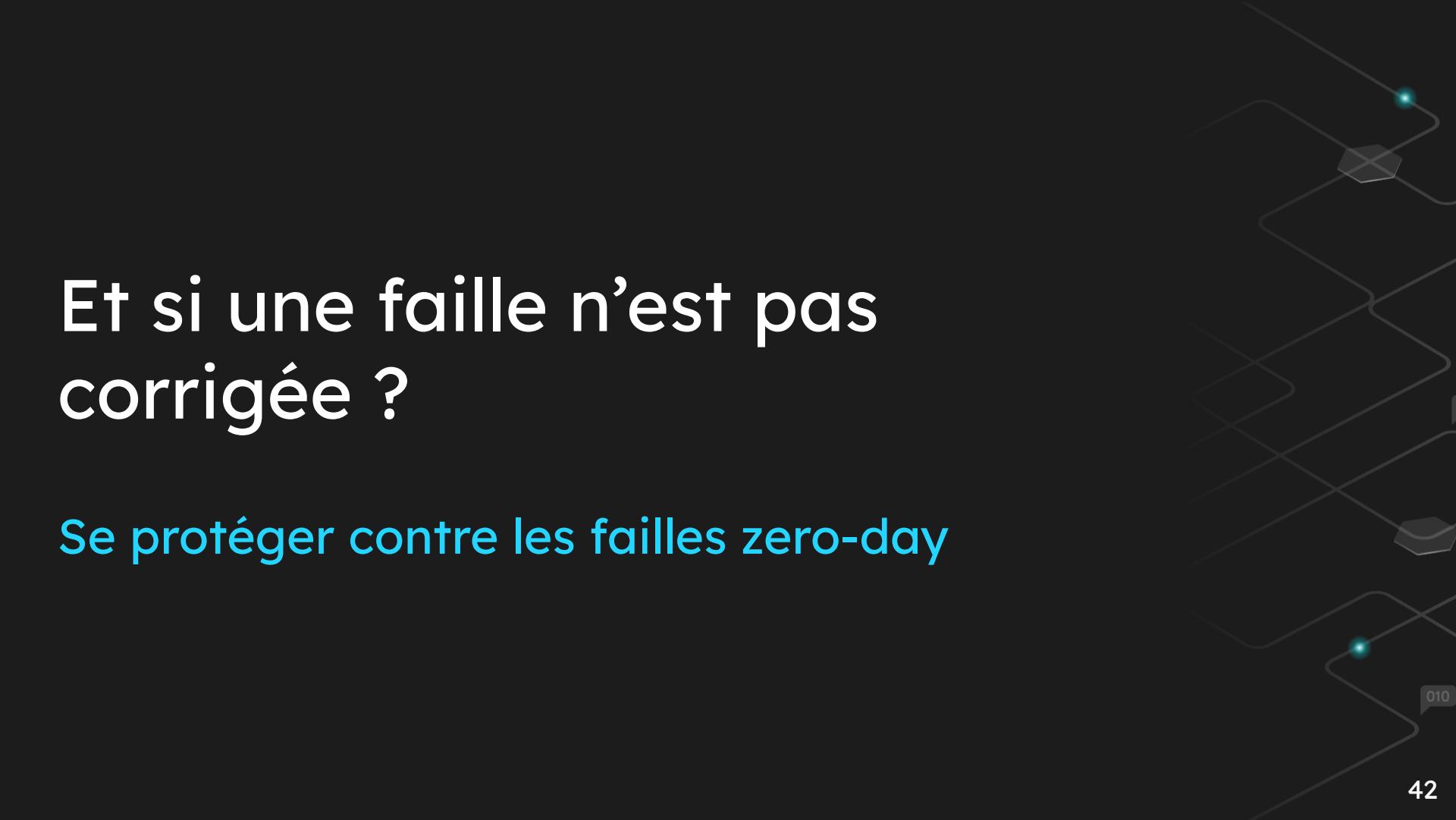


One UI (Samsung)
MIUI, HyperOS (Xiaomi)
Pixel UI (Google)

Android, partiellement open source



LineageOS
CalyxOS
GrapheneOS



Et si une faille n'est pas corrigée ?

