Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Face à la cybercriminalité généralisée, Poweriti propose un bouclier anti-vol de données



C'est Jantien Rault qui a créé la société Poweriti en 2021. Elle est aujourd'hui installée au sein d'Agroparc, où phosphorent une dizaine d'experts qu'il a recrutés pour leurs hautes compétences.

« En France, 54% des PME ont déjà subi une attaque, un piratage. En Vaucluse, 93% des 55 000 entreprises sont des TPE. Nous sommes là pour leur offrir une protection, une sécurisation de leurs mails, imprimantes, scanners. Pour un abonnement mensuel à moindre frais, nous proposons à chacun une solution adaptée au cas par cas. Antivirus, pare-feu, maintenance 24h/24, 7j/7, sauvegarde trois fois par jour, stockage garanti des fichiers, protection infranchissable, en bref, un coffre-fort blindé, étanche à toute intrusion malveillante », explique le jeune patron. Fiabilité rime avec sérénité et les PME peuvent en toute tranquillité renforcer leur visibilité et leur développement.

Aujourd'hui, dans l'Hexagone, on entre dans les grands ministères, administrations, collectivités locales et entreprises comme dans un moulin. Pour le seul 1er trimestre 2026, on a recensé 54 000 « incidents » (+37% par rapport à 2025) et 90 millions de comptes détournés. Notamment, 11,7M pour France Titres qui gère permis de conduire, cartes grises, cartes d'identité au Ministère de l'Intérieur, 15 M pour Cegedim Santé, 678 000 comptes bancaires de contribuables fichés par la DGFIP ces dernières semaines,

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

nombre de fédérations, comme celles des chasseurs, ce qui a facilité, grâce aux noms et adresses figurant sur les documents, le vol d'armes à leur domicile. Sans oublier, La Poste, l'URSSAF et nombre d'hôpitaux…

La France, vice-championne du monde du piratage

À ce rythme, ce n'est plus une succession de brèches ouvertes dans des documents confidentiels, ni une mini-vague de cyber-attaques, c'est carrément un système organisé, massif et exponentiel. La France est vice-championne du monde du piratage derrière les USA et n°1 en Europe, un palmarès dont on se passerait volontiers et qui facilite fraude, usurpation d'identités, faux profils, harcèlement ciblé, ouverture de faux comptes, détournements de fonds à grande échelle

Dans ces conditions, il vaut mieux payer un abonnement pour se protéger que verser les milliers d'euros d'une rançon réclamés par un hacker malveillant. « Nous présentons nos excuses aux Français, ce qui est arrivé est inexcusable », a simplement marmonné le Ministre aux Comptes Publics. À une époque où tout est dématérialisé (déclarations de revenus, cession de véhicule, paiement de factures) et où les séniors non geek doivent demander de l'aide à leurs petits-enfants nés avec une console à la main ou se rendre dans les antennes de France Service pour remplir n'importe quel formulaire administratif…

On frémit quand on sait que dès le 1er septembre prochain, dans une dizaine de jours, toute facturation sera forcément électronique. « Une simplification », « un archivage sécurisé », « un traitement fiable », « une solution validée par l'État », « un gain de productivité », « une gestion facilitée »… vantent les différents organismes en veine de formules marketing. À ce jour, 166 plateformes sont déjà agréées, une véritable usine à gaz pour les commerçants, artisans, indépendants, entrepreneurs, professions libérales… Dans le seul secteur complexe du tourisme ce chantier pharaonique donne des cheveux blancs aux hôteliers, agences de voyages, tour-opérateurs avec les fiches de conformité de la raison sociale de l'entreprise, SIREN/SIRET à jour, n° de TVA valide, adresse de livraison, code postal normalisé pour éviter les erreurs…

Dernière ligne droite pour facturation électronique

Pour la seule année 2024, le coût du piratage numérique avait coûté 118 milliards à la France, depuis il n'a sans doute fait que se développer à la vitesse grand V. « Peu de ministères sont au niveau », a reconnu cette semaine le 1er Ministre. Avant lui, François Bayrou son prédécesseur, avait lancé l'idée d'un filtre anti-hackers jamais abouti. Aujourd'hui, face à la réalité implacable, le locataire de Matignon évoque la création d'une 'unité cyber'. Espérons que ce ne sera pas un énième comité Théodule aussi cher qu'inutile. Qui fait penser au « Pitalugue » de Marcel Pagnol. L'académicien aubagnais avait tourné en dérision un rafiot doté d'une énorme hélice qui faisait tourner le bateau en rond… au lieu de le propulser vers l'avant.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Cyberattaque : et si votre avocat était votre premier rempart juridique ?



