Focus Cybersécurité | novembre 2025

Yannick Pech

La cybersécurité européenne au défi de la protection de la vie privée et des métadonnées, de la construction de la souveraineté, et la sécurisation des chaînes d'approvisionnement

Le mois de novembre 2025 a révélé la fragilité du paysage numérique : une faille d'énumération a exposé 3,5 milliards de numéros WhatsApp, les métadonnées deviennent une arme de *phishing* ; le sommet de Bruxelles a lancé un plan ambitieux de souveraineté (ISO-27001 2025, cloud souverain, fonds cybersécurité) tandis que la fuite massive de secrets chez un cloud français et les attaques contre des SCADA illustrent la vulnérabilité des chaînes d'approvisionnement. Entre fuites de données à la FFF et chez WhatsApp, exfiltration de métadonnées chez OpenAI et le retrait de France de GrapheneOS, l'ensemble souligne l'urgence d'une gouvernance holistique : minimisation des données, auditabilité, protection des métadonnées et édification de la souveraineté numérique du Vieux continent pour 2026.

WhatsApp : 3,5 milliards de numéros exposés. Quand les métadonnées deviennent « la » cybermenace

Plusieurs enquêtes et travaux de chercheurs ont mis en évidence une **faille d'énumération** dans le mécanisme de découverte **de contacts de WhatsApp** — une faiblesse qui permettait, par un processus automatisé et de grande envergure, de tester des numéros de téléphone et d'identifier ceux qui étaient enregistrés sur la plateforme. Le résultat de cette mécanique : l'exposition potentielle de **milliards de numéros**, combinée à **l'agrégation de métadonnées** — photos et informations de profils, statuts, clés publiques cryptographiques — lesquelles, cumulées, forment un « annuaire » d'identités exploitable pour du phishing, de l'usurpation ou du profilage.

Deux leçons se dégagent de cet épisode : d'abord, le chiffrement de bout en bout, aussi indispensable soit-il pour protéger le contenu des échanges, **ne protège pas les métadonnées** : qui a parlé à qui, quand, avec quel terminal, quelles photos sont associées à tel numéro, etc. Autant d'informations précieuses pour des attaquants. Ensuite, la méthode d'attaque repose sur l'**automatisation et l'exploitation d'APIs ou d'interfaces non sécurisées**/durcies — un rappel que l'échelle change la menace : des faiblesses mineures peuvent devenir catastrophiques quand elles sont massifiées.

META a répondu par la mise en place de protections anti-*scraping* et de limitations à l'énumération. Cela réduit le risque immédiat, mais l'événement relance la question de l'utilisation des **numéros de téléphone comme identifiants primaires** et sur **la nécessité d'architectures alternatives** (alias, noms d'utilisateurs, échanges d'empreintes cryptographiques entre locuteurs, anonymisation) pour limiter l'exposition. Pour les opérateurs et décideurs, l'enjeu est clair : maîtriser voire chiffrer les métadonnées, imposer des garde-fous anti-*scraping* et repenser l'authentification et l'identification au-delà du seul numéro de téléphone.

Digital Omnibus Act *: simplifier ou diluer le RGPD ? La crainte d'un affaiblissement du règlement européen*

Présentée comme un volet de « simplification » du droit numérique en Europe, la proposition dite « **Digital Omnibus Act** » a suscité des retours mitigés. Si l'intention d'alléger les procédures et clarifier certains mécanismes administratifs est légitime, des organisations de défense des droits et des spécialistes de la protection des données à caractère personnel (DCP) mettent en garde contre une possible dérive : certaines mesures pourraient **éroder des principes fondamentaux du RGPD** — consentement effectif, proportionnalité, responsabilité accrue des responsables de traitement.

Les critiques pointent des risques concrets : des **assouplissements interprétatifs qui ouvriraient la voie à des pratiques plus permissives**, une réduction des obligations de documentation ou des exceptions mal cadrées qui **affaibliraient la capacité des personnes à exercer leurs droits**. À l'inverse, les partisans de la simplification estiment qu'il faut **alléger des charges administratives disproportionnées pour les PME** et moderniser des processus inadaptés à l'espace numérique actuel.