Se protéger contre les failles zero-day

Protection contre les failles 0-day

Mises à jour

Rappel :

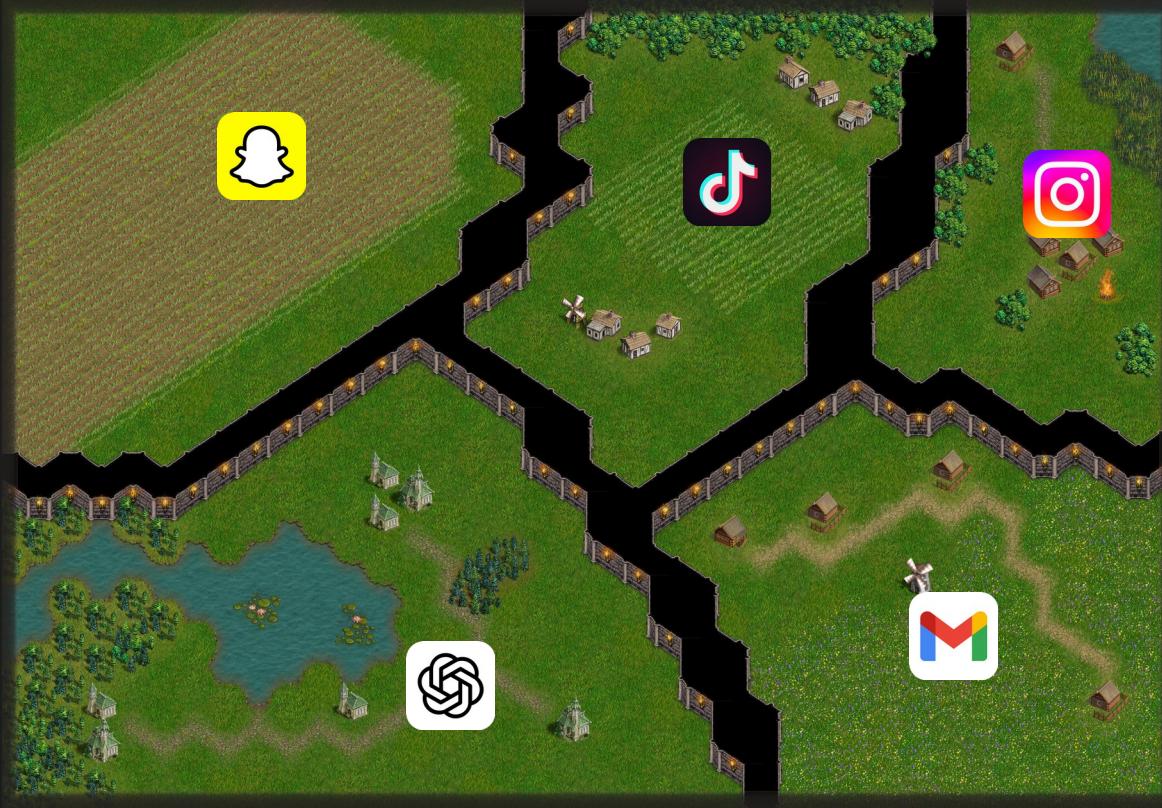
Je surveille et
j'interviens en cas
d'action illégale



010

43

Protection contre les failles 0-day



OPEN SOURCE

Lutte contre les portes dérobées

À JOUR

Lutte contre les failles de sécurité

SÉCURITÉ REFORCÉE

Lutte contre les failles zero-day



010

45

GrapheneOS



Axé sur la sécurité et la confidentialité

Confinement renforcé des applications

Permet d'utiliser les services Google sans privilèges



010

GrapheneOS



Google Pixel et GrapheneOS : la botte secrète des narcotrafiquants pour protéger leurs données de la police

Les analystes de la police judiciaire, spécialisés dans la cybersécurité (OFAC), viennent d'alerter sur le nouvel outil des trafiquants pour dissimuler leurs échanges via leurs téléphones portables : GraphèneOS, un système d'exploitation qui fonctionne sur les Google Pixel et qui détruit leurs données en cas d'intrusion.

Par Julien Constant

Le 19 novembre 2025 à 09h08

Le Parisien

Note du ministère de l'Intérieur

Novembre 2025



"Il suscite l'intérêt de profils de type « survivaliste » mais également d'individus liés à des activités criminelles."

Téléphones protégés utilisés par les narcotrafiquants : « Rien n'est inviolable ! »

Les téléphones Google Pixel équipés du système d'exploitation GrapheneOS permettent à des criminels de dissimuler leurs échanges. Johanna Brousse, magistrate spécialisée dans la lutte contre la cybercriminalité, explique quels sont les moyens de la justice pour contourner ce type d'outils.