En France, 60 % des PME victimes de cyberattaque n'ont pas d'avocat dans leur cellule de crise, ce qui a pour résultat des plaintes mal rédigées, assurances non indemnisées, responsabilités mal gérées. Maitre Djamel Belhaouci* du barreau de Marseille explique pourquoi l'avocat est un acteur incontournable dès la première heure.

Il est 2h du matin, les serveurs d'une PME francilienne viennent d'être chiffrés par un ransomware. Le dirigeant réveille son DSI, contacte son prestataire informatique, alerte son assureur. L'avocat ? Il sera appelé trois semaines plus tard, hélas quand il sera trop tard pour réparer la plupart des erreurs commises.

« Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

fuite de données. »

Maître Djamel Belhaouci

Ce scénario, Maître Belhaouci, avocat en droit de la cybercriminalité, le rencontre chaque semaine dans son cabinet. « Les entreprises pensent que la cyberattaque est d'abord un problème technique. C'est une erreur fondamentale, dès la première heure, elle est surtout un problème juridique. »

« Une entreprise victime de cyberattaque a 72 heures pour notifier la CNIL d'une éventuelle fuite de données. Si cette notification est absente, mal rédigée ou tardive, les sanctions peuvent dépasser le préjudice de l'attaque elle-même. Il est de même pour le dépôt de plainte dans le cadre d'une couverture assurantielle. C'est le premier acte juridique à poser et il doit l'être par un avocat. »

Rappel du cadre légal
Notification CNIL obligatoire : 72 heures après la découverte d'une violation de données à caractère personnel (art. 33 RGPD). Information des personnes concernées : sans délai injustifié lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés (art. 34 RGPD). Infractions applicables : accès frauduleux à un STAD (art. 323-1 CP), atteinte au secret des affaires (loi du 30 juillet 2018), extorsion (art. 312-1 CP).
Face à la recrudescence des cyberattaques en France le nombre d'incidents déclarés à l'ANSSI a progressé de 30% en 2025 , Maitre Belhaouci appelle les chefs d'entreprise à anticiper : « Intégrez votre avocat dans votre plan de continuité d'activité avant la crise. Le moment le plus coûteux pour appeler un avocat spécialisé, c'est le lendemain de l'attaque. »

Les trois erreurs récurrentes commises en l'absence d'un avocat
1. La plainte rédigée sans conseiller juridique: dans la précipitation, les dirigeants déposent des plaintes incomplètes, sans qualification précise des infractions tel l'accès frauduleux à un système de traitement automatisé de données (STAD), l'extorsion, l'atteinte au secret des affaires. Une plainte mal rédigée affaiblit l'ensemble de la procédure pénale et réduit les chances d'indemnisation.

2. L'assureur cyber contacté sans préparation: les polices d'assurance cyber contiennent des clauses d'exclusion précises. Contacter l'assureur sans avoir préalablement sécurisé les preuves et documenté l'incident avec un conseil juridique expose l'entreprise à un refus de garantie. « J'ai vu des entreprises perdre plusieurs centaines de milliers d'euros d'indemnisation pour des déclarations maladroites faites dans les premières heures », témoigne Maitre Belhaouci.

3. La communication de crise sans garde-fou juridique: informer ses clients, ses partenaires ou la presse d'une violation de données engage la responsabilité civile et pénale de l'entreprise. Chaque mot compte. L'avocat est le seul interlocuteur capable de valider ces communications sous couvert du secret professionnel.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

« Ce n’est pas une question de taille d’entreprise. »

L’avocat dans la cellule de crise : un investissement, pas un coût Maître Belhaouci plaide pour une intégration systématique de l’avocat spécialisé en cybercriminalité dans les plans de réponse aux incidents des entreprises au même titre que le responsable informatique ou le DPO. « Ce n’est pas une question de taille d’entreprise. Une PME de 20 salariés est aussi concernée qu’un groupe du CAC 40. Les cyberattaquants ne font pas de distinction. »

Concrètement, l’intervention de l’avocat dès la première heure permet : la préservation des preuves dans des conditions juridiquement recevables, la rédaction de la notification CNIL dans les délais légaux (72 heures), le pilotage de la relation avec les forces de l’ordre et le parquet cybercriminalité, la sécurisation des communications internes et externes, et l’anticipation des recours des tiers éventuellement affectés.