L'enjeu dépasse la technique : il touche à la **légitimité démocratique du cadre européen** et à **la confiance des citoyens**. Toute révision doit donc s'accompagner de garanties fortes — transparence, audits indépendants, maintien des droits fondamentaux — pour éviter une modification qui serait en réalité synonyme de dilution des protections.

GrapheneOS ne veut plus dépendre du cadre juridique français et pointe des pratiques fondées sur la surveillance de masse dignes d'un Etat autoritaire

GrapheneOS (un Android alternatif), projet canadien indépendant reconnu pour son attention portée sur la sécurité et la vie privée, promu par Edward Snowden, a annoncé la suppression de ses serveurs hébergés en France (chez OVH). Motivée par le sentiment de vulnérabilité juridique et médiatique exprimé par les équipes, cette décision symbolise une rupture de confiance entre certains projets centrés sur la vie privée, libres et *open source* et l'environnement juridique français.

Tout a commencé par deux articles à charge et faiblement documentés du *Parisien* en date du 19/11 et articulés sur l'interview d'une magistrate spécialisée dans la cybercriminalité. Lesdits articles cumulent pourtant les contre-vérités et aberrations de nature technique – prétendant par exemple dans un amalgame peu sérieux que GrapheneOS est le système Android des narcotrafiquants, qu'il se télécharge sur le « darknet » ou encore que l'équipe de GrapheneOS ne coopère pas pour livrer les données des utilisateurs hébergées sur ses serveurs. Or ses serveurs n'abritent aucune donnée d'utilisateurs, uniquement les ressources pour télécharger l'OS depuis un site web… de surface. Par ailleurs, beaucoup d'ONG, de dissidents politiques en dictature, de journalistes et experts en cybersécurité ainsi que des citoyens « lambda » utilisent ce système d'exploitation, qui fonctionne uniquement sur certains modèles de terminaux Google (*Pixel*, *Nexus*).

Concrètement, le départ de GrapheneOS s'explique par la crainte d'une exposition à des pressions externes et à des interprétations juridiques jugées inadaptées pour des services axés sur l'anonymat et l'intimité numérique des utilisateurs. Pour la France, c'est un signal préoccupant : perdre des acteurs de niche — mais importants — affaiblit l'écosystème national en matière d'innovations visant la protection du citoyen. Pour GrapheneOS, c'est un glissement typique d'une

« démocratie fatiguée » (François Sureau) qui sombre progressivement vers l'autoritarisme sous couvert de lutte contre le narcotrafic et la cybercriminalité.

Au-delà du cas GrapheneOS, cet épisode pose des questions structurelles, voire interroge notre **modèle de société** : quelles garanties offrir aux hébergeurs et aux projets sensibles ? La sécurité doit-elle primer sur la liberté, avec en toile de fond la célèbre citation attribuée à Benjamin Franklin ? Comment articuler sécurité juridique, confidentialité et coopération avec les autorités ? Répondre à ces questions est indispensable pour bâtir une **souveraineté numérique crédible**, susceptible d'attirer et de retenir les acteurs de la vie privée. Tout est dans le **paradoxe** : l'Etat français déplore le manque de culture de sécurité d'un côté, mais rechigne à accepter que quelques individus (et une minorité de criminels avérés) se dotent d'un outil qui confère un vrai niveau de sécurité et de confidentialité. Là où les iPhones et Apple sont plus rarement pointés du doigt (bien que vulnérables, eux, au bout d'un an aux entreprises spécialisées de type **Cellebrite** et donc à leurs clients, les Etats), les autorités ou du moins la Justice française s'attaquent à un petit projet *open source*. L'ANSSI a pourtant audité, aidé (remontée de bugs) et considère GrapheneOS comme outil sérieux favorisant sécurité et confidentialité des usagers.

