Service de santé des armées

LA LETTRE TRIMESTRIELLE DU SSA SUR LA CYBERSECURITE ET LES CYBERMENACES

Deuxième trimestre 2020

SENSIBILISATION

Comment séparer vos outils numériques et usages personnels et professionnels

L'actualité de la cybersécurité et des cybermenaces

La crise sanitaire de la COVID-19 et le recours massif au télétravail constituent des opportunités sans précédent pour les cybercriminels

Le dossier du trimestre

La Blockchain : quels apports pour la santé ?

PLAN DE LA LETTRE

SENSIBILISATION
Comment séparer vos outils numériques et usages personnels et professionnels

LA SÉPARATION DES USAGES, UN DES GRANDS PRINCIPES DE LA CYBERSÉCURITÉ

Grâce à internet et au développement des technologies mobiles et connectées, la frontière entre vos vies personnelle et professionnelle semble devenir poreuse. Face à cette **évolution il est nécessaire d'adapter les pratiques, notamment en séparant les usages personnel et professionnel.**

Pourquoi séparer les usages ?

Séparer les usages est un principe essentiel de l'hygiène informatique. Il évite qu'un individu malveillant atteigne un périmètre bien plus large de votre vie personnelle (numérique, mais aussi morale ou physique) ou professionnelle.

Par cette bonne pratique, vous contribuerez activement à la sécurité du MINARM et protégerez votre espace de vie privée, vos proches et vos relations professionnelles, en limitant considérablement les risques de cyberattaque et les vols, pertes ou fuites de données.

Comment séparer les usages ?

1. Séparez l'usage des outils numériques personnels et professionnels. Évitez par exemple de :

- consulter des données personnelles sur un périphérique professionnel ;
- consulter des données professionnelles sur un périphérique personnel.

Si vous êtes doté d'outils SMOBI vous permettant le nomadisme, ne consultez que des sites Internet sûrs et évitez les réseaux Wifi publics ou inconnus.

2. **Distinguez aussi vos messageries professionnelles et personnelles. En particulier, ne faites pas suivre vos emails professionnels sur votre messagerie personnelle**, dont le niveau de sécurité est moindre que celle du MINARM. Si votre compte personnel est piraté, vous mettez en danger l'intégrité des informations que vous y avez stockées. Cela permet aussi d'éviter que des informations confidentielles vous échappent vers des contacts personnels.

3. Distinguez rigoureusement les outils de stockage, clés USB et disques durs notamment, à usage personnel et professionnel. Si vous devez transférer des données professionnelles d'un poste de travail à un autre, dédiez à ce besoin une clé USB soigneusement identifiée, et passée au préalable sur station blanche.

4. N'utilisez jamais vos mots de passe personnel sur les applications professionnelles. Et plus généralement, respectez les respecter les règles de cyberhygiène. Utilisez *un mot de passe différent par application* (voir la fiche de sensibilisation du dernier trimestre 2019).

Keepass est un outil permettant le stockage sécurisé de ses mots de passe, rendant cette règle à la portée de tous. Sinon, un cyber criminel peut utiliser votre mot de passe pour accéder à votre compte en banque, ou se connecter sur un réseau sécurisé

5. Sur vos réseaux sociaux, ne dites rien de votre vie professionnelle, ou seulement le strict minimum. Et maitrisez vos propos. Gardez en tête que vous ne maitrisez pas vos lecteurs, qui peuvent rediffuser ou interpréter les informations transmises. Pour vous aider, utilisez le *Guide du bon usage des réseaux sociaux du MINARM*.

6. Ne chargez jamais vos périphériques personnels (téléphones, enceintes, montres connectées, etc.) sur votre poste de travail professionnel, branchez-les sur une prise.

Si vous avez des questions ou des besoins spécifiques, tournez-vous vers votre CSSI, pour qu'il puisse vous aider et vous proposer des solutions sécurisées adaptées à vos besoins (logiciels, etc.) en liaison avec votre CORSIC.

Aller plus loin pour mieux vous protéger

Vous pouvez durcir la sécurité de vos outils personnels et de vos usages : analyse critique des mails reçus, sans clic sur les liens non fiables, mots de passe forts, anti-virus à jour, mise à jour en temps réel de toutes les applications installées, désinstallation des applications devenues inutiles ou non sûres, notamment celles téléchargées hors des « stores » officiels, pas de visite de sites Internet douteux, etc.

Leçon 1 : surveillez vos effets personnels !

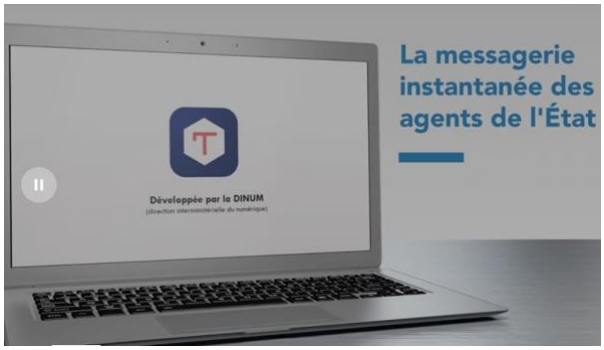
Vidéo lauréate du Grand Prix du Jury du Festival du film de sécurité 2016, commanditée par Eric Ravello, Corporate Security, AIRBUS Group.

Pour aller plus loin, voir :

- La page *Apprendre à séparer ses usages pro-perso* du site cybermalveillance.gouv.fr ;
- *Les 10 règles d'or Cyber en télétravail* de la marine nationale (*en dernière page du fichier*) :
- Le *Guide de recommandation sur le nomadisme numérique* de l'ANSSI.

MESSAGERIE TCHAP
Créez votre compte TCHAP, et utilisez-le sans modération

Développée par la Direction interministérielle du numérique de l'État (*DINUM*), *Tchap* **est une solution de messagerie instantanée et sécurisée dédiée aux agents de l'État pour leurs échanges entre eux et avec leurs partenaires externes, et y compris en mobilité**.



Son fonctionnement est très proche des messageries instantanées habituelles telles WhatsApp ou Messenger : utilisation simultanée possible sur plusieurs appareils (application sur smartphone ou tablette, ou directement dans un navigateur internet), discussions par messages à deux ou en groupe, transferts de fichiers, annuaire intégré, forums privés ou publics de discussion.

Tchap offre un haut niveau de sécurité et de confidentialité : informations chiffrées de bout en bout (hors salons publics) et hébergées sur des serveurs maîtrisés par l'État, pièces jointes inspectées par un antivirus, application maîtrisée car développée à partir de logiciels libres, enrôlement exclusivement à partir d'adresses de messageries institutionnelles, révocation des comptes en cas de non-validation périodique de l'adresse professionnelle, clôture d'office de tout compte inactif pendant plus de 6 mois. Les abonnés peuvent choisir de s'inscrire sur liste rouge.