L.G.

**Maître Djamel Belhaouci est avocat au Barreau de Marseille. Il dirige un cabinet dédié au droit de la cybercriminalité et en défense pénale. Il intervient dans les procédures pénales liées aux infractions informatiques, conseille les entreprises victimes de cyberattaques et accompagne ses clients dans leur mise en conformité.*

Cybercriminalité : avec POWERiti, une start-up innovante d’Avignon, votre sécurité est garantie

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026



Les cyberattaques sont en croissance constante et exponentielle en France : +37% en 2020. En 2021, l'ANSSI (Autorité Nationale de la Sécurité des Systèmes d'Informatique) avait recensé 1082 intrusions et en 2024, le chiffre a explosé à 385 000, dont 330 000 visaient des PME, 37 000 des organismes publics et 17 000 des ETI (Entreprises de taille intermédiaire).

Pêle-mêle : l'Hôpital Simone Veil à Cannes, Engie, la SNCF, La Société Générale, Chronopost, France Travail, Bouygues Telecom, Auchan, les villes de Marseille et Nîmes ont vu leurs serveurs attaqués, leurs données sensibles violées, leurs fichiers clients pillés. Des millions de données, listings de clientèle, dossiers confidentiels utilisés frauduleusement après ces innombrables attaques-éclair. Personne, quelle que soit la taille, n'est à l'abri.

C'est là qu'intervient l'Avignonnais Jantien Rault, qui a créé son entreprise POWERiti en février 2021 à Agroparc, « pour offrir une proposition globale de solutions de sécurisation des données, grâce à une équipe d'experts digitaux soigneusement sélectionnés, une connectivité fiable évolutive, une veille H-24, 7 jours sur 7 et une sauvegarde permanente. »

Grâce à ce système de « coffre-fort numérique », les patrons peuvent dormir sur leurs deux oreilles et retrouver leur sérénité. Les mails, bulletins de salaire de leurs employés, listes de fournisseurs et de clients sont protégés, impénétrables et ne peuvent pas être revendus à d'éventuels concurrents.

Une entreprise en croissance

Et comme la demande grimpe à la vitesse grand V, « en un an, le chiffre d'affaires a grimpé de +50%, le nombre de mes salariés est passé de 9 à 12 et l'investissement se poursuit. Pour 2025, la courbe de la croissance continue de grimper avec un chiffre d'affaires probable estimé à 1,4M€, et pour 2026, la tendance est à la stabilisation des acquis et à la recherche de nouveaux clients », explique le jeune PDG.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Aujourd'hui, l'entreprise compte environ 150 clients, dont un quart dans le Sud-Est de la France. « Je suis fier d'avoir acquis un service qui officie pour le Ministère de la Défense, même si je dois rester discret. Il a validé la qualité et le périmètre de notre accompagnement comme 100% fiable pour des données militaires, donc absolument confidentielles. Nous avons aussi la confiance d'industriels avec des secrets de fabrication, que ce soit dans l'agroalimentaire, la métallurgie, la construction. Certains travaillent à flux tendu jour et nuit avec des équipes qui font les 3 x 8h, Donc la cybersécurité doit être constante, ne jamais interrompre le processus industriel », précise Jantien Rault.

À l'avenir, il compte développer son propre outil pour apporter une vision plus ludique du parc informatique à ses clients, même ceux qui ne sont pas fondamentalement des 'geeks'. « Le sens que nous donnons à ce que nous faisons est important. Comme la confiance qui nous lie à nos clients. Nous devons être transparents, leur assurer une fiablité, un plus. » Et comme il a le sens de la réciprocité, Jantien Rault compte créer une sorte de fondation qui soutiendra des actions caritatives, qui sera au service d'une communauté, de l'intérêt général.

Contact : 04 12 04 01 90

POWERiti, l'allié avignonnais des entreprises contre la cybercriminalité

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026



« Protégez-vous contre la cybercriminalité », implore Jantien Rault, le créateur de POWERiti à Avignon, qui se veut une société proposant des solutions informatiques innovantes et sécurisées afin de propulser les entreprises vers une efficacité et une croissance durables.

« 54% des entreprises françaises sont victimes de hackers et ce chiffre explose à une vitesse exponentielle », déclare le créateur de cette start-up qui est le 1er site en France à proposer une offre globale de sécurisation de vos données sensibles.

