N° 678

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Enregistré à la Présidence du Sénat le 10 juin 2021

RAPPORT D'INFORMATION

FAIT

au nom de la délégation aux entreprises (1) relatif à la **cybersécurité** *des* **entreprises**,

Par MM. Sébastien MEURANT et Rémi CARDON,

Sénateurs

(1) Cette délégation est composée de : M. Serge Babary, *président* ; M Stéphane Artano, Mmes Martine Berthet, Florence Blatrix Contat, MM. Gilbert Bouchet, Emmanuel Capus, Mme Anne Chain Larché, MM. Gilbert-Luc Devinaz, Thomas Dossus, Fabien Gay, Jacques Le Nay, Dominique Théophile, *vice-présidents* ; MM. Rémi Cardon, Jean Hingray, Sébastien Meurant, Vincent Segouin, *secrétaires* ; Mmes Cathy Apourceau-Poly, Annick Billon, Nicole Bonnefoy, MM. Michel Canévet, Daniel Chasseing, Alain Chatillon, Mme Marie-Christine Chauvin, M. Pierre Cuypers, Mme Jacky Deromedi, M. Alain Duffourg, Mme Pascale Gruny, MM. Christian Klinger, Daniel Laurent, Martin Lévrier, Didier Mandelli, Jean-Pierre Moga, Albéric de Montgolfier, Claude Nougein, Mme Guylène Pantel, MM. Georges Patient, Sebastien Pla, Mmes Émilienne Poumirol, Frédérique Puissat, MM. Christian Redon-Sarrazy, Olivier Rietmann, Daniel Salmon.

SOMMAIRE

Pages

L'ESSENTIEL

1. UN ENJEU DÉCISIF DE SURVIE DES ENTREPRISES

La cybercriminalité visant les entreprises se banalise pour quatre motifs :

1. **La numérisation de l'économie, accélérée avec le confinement lié au développement du télétravail et au déploiement de la fibre ;**
2. **La professionnalisation de la cybercriminalité,** facilitée par sa **« plateformisation », son industrialisation, et le développement des cryptomonnaies ;**
3. **La difficulté de la prévention et de la répression**, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
4. **L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique** dont les entreprises sont soit les cibles soit les victimes collatérales.

Or, l'économie numérique, et tout particulièrement le e-commerce, ne peuvent se développer qu'en se fondant sur **la confiance des partenaires de l'entreprise et des consommateurs.**

Les entreprises, quelle que soit leur taille, sont **incitées à numériser** leurs processus de production, à développer le e-commerce, à placer leurs salariés en télétravail. Les entreprises les plus petites pensent être **à l'abri** des cyberattaques. C'est **une illusion, parfois mortelle** : une entreprise peut fermer après une cyberattaque. Les coûts indirects se révèlent parfois avec un fort délai de latence.

Chaque utilisateur d'un outil numérique ou même d'un objet connecté **peut-être potentiellement le maillon faible du filet de cybersécurité tendu dans la Toile. L'explosion des usages numériques s'est accompagnée d'une hausse exponentielle des actes de piratage.** Quelques chiffres suffisent à illustrer ce phénomène :

6 000	*milliards de dollars par an à partir de 2021, contre 3 000 milliards en 2015 , tous secteurs confondus, tel est le coût de la cybercriminalité au niveau mondial*
3ème	*économie mondiale si le cyberrisque était un pays*
43 %	*des PME ont constaté un incident de cybersécurité en 2020*

16 %	*des cyberattaques menacent la survie d'une entreprise en 2020*
+ 155 %	*de fréquentation du site cybermalveillance.gouv.fr en 2020*
X 4	*des attaques au rancongiciel entre 2020 et 2021 selon l'ANSSI*

Le président de la Réserve fédérale des États-Unis, Jerome Powell, considère que les cyberattaques contre les entreprises constituent le **risque actuel le plus important pour l'économie américaine, plus redoutable encore qu'une crise financière similaire à celle de 2008.** Face à cette internationalisation du cybercrime, le Président de la République française a présenté le 12 novembre 2020, au Forum sur la gouvernance d'Internet, un « *appel de Paris* » **pour la sécurité du cyberespace.**

2. UNE PRISE DE CONSCIENCE TARDIVE ET INSUFFISANTE DE L'AMPLEUR DES CYBERMENACES

La cybersécurité était, en 2018, loin d'être considérée comme « *l'affaire de tous* », comme le déplorait CCI France. De trop nombreuses entreprises, notamment les PME et TPE, ne se sentaient pas concernées. Le sujet semblait technique, externalisable, solutionnable par le simple achat d'un pare-feu !

Cependant, un basculement s'est opéré au printemps 2020. La surface d'exposition aux cyberattaques a été nettement augmentée avec plus de 8 millions de salariés en télétravail. Dans un premier temps, de nombreuses entreprises ont même encouragé leurs salariés à utiliser leur propre équipement informatique. Cette situation a créé des brèches de sécurité, l'urgence étant la continuité de l'activité davantage que la sécurité numérique. Les cybercriminels en ont profité, avec une **augmentation de 667 % des attaques par *phishing* enregistrées entre le 1er et le 23 mars 2020**.

Les dirigeants d'entreprise intègrent désormais ce risque de façon croissante, bien qu'inégale.

Face à la montée des failles de sécurité, leurs services informatiques tentent désormais d'imposer le **concept Zero Trust**, modèle de sécurité qui repose sur le principe qu'aucun utilisateur n'est totalement digne de confiance sur un réseau.

Cette nécessité est prise en compte par les grandes entreprises, d'autant que **les agences de notation intègrent le risque cyber dans leur notation financière** et qu'un marché de la notation cyber s'est développé. En outre, **la notation ESG** (environnement, société, gouvernance) comporte également une référence à **la cybersécurité.** Elle constitue une **dimension essentielle de la gouvernance de l'entreprise** mais également de **la**

responsabilité sociétale des entreprises sous l'angle de la protection contre le vol des données. La Plateforme RSE préconise même de créer une « responsabilité numérique des entreprises » (RNE).

Le niveau de cybersécurité des entreprises doit être **rapidement et fortement augmenté avant l'explosion de l'internet des objets** (IoT), qui va étendre de façon exponentielle la surface d'exposition au cyberrisque, **de l'ordinateur quantique** qui démultipliera les capacités d'intrusion, ou encore de **l'Intelligence Artificielle**.

3. UN DISPOSITIF DE CYBERPROTECTION PUBLIQUE PRIVILÉGIANT LES ENTREPRISES D'IMPORTANCE VITALE

Les entreprises qualifiées d'**opérateurs d'importance vitale (OIV)** sont protégées de manière satisfaisante à l'échelle européenne et nationale, par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En revanche, les TPE et PME, comme celles des ETI qui ne sont **pas** identifiées comme **d'importance vitale, ne sont pas assez bien cyberprotégées** par ce dispositif public.

La cybersécurité publique se caractérise par un **équilibre entre centralité de la compétence technique et proximité** des victimes potentielles avec la possibilité de déposer plainte dans les gendarmeries et commissariats**.**

Elle assure une **répartition originale des compétences non en fonction de la localisation de l'infraction (critère territorial) mais en fonction de la famille de rançongiciel à traiter (critère fonctionnel).** La taille de l'entreprise est neutre dans le traitement judiciaire de la cyberattaque.

Ce dispositif public comprend **une capacité de projection de forces d'intervention sur le terrain à même de rassurer un dirigeant d'entreprise,** lequel, le plus souvent, ignore les compétences numériques de la Police nationale ou de la Gendarmerie.

La cybersécurité des entreprises **repose sur le bon fonctionnement d'une quadruple coopération** afin de partager l'information à des fins de prévention, de remédiation et de sanction :

- entre les autorités judiciaires et les forces de cybersécurité,
- entre la police et la gendarmerie, qui se sont chacun dotés d'outils distincts,
- entre le secteur public et les acteurs privés,
- entre la France et ses partenaires européens, et même internationaux.

Toutefois, **la justice reste démunie alors que le cybercrime s'est industrialisé**.

4. UNE CYBERSÉCURITÉ DIFFICILEMENT ACCESSIBLE AUX PME

Des grandes entreprises mieux protégées, des PME plus vulnérables

Les cybercriminels font des études de marché sur leurs cibles. Lorsque celles-ci ont atteint un niveau supérieur de protection, ils réorientent des attaques sophistiquées via leurs fournisseurs ou sous-traitants plus fragiles en termes de cybersécurité. Face à la multiplication des cyberattaques, **les grandes entreprises et les ETI ont pris des mesures de défense compliquant la tâche des cybercriminels**. En particulier, les stratégies de sauvegarde et de reconstruction efficace des systèmes informatiques rendent le blocage des systèmes moins pertinent comme contrepartie à une demande de rançon. **Une meilleure cyberdéfense des grandes entreprises a eu comme contrepartie de détourner la cybercriminalité vers les plus petites entreprises plus vulnérables.** Cette translation du risque vers des fournisseurs, sous-traitants ou clients, continue cependant à affaiblir, par rétroaction, la cybersécurité des grandes entreprises. En effet, l'accès à distance au système d'information de l'entreprise augmente sa surface d'attaque en ouvrant de nouvelles portes.

« L'effet domino » peut être dévastateur. La cybersécurité est donc l'affaire de tous et de toute la chaine de valeur.

Le salarié est souvent le maillon faible de la cybersécurité, voire un « cheval de Troie ».

La cybersécurité est encore trop perçue comme **une contrainte supplémentaire** par les salariés eux-mêmes. L**e fonctionnement en silos** du management d'un certain nombre d'entreprises ne favorise pas toujours ce travail d'équipe. Une collaboration minimaliste ne permet pas de diffuser de façon efficace une culture partagée. Celle-ci doit impliquer tous les échelons de la hiérarchie de l'entreprise, en intégrant les dirigeants et l'ensemble du management, leur rôle d'impulsion étant majeur.