Tchap n'est toutefois pas agréée pour les informations du niveau Diffusion Restreinte ou classifiées de défense.

Tchap ne doit être utilisée que pour des échanges éphémères n'étant pas soumis à une obligation réglementaire d'archivage, car les conversations sont détruites au bout d'une durée limitée, paramétrable mais toujours inférieure à un an.

Tous les agents de l'État ont accès à la solution « Tchap Agent », qui peut être installée sur tous les terminaux Apple ou Android grand public, professionnels ou privés. Tchap Agent est ouvert sur le monde extérieur, par simple invitation d'un abonné, l'invité n'ayant alors que des droits restreints (il ne peut communiquer qu'avec l'invitant, ne peut inviter personne et n'a pas accès à l'annuaire).

Cette messagerie doit être privilégiée à toute autre application comme WhatsApp, Viber ou Telegram pour tous les échanges instantanés au sein du ministère comme avec les correspondants extérieurs (autres ministères, agents territoriaux, famille, réservistes, partenaires industriels et économiques, etc.).

Les téléphones de type SMOBI peuvent être équipés de « TCHAP Secure », qui ouvre un tchat réservé aux seuls utilisateurs de téléphone SMOBI.

Téléchargez l'application et créez votre compte directement dans l'application ou sur le site officiel *https://www.tchap.gouv.fr* (à ne pas confondre avec le site non officiel *www.tchap.fr*). Il suffit ensuite de cliquer sur un lien contenu dans un courriel envoyé à votre adresse professionnelle (en intradef.gouv.fr exclusivement).

Vous pourrez ensuite converser avec les agents de l'État titulaires d'un compte, ou inviter vos correspondants extérieurs à l'administration.

Lisez le *Guide de prise en main*, la *FAQ*, les *Conditions générales d'utilisation* et les directives propres au ministère des armées (disponibles sur Intradef).

Mais attention, l'application ne sécurise pas le téléphone. Par ailleurs, les salon « publics » sont par définition ouverts à tous les autres utilisateurs de Tchap. Ils sont donc visibles par de nombreuses institutions hors MINARM.

ACTUALITE DE LA CYBERSECURITE ET DES CYBERMENACES

LA CYBERCRIMINALITE EN FORTE HAUSSE AVEC LA PANDEMIE DE COVID-19

Comme à chaque période de crise, **la cybercriminalité a fortement augmenté dans le monde depuis le début de la pandémie** : l'anxiété rend en effet la population particulièrement vulnérable aux *cyberimpostures* et arnaques en tout genre et aux *attaques* de *phishing*, promettant par exemple vaccins miracles, livraison rapide de masques ou aide financière. Toute crise constitue également une période propice à la *désinformation* et aux *attaques*, *souvent étatiques*, visant à déstabiliser les pays et organisations internationales, déjà sous forte pression pour gérer la crise et ses conséquences sociales et économiques. Notons aussi que la propension de la population à rediffuser tous les messages angoissants, humoristiques ou d'espoir constitue, un facteur de viralité des attaques.

A ces menaces accrues liées à toute crise, **s'est ajoutée, lors de la pandémie actuelle, une explosion sans précédent de la « surface d'attaque numérique »**, que les cybercriminels se sont empressés d'exploiter. En effet, le confinement très strict décidé par de très nombreux pays et la fermeture des frontières ont conduit à un développement extraordinaire des usages numériques, en urgence et donc souvent sans possibilité d'en durcir la sécurité, notamment pour répondre aux besoins accrus d'information des dirigeants et de la population et pour assurer autant que possible les activités à distance via des solutions de télétravail et de téléconférence. Comme cela est présenté plus loin, ce développement des usages numériques a été particulièrement fort dans le monde de la santé.

Des attaques visant tout particulièrement les organisations de santé

Si tous les secteurs ont été concernés par l'augmentation de la cybercriminalité depuis le début de la pandémie, celui de la santé, déjà sous forte menace permanente, a été plus ciblé que les autres. La menace exercée en permanence sur les organisations de santé a été accrue sans doute du fait de sa sursollicitation, alors que les autres secteurs connaissaient une très importante baisse de leur activité.

EUROPOL a déclaré que presque tous *ses 27 pays membres avaient signalé une intensification des cyberattaques* sur leurs systèmes de santé. En particulier, des rançons ont été demandées par des pirates informatiques aux hôpitaux surchargés de patients atteints de la COVID-19, en verrouillant les dossiers de leurs patients et en menaçant de les publier, entrainant une pression supplémentaire sur les systèmes de santé et leurs services informatiques.

En France, en mars, *l'AP-HP* a souffert d'une attaque par déni de service (DDoS). L'attaque a été maitrisée mais il a fallu diminuer l'accès à Internet, bloquant ainsi l'accès externe à la messagerie interne et aux applications de l'AP-HP.

En mars également, le second plus grand *hôpital de la République Tchèque*, dont l'activité avait été réorientée pour dépister et traiter la COVID-19, a dû décaler des opérations et transférer des patients à la suite d'une cyberattaque.

Les États-Unis ont annoncé que de nombreuses attaques DDoS avaient tenté de paralyser des établissements de santé. Le *ministère de la santé* lui-même (*US Department of Health and Human Services*, DHHS) a vu son site Internet bloqué par une telle attaque, qui a notamment perturbé la publication d'informations sur la gestion de la COVID-19.

Plusieurs cas de ransomware ont également été rapportés, comme celui qui a affecté en avril le *Parkview Medical Center* américain.

L'*Organisation mondiale de la santé* (OMS) a été régulièrement attaquée depuis le début de la pandémie. En particulier, un site imitant son système de messagerie interne a été réalisé par des hackers pour l'espionner. La même méthode aurait été utilisée pour cibler d'autres organisations de santé et d'aide humanitaire.

Enfin, selon Trend Micro, des *cyberattaques sophistiquées de type APT* (*Advanced Persistent Threat*) ont été détectées sur les systèmes d'information d'établissements de santé pour les espionner, voler des données ou perturber leur fonctionnement.

Une forte mobilisation contre les cyberattaques sur les organisations de santé

Les acteurs publics de la santé et de la cybersécurité se sont rapidement mobilisés pour aider les établissements de santé à lutter contre les cyberattaques durant la pandémie.

L'ANSSI a mis à la disposition des structures de santé, via l'Agence du numérique en santé (ANS), une analyse des *marqueurs techniques liés à des attaques ayant récemment ciblé des hôpitaux* en Europe (notamment les codes malveillants découverts et leur rôle), ainsi que des *lots de marqueurs de détection de cyberattaque* (adresses IP, noms de domaine, empreintes de fichiers malveillants).

L'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux (ANAP) a lancé le 26 mars un *dispositif exceptionnel d'entraide* pour assister les établissements rencontrant des difficultés à mettre en œuvre des plans de continuité d'activité, mettre en place la téléconsultation, ou encore se protéger des cyberattaques. L'ANAP a ainsi mis à leur disposition son réseau d'experts en systèmes d'information, complété par des experts volontaires.

