# Cybersécurité et Responsabilité sociale des entreprises

Trente après la création d'Internet qui visait à décloisonner le monde, force est de constater que certains aspects négatifs n'ont pas été anticipés : fake news, fracture numérique, insécurité, criminalité, protection des données personnelles, employabilité, usages des algorithmes, pour n'en citer que quelques-uns...

**5 min**

La cybersécurité est beaucoup plus large que la lutte contre les cyberattaques : en effet, des données peuvent fuir ou être perdues par négligence ou manque de processus, un système informatique peut s'arrêter à cause de la canicule, ou d'un incendie...

Les impacts sociaux d'une défaillance numérique sont directs : impossibilité de soigner, incapacité à protéger les données des clients ou des patients, licenciements, pertes financières, perte de confiance, employabilité.

Deux exemples illustrent ces impacts sociaux :

- The Gardian, le 7 août 2022, relate que « deux des principaux hôpitaux du Royaume-Uni ont dû annuler des opérations, reporter des rendez-vous et détourner des patients gravement malades vers d'autres centres au cours des trois dernières semaines après que leurs ordinateurs se sont écrasés au plus fort de la canicule du mois de juillet ». « Nous naviguions à vue », a déclaré un médecin senior. Récupérer les résultats des laboratoires était un cauchemar absolu et impliquait des porteurs transportant des bouts de papier vers et depuis le laboratoire »
- Le témoignage du directeur IT de Manutan à la suite d'une attaque informatique réussie : « L'impact psychologique est le plus terrible. Plus rien ne fonctionne, comme dans un incendie, mais aucun bien physique n'est détruit. 2 400 personnes se retrouvent du jour au lendemain à ne plus pouvoir travailler. Et à ne pas savoir quand elles reprendront le travail ni même si elles le reprendront. Ni même, d'ailleurs, pourquoi elles ne le reprennent pas. Parce que, lorsque vous subissez une telle attaque, d'un ennemi invisible, vous êtes paralysés par l'idée de ne pas savoir d'où viendra le prochain coup. Alors vous n'informez vraiment personne. Vous demandez juste à votre personnel d'attendre ».

## Protéger les consommateurs (ou les patients) et leurs données

Cela fait partie de la responsabilité sociale de chaque entreprise ou acteur public. Les responsables du secteur médical ne peuvent pas se permettre de dire, à l'occasion d'une fuite ou d'un vol de données médicales, « ce n'est pas grave », comme nous l'entendons parfois. Eh bien si, c'est grave. De même qu'un vol de données fiscales, d'une entreprise, ou d'un

particulier, c'est grave ! Les impacts sociaux sont évidents.

Les consommateurs attendent des marques qu'elles protègent leurs données personnelles. Afficher de bonnes pratiques de cybersécurité est déjà une pierre angulaire du modèle commercial, mais cela doit aussi faire partie du programme social.

Il est également de leur devoir de s'assurer que les fournisseurs, sous-traitants et prestataires de services qui ont accès à leurs données prennent eux aussi les mesures nécessaires à leur protection.

## Les effets du numérique sur l'emploi et l'employabilité

Les directions d'entreprises gèrent-elles les impacts de leur transformation numérique et des nouvelles technologies sur le monde du travail : mise en place de programmes de formation et d'acquisition de nouvelles compétences, soutien nécessaire à la reconversion pour les employés concernés par l'automatisation et l'intelligence artificielle ?



## Les impacts environnementaux et sociaux du numérique

Dans le bilan carbone des entreprises, l'impact du numérique est-il mesuré ? Deux fois plus que l'aviation commerciale aujourd'hui, et bientôt quatre fois plus! Les utilisateurs n'ont pas conscience de cet impact, ni des autres effets : pollution, manque d'eau, raréfaction des métaux rares, consommation d'énergie, câbles sous-marins au fond des océans, serveurs, exploitation des métaux rares, déchets...

La négligence d'un conseil d'administration lui serait reprochée, si aucune action n'était engagée dans le domaine de la cybersécurité de l'entreprise, et si les défaillances informatiques et des processus de protection des données avaient des conséquences significatives pour le bon

fonctionnement de l'entreprise, sa rentabilité, sa réputation… Et son impact social !

La politique RSE doit permettre une prise de conscience des enjeux, des principes de gouvernance et de la politique de cybersécurité, pour trouver un meilleur équilibre entre performance numérique, bien-être des collaborateurs, et performance du business.