Par Julien Constant

Le 19 novembre 2025 à 11h15

Le Parisien

010

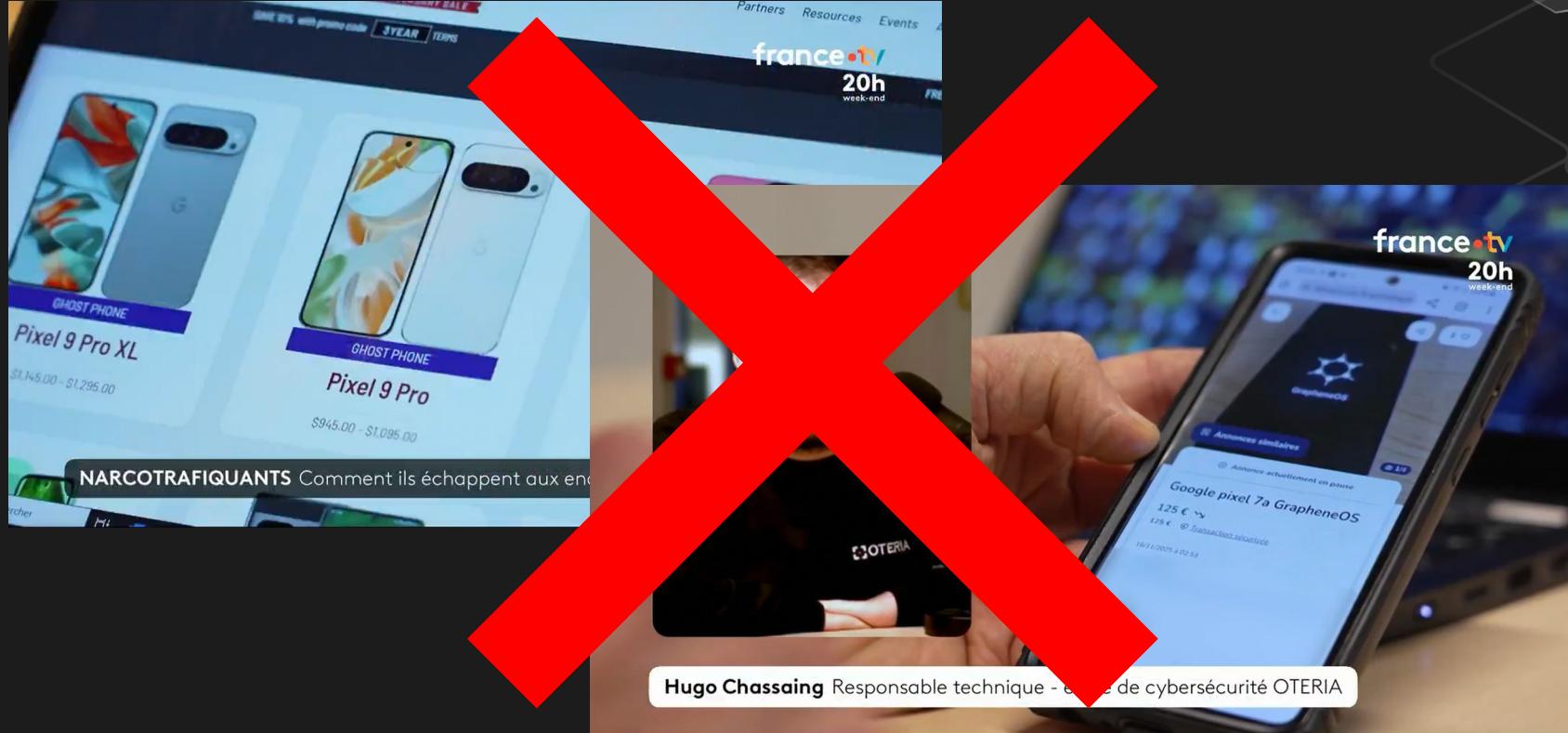
GrapheneOS



INCONVÉNIENTS

- _HEX_ Disponible sur peu de téléphones
- _HEX_ Un peu technique à installer
- _HEX_ Suspect aux yeux des forces de l'ordre

Obtenir GrapheneOS



Obtenir GrapheneOS



Installez-le vous-mêmes.

En suivant les instructions sur le site officiel.

<https://grapheneos.org/install/web>



GrapheneOS



Pierre Beyssac   

@pbeyssac

23 nov. 2025 19:54:21

À marteler : en fait, le problème n'est pas, contrairement à ce que nous dit la police, que @GrapheneOS soit "trop" sécurisé. Le problème est que les autres versions d'Android ne le soient pas autant. Inversion des valeurs élémentaires de protection de notre intégrité numérique.

5

117

481



010

Conclusion

La sécurité est l'affaire de tous.

Des personnes malveillantes peuvent passer par vous pour atteindre vos proches.

Des questions ?



- **Ne comptez pas sur la loi pour vous protéger**
- La sécurité des applications dépend de la sécurité du système d'exploitation.
- **Maintenez vos appareils à jour.**
- L'Open Source protège contre les portes dérobées.
- **Open Source ≠ Sécurisé**
- Les mises à jour suppriment des failles de sécurité.
- **Un système renforcé protège des failles zéro-day.**
- Utilisez GrapheneOS et installez-le vous-mêmes.



cm.conferences@proton.me

Références & diapositives :