De nombreux acteurs privés de la cybersécurité, en collaboration avec les autorités nationales, ont proposé de venir en aide au secteur de la santé, parfois gratuitement. *Orange Cyberdéfense* a ainsi proposé gracieusement un service de conseil en cybersécurité et l'activation de son service de protection contre les attaques DDoS.

Par ailleurs, plusieurs groupes internationaux d'experts en cybersécurité se sont formés pour prêter main forte aux établissements de santé et traquer les cybercriminels profitant de la crise sanitaire, comme la *COVID-19 CTI League*, qui a réuni *400 experts de plus de 40 nationalités différentes*, ou la *COVID-19 Cyber Threat Coalition*. Au Royaume-Uni, un groupe s'est créé à l'occasion de la pandémie, le *Cyber Volunteers 19* , pour mettre les organisations de santé en relation avec des experts en cybersécurité et leur apporter une aide dans tous les domaines de la cybersécurité.

L'APPORT ESSENTIEL DU NUMERIQUE DANS LA GESTION DE LA CRISE SANITAIRE

Les usages numériques se sont fortement développés dès l'avènement de la pandémie, notamment dans tous les domaines d'action du secteur de la santé : téléconsultations, télétravail des personnels de santé, télé-expertise par visioconférence entre soignants, suivi médical à distance, gestion des capacités hospitalières et des équipes de soins, essais cliniques, recherche médicale, logistique médicale, etc. Quelques-uns de ces usages sont précisés ci-après.

Les téléconsultations et la télésurveillance

Le nombre de téléconsultations a explosé en France, dépassant les 500 000 actes facturés par semaine fin mars 2020 contre 10 000 en moyenne les mois précédents. Ce succès tient autant à la sécurité qu'elles apportent aux patients et soignants en période de pandémie qu'à leur prise en charge à 100% par l'Assurance maladie. *La téléconsultation est aussi entrée à l'hôpital*, alors qu'elle était inexistante auparavant.

De nombreuses applications de télésurveillance ont été développées à l'occasion de la pandémie, comme l'application gratuite *Covidom* utilisée par l'AP-HP pour suivre à distance ses patients atteints de la COVID-19 ou suspectés de l'être.

La Société de pneumologie de langue française a lancé un outil numérique original, *Covid-Quest*, pour aider toute personne ayant des symptômes évoquant la Covid-19 à obtenir un avis médical. En fonction des réponses à un questionnaire en ligne, l'application

crée un fichier synthétisant la situation du patient, qui peut être envoyé par courriel à son médecin ou transféré dans son dossier médical personnel. Certaines réponses peuvent déclencher des conseils, voire des alertes.

Dès mars 2020, *le ministère de la santé a encouragé tous les professionnels de santé à exercer en télésanté* (télémédecine et télésoins), et les accompagne dans leur choix d'outils numériques en publiant une *liste de solutions référencées* sur le site de l'ANS. Ce référencement tient compte de la sécurité des solutions, et notamment du respect du RGPD et de la Politique générale de sécurité des systèmes d'information en santé (PGSSI-S), de la certification HDS ou encore de la sécurisation des flux.

L'impression 3D

L'impression 3D a permis de répondre très rapidement à de nombreux besoins urgents de matériel médical ou de protection.

*L'AP-HP s'est rapidement dotée de 60 imprimantes 3D pour pallier la pénurie de matériel médica*l : visières de protection pour le visage, valves pour respirateur artificiel d'urgence, matériel d'intubation, masques, poignées, etc.

Imprimantes 3D déployées à l'AP-HP

(Source : https://www.usine-digitale.fr/article/covid-19-l-ap-hp-se-dote-de-60-imprimantes-3d-pour-pallier-la-penurie-de-materiel-medical.N950626)

De *très nombreuses autres initiatives d'impression 3D* ont été lancées, en France comme dans le monde, tant par des startups que par de grandes entreprises, pour épauler les hôpitaux. Parmi les nombreux exemples, un consortium international a permis la *production industrielle d'un adaptateur pouvant se fixer sur les masques de plongée de Décathlon*,

Dans le but de fédérer les initiatives de conception et d'impression 3D, l'AP-HP a créé le *site 3D COVID* fournissant notamment la longue liste de ses besoins en équipements médicaux, de protection ou de maintenance. D'autres plateformes en ligne, comme *la plateforme 3dchampions*, font appel à toute personne ou société pouvant participer à la fabrication 3D de produits nécessaires à la gestion de la COVID-19.

La géolocalisation au service de la lutte contre la COVID-19

De nombreux pays ont développé des applications permettant de *géolocaliser les personnes atteintes de la COVID-19*, en général de manière anonyme et dans le principal but de prévenir tous ceux qu'ils ont pu infecter, parfois pour *vérifier le respect des mesures de quarantaine imposées*. En France, le Gouvernement a lancé *l'application StopCovid*, objet de nombreuses controverses même si *la CNIL* ne s'y est pas opposée tout en posant ses conditions (consentement des intéressés, anonymisation et conservation limitée dans le temps des données notamment).

Des initiatives identiques ont été lancées par des entreprises privées, comme *l'application CoronApp* créée par un agence web parisienne.

La Blockchain pour le suivi anonyme des malades de la COVID-19

Plusieurs initiatives ont été lancées par des experts de la Blockchain pour contribuer à la lutte contre la COVID-19. Parmi elles, la solution *CARE* déployée sur une Blockchain propose de télécharger les résultats du test Covid-19 sur son portable, sans dévoiler son identité ni même fournir des données d'identification. De son côté, le consortium *Block Covid* développe la *solution Dépistage* visant à assurer, au profit des seules autorités de santé, la traçabilité des tests de dépistage effectués dans le registre distribué d'une Blockchain, afin "d'identifier les personnes qui sont immunisées et non contagieuses de manière à pouvoir créer des "vides sanitaires" auprès des personnes à risque", et de consolider les données au niveau national, voire européen.

Intelligence artificielle (IA) et lutte contre la COVID-19

De nombreuses initiatives visent à déployer des algorithmes d'intelligence artificielle pour notamment :

- *Prédire les aggravations de l'état des patients atteints de la COVID-19* et permettre aux médecins de savoir quels patients traiter en priorité, ce qui permet également une meilleure gestion de l'engorgement des établissements ;
- *Mieux comprendre le fonctionnement* de la COVID-19 et donc faciliter la recherche de traitements et médicaments ;
- Mieux détecter la propagation du virus ;
- Améliorer l'analyse de l'imagerie médicale ;
- Suivre les effets du virus et du confinement sur la santé mentale des populations ;
- Permettre *d'optimiser la sortie du confinement*.

