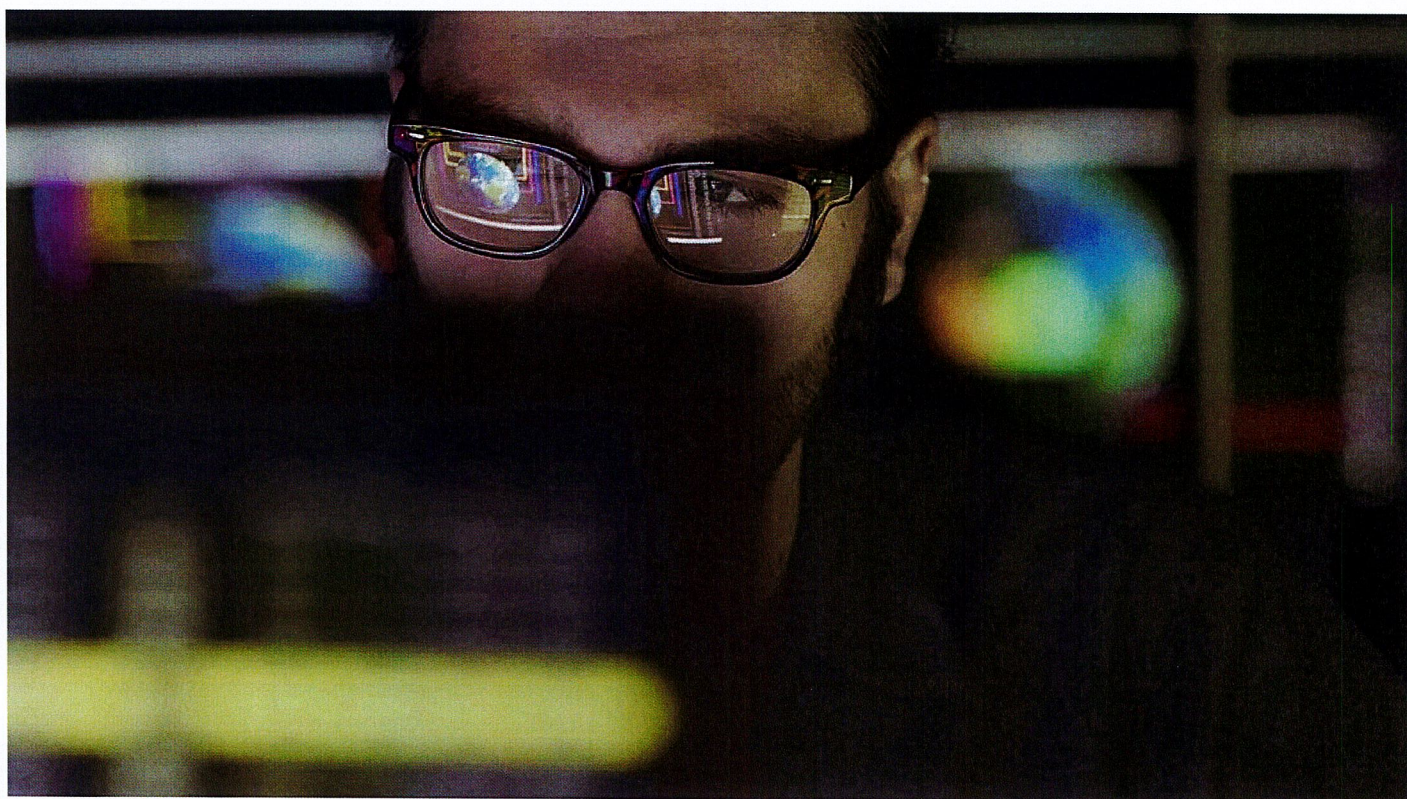


« OSINT : une pratique indispensable, un cadre juridique absent »

Une législation consacrée à l'OSINT permettrait de reconnaître explicitement la liberté de collecter des informations en sources ouvertes dans le respect du droit, et offrirait une sécurité juridique aux personnes agissant pour un motif légitime, plaide la députée Sabine Thillaye.