Menace technique convergente : la fragilité des chaînes d'approvisionnement numériques

Novembre 2025 a mis également en évidence une faiblesse structurelle partagée entre deux types d'incidents : d'une part, la fuite massive de données chez un grand fournisseur de services cloud français, révélant des **erreurs de configuration et la persistance de secrets non renouvelés** (identifiants, clés API, certificats cryptographiques…) ; d'autre part, des *ransomgangs* ou des hacktivistes auraient exploité des vecteurs de *phishing* ou des vulnérabilités (*cross-site scripting* – XSS) pour pénétrer des environnements industriels en Europe et Amérique du Nord et chiffrer des bases de données SCADA/OT (systèmes informatiques industriels/technologie opérationnelle logicielle-matérielle de l'informatique industrielle), voire altérer le fonctionnement des systèmes instrumentés de sécurité (SIS). Dans les deux scénarios, la **chaîne d'approvisionnement logicielle apparaît comme le maillon le plus vulnérable** : des composants tiers (bibliothèques JavaScript, services cloud, solutions de virtualisation) ont servi de porte d'entrée, permettant à des acteurs malveillants de compromettre des infrastructures critiques. Cette convergence souligne **l'urgence d'adopter une approche holistique de la cybersécurité, intégrant la gestion des identités** (IAM), la **rotation systématique des secrets**, la **surveillance continue des dépendances logicielles et des audits de configuration automatisés** afin de réduire la surface d'exposition globale.

Sommet de souveraineté numérique européenne : un tournant historique ?

Le sommet européen sur la souveraineté numérique qui s'est déroulé à Bruxelles fin novembre a rassemblé chefs d'État, régulateurs et dirigeants du secteur technologique autour d'un agenda centré sur la réduction de la dépendance aux fournisseurs étrangers et le renforcement des capacités locales. Parmi les décisions phares, les participants ont convenu **d'accélérer la mise en œuvre de la nouvelle version de la norme ISO-27001:2025**, d'investir massivement dans des **projets de clouds souverains certifiés** et de **créer un cadre commun pour la certification des**

logiciels critiques, incluant des **exigences de transparence sur les chaînes d'approvisionnement**.

Le sommet a également annoncé la création d'un **fonds européen dédié à la recherche en cybersécurité**, destiné à soutenir les **start-ups développant des solutions de protection des infrastructures essentielles**. Ces engagements visent à garantir que l'Europe puisse maîtriser ses données sensibles tout en restant résiliente face aux menaces transnationales – mais aussi, espérons-le, internationales –, marquant ainsi un pas décisif vers une autonomie numérique durable. Il faudra bien sûr suivre de très près ces lettres d'intention.

*OpenAI / Mixpanel : lorsque l'***analytics** *web transforme les métadonnées en risque partagé*

Fin novembre, OpenAI a indiqué qu'un incident touchant Mixpanel (prestataire d'analyses statistiques d'utilisateurs) avait permis **l'exfiltration de métadonnées** liées à des comptes API : adresses électroniques, noms, localisations approximatives, OS/navigateurs, sites référents et identifiants organisationnels. OpenAI a précisé que **les contenus des requêtes, les clés API, les informations de paiement et les identifiants sensibles n'étaient pas concernés**, mais l'événement illustre un principe inquiétant : **confier des données comportementales à des tiers analytiques crée un point de vulnérabilité** qui peut produire des conséquences en cascade pour des dizaines, centaines, voire milliers d'organisations clientes.

La leçon est multiple : d'une part, la **minimisation des données** envoyées aux prestataires **est une exigence opérationnelle** : on ne doit transmettre que ce qui est **strictement nécessaire** ; d'autre part, les **contrats de sous-traitance doivent intégrer des clauses robustes** (accès, réversibilité, localisation des données, audits indépendants). Enfin, pour les secteurs sensibles, envisager des **solutions d'*analytics* internes** ou des offres « **cloud de confiance** » devient une exigence de sécurité.

Fuite à la FFF : données publiques et réputation en jeu

Une fuite de données affectant la Fédération Française de Football (FFF) a été relayée au cours du mois, constituant une **troisième atteinte en deux ans**. Les éléments exfiltrés couvrent des fiches administratives et des informations de contact, des **données personnelles** (noms, dates de naissance, adresses électroniques, numéros de téléphone) de millions de licenciés dont un **grand nombre d'enfants et adolescents**. La FFF a indiqué que son **système de gestion des licences avait subi une intrusion perpétrée** par des **attaquants en possession d'identifiants volés**. Le compte interne compromis a été désactivé par la Fédération. Bien sûr, ces données pourraient donner lieu à des **attaques ciblées** (*spear phishing*), en particulier **sur des mineurs**.