Si l'IA est très prometteur pour lutter contre les pandémies, *certains acteurs de l'IA en santé soulignent qu'ils ne disposent pas suffisamment de données* sur la COVID-19 pour pouvoir faire fonctionner correctement leurs solutions.

Plateformes en ligne de mobilisation de personnels pour la santé

L'ARS d'Ile de France a mis en place la plateforme en ligne à vocation nationale *Renfort-Covid* qui recense les besoins de renfort des structures sanitaires ou médico-sociales et les volontaires pour assurer ces renforts parmi les étudiants, professionnels ou retraités ayant les compétences nécessaires.

LES BONNES PRATIQUES POUR FAIRE FACE A CETTE AUGMENTATION DE L'EXPOSITION AUX CYBERATTAQUES

Comme déjà signalé, l'extraordinaire développement des usages numériques lié à la crise de la COVID-19 s'est accompagné d'un très fort accroissement de la surface d'attaque, dont les cybercriminels ont cherché à exploiter toutes les possibilités. Pour aider à faire face à ces menaces, la plupart des agences de cybersécurité et des grandes entreprises numériques internationales ont mis en ligne des guides de bonnes pratiques et de durcissement de la sécurité des systèmes d'information.

Certains de ces guides sont à destination principale des organisations de santé, comme le recueil de bonnes pratiques publié par *Microsoft* sur la lutte contre les ransomwares.

Les autres, bien que non spécifiques à la santé, sont bien sûr à prendre en compte aussi strictement que possible par les organisations de santé. Leurs principales recommandations sont rappelées ci-après.

Recommandations de *Cybermalveillance.gouv.fr* pour le télétravail en situation de crise

- Si vous disposez d'équipements professionnels, séparez vos usages ;
- Appliquez strictement les consignes de sécurité de votre entreprise ;
- Ne faites pas en télétravail ce que vous ne feriez pas au bureau ;
- Appliquez les mises à jour de sécurité sur tous vos équipements connectés (PC, tablettes, téléphones…) ;
- Vérifiez que vous utilisez bien un antivirus et scannez vos équipements ;
- Renforcez la sécurité de vos mots de passe ;
- Sécurisez votre connexion WiFi ;
- Sauvegardez régulièrement votre travail ;
- Méfiez-vous des messages inattendus ;
- N'installez vos applications que dans un cadre « officiel » et évitez les sites suspects.

Consignes de cybersécurité du site *Cybermalveillance.gouv.fr* pour la crise sanitaire

- Méfiez-vous des messages (mail, SMS, chat …) ou appels téléphoniques inattendus ou d'origine inconnue ;
- Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs ;
- Vérifiez la fiabilité et la réputation des sites que vous visitez ;
- Soyez vigilants aux fausses informations ;
- Attention aux appels aux dons frauduleux ;
- Ne vous précipitez pas et prenez toujours le temps de la réflexion/confirmation ;
- Faites régulièrement des sauvegardes de vos données (ordinateurs, téléphone…) et gardez-en une copie déconnectée ;
- Appliquez les mises à jour de sécurité sur vos équipements connectés (serveurs, ordinateurs, téléphones…) dès qu'elles sont disponibles ;
- Utilisez des mots de passe uniques et solides et activez la double authentification chaque fois que possible.

Exemples de signes de compromissions de votre SI

Pour mieux détecter un risque de compromission de votre SI durant cette période de crise, voici *quelques signes à connaitre* :

- Des fenêtres contextuelles s'ouvrent dans votre système alors qu'il n'y en avait pas avant ;
- La page d'accueil de votre navigateur n'est plus la même ;
- Le système et des applications ne fonctionnent pas comme d'habitude (p. ex., une page, une application ou un système plante) ;
- Votre ordinateur est plus lent ;
- Des programmes inconnus sont en fonction dans votre système ;
- Le système de protection contre les programmes malveillants est désactivé ;
- Certains de vos mots de passe ont été changés ou vous recevez des demandes non sollicitées de changement ou de validation de mot de passe.

5 conseils pour *éviter de la propager la désinformation sur la Covid-19*

- Rester critiques sur les médias sociaux ;
- Ne pas laisser de fausses informations dans nos réseaux en ligne. On peut demander poliment à la personne qui l'a partagé de l'enlever ;
- Signaler toute fausse information aux administrateurs de la plate-forme ;
- En cas de doute, prendre le temps de vérifier l'information partagée ;
- Faire plus de « bruit » que les personnes qui partagent des informations erronées.

Pour aller plus loin, consultez :

- les bonnes pratiques de l'ANSSI pour la *navigation sur l'Internet* ;
- les conseils d'AVG pour *vérifier si un site Web est sûr* ;
- Le *guide d'hygiène de cybersécurité* de CGI pour la pandémie de COVID-19.

LA CRISE SANITAIRE, UNE OPPORTUNITE POUR LES GEANTS DU NUMERIQUE

La pandémie et le rôle incontournable que joue le numérique dans la crise constituent aussi une nouvelle opportunité pour les géants du numérique (GAFAM). Ces derniers, en effet, très sollicités dans le cadre de la crise mondiale, devraient largement *renforcer leur position* et *leur modèle économique* dans le secteur de la santé. A titre d'exemple, *la société américaine de traitement des données Palantir* a proposé ses solutions pour analyser les données de l'AP-HP. Notons cependant que *l'AP-HP a refusé la proposition de la société américaine*, notamment pour des raisons de protection des données de santé et de souveraineté.

VULNERABILITES ET NOUVELLES MENACES POUR LA SANTE

Les vulnérabilités du trimestre

Le *Portail d'Accompagnement Cybersécurité des Structures de Santé* mis en ligne par l'ANS signale de nombreuses nouvelles vulnérabilités, dont 2 pourraient affecter des dispositifs médicaux :

- Douze vulnérabilités, appelées « *SweynTooth* », peuvent permettre à un attaquant à portée de communication BLE (Bluetooth à basse consommation) de provoquer un déni de service et un contournement de la politique de sécurité ;
- Une *vulnérabilité* découverte dans *Insulet Omnipod*, un dispositif médical utilisé en tant que pompe à insuline, permet d'intercepter et de modifier les données échangées entre la pompe "patch" et son contrôleur électronique.

De nouvelles menaces détectées pour la santé

Selon un chercheur de l'entreprise de cybersécurité Fortinet, les *cybercriminels cherchent de nouvelles surfaces d'attaque* dans les dispositifs médicaux connectés. Deux exemples ont été donnés :

- L'exploitation de failles sur un outil de diagnostic d'imagerie permettant à un attaquant de modifier les résultats d'un scanner ;
- L'exploitation d'une faille sur les communications NFC d'un outil de mesure du glucose connecté avec un smartphone, permettant à l'attaquant de visualiser les données partagées.

Le chercheur a également souligné le risque d'exploitation des besoins des patients en matière d'outils d'assistance médicale pour vendre des produits frauduleux ou des applications malveillantes.