Lors d'une soirée à l'Hostellerie des Fines Roches de Châteauneuf-du-Pape, ce jeune avignonnais, qui a fait ses études d'informatique et de commerce à Saint-Jean-Baptiste de la Salle et Saint Vincent-Paul, s'est adressé à un parterre d'environ 300 chefs d'entreprises pour les sensibiliser aux risques qu'on entre comme dans un moulin dans leurs mails, fichiers clients, fournisseurs, fiches de paie des salariés, dossiers sensibles stratégiques. « Nous avons '*My serenity*' , une solution tout-en-un (99,90€ par mois) pour rendre impénétrables toutes vos données avec une mise à jour automatique et un support illimité, 100% transparent et sans surprise. »

La cybercriminalité mise en pratique pour cibler les problèmes

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Pour faire une démonstration aux chefs d'entreprises, Jeremy Nedjar, venu de la Direction des Finances Publiques, s'est présenté comme 'hacker éthique' de sa société L-Exploit Cyber Expert. « Quand je travaille pour un client, je deviens testeur d'intrusion. Je vois s'il est facile de craquer son mot de passe et c'est souvent le cas. Je me fais passer pour un livreur et j'arrive avec une simple clé USB à entrer dans le réseau et capter toutes les données », martèle-t-il. « On a vu des hôpitaux attaqués pour les données de leurs patients, leur numéro de Sécurité sociale, mais aussi des banques. HSBC, par exemple, a ainsi perdu 1,2Md€, même si on n'a pas tous les chiffres de ce que représente le vol de données. »

> « Il vaut mieux payer une prime pour se protéger qu'une rançon hors de prix d'un hacker malveillant. »
>
> *Jeremy Nedjar*

Il poursuit : « Votre adresse IP, c'est une identification unique, comme votre empreinte digitale. Avant tout, trouvez un code compliqué avec des chiffres, étoiles, slashes, underscores, caractères bizarres, alternez lettres minuscules et majuscules, mais surtout pas toto 1, 2, 3… Sinon, c'est la porte ouverte au sabotage industriel et à la concurrence déloyale. Prémunissez-vous contre ces gens qui veulent forcer votre coffre-fort numérique sans pied-de-biche. Payez 1 000 ou 2 000€ pour sécuriser vos données, ce n'est rien par rapport aux risques encourus. Veillez aussi à ce que vos salariés ne jouent pas avec l'ordinateur du bureau et aient le même code que chez eux, sinon votre entreprise sera vulnérable, donc facilement piratée. 1/3 des sociétés cyberattaquées déposent le bilan quelques mois après. Si vous perdez votre comptabilité, vous ne pouvez plus facturer, bonjour les dégâts. »

POWERiti garantit sécurité et tranquillité

Jantien Rault conclura la soirée en insistant sur l'apport des solutions POWERiti qu'il propose avec ses collaborateurs. « Changer de mot de passe régulièrement, avoir une double authentification, un système anti-phishing, être connecté 24h/24 et 7j/7. Un de ses clients acquiesce : « Avant, dans mon entreprise de 45 salariés et 140M€ de chiffre d'affaires, je faisais tout, même changer le toner de la photocopieuse. J'avais un partenaire informatique nul, qui ne venait jamais quand il y avait une urgence, qui m'avait proposé un contrat de 48 mois totalement opaque, bref, qui était un escroc. Puis, j'ai rencontré Jantien Rault, il a audité scrupuleusement poste après poste, fait des préconisations pour la téléphonie, l'informatique, proposé une maintenance chiffrée, il m'a changé la vie. Certes, ça coûte, mais c'est le prix de ma tranquillité et de la sécurité de ma boîte. En particulier, le retour sur investissement a été rapide grâce à ce qu'il m'a permis d'éviter comme chausse-trappe numérique. »