Si l'impact direct sur la sécurité financière est limité, l'atteinte à la **confidentialité des adhérents et licenciés** soulève des questions de gouvernance et de protection des bases de données au sein d'associations de grande taille. L'événement souligne par ailleurs la **vulnérabilité de telles plateformes centralisées** qui gèrent les données d'un grand nombre d'entités, et rappelle que la menace touche aussi les **organismes sportifs et associatifs**, parfois moins préparés à gérer des incidents de grande ampleur.

Suites du projet ChatControl et témoignage du RSSI d'OVH : régulation, sécurité opérationnelle et responsabilité industrielle

Les débats autour du projet de loi européen dit « ChatControl » continuent : entre positions politiques, critiques d'ONG et craintes des éditeurs, la discussion illustre le difficile équilibre entre **lutte contre les contenus illicites et préservation du chiffrement et des droits fondamentaux.** Les évolutions et amendements récents montrent que l'enjeu technique (détection pré-transmission) renvoie surtout à un **choix politique** clair sur la place du chiffrement et des portes dérobées (*backdoors*). **L'Allemagne s'y était d'ailleurs finalement opposée**, à travers la voix du président du groupe CDU/CSU au Bundestag : « *Cela reviendrait*, a-t-il dit, *à ouvrir toutes les lettres à titre préventif pour vérifier qu'elles ne contiennent rien d'illégal. C'est inacceptable, cela n'arrivera pas avec nous.* »

Parallèlement, le RSSI de l'hébergeur français OVH a partagé sa vision sur l'évolution de la cybermenace. Il insiste sur la **responsabilité industrielle** : les opérateurs doivent non seulement sécuriser leurs infrastructures, mais aussi **contribuer à la résilience collective en communiquant clairement sur les risques**, en facilitant la **réversibilité** et en participant à **des exercices de crise**. Ce double mouvement — régulation accrue et responsabilité opérationnelle des acteurs — dessine un cadre où **la confiance se construit par des engagements concrets et vérifiables**. Evoquant par ailleurs **l'IA, il a précisé que celle-ci permettait aux cybercriminels d'affiner et optimiser** leurs attaques. Au-delà de cette automatisation partielle qui rend leur détection plus malaisée, c'est aussi et surtout la **professionnalisation de ces offensives qu'il faut décrypter et comprendre pour mieux adapter les défenses** et anticiper la menace. En effet, le **cybercrime** procède aujourd'hui comme le ferait des entreprises légales, avec des chaines d'approvisionnement, sous-traitances et découpages des tâches **de niveau industriel**.

Perspectives

Novembre 2025 confirme que la cybersécurité franchit continument des paliers : l'attention se partage entre les correctifs techniques et les bases d'hygiène informatique, la gouvernance des données, la maîtrise de la chaine logistique et de l'écosystème numérique, et la souveraineté industrielle. Protéger les contenus sans protéger les métadonnées ne suffit plus ; simplifier le droit sans maintenir des garde-fous n'est pas tenable ; attirer des projets centrés sur la vie privée suppose des garanties opérationnelles et juridiques solides ; protéger les systèmes d'information doit s'accompagner de mesures solides sur les systèmes de contrôle industriel et les infrastructures logicielles…

En guise de feuille de route pour 2026 : prioriser la **minimisation des flux vers les tiers**, contractualiser la **réversibilité et l'auditabilité**, développer des **offres cloud de confiance européennes**, et intégrer la **gestion des métadonnées** dans les politiques de risque. Le Forum InCyber Europe 2026 devra être l'occasion opportune de traduire ces exigences en projets concrets.

Résumé

1. **WhatsApp** : la faille d'énumération pourtant sur 3,5Mds de comptes a mis en lumière la vulnérabilité des métadonnées à l'échelle planétaire, et une énième faille basique chez META.

2. **Digital Omnibus** : la simplification proposée suscite des craintes d'affaiblissement du RGPD ; vigilance nécessaire.

3. **GrapheneOS** : retrait des serveurs français après offensive informationnelle juridique et médiatique contre le projet d'OS Android sécurisé et *open source* — signal d'alerte sur la confiance et la souveraineté et critique de l'Etat français jugé comme empruntant une pente autoritaire.

4. **Chaîne d'approvisionnement** et **recrudescence d'attaques sur systèmes industriels** : la tendance initiée dans les années 2010 revient : les SCADA redeviennent une cible de choix. Plus généralement, la chaine logistique et l'infrastructure logicielle révèlent leurs faiblesses : leurs composants tiers sont le maillon le plus vulnérable.