La lutte contre les cybervirus suppose une **hygiène numérique constante** et des « **gestes barrières »** permanents de la part de chacun. L'augmentation du budget alloué aux outils n'est pas une réponse suffisante face à la multiplication des menaces de plus en plus sophistiquées. **Chaque salarié dispose de la clé de la cybersécurité de son entreprise.**

La pénurie d'expertise humaine en matière de cybersécurité est mondiale. Dès lors, **ce handicap est particulièrement aggravé pour les TPE-PME** pour lesquelles la ressource humaine devient pratiquement inaccessible. Au déficit de compétences en cybersécurité s'ajoute le fait que les entreprises **ne mesurent pas à sa juste valeur l'intérêt de sécuriser l'information.**

Un recours croissant au cloud dans une relation commerciale déséquilibrée

Pour **accéder au cloud**, les PME sont dans une situation inconfortable. Elles n'en maîtrisent pas techniquement les enjeux et souffrent **d'une relation commerciale déséquilibrée**. Certains fournisseurs déclinent même toute responsabilité en matière de disponibilité ou de fonctionnalité du service.

Malgré le principe de libre circulation des données, traduite par le règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018, et les lignes directrices du 29 mai 2019, **le processus d'autorégulation du marché du cloud s'est interrompu** en novembre 2019, faute d'accord sur la rédaction de codes de conduite.

Il existe une **asymétrie systémique entre grands fournisseurs mondiaux de services cloud et leurs utilisateurs.** Pour une PME, accéder au cloud s'apparente parfois à conclure un contrat d'adhésion pouvant contenir des clauses parfois abusives.

V. LE SURSAUT OU LE CHAOS : L'URGENTE CONSOLIDATION DE L'ÉCOSYSTÈME FRANÇAIS DE LA CYBERSÉCURITÉ

Un objectif ambitieux de leadership en matière de cybersécurité

Si la cybersécurité est une menace pour les entreprises, elle constitue également une **opportunité de développer un marché porteur.** Elle représente en France **13 milliards d'euros de chiffre d'affaires.** Ce secteur est en forte croissance. Il dégage 6,1 milliards d'euros de valeur ajoutée et emploie 67 000 personnes. Le marché mondial de la cybersécurité devrait représenter **150 milliards de dollars en 2023.**

L'offre française de cybersécurité demeure **très fragmentée** avec une **forte exposition à la concurrence** mondiale. Notre pays comporte toutefois des leaders mondiaux. Il dispose **d'atouts** de premier plan pour pérenniser son **avance technologique et économique**, notamment dans trois domaines : l'**Intelligence Artificielle** et l'apprentissage automatique (le ***machine learning***), la **cryptographie** et la **technologie post-quantique.**

Associée jusqu'ici à l'idée de contraintes et de dépenses, la cybersécurité doit être considérée aujourd'hui comme un atout compétitif et un investissement productif. Un comportement cybersécurisé devient un critère de sélection pour les clients soucieux à l'idée de confier des données personnelles, voire sensibles, à une entreprise.

La **stratégie de l'État** vise à encourager le développement d'un **écosystème** de la cybersécurité.

La cybersécurité et la sécurité de l'Internet des Objets (IoT) est l'une des cinq priorités du contrat stratégique de la filière « industries de sécurité » du 29 janvier 2020, avec la sécurité des grands évènements et des Jeux Olympiques de Paris 2024, l'identité numérique, les territoires de

confiance et le numérique de confiance. Il s'agit de « *positionner l'industrie française comme* ***leader mondial*** *de la cybersécurité et de la sécurité de l'IoT* ». **L'objectif est ambitieux.**

Le développement de l'excellence de la filière française de cybersécurité devrait davantage se traduire par une politique publique d'achat de solutions de cybersécurité françaises. Ce n'est hélas pas le cas. L'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France. Il manque une culture d'achat de produits français de cybersécurité.

Afin de **fédérer la communauté** de la cybersécurité, un **cybercampus** doit s'installer à l'automne 2021 à la Défense. Ce « *lieu totem de la cybersécurité* » doit rassembler les principaux acteurs nationaux, publics et privés, et les inciter à développer des **synergies**. Il est indispensable qu'il incarne le sursaut de la France face au volume exponentiel des cyberattaques qui menacent toutes les organisations, tant privées que publiques. **À défaut de sursaut, nous risquons le chaos à brève échéance !**

Une impossible reconquête de la souveraineté numérique dans le cloud

Le marché du cloud devrait exploser en passant de 63 milliards d'euros en 2021 à 560 milliards en 2030. La maîtrise des données des entreprises est un enjeu de souveraineté. Il est difficile à la France de **recouvrer sa souveraineté dans le cloud**, dominé actuellement par **trois acteurs américains qui possèdent 70 % de parts de marché.** Il s'agit pourtant du **socle incontournable du développement des entreprises, y compris des PME,** comme celles des entités publiques, soumises aux mêmes menaces.

La volonté de retrouver la souveraineté des données est régulièrement évoquée en France depuis 2010. Après **l'échec d'Andromède**, l'État français rejoint en mai 2020 l'initiative allemande **Gaia-X** et abandonne l'idée de créer *ex-nihilo* une nouvelle entreprise soutenue par la puissance publique et de grandes entreprises. L'objectif est désormais de former une infrastructure européenne articulée autour d'un organisme de gouvernance et de coordination chargé d'émettre des standards de sécurité, d'interopérabilité et de portabilité des données.

La stratégie nationale pour le cloud de mai 2021 acte l'avance non rattrapable du **secteur privé américain**. Il s'agit désormais de **maîtriser notre dépendance dans la durée**. Le pari gouvernemental invoque le précédent du nucléaire, notre autonomie s'étant développée sous licence de technologies américaines.

VI. METTRE LA CYBERSÉCURITÉ À LA PORTÉE DE TOUTES LES ENTREPRISES

L'adage « *mieux vaut prévenir que guérir* » s'applique tout particulièrement à la cybersécurité. La réalité oblige à traiter ces deux volets. S'y ajoute la nécessaire sanction des cybercriminels.

Le rapport propose trois axes de propositions pour développer le cercle vertueux de la cyberprotection : tester, alerter, protéger.

AXE 1 : TESTER ET RENFORCER LA RÉSISTANCE ET LA CYBERRÉSILIENCE DES ENTREPRISES

Le dispositif ***cybermalveillance.gouv.fr*** doit être mieux promu auprès des entreprises et un service d'urgence doit être dédié aux entreprises, en mobilisant des **jeunes** en service civique et disposant des compétences numériques adéquates **(proposition n°1)**.

Un **recueil anonymisé des plaintes** doit être ouvert afin d'encourager les entreprises à signaler les cyberattaques sans porter atteinte à leur réputation, tout en décourageant la publicité autour des logiciels malveillants, afin de disposer de statistiques fiables **(proposition n°2).**

Des équipes de réponse aux incidents informatiques (CSIRT : *Computer Security Incident Response Team*) doivent être déployées **dans les Régions,** afin de faciliter l'accès des PME à la cyberprotection tout en **sensibilisant les collectivités locales**. Ces dernières sont, avec les hôpitaux publics, les **nouvelles cibles de la cybercriminalité (proposition n°3).**

Pour renforcer la résistance du tissu entrepreneurial, l'État doit :

- élaborer **des plans nationaux de prévention des cyberrisques** ;

- **coordonner les réponses** des pouvoirs publics et des acteurs privés **en cas d'attaque numérique systémique,** affectant une part significative des entreprises quelle que soit leur taille,

- et organiser régulièrement des **exercices de simulation** (proposition n°5).

AXE 2 : ALERTER, CONSEILLER, FORMER SUR LE PÉRIL CYBER

Salariés et dirigeants d'entreprise doivent être davantage sensibilisés à la cybersécurité, à l'hygiène numérique et ses gestes barrières :

- Les salariés, en se voyant proposer une **sensibilisation à la cybersécurité par la voie de la formation professionnelle** (**proposition n°9**).
- Les **dirigeants**, dont la responsabilité personnelle peut être engagée en cas de cyberattaque de la chaîne de valeur dont ils sont partie prenante, en étant mieux sensibilisés du risque de devenir à la fois être victime et responsable. Le sujet doit être traité lors de la définition de la stratégie de l'entreprise (**proposition n°15**).

La certification par un **référentiel de cybersécurité** accessible aux PME et TPE doit être encouragée (**proposition n°14**).

Afin de souligner la nécessité de renforcer la **conception sécurisée** (*security by design)*, la « garantie logicielle », concernant les mises à jour de sécurité, doit être étendue aux entreprises ; et un **hackathon de la cybersécurité des entreprises** pourrait être organisé avec le support de l'ANSSI, ciblant notamment les logiciels mis sur le marché, chaque 30 novembre, Journée mondiale de la cybersécurité (**proposition n°13**).

Afin de sensibiliser le grand public à la cybersécurité, un **cyberscore des plateformes numériques** doit être instauré, comme le Sénat l'a récemment proposé (**proposition n°22**), et une **campagne massive de promotion des métiers** de la cybersécurité doit être déployée (**proposition n°10**).

AXE 3 : PROTÉGER LES ETI, PME ET TPE PAR DES OUTILS ADAPTÉS

- ***Le dispositif public de cyberprotection doit être renforcé en moyens humains et financiers.***

La création d'un **cybercampus** fédérant les acteurs publics et privés de la cybersécurité constituera un atout dans la lutte contre la cybercriminalité.

Pour renforcer la réponse pénale à la cybercriminalité, il faut développer la formation initiale et continue des magistrats en matière de cybercriminalité ; augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ; doter les forces de cybersécurité de moyens financiers

adéquats ; étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ; et créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité (**proposition n°6**).

Pour répondre à l'industrialisation de la cybercriminalité, **les procédures pénales doivent être adaptées pour accélérer la réponse judiciaire et renforcer la coopération** avec l'ANSSI au-delà de la lutte contre le terrorisme (**proposition n°7**).