Il s'agit de mettre en place de meilleurs usages, « un code de la route », un « permis de conduire ». La vitesse n'est pas le seul objectif ! Éviter les accidents passe par une responsabilité de chaque utilisateur, et peut-être une plus grande sobriété ?

La rédaction d'un code de responsabilité numérique permet de s'assurer que la stratégie numérique de l'entreprise est exécutée dans le respect de la vie privée et des données, et dans le respect de règles éthiques dans le cadre de l'utilisation de l'intelligence artificielle : compréhension des algorithmes et traçabilité des processus de décisions pour garantir que les décisions prises à l'aide de l'intelligence artificielle (recrutement, santé, surveillance…) ne sont pas biaisées. Capacité à passer en « mode manuel », si une décision prise à l'aide d'intelligence artificielle s'avère ne pas correspondre aux objectifs fixés ou aux principes éthiques fixés par l'entreprise.

## La cyberculture : une priorité

Les responsabilités reposent trop souvent sur les responsables de la sécurité, qui sont à la fois chargés de l'estimation des risques, de la proposition de solutions, du choix de ces solutions, et de leur mise en œuvre. Les burn-out de RSSI sont malheureusement trop courants, et les RSSI qui souhaitent quitter ces fonctions sont trop nombreux.

Le nouveau code de gouvernance anglais recommande aux conseils d'administration d'évaluer la culture et surveiller son évolution. De même les Pays-Bas et le Japon ont révisé leur code de gouvernance et insistent sur l'importance de la culture : comment la définir, mesurer et surveiller son

évolution. Ce qui vaut pour la culture en général, vaut pour la cyberculture.