5. **Sommet sur la souveraineté numérique de l'UE** : adoption accélérée d'ISO-27001:2025, lancement d'un cloud souverain certifié et d'un cadre commun de certification des logiciels critiques, projet de création d'un fonds européen pour les start-ups spécialisées pour réduire la dépendance aux fournisseurs étrangers.

6. **OpenAI / Mixpanel** : les prestataires en analyse statistique Web exposent des métadonnées sensibles — audit des sous-traitants impératif.

7. **Fuite de données de la FFF :** exposition de millions de données personnelles notamment de mineurs via un compte interne compromis, générant un risque de *spear-phishing*. Nécessité de cloisonner et sécuriser les plateformes centralisées et d'une gouvernance stricte sur les bases de données associatives.

8. **ChatControl / OVH** : débats réglementaires sur le projet de loi européen décrié, et témoignage du RSSI d'OVH soulignent l'interdépendance entre régulation, respects de la vie privée, industrie et sécurité opérationnelle.

Sources principales utilisées

TechRepublic — *WhatsApp flaw exposed billions of users*. https://www.techrepublic.com/article/news-whatsapp-flaw-exposed-billions-users/

Futura-Sciences — *3,5 milliards d'utilisateurs WhatsApp concernés*. https://www.futura-sciences.com/tech/actualites/cybersecurite-chercheurs-alertent-35-milliards-utilisateurs-whatsapp-concernes-plus-grande-fuite-donnees-histoire-127731/

WIRED — *A Simple WhatsApp Security Flaw Exposed 3.5 Billion Phone Numbers*. https://www.wired.com/story/a-simple-whatsapp-security-flaw-exposed-billions-phone-numbers/

PrivacyImpact — *Digital Omnibus Act et RGPD 2.0 : simplifier n'est pas diluer* (12 nov. 2025). https://www.privacyimpact.fr/2025/11/12/digital-omnibus-act-et-rgpd-2-0-simplifier-nest-pas-diluer/

NOYB — *Digital Omnibus: EU Commission wants wreck core GDPR principles*. https://noyb.eu/en/digital-omnibus-eu-commission-wants-wreck-core-gdpr-principles

FrAndroid — *Pourquoi GrapheneOS retire ses serveurs de France*. https://www.frandroid.com/android/2881329_nous-ne-nous-sentons-plus-en-securite-en-france-pourquoi-grapheneos-retire-ses-serveurs-de-france-suite-a-un-article-du-parisien

IT-Connect — *GrapheneOS quitte la France et OVHcloud : pourquoi ?* https://www.it-connect.fr/grapheneos-quitte-la-france-et-ovhcloud-pourquoi/

OpenAI — *Mixpanel incident* (communiqué incident). https://openai.com/index/mixpanel-incident/

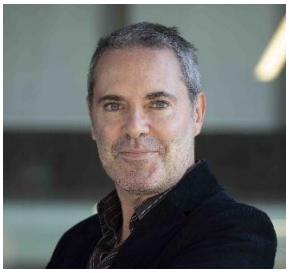
Cybersecuritycue — *vulnérabilité sur Scadabr exploitée par un hacktiviste caractérisée par la CISA.*
https://cybersecuritycue.com/scadabr-vulnerability-hacktivist-attack-cisa/

ZATAZ — *Les activistes intensifient leurs attaques sur les SCADA canadiens.*
https://www.datasecuritybreach.fr/les-hacktivistes-intensifient-leurs-attaques-contre-les-infrastructures-canadiennes/

Cyber-securite-.fr — *la CISA intègre la faille XSS sur Scadabr aux CVE.*
https://www.cyber-securite.fr/cisa-integre-la-vulnerabilite-xss-exploitee-cve-2021-26829-de-openplc-scadabr-dans-sa-liste-des-menaces-cles/

Pro-Tech Systems Group — *Ce qu'implique les récentes cyberattaques contre les SCADA*
https://www.pteinc.com/recent-scada-cybersecurity-breaches-implications/

Veillecyber.fr — novembre 2025



Yannick PECH est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, certifié *pentester* junior. Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste à la CEIS, et réserviste opérationnel de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie. Il prépare actuellement les certifications EBIOS-RM et ISO-27001.