La présidence française de l'Union européenne au premier semestre 2022 doit être mise à profit pour accélérer les négociations sur les **amendements à la convention de Budapest de 2001 du Conseil de l'Europe** sur la cybercriminalité et sur le **projet de règlement européen sur les preuves électroniques** (« *e-evidence* »), **et reprendre les négociations entre l'Union européenne et les États-Unis,** afin de renforcer la coopération internationale contre la cybercriminalité **(proposition n°8)**.

Pour aider à la consolidation de l'écosystème français de la cyberprotection, **le droit de la commande publique doit évoluer :**

- en pérennisant les dispositions du décret du 24 décembre 2018 permettant aux collectivités locales de passer un marché sans mise en concurrence pour des « services innovants » ;
- en permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;
- et en étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité (**proposition n°4**).

- ***Pour renforcer la cybersécurité des entreprises, le rôle des assurances est décisif.***

Dans un premier temps, **l'assurabilité tant des rançongiciels que des sanctions administratives en cas de violation de la réglementation sur la protection des données à caractère personnel, doit être interdite,** à la fois au niveau européen et national (**proposition n°12**).

Dans un deuxième temps, **le marché de l'assurance doit être conforté :**

- par une **meilleure compréhension du risque,** en ayant la connaissance la plus exhaustive possible des sinistres ;
- par **l'utilisation de logiciels et d'experts en cybersécurité certifiés,** afin de promouvoir le **label *Expert Cyber*** ;
- par la **création d'une agence de cybernotation européenne, utilisant les référentiels** de l'Agence européenne chargée de la sécurité des réseaux et

de l'information (ENISA)**, ou française,** utilisant ceux de l'ANSSI **(proposition n°16)**

Dans un troisième temps, **l'éligibilité au remboursement d'un dommage lié à une cyberattaque par les assurances devra être subordonnée au recours à un prestataire labellisé *Expert Cyber* (proposition n°11).**

- ***Des solutions simples et mutualisées à destination des PME et TPE***

Pour **remédier** à la **pénurie** de ressources humaines en expertise, il faut **faciliter la mutualisation de responsables de sécurité des systèmes informatiques (RSSI) pour les PME,** par exemple par la constitution **de groupements d'employeurs** ayant un statut de tiers de confiance **(proposition n°17).**

Pour **simplifier** la vie des entreprises, il faut développer l'offre d'un **« *package* » de solutions de cybersécurité pour les TPE et PME (proposition n°18)** et notamment: étudier la faisabilité d'une **solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI. Par ailleurs, une approche commune franco-allemande pourrait plaider en faveur d'une meilleure prise en considération des PME** dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA **(proposition n°20).**

Pour **financer** cette mise à niveau en cyberprotection, il faut, comme le Sénat l'a préconisé à de multiples occasions, mettre en place **un crédit d'impôt à destination des TPE et PME. Celui-ci couvrirait une partie des dépenses d'équipement** (logiciels ou abonnement cloud) et de **formation des chefs d'entreprise et des salariés à la cybersécurité (proposition n°21).**

Pour **rétablir l'égalité** des relations contractuelles dans le cloud, il faut **accorder aux TPE et PME dont le champ de l'activité principale n'est pas le numérique, la protection de l'article L.212-1 du Code de la consommation sur les clauses abusives (proposition n°19).**

22 PROPOSITIONS POUR RENFORCER LA CYBERSÉCURITÉ DES ETI, PME ET TPE

Proposition n°1 : Promouvoir davantage le dispositif *cybermalveillance.gouv.fr* auprès des entreprises et dédier un service d'urgence aux entreprises ; des étudiants disposant des compétences numériques adéquates pourraient y effectuer leur service civique.

Proposition n°2 : Ouvrir un guichet de recueil anonymisé des cyberattaques frappant les entreprises, afin de disposer de statistiques fiables.

Proposition n°3 : Décliner des équipes de réponse aux incidents informatiques (CSIRT, *Computer Security Incident Response Team*) dans les **Régions** et inclure la cybersécurité dans les schémas régionaux de développement économique, d'internationalisation et d'innovation (SRDEII) afin de sensibiliser les collectivités locales.

Proposition n°4 : Adapter le droit de la commande publique pour favoriser l'écosystème de la cybersécurité en :

- Pérennisant les dispositions du décret du 24 décembre 2018 au profit des collectivités locales permettant l'achat sans mise en concurrence de « services innovants » ;
- Permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;
- Étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité.

Proposition n°5 : Élaborer des plans nationaux de prévention des cyberrisques, afin de coordonner la réponse des pouvoirs publics et des acteurs privés en cas d'attaque numérique systémique affectant une part significative des entreprises quelle que soit leur taille. Des **exercices de simulation** devraient être régulièrement organisés.

Proposition n°6 : Renforcer la réponse pénale à la cybercriminalité :

- Développer la formation initiale et continue des magistrats en matière de cybercriminalité ;
- Augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ;
- Doter les forces de cybersécurité de moyens financiers adéquats ;

- Étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ;
- Créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité.

Proposition n°7 : Adapter les procédures pénales à la cybercriminalité et renforcer la coopération des institutions judiciaires avec l'ANSSI au-delà de la lutte contre le terrorisme.

Proposition n°8 : Accélérer les négociations européennes sur le projet de règlement sur la **preuve électronique** (« *e-evidence* ») **et reprendre les négociations entre l'Union européenne et les Etats-Unis,** afin d'approfondir la coopération internationale concernant la cybercriminalité.

Proposition n°9 : Prévoir que les salariés doivent se voir proposer une sensibilisation à la cybersécurité, dans le cadre de la formation professionnelle au numérique.

Proposition n°10 : Déployer une campagne massive de promotion des métiers de la cybersécurité, cofinancée par l'État et les acteurs privés du secteur.

Proposition n°11 : Réserver à terme l'éligibilité à un remboursement par les assurances aux entreprises ayant eu recours aux services des prestataires labellisés *Expert Cyber*.

Proposition n°12 : Interdire l'assurabilité tant des rançongiciels que des sanctions administratives en cas en cas de violation de la réglementation sur la protection des données à caractère personnel, par un amendement à la convention de Budapest du Conseil de l'Europe, par un règlement européen, et par une disposition législative expresse dans le code des assurances.

Proposition n°13 : Afin de renforcer la conception sécurisée (*security by design)* :

- étudier l'extension aux entreprises de la « garantie logicielle » concernant les mises à jour de sécurité ;
- organiser, avec le support de l'ANSSI, un « hackathon de la cybersécurité » des entreprises, lors de la Journée mondiale de la cybersécurité, le 30 novembre.

Proposition n°14 : Construire un référentiel accessible aux TPE et PME pour renforcer la **certification** en matière de cybersécurité.

Proposition n°15 : Sensibiliser les PME sur la responsabilité personnelle des dirigeants en cas de cyberattaque de la chaîne d'approvisionnement dont ils sont partie prenante.

Proposition n°16 : Affermir le marché de l'assurance en matière de cybersécurité par :

- Une meilleure compréhension du risque, en ayant la connaissance la plus exhaustive possible des sinistres ;
- L'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label ExpertCyber ;
- La création d'une agence de cybernotation européenne, utilisant les référentiels de l'Agence européenne chargée de la sécurité des réseaux et de l'information –ENISA-, ou française, utilisant ceux de l'ANSSI.

Proposition n°17 : Faciliter la mutualisation des responsables de la sécurité des services informatiques (RSSI) pour les PME, par exemple par la constitution de groupements d'employeurs, ayant un statut de tiers de confiance.

Proposition n°18 : Développer l'offre d'un « package » simplifié de solutions de cybersécurité aux TPE et PME.

Proposition n°19 : Accorder aux TPE et PME, dont le champ de l'activité principale n'est pas le numérique, la **protection** de l'article L.212-1 du Code de la consommation sur les **clauses abusives** pour les contrats conclus en matière de cybersécurité.

Proposition n°20 : Étudier la faisabilité d'une solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI et d'une approche commune franco-allemande en faveur d'une meilleure prise en considération des PME dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA.

Proposition n°21 : Mettre en place un crédit d'impôt à destination des chefs d'entreprise et des salariés des PME, prenant en charge une partie des dépenses d'équipement et de formation à la cybersécurité.

Proposition n°22 : Instaurer un cyberscore des plateformes numériques destinées au grand public, afin de sensibiliser les citoyens à la cybersécurité.

I. LA CYBERSÉCURITÉ, UN ENJEU DÉCISIF DE SURVIE DES ENTREPRISES

A. DES ENTREPRISES DE PLUS EN PLUS NUMÉRISÉES ET CYBERATTAQUÉES

Qu'est-ce qu'une **cyberattaque**[1] **?** C'est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

La cybercriminalité visant les entreprises se banalise sous le quadruple effet :

- de la **numérisation de l'économie**, accélérée avec le confinement lié au développement du télétravail et le déploiement de la fibre et de la 5G, catalyseur de l'extension du cyberespace en connectant des systèmes jusqu'alors isolés et en créant des interdépendances entre eux ;
- de **l'industrialisation de la cybercriminalité** : « *de plus en plus de groupes cybercriminels possédant des ressources financières et des compétences techniques importantes favorisent le ciblage d'entreprises et institutions particulières dans leurs attaques par rançongiciel* »[2] ;
- de la **difficulté de la prévention et de la répression**, lesquelles nécessitent une coopération internationale et une mise à niveau de notre dispositif répressif, comme l'a récemment souligné le Sénat[3] ;
- de **l'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique,** dont les entreprises sont soit les cibles soit les victimes collatérales[4].