De son côté, Microsoft alerte sur une nouvelle stratégie adoptée par les cybercriminels en matière de ransomware, les « *human-operated ransomware attacks* » : l'attaquant ne se contente plus de diffuser le malware et d'attendre que la cible soit infectée, mais joue un rôle actif en verrouillant lui-même les données en fonction des opportunités qui se présentent, afin de maximiser ses chances. Face à cette nouvelle stratégie, *Microsoft recommande* de renforcer le pare-feu, de faire attention aux accès à distance au réseau et de réduire au maximum la surface d'attaque du SI.

Enfin, notons que la mise sur pied rapide de nouvelles capacités dans le cadre de la pandémie de COVID-19, comme la création de centres temporaires ou le déploiement de nouveaux dispositifs médicaux, constituent *de nouvelles surfaces d'attaque à prendre en compte* lors de leur connexion au système d'information d'un établissement de santé.

LA BLOCKCHAIN : QUELS APPORTS POUR LA SANTE ?

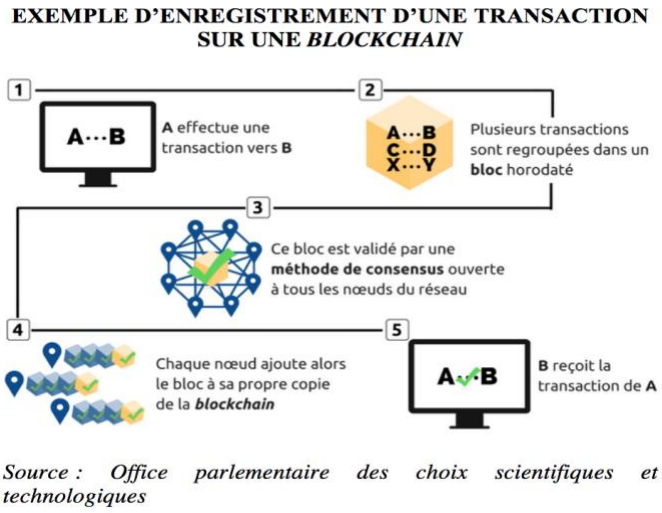
DEFINITION ET PRINCIPES DE LA BLOCKCHAIN

Développée à la fin des années 2000 pour les crypto-monnaies (monnaies virtuelles comme le Bitcoin par exemple), la Blockchain se définit selon la CNIL comme « *une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création, sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne*. »

Une Blockchain fonctionne grâce à une combinaison de technologies informatiques et cryptographiques qui permet d'assurer une confiance inaltérable dans la validité et l'intégrité des informations échangées et stockées, et qui garantit la résilience du système : réseau utilisant la technologie de pair à pair (P2P, « Peer-to-peer »), cryptographie asymétrique et fonctions de hachage.

Le principe de la Blockchain consiste à réunir dans un bloc horodaté des données validées, puis de lier (chainer) chaque nouveau bloc au bloc précédent en y intégrant la signature de ce dernier, de façon telle que chaque bloc n faisant référence au bloc n-1, la moindre modification d'une donnée enregistrée dans la chaine de blocs (Blockchain) modifierait l'ensemble de la chaine, rendant immédiatement visible toute tentative de fraude.

Exemple du processus de la Blockchain en 5 étapes



Source : http://www2.assemblee-nationale.fr/static/15/commissions/CFinances/blockchain-synthese.pdf

On distingue deux types de Blockchain :

- **Les Blockchains ouvertes (ou publiques)** : ces Blockchains étant librement accessibles depuis leurs interfaces Internet, toute personne peut à la fois consulter les informations stockées, introduire des données et participer à la validation des nouveaux blocs et des échanges sur le réseau. Il s'agit d'une complète décentralisation. Ce type

de Blockchain est celui qui présente le plus d'intérêt en matière d'innovation mais aussi le plus de difficultés techniques dans son fonctionnement ;

- **Les Blockchains privées (ou de consortium)** : ces Blockchains sont réglementées et administrées par une autorité, qui en autorise l'accès aux utilisateurs qu'il choisit et leur attribue des droits de lecture et d'écriture différenciés. Plus faciles à mettre en œuvre que les Blockchains ouvertes, les Blockchains privées sont celles dont les usages se sont le plus rapidement développés.

Comme le souligne le *rapport parlementaire sur la Blockchain et ses usages de décembre 2018*, les Blockchains présentent trois principaux atouts :

- Un gain de rapidité en matière de partage d'information (il ne faut que quelques minutes pour valider un bloc) ;
- Une sécurité plus efficace des échanges (la surveillance et le contrôle des échanges par l'ensemble des utilisateurs du réseau permettent de se prémunir contre d'éventuels actes malveillants) ;
- Un gain de productivité (la Blockchain réduit le nombre d'intermédiaires et d'opérations à réaliser pour partager des informations et permet ainsi une réduction des coûts).

La Blockchain intéresse la plupart des secteurs d'activité, et des applications se développent rapidement, notamment dans les banques, les assurances, la logistique et l'énergie.

Dans le domaine de la santé, l'usage de la Blockchain reste encore embryonnaire. Quelques applications concrètes ont déjà été réalisées, mais les projets foisonnent et semblent prometteurs. Reste cependant à en mesurer les limites et à en prouver l'efficience par rapport aux autres solutions numériques.

LES OPPORTUNITES DE LA BLOCKCHAIN POUR LA SANTE

Une Blockchain étant complexe à mettre en œuvre quel qu'en soit le type, son usage ne se justifie que si ses atouts permettent de mieux répondre que les autres systèmes aux différents défis qui se posent dans le secteur de la santé.

Les cas d'usage potentiels sont donc à rechercher dans toutes les situations où l'on peut tirer un réel avantage de l'incomparable capacité de la Blockchain à stocker et partager en temps quasi-réel des informations, y compris l'origine et le moment précis de leur insertion, avec la garantie de leur parfaite intégrité dans le temps.

Les études ont mis en évidence trois premiers domaines d'intérêt[1] : la gestion des données de santé, la recherche et le domaine pharmaceutique. Les cas d'usage peuvent concerner tant la médecine civile que le service de santé des armées.

Il convient de noter que si certains cas d'usage peuvent ne reposer que sur une Blockchain, d'autres combineront une Blockchain avec d'autres technologies comme l'intelligence artificielle ou les objets connectés pour proposer des solutions plus larges de partage et de traitement.