L'OSINT consiste à collecter et analyser des informations librement accessibles sur Internet. (iStock / Istockphoto)

Par **Tribune collective**

Publié le 27 avr. 2026 à 10:40 | Mis à jour le 27 avr. 2026 à 15:17

 Votre abonnement vous permet d'accéder à cet article

En 2025, la France a publié sa dernière revue nationale stratégique, plaçant la cybersécurité au cœur de notre sécurité nationale et entend rester dans le premier cercle des puissances cyber mondiales. Hôpitaux, collectivités, entreprises, administrations, **aucune organisation n'est à l'abri d'une cyberattaque**. Celle qui a touché le ministère de

l'Intérieur en décembre 2025, avec le vol de dizaines de fichiers confidentiels, met en évidence l'évolution et l'adaptation des cybercriminels malgré un environnement de plus en plus contraignant. Pas un jour ne passe sans qu'une fuite de données en lien avec des organismes privés comme étatiques ne soit révélée...

Face à cette réalité, l'Union européenne a franchi un cap avec **l'adoption de la directive NIS2**, qui vise à assurer un niveau élevé commun de cybersécurité pour un certain nombre d'acteurs privés et publics considérés comme essentiels ou importants. Le projet de loi de transposition, après avoir été discuté au Sénat et en commission spéciale à l'Assemblée nationale, qui doit être discuté en séance publique dans le courant de l'année peine à figurer à l'ordre du jour.

Sources ouvertes

L'article 21, paragraphe 2, alinéa (e) de la directive NIS2 impose aux entités essentielles et importantes de mettre en oeuvre « la sécurité dans l'acquisition, le développement et la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ». Cette obligation exige l'identification et le traitement des vulnérabilités et la recherche de vulnérabilités en sources ouvertes (OSINT) constitue un moyen essentiel.

LIRE AUSSI :

- **ANALYSE – Pourquoi la France est une cible si facile sur le front cyber**

L'OSINT consiste à collecter et analyser des informations librement accessibles sur Internet afin notamment d'identifier des failles de sécurité, des expositions de données ou des menaces, sans recourir à des moyens illégaux ou coercitifs, à la ruse ou au piratage. Plus largement, l'OSINT permet de produire du renseignement à partir de sources ouvertes pour comprendre des environnements complexes et est un pilier dans le renforcement de notre résilience cyber.

Flou juridique

Pourtant, en droit français, cette discipline ne bénéficie d'aucun cadre général clair. En dehors de quelques régimes spécifiques protecteurs comme les journalistes qui bénéficient du secret des sources, et certaines administrations ou services spécialisés, la

pratique générale de l'OSINT repose sur une incertitude juridique et l'analyse de données issues de fuites peut exposer les professionnels de la cybersécurité à un risque pénal au titre du recel, nous plongeant dans de nouvelles dépendances, un comble quand on prône la souveraineté.

« Une banque victime d'une fuite de données et souhaitant les récupérer sur le dark web avait exprimé sa crainte de le faire, par peur d'être condamnée pour recel de vol de données »

Ce flou juridique perturbe de nombreux acteurs victimes de cyberattaques qui souhaiteraient recourir à l'OSINT. Par exemple, une banque victime d'une fuite de données et souhaitant les récupérer sur le dark web avait exprimé sa crainte de le faire, par peur d'être condamnée pour recel de vol de données. Cette contradiction juridique paralyse les acteurs, freine l'innovation et pousse des organisations à se tourner vers des solutions étrangères, échappant à notre contrôle et exigences.

L'OSINT va au-delà des seuls intérêts marchands ou de la protection de nos organismes stratégiques. C'est une véritable discipline, pratiquée par des passionnés comme par des professionnels, et utilisée dans des domaines très divers comme la cartographie. Une législation consacrée à l'OSINT permettrait, d'une part, de reconnaître explicitement la liberté de collecter des informations en sources ouvertes dans le respect de la vie privée, des données personnelles, des secrets protégés par la loi et des droits de propriété intellectuelle. D'autre part, elle offrirait une sécurité juridique minimale aux personnes agissant pour un motif légitime.