1. Des entreprises incitées à se numériser

L'injonction est générale. L'avenir de l'économie est numérique. **Toutes les entreprises, quelle que soit leur taille, sont incitées à numériser** leur processus de production, à vendre sur des plateformes, à intégrer dans leur chaîne de valeurs des process faisant un appel croissant aux

---

1 *« Les 10 types de cyberattaques les plus courants », Pierre-Louis Lussan, Netwrix Blog, 18 septembre 2019.*

2 *« État de la menace rançongicielle à l'encontre des entreprises et institutions », ANSSI, 5 février 2020.*

3 *Rapport d'information du 9 juillet 2020, de la commission des affaires européennes et de la commission des lois, sur le dispositif de lutte contre la cybercriminalité.*

4 *« Le cyberespace, un champ d'affrontement géopolitique », Frédérick Douzet dans Les conflits dans le monde (2016), « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », Frédérick Douzet, Aude Géry, dans Hérodote 2020/2-3 (N° 177-178).*

technologies numériques, comme l'a souligné en juillet 2019 le rapport de la Délégation aux entreprises consacré à la numérisation des TPE, PME et ETI[1].

Or, l'économie numérique, et tout particulièrement le e-commerce, ne peuvent se développer qu'en se fondant sur **la confiance du public et des consommateurs.**

Pour l'OCDE[2] : l'action publique doit donc : « *aider les petites et moyennes entreprises à saisir les opportunités qu'offre le numérique en renforçant la sensibilisation et en promouvant de bonnes pratiques de gestion du risque par des efforts publics et privés* ».

EXTRAIT DE LA DÉCLARATION MINISTÉRIELLE SUR L'ÉCONOMIE NUMÉRIQUE : INNOVATION, CROISSANCE ET PROSPÉRITÉ SOCIALE (« DÉCLARATION DE CANCÚN ») 21-23 JUIN 2016

[*Nous, États de l'OCDE, déclarons notre volonté de :]*

« *5. Promouvoir la gestion du risque de sécurité numérique et la protection de la vie privée, au plus haut niveau de décision, afin de renforcer la confiance ; mettre au point, à cet effet, des stratégies collaboratives qui reconnaissent le rôle déterminant de ces problématiques dans la prospérité économique et sociale, favorisent la mise en œuvre de pratiques cohérentes de gestion du risque de sécurité numérique et d'atteinte à la vie privée, tout en portant une attention particulière à la liberté d'expression et aux besoins des petites et moyennes entreprises et des individus, stimulent la recherche et l'innovation et s'inscrivent dans une politique générale de responsabilité et de transparence* ».

Dans son récent rapport « *Encouraging vulnerability treatment* »[3] publié le 11 février 2021, l'OCDE estime que « *les vulnérabilités* [numériques] *n'ont pas reçu suffisamment d'attention politique* » et propose aux gouvernants un guide de bonnes pratiques.

Pour l'Union européenne : suite aux conclusions de la réunion extraordinaire du Conseil européen des 1er et 2 octobre 2020, la Commission européenne et le Service européen pour l'action extérieure (SEAE) ont présenté, en décembre 2020, une nouvelle stratégie de cybersécurité dont l'objectif est de **renforcer la résilience de l'Europe** face aux cybermenaces et

---

[1] *« Accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ? », rapport d'information de Mme Pascale Gruny, fait au nom de la Délégation aux entreprises n° 635 (2018-2019) du 4 juillet 2019.*

[2] *« Vers le numérique : forger des politiques au service de vies meilleures », 4 novembre 2019.*

[3] *https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf?expires=1621532811&id=id&accname=guest&checksum=AA5A78916F4E6BBB6555BE903169BDAF*

de faire en sorte que « *tous les citoyens et toutes les entreprises puissent bénéficier pleinement de services et d'outils numériques fiables et dignes de confiance* ».

Le 22 mars 2021, le Conseil a adopté des conclusions sur cette stratégie[1], soulignant que la cybersécurité est « *essentielle à l'**édification d'une Europe résiliente, verte et numérique*** ». Les ministres de l'Union européenne ont fixé comme objectif clé de : « *parvenir à une autonomie stratégique tout en préservant une économie ouverte. Il s'agit notamment d'accroître la capacité à opérer des choix autonomes dans le domaine de la cybersécurité afin de renforcer le **leadership numérique** et les capacités stratégiques de l'Union européenne* ».

Deux propositions législatives devraient traduire cette stratégie face aux risques actuels et futurs en ligne et hors ligne : une directive actualisée pour mieux protéger les réseaux et les systèmes d'information, et une nouvelle directive sur la résilience des entités critiques.

La Commission européenne commence à se préoccuper des relations *BtoB*, qui concernent les relations entre professionnels, dans le prolongement du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, dit règlement « *Platform to Business* », entré en vigueur le 12 juillet 2020 dernier. Son objectif est de promouvoir un « *environnement équitable, prévisible, durable et inspirant confiance* », protecteur des entreprises utilisant des plateformes.

Cependant, **aucun dispositif de protection spécifique des TPE et PME en matière de cybersécurité n'est inscrit à l'agenda de la Commission européenne, lequel demeure centré sur les « entités critiques ».**

2. Des cyberattaques croissantes

Les types de failles de sécurité, les mesures pour les prévenir, les enjeux globaux de la cybersécurité pour les entreprises ont fait l'objet, **dès 2015**, d'un **rapport de M. Bruno Sido, sénateur et Mme Anne-Yvonne Le Dain, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPESCT) et consacré à la « *Sécurité numérique et risques : enjeux et chances pour les entreprises* »**[2]. Sa publication était intervenue entre un débat d'orientation pour la stratégie numérique de la France, devant l'Assemblée nationale le 14 janvier 2015, et la publication de la stratégie numérique de la France en mars 2015. Ce rapport, qui comportait une soixantaine de recommandations dont certaines reprenant les préconisations du « *Guide des règles d'hygiène informatique* » élaboré par l'ANSSI, reste encore d'actualité dans ses grandes lignes.

---

1 *Consultable sur : https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/fr/pdf*

2 *N° 271 tome I et II (2014-2015), 2 février 2015. http://www.senat.fr/rap/r14-271-1/r14-271-1_mono.html#toc970*

a) La cybercriminalité dans le monde

Le coût global des cyberattaques atteindrait **600 milliards de dollars**. En 2018, le coût moyen par entreprise aurait été de 8,6 millions d'euros pour les entreprises françaises et de 27,4 millions de dollars en moyenne pour les entreprises américaines[1].

Les cyberattaques contre les entreprises constitueraient, selon le président de la Réserve fédérale des États-Unis, Jerome Powell[2], le **risque actuel le plus important pour l'économie américaine, plus redoutable encore qu'une crise financière similaire à celle de 2008**, mais également le plus surveillé, les entreprises investissant de plus en plus dans la cybersécurité, comme la Fed elle-même[3].

Suite à la cyberattaque « ***SolarWinds*** », qualifiée de « ***Pearl Harbour de la cybersécurité*** » outre-Atlantique, le Président des États-Unis a ainsi signé le 12 mai 2021 un « *executiv order* » prescrivant des exigences de sécurité plus strictes pour les sous-traitants de logiciels, de nouvelles normes de cryptage et d'authentification pour les agences gouvernementales et la création d'un comité d'examen des cyberincidents sur le modèle du *National Transportation Safety Board*[4].

Outre les traditionnels **rançongiciels**, en forte augmentation, l'année 2020 a été marquée par une augmentation du nombre **d'attaques par déni de service (DDoS)**, manière d'interrompre les communications internes et externes d'une entreprise en la submergeant d'un flot d'informations qui finit par dégrader l'activité de ses serveurs. Ces attaques auraient crû de 15 à 20 %[5] avec un pic en mars, au plus fort du premier confinement en Occident. L'année 2020 aurait été également marquée par une **hausse de plus de 90 % du nombre des fuites de données.** Une société britannique de cybersécurité aurait ainsi identifié 1,7 million de fuites de données, avec une accélération de 47 % entre le troisième et le quatrième trimestre[6]. L'*Information Commissioner's Office* (ICO), l'équivalent britannique de la CNIL, a vu le volume des amendes pour infraction au Règlement européen sur la protection des données (RGPD) augmenter d'un **facteur 20**, à 45 millions d'euros.

---

1 *Selon une étude d'Accenture et du Ponemon Institute, « Cost of CyberCrime Study », avril 2019.*

2 *Le 11 avril 2021, dans l'émission de CBS « 60 Minutes ».*

3 *Un piratage de son système pourrait avoir des conséquences désastreuses, d'autant que la Fed a accru son rôle dans l'économie américaine durant la pandémie en soutenant les marchés, rachetant de la dette aux entreprises et opérant en direct des programmes du Trésor, accumulant des informations stratégiques sur les entreprises. Par ailleurs, 3 000 milliards de dollars transitent chaque jour par son système de paiement.*

4 *Agence indépendante du gouvernement des États-Unis, responsable des enquêtes sur les accidents aéronautiques, routiers, maritimes, ferroviaires et ceux concernant les pipelines (gazoducs et oléoducs).*

5 https://www.itproportal.com/news/a-record-number-of-ddos-attacks-took-place-in-2020/

6 https://www.itproportal.com/news/data-leakage-attacks-saw-huge-rise-in-2020/

30 STATISTIQUES SUR LA CYBERSÉCURITÉ DES PETITES ENTREPRISES AUX ÉTATS-UNIS

43 % des cyberattaques ciblent les petites entreprises.

60 % des petites entreprises victimes d'une cyberattaque font faillite dans les six mois.

La cybercriminalité coûte aux petites et moyennes entreprises plus de 2,2 millions de dollars par an.

Il y a eu une augmentation de 424% des nouvelles cyber-violations des petites entreprises en 2019-2020.

La santé est le secteur le plus exposé aux cyberattaques.

66 % des petites entreprises sont préoccupées ou extrêmement préoccupées par le risque de cybersécurité.

14 % des petites entreprises jugent leur capacité à atténuer les cyber-risques et les attaques très efficace.

47 % des petites entreprises ne savent pas comment se protéger contre les cyberattaques.

66 % des petites entreprises sont les plus préoccupées par la compromission des données client.