[1] Exemples d'études sur la Blockchain en santé :

- *Opportunités et enjeux de la technologie Blockchain dans le secteur de la santé*, Anca Petre et Nassima Haï ;
- *Blockchain et santé*, Blockchain Partner ;
- *Blockchain in the NHS*, Reformer Thoughts

La gestion des données de santé

La Blockchain permet de répondre aux défis actuels suivants :

- Résoudre le problème de l'éparpillement des données des patients (historique de soins, ordonnances, résultats d'examens, antécédents médicaux, comptes rendus d'hospitalisation, directives anticipées pour la fin de vie, etc.), encore très largement réparties entre le patient lui-même et tous les centres de soins où il s'est rendu.
- Résoudre les difficultés rencontrées pour transférer des données de patients détenues par un établissement à un autre qui en a un besoin urgent : délais de recherche par le premier établissement, délais de transmission, risque d'erreurs, problèmes fréquents d'interopérabilité entre les systèmes utilisés par les différents établissements.
- Garantir le respect des dispositions légales en matière de protection des données à caractère personnel, d'autant plus qu'il s'agit de données sensibles, par l'inscription dans une Blockchain de tous les accès à ces données, voire même de tous les traitements effectués. Ce cas d'usage permet en outre de connaitre en temps réel les éventuels vols ou fuites de données de santé. Comme indiqué ci-après, l'Estonie a mis en place un tel système.

Les deux premiers objectifs sont déjà ceux recherchés par le Dossier Médical Partagé (DMP), mais la Blockchain peut apporter des garanties supplémentaires : tout document stocké sera horodaté et infalsifiable, sans risque d'erreur ou de disparition ; celui qui l'a mis dans la Blockchain sera parfaitement identifié, donnant ainsi une meilleure garantie d'authenticité ; la réplication des blocs sur plusieurs nœuds garantit la disponibilité de l'ensemble des données stockées, mieux que les sauvegardes habituelles ; enfin, le partage des données entre le patient et l'ensemble des personnels de santé ayant besoin d'y accéder sera a priori plus rapide et facile, avec un coût en principe bien inférieur.

La recherche médicale

En matière de recherche, la Blockchain présente de nombreux atouts :

- Pour les essais cliniques, rassembler dans un système unique, de manière parfaitement fiable, intègre et datée, le consentement des patients, les protocoles et les résultats, et les partager en temps réel avec les chercheurs ayant à en connaitre.
- Offrir aux centres de recherche l'accès à une masse considérable de données de santé, après en avoir garanti l'anonymisation, ouvrant la voie à des analyses de Big Data pouvant être particulièrement utiles.
- De manière générale, mettre en place un modèle de recherche plus collaboratif.

Le domaine pharmaceutique

La Blockchain, grâce à sa transparence et son inaltérabilité, constitue un outil particulièrement adapté pour :

- garantir la traçabilité et l'authenticité des médicaments, des ordonnances médicales ou encore des brevets, permettant ainsi de mieux lutter contre les contrefaçons et les fraudes ;
- améliorer et fluidifier la logistique des médicaments, grâce à son registre distribué qui permettrait aux acteurs des diverses chaines de produits de connaître et de vérifier en temps réel chaque étape des approvisionnements, de la fabrication et de la distribution, réduisant ainsi considérablement les contraintes de procédure.

Ces cas d'usage devraient arriver rapidement à maturité, étant de même nature que des usages déjà existants ou proches de l'être, par exemple dans les domaines du cadastre, de la certification des diplômes universitaires, de la traçabilité des produits alimentaires et de la logistique industrielle.

LES APPLICATIONS DE LA BLOCKCHAIN DANS LA SANTE

Quelques applications sont déjà opérationnelles, et d'autres proches de l'être.

L'Estonie sécurise déjà ses données de santé par une Blockchain

L'Estonie, *l'un des pays les plus avancés en matière d'usages numériques*, est le premier pays qui utilise la Blockchain à l'échelle nationale dans le secteur de la santé. Lancée en 2016 par l'*Estonian eHealth Foundation*, *une application permet de protéger les dossiers de santé des 1,3 million de résidents* en utilisant la Blockchain comme couche de sécurité supplémentaire pour en garantir l'intégrité. Ce ne sont pas les dossiers médicaux qui sont stockés sur la Blockchain, mais les activités de traitement effectuées sur ces dossiers et les personnes autorisées à effectuer ces traitements, garantissant ainsi à la fois l'intégrité des données médicales et la légitimité de toute consultation ou modification.

Exemples d'applications de la Blockchain en santé par domaine

Domaine	Applications
Gestion des données	• *Iryo* est une plateforme de registre patient ouvert utilisant la Blockchain pour le partage sécurisé des données • *Patientory* ou *Guardtime* sont des solutions Blockchain développées pour sécuriser les données médicales et assurer l'intégrité des données patients dans leur parcours de soin • *Coral Health* permet aux patients de créer son registre patient et de contrôler le partage de ses informations avec les professionnels de santé dans le but de mieux personnaliser la médecine • *Medicalchain* est une solution de partage de données de santé entre patients et professionnels de santé qui combine notamment la Blockchain avec la télémédecine • *SimplyVital Health* est une solution qui utilise la Blockchain et les données patients au service notamment de l'administration des soins (durée des soins, coûts et remboursement par exemple)
Recherche	• *Nebula Genomics* utilise la Blockchain pour la protection des données génomiques afin de permettre leur bonne exploitation • *Doc.AI* est une plateforme basée sur la Blockchain et l'IA qui permet de croiser de manière sécurisée des données patients et de les analyser à des fins de recherche
Pharamaceutique	• *Chronicled* est une solution qui combine la Blockchain et les objets connectés pour optimiser la chaine de distribution pharmaceutique • *Blockpharma* est une solution dédiée à la traçabilité des médicaments, notamment pour lutter contre la contrefaçon et les fraudes
Milieu militaire	• *ManTech* propose une solution de Blockchain pour gérer les dossiers des patients du Département de la défense américain (DOD) et du Département des vétérans

L'Ouganda envisage d'utiliser la Blockchain pour lutter contre la contrefaçon de médicaments. *L'Afghanistan* a lancé fin 2019 un projet plus ambitieux encore, visant en plus à numériser les dossiers médicaux des patients et à créer des registres médicaux dans les hôpitaux.

LES LIMITES DE LA BLOCKCHAIN EN SANTE

La Blockchain présente un certain nombre de limites liées à la technologie elle-même ou à son application dans le domaine de la santé, ce qui explique le nombre encore réduit d'applications réellement opérationnelles.