Encadrer l'OSINT n'est pas un sujet technique réservé aux experts. C'est une condition nécessaire au renforcement de notre résilience cyber et **un enjeu de souveraineté numérique** car il s'agit d'améliorer la cybersécurité de nos infrastructures les plus sensibles. Donner un cadre clair à l'OSINT, c'est donner aux défenseurs du cyberespace les moyens d'agir, en sécurité et au service de l'intérêt général.

- **Salaires : ces nouveaux métiers dans la cybersécurité qui affolent les compteurs**

Les signataires de la tribune sont :

Sabine Thillaye, députée (Les Démocrates) de la 5e circonscription d'Indre-et-Loire, vice-présidente de la commission de la Défense nationale et des Forces Armées et membre de la commission des Affaires Européennes.

Emilie MUSSO, Docteure en droit de la cybersécurité et responsable juridique chez Anozr Way

Michel SEJEAN, professeur agrégé de droit à l'Université Sorbonne Paris Nord et chercheur associé à l'IHEDN, spécialiste de droit de la cybersécurité et de droit comparé

Bertrand WARUSFEL, avocat, professeur agrégé des facultés de droit

Jean PEETERS, Professeur, Université Bretagne Sud

France CHARRUYER, Présidente de l'association d'intérêt général Data-Ring et avocate fondatrice d'Altij avocats

Julien METAYER, Osinter Indépendant, Expert Cybersécurité offensive OPIX, Commandant réserviste ministère de l'intérieur.

Arnaud LATIL, Maître de conférences, Sorbonne université

Jean-Michel MIS, Ancien député de la Loire, Président ViaPublica

Thomas GASSILLOUD, député du Rhône

Julien MONGENET, responsable des équipes de réponse aux incidents cyber pour le groupe Thales

Ludovic HAYE, Sénateur du Haut-Rhin, membre de la Commission des Affaires étrangères, de la Défense et des Forces armées ainsi que de la Commission spéciale sur le PJI résilience des infrastructures critiques et renforcement de la cybersécurité

Gregory WINTREBERT, directeur exécutif des relations institutionnelles et des partenariats stratégiques de SOPRA STERIA, Président de l'Alliance pour la Confiance numérique (ACN)

Gabriela BELAID, Présidente de CentraleSupélec au Féminin, Directrice numérique et Cyber sécurité

Jean-Nicolas ROBIN, Avocat associé - Docteur en droit AVOXA Cyber

Marie RECALDE, Députée de la 6ème circonscription de la Gironde

Catherine MORIN-DESAILLY, Sénatrice de la Seine-Maritime, membre de la Commission spéciale sur le PJJ résilience des infrastructures critiques et renforcement de la cybersécurité

Fily KANTE, président et fondateur de la structure ID Protect, 1er outil de prévention contre l'usurpation d'identité.

Geneviève DARRIEUSSECQ, députée des Landes, Ancienne ministre

Virginie DUBY-MULLER, députée de la 4ème circonscription de la Haute-Savoie, Vice-Présidente, membre de la Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Marc WATIN-AUGOUARD, Coauteur du code de la cybersécurité, fondateur du Forum INCYBER

Philippe LUC, co-fondateur de Anozr WaySébastien GARNAULT, président de la CyberTaskForce

Tribune collective

THÉMATIQUES ASSOCIÉES

Assemblée Nationale

Télécoms

Cybersécurité

Indre-et-Loire



Les Echos

Publiez votre expertise dans Les Echos

En tant qu'abonné Premium, vous avez accès au Cercle : publiez votre tribune dans Les Echos pour partager vos analyses, affirmer votre vision et nourrir le débat auprès des décideurs économiques.



[Je rédige ma tribune](#)