3 petites entreprises sur 4 déclarent ne pas disposer du personnel nécessaire pour assurer la sécurité informatique.

22 % des petites entreprises chiffrent leurs bases de données.

Les erreurs humaines et les défaillances du système représentent 52% des failles de sécurité des données.

63 % des violations de données confirmées utilisent un mot de passe faible, par défaut ou volé.

Les cyberattaques causées par des mots de passe d'employés compromis coûtent en moyenne 383 365 $.

1 e-mail sur 323 envoyé aux petites entreprises est malveillant.

La petite entreprise médiane a reçu 94 % de ses logiciels malveillants détectés par e-mail.

54 % des petites entreprises pensent qu'elles sont trop petites pour une cyberattaque.

25 % des petites entreprises ne savaient pas que les cyberattaques leur coûteraient de l'argent.

83 % des petites entreprises n'ont pas mis d'argent de côté pour faire face à une cyberattaque.

54 % des petites entreprises n'ont pas de plan en place pour réagir aux cyberattaques.

65 % des petites entreprises n'ont pas agi à la suite d'un incident de cybersécurité.

50 % des petites et moyennes entreprises ont déclaré avoir subi au moins une cyberattaque au cours de la dernière année.

Les petites entreprises dépensent en moyenne 955 429 $ pour rétablir leurs activités normales à la suite d'attaques réussies.

Le simple fait de comprendre comment une cyberattaque s'est produite pourrait coûter 15 000 $.

40 % des petites entreprises ont connu au moins 8 heures d'indisponibilité en raison d'une cyber-violation.

Ce temps d'arrêt représente en moyenne 1,56 million de dollars de pertes.

Les cyberattaques devraient causer 6 milliards de dollars de dommages d'ici 2021.

Les experts du secteur affirment que le budget de cybersécurité d'une petite entreprise devrait représenter au moins 3% des dépenses totales d'une entreprise.

91% des petites entreprises n'ont pas d'assurance responsabilité civile.

Cette plus grande cyberattaque à ce jour est arrivée à Yahoo! En août 2013, lorsque 3 milliards de comptes ont été piratés.

Source : 30 Surprising Small Business Cyber Security Statistics (2021), Maddie Shepherd, Fundera, 16 décembre 2020.

Dans le cloud, **les cyberattaques seront plus nombreuses et plus efficaces en 2021 car la surface d'attaque des entreprises s'est élargie avec le recours massif au télétravail et aux applications qui y sont logées.**

L'éditeur de logiciel McAfee a noté **une augmentation moyenne en 2020 de 667 % des attaques sur les comptes cloud**, avec des variations selon le secteur visé : le transport a été le secteur le plus touché avec une augmentation de 1 350 %, suivi par l'éducation (+1 114 %), les administrations publiques (+773 %), l'industrie manufacturière (+679 %), les services financiers (+571 %), l'énergie et les services publics (+472 %).

Cette explosion s'explique par l'augmentation du recours accru aux services proposés par le cloud aux entreprises, qui a crû de 50 % durant les quatre premiers mois de l'année 2020, principalement dans les secteurs de la fabrication et des services financiers, utilisant traditionnellement des applications sur site. L'utilisation des outils de collaboration cloud a augmenté jusqu'à 600 %. Le secteur où la croissance est la plus marquée est celui de l'éducation en raison de l'enseignement à distance.

Au total, **le risque numérique figure parmi les dix risques les plus préoccupants au niveau international** comme le note le rapport sur les risques globaux du Forum Économique Mondial de 2020[1].

b) La cybercriminalité en France

Ce risque était classé au premier rang des risques d'entreprise identifié pour 2020 par l'assureur Allianz[2] , quelques mois avant l'essor fulgurant du télétravail et des cyberattaques lié à la pandémie.

Selon le ministère de l'Intérieur[3], **en 2018 déjà, 80 % des entreprises avaient connu une cyberattaque et 32 % en auraient connu plus de 10.** Ce taux est en baisse, car elles sont de plus en plus ciblées sur les entreprises les plus vulnérables, car les moins bien protégées.

Depuis 2017, les entreprises sont la cible privilégiée d'attaques au rançongiciel.

Selon le Symantec[4], la baisse de 20 % des infections par rançongiciel, en 2019 a été compensée par une hausse de 12 % à l'encontre des entreprises, en ciblant leurs salariés.

Dans son rapport d'état de la menace rançongicielle en France en 2020[5], l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pointe **une hausse des signalements d'attaque de 255 % par rapport à 2019**. En **2020**, l'agence estime que le nombre de rançongiciels a **quadruplé**.

Plus d'une entreprise sur deux aurait connu une cyberattaque en 2020 selon le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN)[6].

Cependant, les chiffres de la cybersécurité sont **à prendre avec précaution,** toutes les entreprises ne déclarant pas aux autorités judiciaires les préjudices dont elles ont été victimes.

---

1 *« The Global Risks Report 2020 », World Economic Forum, Insight Report 15th Edition, in partnership with Marsh & McLennan and Zurich Insurance Group.*

2 *Communiqué de presse du 14 janvier 2020.*

3 *« L'état de la menace liée au numérique en 2019 ».*

4 *« Internet Security Threat Report 2019 », février 2019.*

5 *« Attaques par rançongiciels, tous concernés : comment les anticiper et réagir en cas d'incident ? », ANSSI, août 2020.*

6 *Créé en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique, le CESIN est un lieu d'échange, de partage de connaissances et d'expériences. Il permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte plus de 600 membres issus de tous les secteurs d'activité économiques et de l'administration.*

LE 6ÈME BAROMÈTRE DE LA CYBERSÉCURITÉ DES ENTREPRISES (FÉVRIER 2021) DU CLUB DE SÉCURITÉ DE L'INFORMATION FRANÇAIS[1]

Une vulnérabilité des entreprises aux cyber-attaques toujours avérée...

57 % des entreprises déclarent avoir connu au moins une cyber-attaque en 2020 : une vulnérabilité toujours présente donc, malgré un taux en légère baisse par rapport à l'année dernière (65 %).

Une entreprise sur 5 (19 %) a été victime d'une attaque de type rançongiciels provoquant un chiffrement ou un volet chantage de données. Les entreprises, conscientes de la recrudescence de la menace rançongiciels en 2020 renforcent la sensibilisation des utilisateurs (83 %) à ce type d'attaque. Les vecteurs d'attaque par *phishing* (80 %) et exploitation des failles (52 %) restent les plus répandues, menant le plus souvent à un vol de données (30 %) ou à un déni de service (29 %).Une des principales causes de cyber-risques est le *ShadowIT* pour 44 % des entreprises, suivies par la vulnérabilité résiduelle permanente (36 %) et la cyber-attaque opportuniste (36 %). Plus de la moitié des entreprises (56 %) estiment que le niveau des menaces relatives au cyber-espionnage est élevé. Similairement à l'année dernière, 58 % des cyber-attaques ont un impact sur le business, entraînant le plus souvent une perturbation de la production (27 %).

Les entreprises ne peuvent que progresser sur leur capacité à répondre aux attaques.

85 % des entreprises jugent les solutions de protection disponibles sur le marché plutôt adaptées aux besoins de leur entreprise. Elles sont d'ailleurs 69 % à s'estimer prêtes à gérer une cyber-attaque en termes de moyens de prévention, mais moins nombreuses à l'être en termes de moyens de détection (59 %). Pour ce faire, elles mettent en place en moyenne 10 solutions, et en priorité le VPN, le proxy & filtrage d'URL et la passerelle de sécurité mail. Toujours dans une démarche de prévention, 29 % des entreprises ont mis en place le concept de ZeroTrust et 45% sont en train de l'étudier. Toutefois, seules 46% des entreprises se disent confiantes quant à leur capacité de réponse à une cyber-attaque. 33 % des entreprises mettent en place un programme d'entraînement à la cyber-crise et 24 % ont déjà fait appel à leur cyber-assurance en cas d'attaque. 47 % des entreprises ont porté plainte à la suite d'une ou plusieurs cyber-attaques, mais seulement 15 % des enquêtes ont débouchés sur une identification ou une interpellation des attaquants.

La crise sanitaire apporte de nouveaux risques avec la généralisation du télétravail (37 %) et l'augmentation des crises cyber liée aux nouveaux risques (35 %). Par ailleurs, 43 % des entreprises se disent prêtes à augmenter les budgets liés à la cybersécurité pour faire face à ces nouveaux risques.

Une sensibilisation des salariés en continu : 77 % des entreprises estiment que leurs salariés sont sensibilisés à la cybersécurité, mais tous ne semblent pas appliquer les recommandations (63 %). D'après les responsables de la sécurité des

[1] *Effectué par entretiens réalisées entre le 7 décembre 2020 et le 11 janvier 2021 auprès de 228 entreprises de toutes tailles (dont 9 % de PME), avec une marge d'erreur de +/- 6,5 points.*

systèmes d'information (RSSI), les usages numériques des salariés présentent de nombreux risques, et plus particulièrement l'utilisation de services cloud non approuvés (84 %) ou encore la gestion des partages de données à l'initiative des salariés (80 %).

Les RSSI mettent en avant plusieurs **risques à l'utilisation du Cloud**, les plus forts étant la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (51 %), la difficulté de contrôler les accès par des administrateurs de l'hébergeur (45 %) et la non-maîtrise de l'utilisation qui en est faite par les salariés de l'entreprise (44 %). 86% des entreprises estiment par ailleurs que les outils fournis par les prestataires de solutions Cloud ne permettent pas de sécuriser les données et qu'il est nécessaire d'utiliser des dispositifs et outils spécifiques.

Les entreprises sont **inquiètes, mais clairvoyantes** sur les enjeux de demain. Au final, une sur deux est inquiète quant à sa capacité à faire face aux cyber-risques. Les entreprises **identifient 3 principaux enjeux pour demain** :

① Placer la cybersécurité au centre de la gouvernance de l'entreprise (60 %), les entreprises se disent d'ailleurs confiantes quant à la prise en compte des enjeux de la cybersécurité au sein du COMEX (72 %/+8 points par rapport à 2019).