Limites liées à la technologie

Il est possible d'identifier trois principales *limites liées au fonctionnement même de la Blockchain*, qui peuvent notamment impacter le SSA :

- Un coût et une consommation d'énergie et de bande passante non négligeables : la Blockchain fait travailler de nombreux ordinateurs en réseau et en temps réel, avec des flux pouvant être importants, ce qui nécessite de disposer d'un réseau et d'infrastructures adaptés tant au niveau matériel que logiciel. Ce type d'infrastructure peut d'ailleurs se révéler problématique en milieu opérationnel pour le SSA ;
- Une capacité de stockage limitée : les contraintes de la Blockchain ne permettent pas d'y stocker des données volumineuses, comme les dossiers d'une population importante ou les images médicales par exemple. Cette difficulté peut être contournée en ne stockant sur la Blockchain que les éléments de sécurité (la signature notamment) garantissant l'intégrité parfaite des documents, ces documents étant placés sur des serveurs classiques de grande capacité, comme dans la solution retenue par l'Estonie ;
- Une sécurité qui ne peut être absolue et éternelle : même si aucune attaque n'a a priori encore réussi sur les Blockchains existantes elles-mêmes, le système global peut présenter des vulnérabilités :
  - La sécurité des Blockchains repose exclusivement sur des éléments technologiques, comme les algorithmes cryptographiques, dont l'obsolescence ne peut être écartée à moyen ou long terme ;
  - Une attaque prononcée sur un élément périphérique d'une Blockchain monétaire a déjà permis d'y introduire des données illégitimes[2]. Ces données une fois introduites ne peuvent être effacées, ce qui peut être particulièrement dommageable dans les cas d'usage cités pour la santé ;
  - Dans une Blockchain ouverte, un utilisateur peut chercher à influencer le réseau à l'aide d'une fausse identité. Dans les applications de santé, l'immense majorité des Blockchains utilisées seront a priori privées, et donc non concernées par ce risque ;
  - Une attaque du type « Man-in-the-middle » peut permettre l'interception des communications entre les utilisateurs du réseau, comme cela est déjà le cas au sein de tout réseau. Le risque est limité dans le cas des Blockchains de santé, la sensibilité des données de santé rendant obligatoire leur chiffrement lors de leur transmission, voire dans certains cas de leur stockage dans la Blockchain.

Limites liées au domaine de la santé

L'utilisation de la Blockchain dans le domaine de la santé nécessite notamment d'appréhender les quatre problématiques suivantes :

- *L'implémentation de la Blockchain dans les organisations de santé* : les parties prenantes doivent être en mesure de pleinement coopérer, ce qui implique pour les organisations de santé de « *réaliser un travail amont important de numérisation des données, d'automatisation des processus, d'éducation du personnel et d'encadrement réglementaire* » ;
- *La conformité aux règles de protection des données personnelles* : le caractère inaltérable de la Blockchain soulève des difficultés particulières pour les données de santé dans l'application du droit à l'effacement, du droit de rectification et du droit d'opposition garantis par le RGPD et la loi informatique et libertés.

2 *https://www.usine-digitale.fr/article/dao-perd-50-millions-de-dollars-lors-d-un-piratage.N397787*

L'opportunité de la mise en œuvre d'une Blockchain et son fonctionnement doivent faire l'objet d'études approfondies dans le cadre d'un projet de santé ;

- *L'accès au registre d'un patient incapable de fournir sa clé* : l'accès au registre d'un patient qui n'est pas en état d'utiliser sa clé privée, pour des raisons médicales par exemple, constitue un défi pour la Blockchain de santé. Des méthodes alternatives doivent être prévues pour permettre aux soignants d'accéder aux données en cas d'urgence (système « bris de glace » mis en place sur le DMP ou accord d'une ou plusieurs personnes de confiance par exemple) ;
- *La monétisation des données de santé* : le contrôle que la Blockchain donne aux patients sur leurs données de santé pourrait leur permettre de les vendre au plus offrant et d'entrainer un phénomène de monétisation des données de santé.

CONCLUSION

La Blockchain présente des opportunités certaines pour le secteur de la santé et plus spécifiquement pour des organisations militaires de santé comme le SSA. Néanmoins, les caractéristiques de cette technologie invitent à bien identifier en amont ses apports et ses limites. A ce titre, les exigences du secteur de la santé et du milieu militaire incitent à adopter des Blockchains privées pour le SSA. Enfin, il convient d'appréhender la Blockchain comme un outil au service de la transformation numérique qui doit pouvoir s'articuler avec d'autres technologies comme l'IA ou les objets connectés, plutôt qu'une solution généraliste aux problèmes de sécurité des données de santé et d'interopérabilité des systèmes d'information.

BIBLIOGRAPHIE

- **Sensibilisation**

https://www.defense.gouv.fr/actualites/articles/sortie-du-nouveau-guide-du-bon-usage-des-reseaux-sociaux

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

https://www.defense.gouv.fr/content/download/579821/9899697/20200327_COVID-19_SIRPA-M_SITREP%20n°3.pdf

https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

https://numerique.gouv.fr/

https://numerique.gouv.fr/produits-services/tchap-messagerie-instantanee-etat/

https://www.tchap.gouv.fr

https://www.tchap.gouv.fr/tchap-prise-en-main.pdf

http://www.tchap.fr/

https://www.tchap.gouv.fr/tchap-prise-en-main.pdf

https://www.tchap.gouv.fr/faq/

https://www.tchap.gouv.fr/tchap-prise-en-main.pdf

https://www.tchap.gouv.fr/faq/

https://www.tchap.gouv.fr/cgu/

- **Actualité**

https://www.caducee.net/actualite-medicale/14250/cyberimposture-hopitaux-professionnels-de-sante-et-patients-en-ligne-de-mire.html

https://www.techopital.com/l-agence-du-numerique-en-sante-(ans)-alerte-sur-des-cyberattaques-liees-au-coronavirus-NS_4843.html

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1764-europe-analyse-dune-campagne-de-lapt-gamaredon-utilisant-le-covid-19-2020-04

https://www.courrierinternational.com/article/la-lettre-de-leduc-special-confinement-coronavirus-une-epidemie-dinfox

https://www.usine-digitale.fr/article/comment-les-hackers-surfent-sur-le-coronavirus-pour-multiplier-les-actes-malveillants.N940051

https://www.capital.fr/entreprises-marches/thales-alerte-sur-la-multiplication-des-cyberattaques-des-etats-1366176

https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/

https://www.usine-digitale.fr/article/en-pleine-pandemie-de-covid-19-l-ap-hp-est-victime-d-une-attaque-par-deni-de-service.N944741

https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

https://www.lemondeinformatique.fr/actualites/lire-le-ministere-us-de-la-sante-et-des-services-sociaux-essuie-une-attaque-ddos-78474.html

https://healthitsecurity.com/news/ransomware-shuts-down-colorado-hospital-it-network-amid-covid-19

https://www.begeek.fr/piratage-le-site-de-loms-attaque-a-de-multiples-reprises-339236

https://www.informatiquenews.fr/les-cyberattaques-sur-les-etablissements-de-sante-se-multiplient-de-facon-exponentielle-69504

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1772-lanssi-realise-une-analyse-dindicateurs-techniques-lies-des-attaques-ayant