Contact : global@lxploit.com

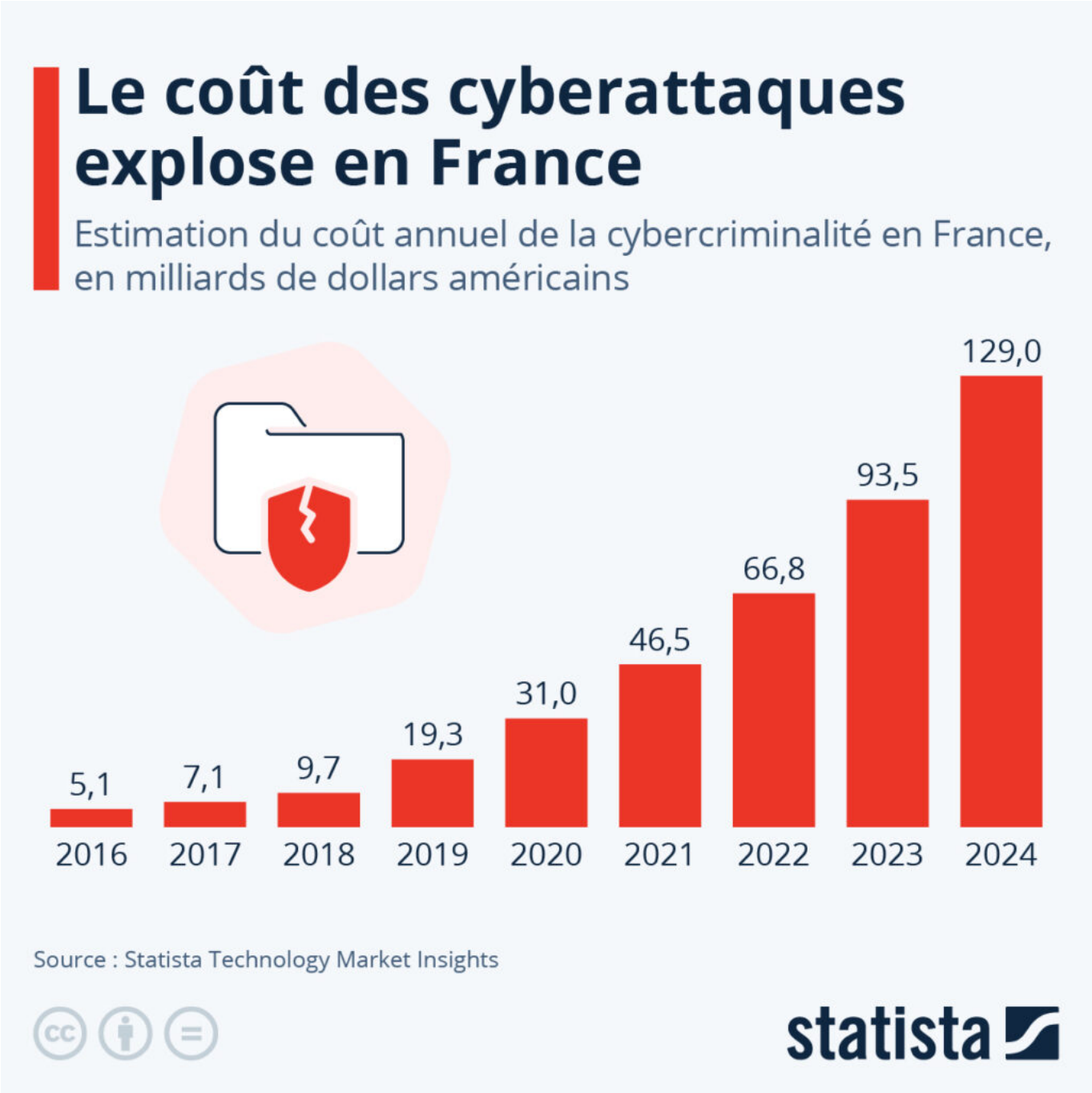
Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Le coût de la cybercriminalité explose en France

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026



Le coût annuel de la cybercriminalité en France est aujourd'hui évalué à plus de 100 milliards d'euros. Selon les dernières estimations issues des Technology Market Insights de Statista, le coût total des cyberattaques et autres actes malveillants en ligne devrait atteindre 129 milliards de dollars américains dans le pays en 2024 (soit environ 119 milliards d'euros), contre près de 94 milliards de dollars l'an passé.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 7 novembre 2026

Comme le retrace notre infographie, le coût de la cybercriminalité en France a littéralement explosé ces huit dernières années. En 2016, ce chiffre n'était évalué qu'à 5,1 milliards de dollars, avant de connaître une hausse moyenne de plus de 30 % chaque année. Cette tendance va de pair avec la multiplication, la diversification et le perfectionnement des cyberattaques au cours de la période étudiée.

D'après l'édition 2024 du baromètre du CESIN, près d'une entreprise française sur deux a été victime d'une cyberattaque avec un impact significatif l'an dernier. En outre, le cyberespionnage représenterait un risque élevé pour deux entreprises sur cinq (toutes industries confondues). Les auteurs du rapport soulignent notamment « la complexité croissante du paysage de la cybersécurité, avec des attaquants qui ajustent leurs tactiques ».

De Tristan Gaudiaut pour Statista