② Former et sensibiliser les usagers à la cybersécurité (56 %), il s'agit d'un processus déjà mis en place puisque la sensibilisation est le premier dispositif (83 %) à avoir été renforcé par les RSSI face à la vague des cyber-attaques.

③ Allouer davantage de budgets et de ressources à la cybersécurité (46 %). 57 % des entreprises comptent augmenter les budgets pour la protection contre les cyber-risques. En termes de ressources, les entreprises souhaitent augmenter les effectifs de cybersécurité (52 %). L'augmentation du budget passe également par l'acquisition de nouvelles solutions techniques désirée par 85 % des entreprises.

Source : CESIN, février 2021.

Les cyberattaques surviennent souvent à un moment particulier de la vie de l'entreprise et prennent la forme d'un dévoiement criminel de la compétition économique.

Ainsi, selon le ministère de l'Intérieur, « *une exfiltration de données renseignera une entreprise sur l'état de santé d'un concurrent ou sur les vulnérabilités d'un cadre dirigeant, tandis qu'un déni de service empêchera l'entreprise de fournir un service en ligne en période d'affluence. L'attaquant ou son commanditaire pourra ainsi obtenir plus facilement une position déterminante pour mettre en œuvre son projet (acquisition, délivrance d'une sanction financière, abandon d'un marché, etc…). Il n'est en effet pas rare d'observer une concomitance entre une attaque informatique et des faits plus traditionnels (mouvement de personnel, participation à un marché gouvernemental, etc…)* ».

Afin de limiter tout risque d'ingérence : « *une attention particulière doit donc être portée à la protection des systèmes d'information, lorsque l'entreprise affronte* ***un moment clé de son fonctionnement*** *(acquisition, négociations salariales, réalisation d'audits de conformité - en particulier dans le cas d'une*

démarche de mise en conformité soutenue par des cabinets de conseil et des sociétés d'investigation numérique étrangers, bilan annuel, renégociation contractuelle, etc.) ». En outre, **la cybersécurité doit être renforcée dans une phase de conquête de marchés à l'exportation** et les entreprises « *doivent prendre conscience des risques d'ingérence économique lorsqu'elles pénètrent sur des marchés stratégiques pour d'autres entités* ».

Compte tenu de **l'impossibilité de créer un environnement numérique totalement sûr et sécurisé**, la cybersécurité vise à **gérer ce risque et non à l'éliminer.**

3. Une cybercriminalité qui s'industrialise

Au niveau mondial, **la cybercriminalité pourrait coûter 6 000 milliards de dollars par an à partir de 2021, contre 3 000 milliards en 2015**[1]**,** tous secteurs confondus.

La cybercriminalité a par ailleurs changé, délaissant les particuliers pour s'orienter de façon privilégiée vers les entreprises.

Avant 2017, selon Kapersky[2], « *les victimes de rançongiciels étaient principalement des passants occasionnels. Les cybercriminels lançaient des spams partout en espérant trouver au moins un utilisateur qui aurait des fichiers importants dans son ordinateur, et qui ouvrirait la pièce jointe malveillante.*

*La situation a changé en 2016. Les listes aléatoires des spammeurs ont été de plus en plus remplacées par les adresses des employés d'une entreprise qui avaient été trouvées en ligne, et spécifiquement collectées. Les coupables avaient clairement compris qu'**il était beaucoup plus rentable d'attaquer les entreprises**. Par conséquent, le contenu des messages changeait également. Au lieu de se faire passer pour une correspondance personnelle, les messages semblaient désormais avoir été envoyés par des collaborateurs, des clients et les services fiscaux. La situation a de nouveau changé en 2017 ; radicalement cette fois. Deux épidémies à grande échelle ont affecté des millions de personnes et ont montré que le ransomware pouvait avoir différents objectifs autres que l'extorsion* »[3], notamment avec les rançongiciels *WannaCry*, qui infecta, en mai 2017, en une seule journée au moins 200 000 machines dans plus de 150 pays, avait pour principal objectif la destruction de données, et *ExPetr*, exposant au risque d'infection les entreprises ayant une activité en Ukraine.

---

[1] *Étude « 2019 Official Annual Cybercrime Report ». Selon son auteur, Steve Morgan : « Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades » (L'activité cybercriminelle est l'un des plus grands défis auxquels l'humanité sera confrontée au cours des deux prochaines décennies).* https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[2] *Entreprise multinationale spécialisée dans la sécurité des systèmes d'information proposant des antivirus, anti-spyware, anti-spam ainsi que d'autres outils de sécurité.*

[3] *« L'évolution du ransomware – et les outils pour y faire face », 19 juin 2018.*

L'essor de cette cybercriminalité est facilité par sa « plateformisation », son industrialisation[1], et le développement des cryptomonnaies. Elle est devenue « low cost ».

Selon l'état de la menace liée au numérique en 2019, réalisé par le ministère de l'Intérieur : « *tout un écosystème facilitant la mise en œuvre d'attaques cyber par des individus ou groupes criminels est désormais en place, induisant la notion de « crime-as-a-service ». Malwares, plateformes d'exploits, de service ou prestataires d'infrastructure se trouvent aisément, notamment sur les darknets* ».

Ces attaques ciblées, connues sous le nom de « *Big Game Hunting* »[2], mettent en œuvre des méthodes et techniques auparavant réservées à des opérations d'espionnage informatique opérées par des attaquants étatiques. **La rentabilité de telles attaques criminelles est énorme**, grâce à la vente régulière d'accès RDP[3] sur les marchés noirs à des prix parfois dérisoires (quelques dizaines de dollars), et au profit considérable que rapportent ces rançons.

Les activités cybercriminelles (dont les rançongiciels ne représentent qu'un faible pourcentage), correspondraient à une masse financière de **plus de 1 500 milliards de dollars en 2018**, des bénéfices estimés à **2 milliards de dollars annuels** et un gain pour un groupe cybercriminel moyen d'environ 900 000 dollars par an[4].

Cette criminalité prospère grâce à **5 milliards de données** (données bancaires, d'identité, couple login/mot de passe, etc.) qui seraient hébergées en 2018 sur les places de marché cybercriminelles[5].

---

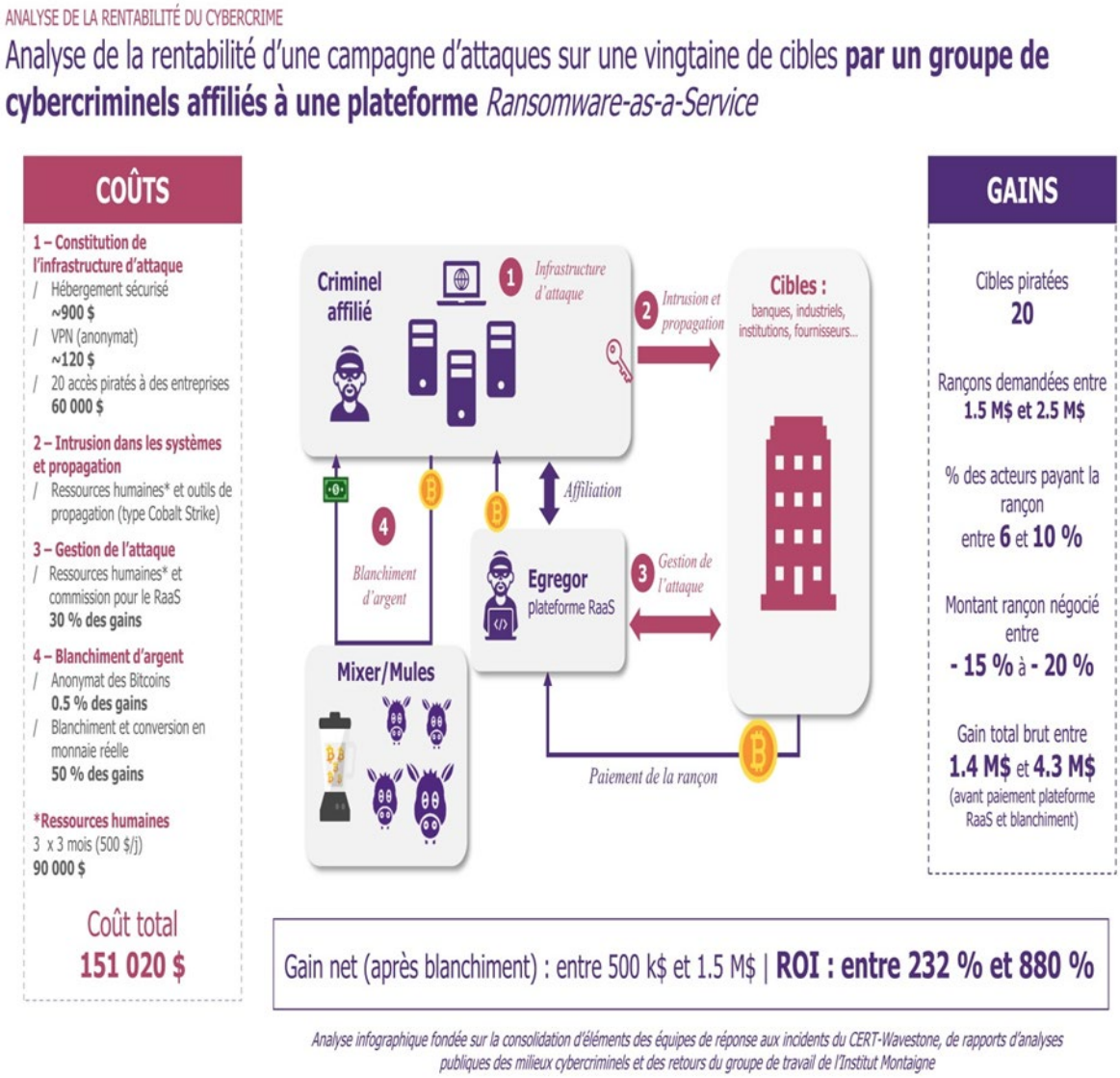
1 *« Cybercrime : plongée dans l'écosystème », Gérôme Billois, Marwan Lahoud, Blog de l'Institut Montaigne, 15 mars 2021. Un extrait de cet article figure en annexe.*

2 *« Le ransonware au cœur des cyberattaques en 2019 », Séverine Fontaine, 4 février 2020, Techniques de l'Ingénieur.*

3 *Le Remote Desktop Services est un composant de Microsoft Windows (dans les versions clientes et serveur) qui permet à un utilisateur d'accéder à des applications et des données sur un ordinateur distant, via n'importe quel type de réseau.*

4 *« Into the Web of Profit. Understanding the growth of the cybercrime economy », Dr. Mike McGuire, 20 avril 2018, étude soutenue par Bromium, entreprise de cybersécurité créée en 2010.* https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

5 *Selon le rapport « The Data Breach Epidemic Report », 17 juin 2019 de la société d'analyse de cybersécurité Verint.*



Source : « Cybercrime : plongée dans l'écosystème »,
Gérôme Billois, Marwan Lahoud, Blog de l'Institut Montaigne, 15 mars 2021.