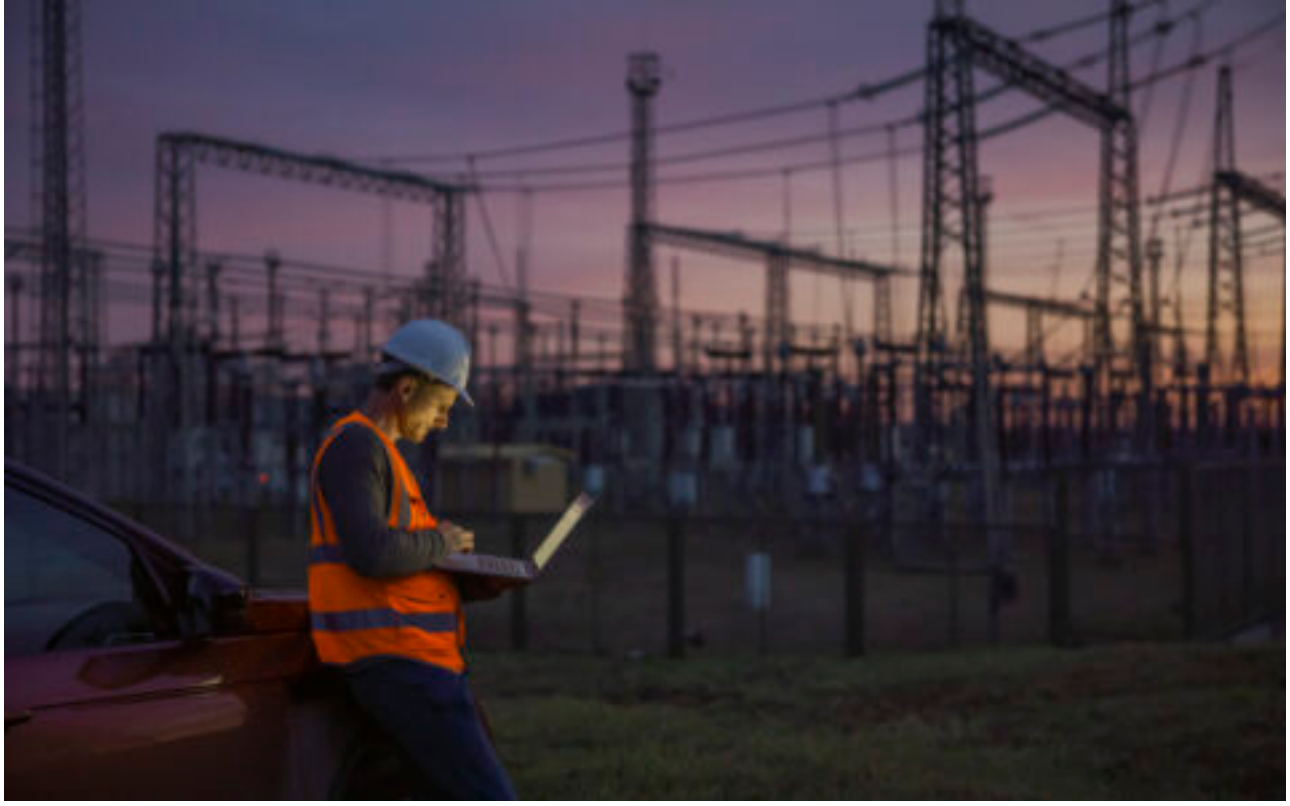
Revenir à l'accueil

- **Transformation numérique**
- **Cyber sécurité industrielle**
- **Sécurité et stabilité du cyberespace**
- **Cyber criminalité**
- **Souveraineté numérique**
- **Identité numérique & KYC**
- **Lutte anti-fraude**
- **Sécurité opérationnelle**
- **Cyber risques**

**30 octobre 2022**

## CPF : FranceConnect+ désormais obligatoire

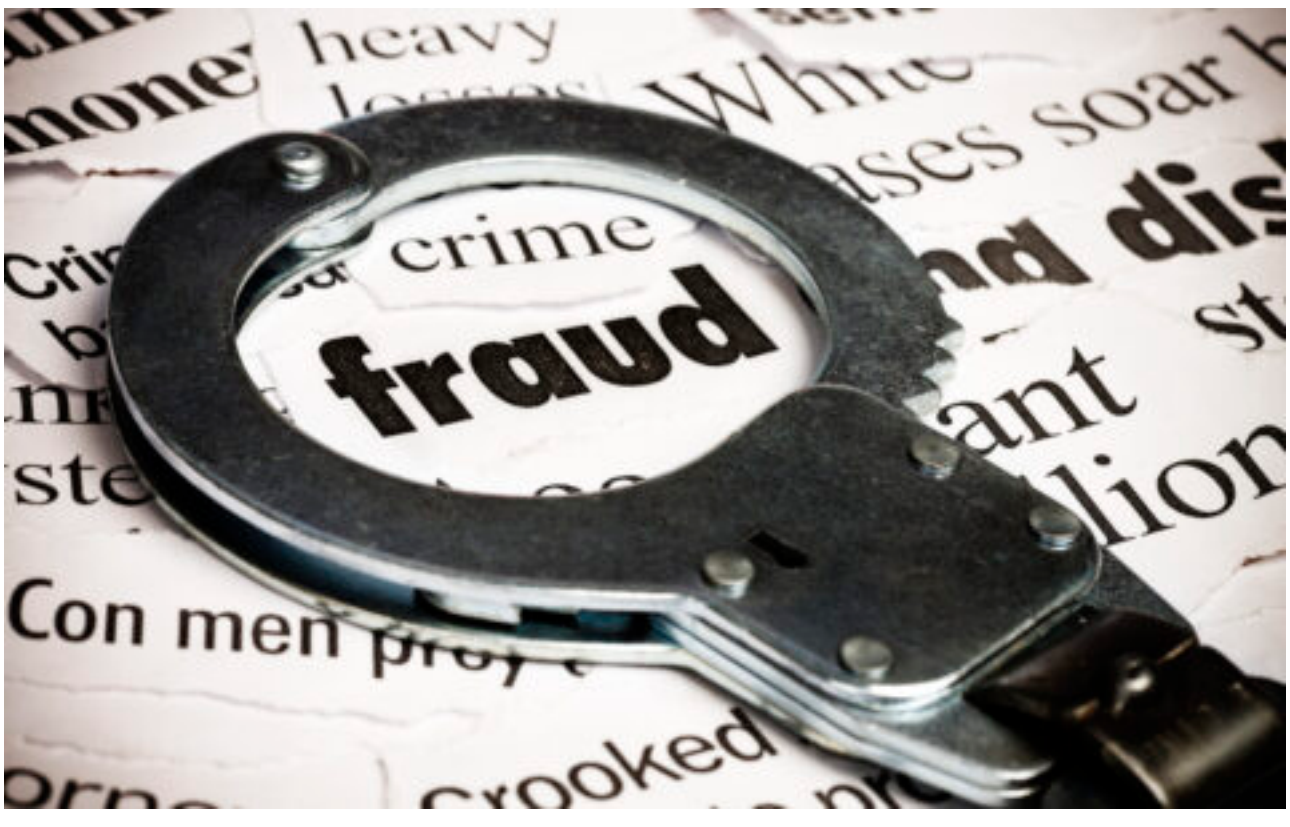
Pour lutter contre la fraude au Compte personnel de formation sur FranceConnect, il faudra désormais passer par le service FranceConnect+. Ce dernier est doté d'une authentification à double ...