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1755-le-cert-fr-propose-aux-structures-de-sante-de-mettre-en-detection-des-lots

https://www.anap.fr/annexes/covid-19-dispositif-exceptionnel-dentraide/

https://www.cyberveille-sante.gouv.fr/index.php/cyberveille-sante/1712-orange-cyberdefense-met-gratuitement-disposition-ses-equipes-pour-les

https://cti-league.com/services/

https://siecledigital.fr/2020/03/27/covid-19-cti-league-des-experts-en-cybersecurite-luttent-contre-les-attaques-pendant-la-pandemie/

https://www.cyberthreatcoalition.org/

https://cyberv19.org.uk/

https://www.gerda2014.com/sante/coronavirus-le-nombre-de-teleconsultation-explose-en-france/

https://www.latribune.fr/technos-medias/internet/coronavirus-explosion-des-teleconsultations-en-france-doctolib-grand-gagnant-844660.html

https://www.paris.fr/pages/covidom-une-appli-pour-le-suivi-des-patients-porteurs-ou-suspectes-du-covid-19-7705

https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment

https://esante.gouv.fr/actualites/solutions-teleconsultation

https://www.lefigaro.fr/a-paris-une-batterie-d-imprimantes-3d-pour-endiguer-le-coronavirus-20200403

https://www.usine-digitale.fr/article/covid-19-l-ap-hp-se-dote-de-60-imprimantes-3d-pour-pallier-la-penurie-de-materiel-medical.N950626

https://www.lefigaro.fr/secteur/high-tech/coronavirus-l-impression-3d-a-la-rescousse-face-a-la-penurie-de-materiel-medical-20200327

https://www.zdnet.fr/actualites/covid-19-la-riposte-de-l-impression-3d-s-organise-39902381.htm

https://www.zdnet.fr/actualites/covid-19-la-riposte-de-l-impression-3d-s-organise-39902381.htm

https://covid3d.org/projects

https://www.3dchampions.org/

https://www.bfmtv.com/tech/covid-19-la-geolocalisation-des-smartphones-une-arme-controversee-pour-endiguer-l-epidemie-1877013.html

https://www.bastamag.net/Application-stopcovid-tracking-tracage-surveillance-libertes-vie-privee-geolocalisation

https://www.journaldugeek.com/2020/04/10/stopcovid-contact-tracing-cnil/

https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid

https://www.nouvelobs.com/coronavirus-de-wuhan/20200326.OBS26600/coronapp-une-application-francaise-pour-geolocaliser-les-porteurs-du-virus-covid-19.html

https://cryptoast.fr/france-solution-blockchain-depister-covid-19-anonyme/

https://www.linformaticien.com/actualites/id/54207/covid-19-block-covid-ou-la-blockchain-pour-aider-aux-depistages.aspx

https://www.zdnet.fr/actualites/comment-l-intelligence-artificielle-s-attaque-au-covid-19-39902039.htm

https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-ia-formee-predire-complications-liees-covid-19-80324/

https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/l-ia-de-deepmind-tente-aussi-de-contrecarrer-covid-19_142602

https://www.usine-digitale.fr/article/covid-19-un-consortium-mise-sur-l-intelligence-artificielle-pour-sortir-plus-vite-du-confinement.N951111

https://www.frenchweb.fr/e-sante-lefficacite-de-lintelligence-artificielle-mise-a-rude-epreuve-par-le-coronavirus/394689

https://www.renfort-covid.fr/

https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite

https://www.cgi.com/sites/default/files/2020-04/fr-basic_cybersecurity_hygiene_guide_final.pdf

https://theconversation.com/linfodemie-sur-la-covid-19-est-un-fleau-cinq-conseils-pour-eviter-de-la-propager-136127

https://www.ssi.gouv.fr/particulier/precautions-elementaires/bonnes-pratiques-de-navigation-sur-linternet/

https://www.avg.com/fr/signal/website-safety

https://www.cgi.com/sites/default/files/2020-04/fr-basic_cybersecurity_hygiene_guide_final.pdf

http://www.slate.fr/story/189579/tribune-crise-sanitaire-covid-19-emprise-gafam-etats-services-publics

https://theconversation.com/mobilisation-des-gafa-contre-la-pandemie-covid-19-business-as-usual-132064

https://www.zdnet.fr/actualites/palantir-pourrait-aider-l-ap-hp-a-gerer-l-epidemie-de-covid-19-39901771.htm

https://www.bfmtv.com/tech/donnees-de-sante-l-ap-hp-ecarte-la-proposition-de-palantir-1894772.html

https://www.cyberveille-sante.gouv.fr/

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1672

https://www.cyberveille-sante.gouv.fr/index.php/cyberveille-sante/1701-vulnerabilite-dans-insulet-omnipod-2020-03-23

https://www.myomnipod.com/fr-fr/home

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1664-etats-unis-analyse-des-nouvelles-surfaces-dattaques-dans-le-domaine-de-la

https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

https://www.usine-digitale.fr/article/covid-19-microsoft-previent-des-hopitaux-que-leurs-infrastructures-les-exposent-a-des-ransomwares.N949496

https://www.healthcareitnews.com/news/temporary-hospitals-are-rife-cybersecurity-vulnerabilities

- **Dossier**

https://www.cnil.fr/fr/definition/blockchain

http://www2.assemblee-nationale.fr/static/15/commissions/CFinances/blockchain-synthese.pdf

http://www.ipubli.inserm.fr/bitstream/handle/10608/9876/MS_2018_10_852.html

https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf

https://reform.uk/sites/default/files/2018-12/Blockchain in the NHS - VF_1.pdf

https://e-estonia.com/solutions/healthcare/

https://nortal.com/blog/blockchain-healthcare-estonia/

https://iryo.network/#features

https://patientory.com/

https://guardtime.com/health

https://mycoralhealth.com/product/

https://medicalchain.com/en/

https://www.forbes.com/sites/jessedamiani/2017/11/06/simplyvital-health-blockchain-revolutionize-healthcare/#1d9fbb28880a

https://nebula.org/technology/

https://doc.ai/

https://www.chronicled.com/

https://www.blockpharma.com/

https://www.mantech.com/blockchain-applications-dod-and-va-healthcare

https://www.coindesk.com/ugandan-president-backs-bid-to-tackle-fake-meds-with-blockchain

https://www.iracm.com/2019/12/afghanistan-introduction-de-la-technologie-blockchain-pour-securiser-la-chaine-du-medicament/

https://www.sia-lab.fr/sites/sia/files/images/note_strat_-_blockchain_defense_-_bat.pdf

http://www.ipubli.inserm.fr/bitstream/handle/10608/9876/MS_2018_10_852.html

https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

https://www.usine-digitale.fr/article/dao-perd-50-millions-de-dollars-lors-d-un-piratage.N397787

https://blockchainpartner.fr/wp-content/uploads/2017/06/Sant%C3%A9-Industrie-Pharmaceutique-Blockchain.pdf

https://www.zdnet.fr/actualites/blockchain-et-si-les-patients-controlaient-et-monetisaient-leurs-donnees-de-sante-39880849.htm

Cette Lettre trimestrielle est réalisée pour la DCSSA par CEIS

ceis