Face à cette internationalisation du cybercrime, le Président de la République a présenté **le 12 novembre 2020**, au Forum sur la gouvernance d'Internet, un **« *appel de Paris* » pour la sécurité du cyberespace**[1], signé par 370 États, ONG ou entreprises. Les signataires de cet Appel de Paris se déclarent notamment « *résolus à agir de concert* » pour empêcher les cyberactivités malveillantes « *qui causent des dommages importants, sans discernement ou systémiques* ». Ils s'engagent à développer les capacités pour « *empêcher des acteurs étrangers de perturber des processus électoraux* » et promettent également d'empêcher des acteurs privés de répliquer aux attaques informatiques par d'autres attaques informatiques, au risque de provoquer un embrasement général.

[1] https://pariscall.international/fr/

B. L'UTILISATION DE TERMINAUX PERSONNELS : UN « CHEVAL DE TROIE »

L'utilisation par les salariés de leurs propres appareils (téléphone portable, ordinateur, tablette) sur leur lieu de travail, dans le cadre de leur activité est de plus en plus fréquente.

1. Une pratique née dès le début du XXIème siècle

Cette pratique, **« BYOD »** (*Bring Your Own Device*, en français : « *Apportez Votre Equipement personnel de Communication* » ou AVEC) voit le jour au milieu des années 2000 dans certaines écoles nord-américaines. Les étudiants sortant de leurs études et entrant dans le monde du travail ont pris l'habitude d'utiliser leur smartphone ou leur tablette informatique durant toute la journée, tant pour consulter leurs mails que pour se tenir au courant de l'actualité. Les entreprises ont favorisé, dans un premier temps, cette pratique compte-tenu de la flexibilité apportée par cette nouvelle façon de consommer l'informatique, « ATAWAD » (« *Any Time, Any Where, Any Device* »), conduisant à une mutation des solutions d'accès à leur système d'information, et notamment l'assouplissement des contraintes liées aux horaires, aux terminaux ou aux moyens de connexion.

Si le Code du travail demande à l'employeur de fournir à ses employés les moyens nécessaires à l'exécution de leurs tâches professionnelles, il n'interdit pour autant pas à l'employeur de permettre l'utilisation des moyens personnels des employés, souvent perçus comme plus agréables à utiliser, car plus familiers.

Désormais, la plupart des salariés possèdent plusieurs interfaces informatiques de travail, à tel point qu'une grande majorité d'entre eux n'envisagent pas de travailler sans leurs outils personnels. Les entreprises ont dû s'adapter à cette tendance. Selon une enquête menée par Dell[1] au début de l'année **2014, 93 %** des responsables informatiques interrogés **autorisaient l'accès** au réseau de leur entreprise via des terminaux personnels.

70 % des entreprises qui ont mis en place le « BOYD » ont déclaré avoir obtenu des gains de productivité liés à leurs salariés et une économie de coûts liée à l'absence d'achats de nouveaux terminaux informatiques, pratique leur faisant économiser jusqu'à 180 000 euros en moyenne sur cinq ans selon une étude de 2014[2]. **Cette « aubaine » pour les services informatiques des entreprises a cependant encouragé la diffusion de**

---

[1] *Enquête « Protecting the organisation against the unknown ». « Dell Helps Customers Fight Back Against a new Generation of Unknown Network Threats », 21 février 2014.*

[2] *« Les DSI ont tout à gagner à laisser les utilisateurs entrer dans le SI avec leur propre matériel informatique », selon Frédéric Pierresteguy, directeur général Europe du Sud de Landesk, auteur de l'étude.*

comportements qui se sont révélés à terme dangereux pour leur sécurité numérique, et également coûteux.

La CNIL souligne ainsi que « *la possibilité d'utiliser des outils personnels relève avant tout d'un choix de l'employeur qui peut tout aussi bien* ***l'autoriser sous conditions, ou l'interdire*** »[1], ce qui était la position du directeur général de l'ANSSI en 2012, pour qui il fallait « ***entrer en résistance*** *vis-à-vis de la liberté totale de l'usage des nouvelles technologies en entreprise* » car « *la sécurité c'est aussi le courage de dire non* ». L'agence publie en mai 2013 une note mettant en évidence le fait qu'il est impossible d'avoir un haut niveau de sécurité avec un ordinateur ou une tablette ordinaire[2].

En effet, ***« ouvrir son système d'information à n'importe quel terminal depuis n'importe quel lieu augmente forcément la surface d'attaque*** », avertit le Livre blanc de la cybersécurité à l'usage des dirigeants d'entreprise[3].

BYOD, LE RISQUE « *BRING YOUR OWN DISASTER* »

« *Même dans un environnement informatique traditionnel, il n'est pas toujours facile de bien comprendre, différencier, sélectionner et, enfin, implémenter divers modèles de licences logicielles en parallèle. Ajoutez-y des postes de travail virtuels, des terminaux mobiles, des modèles alternatifs de déploiement applicatif et une dose de BYOD, et les choses se compliquent alors sérieusement. Jusqu'ici, les fournisseurs de solutions de gestion des licences ont plus ou moins ignoré la tendance du BYOD. Par conséquent, difficile pour les entreprises d'adapter des modèles de licences d'hier, basés sur le matériel, aux environnements mobiles et orientés utilisateurs d'aujourd'hui – sans compter les coûts et les problèmes importants liés au monitoring d'un plus grand nombre d'utilisateurs et de terminaux. À mesure que le parc matériel s'enrichit de nouveaux terminaux mobiles, vos coûts et les risques d'infraction aux réglementations augmentent. Vous devez non seulement tenir un inventaire précis des logiciels et terminaux utilisés par chaque collaborateur, mais aussi estimer la valeur de ces informations, trouver un moyen de gérer les spécificités des licences de chaque éditeur et respecter leurs conditions d'utilisation.*

Vous devrez décider à qui revient la responsabilité de la gestion des licences logicielles. Selon une récente étude[4]*,* ***près de 70 % des salariés aux États-Unis et en Europe arrêteraient d'utiliser leur propre appareil au travail s'ils savaient que leur employeur pouvait l'effacer ou le verrouiller à distance****. D'autre part, 83 % ne s'en serviraient plus, ou avec une certaine appréhension, s'ils savaient que leur entreprise pouvait suivre leurs faits et gestes en permanence. Or, pour protéger correctement ses données et assurer sa sécurité, l'entreprise devra forcément accéder aux appareils personnels de ses salariés. En outre, si l'effacement total du contenu de l'appareil s'avère*

1 *« BYOD : quelles sont les bonnes pratiques ? », site internet de la CNIL, 24 mars 2019.*

2 *« Recommandations de sécurité relatives aux ordiphones », ANSSI, mai 2013.*

3 *Co-réalisé par l'OSSIR et le CLUSIF, publié le 29 janvier 2020.*

4 « Study: Employees Unaware Of Employers BYOD Policies », Nathan Eddy.

inévitable, le collaborateur risque de perdre ses fichiers personnels. Si vous décidez au contraire de confier la sécurité de l'appareil à vos collaborateurs, vous devrez leur faire signer un contrat d'utilisateur final. Mais que se passera-t-il si le terminal tombe entre les mains d'un inconnu ou qu'un proche s'en sert ?

Pour « atteindre ces objectifs et éviter des sanctions financières coûteuses en cas d'infraction, les entreprises ont souvent recours à des licences collectives couvrant tous les terminaux d'un même site. Or, si seuls 60 % des collaborateurs ont besoin d'un logiciel particulier, pourquoi payer en pure perte pour les 40 % restants ? Et la facture se corse encore davantage en fonction de l'architecture et de la méthode d'accès réseau, de la localisation et du type de terminal, et du modèle de licences choisi par l'entreprise ».

Source : « BYOD : Bring Your Own Disaster *? Comment le rêve de toute organisation peut tourner au pire cauchemar » Pierre-Yves Popihn, Solution Architect Manager pour NTT Com Security, DocAuFutur, 9 octobre 2014.*

Dès 2017, le CESIN alertait sur **le risque du *shadow IT***[1], phénomène qui s'est ainsi développé avec la gratuité de nombreux services en ligne et auxquels les utilisateurs se sont inscrits sans toujours se rendre compte du danger représenté pour le patrimoine informationnel de l'entreprise. Lorsque les directions des services informatiques (DSI) des entreprises répertorient en moyenne **entre 30 à 40 applications Cloud, 1 700 applications seraient utilisées par leurs employés.**

Cette pratique permet toutefois également de repérer des solutions innovantes et de répondre aux besoins des métiers en étoffant le catalogue de la DSI et d'intégrer la stratégie de cybersécurité de l'entreprise.