**03 novembre 2022**

## Quelle stratégie de cyberdéfense pour EDF ?

Dans une récente interview, le directeur de la cybersécurité d'EDF, Olivier Ligneul, détaille la stratégie cyber de l'énergéticien, « opérateur supercritique »

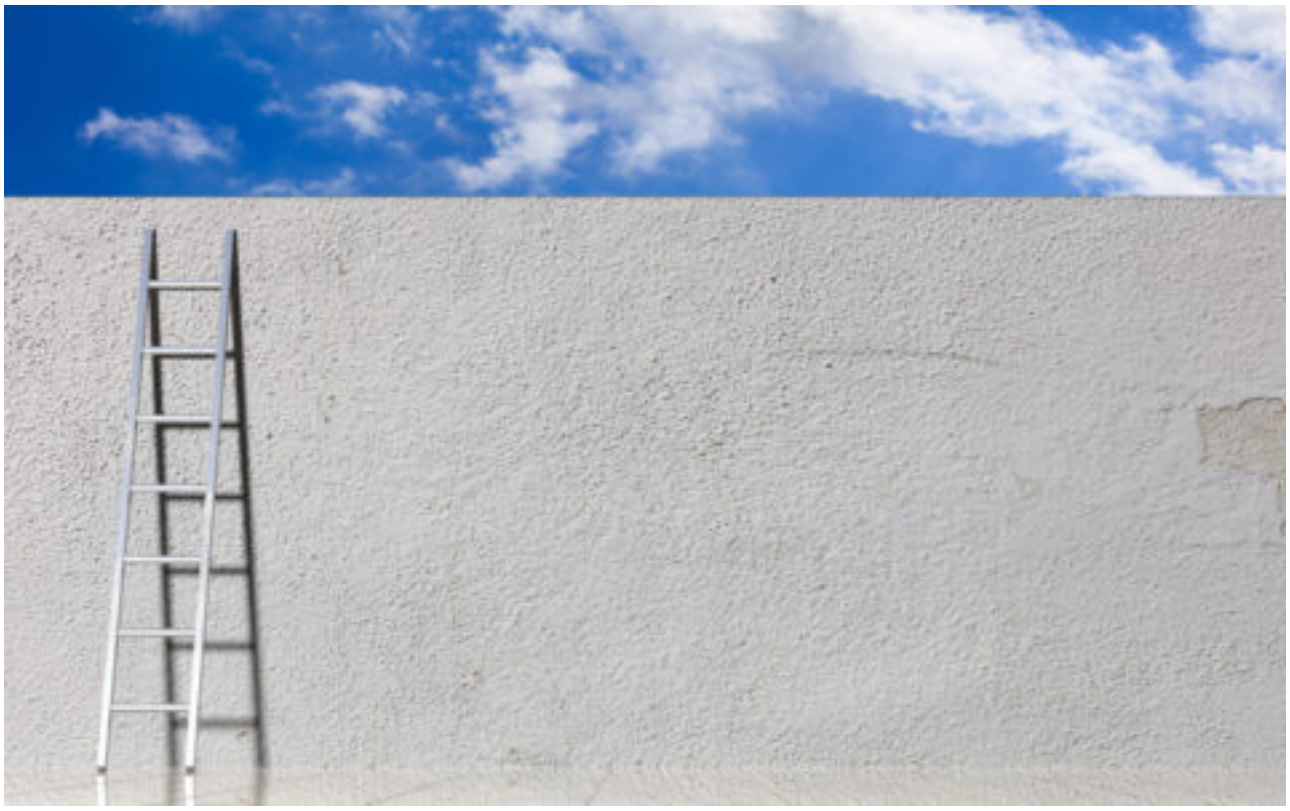



**25 juillet 2022**

## La DGCCRF dresse son bilan numérique 2021

La DGCCRF a présenté le bilan de son action sur le numérique en 2021, qui

comprend notamment 16 000 sites Internet inspectés et le déréférencement de Wish.



**14 octobre 2022**

## TEHTRIS lève 44 millions d’euros

Spécialiste français du XDR, TEHTRIS annonce une levée de fonds de 44 millions d’euros, pour renforcer sa présence à l’international