LE DÉVELOPPEMENT DU *SHADOW IT*

« *Cela peut aller de la création d'un Réseau Social d'Entreprise hors contrôle de cette dernière avec des offres gratuites comme LinkedIn ou Facebook, à la constitution de services collaboratifs pour des besoins ponctuels en recourant à la gratuité avec à la clé une protection des données réduite à sa plus simple expression. La principale calamité en la matière restant les sites de partage de fichiers qui pullulent sur le WEB et dont la protection laisse le plus souvent à désirer. Or, jusqu'à une période récente, le RSSI était aveugle sur ces usages de services gratuits. Tout au plus disposait-il de statistiques de consommation Internet obtenues à partir des outils de filtrage WEB mais la foisonnance des sites consultés ne pouvait pas lui donner beaucoup d'indications sur l'utilisation réelle de ces services et sur l'ampleur du phénomène. Depuis quelques années de nouveaux outils sont apparus qui devraient redonner au RSSI davantage de visibilité sur ces usages : il s'agit de produits dit CASB (Cloud Access Security Broker) qui sont des points de concentration, déployés dans l'entreprise ou dans le Cloud, placés entre les utilisateurs et les services du Cloud, utilisés pour appliquer les politiques de sécurité de*

[1] *Voir : https://www.cesin.fr/uploads/files/2018_04_Symantec_CESIN%20Shadow%20IT%20Report%20France.pdf*

l'entreprise. Ces CASB adressent des sujets très divers comme l'authentification, l'autorisation d'accès, le SSO[1] mais aussi la visibilité des applications utilisées dans le Cloud. L'idée est de montrer par « qui » et « comment » sont utilisées ces applications tout en proposant une vision globale de l'utilisation de celles-ci ainsi que certains conseils pour se prémunir des risques principaux ».

Source : Rapport Shadow IT France 2017.

Avec l'apparition de risques de failles de sécurité liés au BYOD, les systèmes **CYOD** (*Choose Your Own Device*), aussi appelés COPE (*Corporate Owned Personally Enabled*), ont commencé à être utilisés dans les entreprises. Le CYOD prend le contre-pied du BYOD : au lieu de permettre aux salariés d'utiliser leur appareil personnel au travail, le CYOD leur propose un choix de terminaux détenus par l'entreprise dont ils pourront se servir pour leurs activités professionnelles et personnelles. Le terminal appartenant à l'entreprise, ses données peuvent être effacées et sa connexion réseau bloquée à tout moment.

Avec l'essor des smartphones grand public en 2007, les entreprises ont ainsi développé le « ***Mobile Device Management*** »[2], applications permettant la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes ou de smartphones, en s'assurant que tous ses collaborateurs aient des programmes à jour et que leurs appareils soient correctement sécurisés. Le département informatique de l'entreprise gérant les applications mobiles, les réseaux et les données utilisées par les appareils mobiles de l'entreprise ainsi que les appareils mobiles eux-mêmes à l'aide d'un seul logiciel, la propagation de patchs de sécurité ou de nouveaux logiciels pour l'ensemble des collaborateurs est facilitée.

Pour sécuriser ce « BOYD », les entreprises utilisent des **logiciels de type EDR** (*Endpoint Detection and Response*), technologie de détection des menaces sur les ordinateurs et serveurs connectés au réseau et non le réseau lui-même. Il définit une catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information.

Ces logiciels peuvent également contribuer à assurer une surveillance et une protection contre les **APT** (*Advanced Persistent Threats*), qui utilisent souvent des techniques de piratage sans malware[3] et des failles

---

[1] *Le SSO, pour « Single Sign-On », désigne un système d'authentification permettant à un utilisateur d'accéder à de nombreuses applications sans avoir à multiplier les authentifications.*

[2] *« Best MDM solutions in 2021 : Mobile Device Management for BYOD policies », par David Nield, Brian Turner, dans Techradar.com, 11 mars 2021.*

[3] *Également appelé attaque sans fichier (file-less) ou sans empreinte (zero-footprint), le piratage sans malware utilise généralement PowerShell sur les systèmes sous Windows pour exécuter de manière furtive des commandes visant à rechercher et exfiltrer du contenu ayant de la valeur.*

de sécurité pour accéder à un réseau. Les anciens logiciels antivirus ne peuvent détecter un malware que lorsqu'ils trouvent une signature correspondante. Ils sont incapables de surveiller les activités d'un pirate pour déterminer qu'il a accès à un ordinateur. Les logiciels EDR utilisent de l'intelligence articifielle et sont auto-apprenants : ils n'ont pas besoin de se connecter sur internet pour mettre à jour leurs bases de données.

Par ailleurs, **la technologie MPLS** (*MultiProtocol Label Switching*) **est désormais accessible aux PME et TPE**, alors qu'elle était jusqu'à présent réservée aux grandes entreprises. Le MPLS est un réseau privé de bout en bout, qui ne transite pas sur Internet. Les risques d'intrusions ou de failles de sécurité sont moins importants qu'avec un réseau privé virtuel (VPN)[1]. Cette solution est paramétrée par un seul opérateur qui supervise et maintient l'ensemble du réseau de l'entreprise. Ainsi, l'entreprise s'adresse à un interlocuteur unique qui gère l'ensemble de son infrastructure. Le réseau est centralisé et mutualisé entre les différents sites de l'entreprise. Un seul *firewall* mutualisé suffit pour sécuriser l'ensemble des sites.

Enfin, les entreprises développent le **concept Zero Trust[2]**, modèle de sécurité qui repose sur le principe qu'aucun utilisateur n'est totalement digne de confiance sur un réseau. En conséquence, des utilisateurs, ne peuvent accéder à des ressources qu'après vérification de leur légitimité et de leur autorisation. Ce modèle met en place un « accès basé sur des droits minimums », permettant ainsi de restreindre l'accès des utilisateurs ou groupes d'utilisateurs aux seules ressources dont ils ont besoin.

Cette stratégie de cybersécurité rejette en grande partie l'approche traditionnelle de type « *château entouré de douves* », qui cherche à défendre la sécurité d'un périmètre, empêcher les attaquants d'entrer, tout en supposant que toutes les personnes et tous les éléments présents à l'intérieur du périmètre disposent d'un accès valide et ne posent ainsi aucun risque pour l'organisation. Cette approche s'appuyant sur des pare-feu et autres mesures de sécurité similaires, s'est avérée impuissante face à la menace posée par des acteurs malveillants situés à l'intérieur des entreprises et qui ont obtenu (ou à qui l'on a donné) l'accès à des comptes à privilèges. Avec la stratégie Zero Trust, chaque utilisateur ne se voit accorder que les privilèges nécessaires à l'accomplissement de ses propres tâches (principe du moindre privilège). Pour chaque session, chaque utilisateur, dispositif et application doit passer la procédure d'authentification et prouver qu'il a le droit d'accéder aux données en question. Ainsi, le piratage d'un compte utilisateur individuel ne compromet qu'une partie de l'infrastructure.

Cette démarche, qui se déploie au niveau de chaque utilisateur individuel, est cependant **longue et fastidieuse** surtout pour les entreprises

---

[1] *Ils permettent de créer un lien direct entre des ordinateurs distants, isolant leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.*

[2] *Le modèle Zero Trust, inventé par l'analyste John Kindervag en 2010.*

déjà dotées d'un système d'information qui doit être totalement repensé. Google, par exemple, a eu besoin de sept ans pour construire le cadre « BeyondCorp », fondé sur la stratégie Zero Trust.

L'entreprise est ainsi exposée en permanence au dilemme entre la flexibilité demandée par les salariés et l'impératif du contrôle de sa cybersécurité.

2. Une généralisation des comportements liée au travail à distance

Au printemps 2020, et en quelques jours, 8 millions de salariés ou fonctionnaires ont basculé la totalité de leur activité en télétravail. « *Rares sont les organisations qui avaient pu anticiper un basculement de cette ampleur ou l'envisager de façon cohérente et intégrée à un plan de continuité d'activité. La bascule a été effectuée dans l'urgence, parfois avec les moyens du bord* », non sécurisés, comme l'ont rappelé les sénateurs Olivier Cadic et Rachel Mazuir dans leur rapport d'information sur le suivi de la cybermenace pendant la crise sanitaire[1].

Comme en témoigne Tech in France et le Syntec[2] : « *même certaines entreprises dites « matures » ont mis en place massivement le télétravail sans sécurité, voire demandent à leurs collaborateurs l'utilisation d'ordinateurs personnels sur lesquels les RSSI n'ont aucune prise.* ***La prise de conscience de la nécessité de protection est disparate, et dans l'urgence elle est souvent mise au second plan*** **».**

Malgré les risques avérés, les salariés, travaillant à domicile, ont dû parfois s'équiper en matériel informatique, en logiciels ou en applications qui échappent au contrôle de la DSI des entreprises : utilisation d'une plateforme d'échange publique (WeTransfer, Dropbox, Google Drive, etc.) pour l'envoi de documents confidentiels, appel à un prestataire au niveau de sécurité non connu pour la gestion de bases de données clients, utilisation de clés USB personnelles sur son lieu de travail, le téléchargement d'interfaces de programmation (API) sur internet…

L'impératif de continuité de l'activité a donc pu contribuer à reléguer la sécurité à un second plan. Ceci a favorisé l'essor d'une cybercriminalité d'opportunité, profitant de la réorganisation liée au télétravail pendant le confinement.

Ainsi, on a constaté une **augmentation de 667 % des attaques par *phishing* enregistrées entre le 1er et le 23 mars 2020[3], à l'occasion du premier confinement général de la population française**...

---

1 *Rapport n°502 (session ordinaire 2019-2020) du 10 juin 2020.*

2 *Dans leurs propositions conjointes : « Crise Covid-19 et relance de l'économie », mai 2020.*

3 *Selon « Threat Spotlight: Coronavirus-related phishing », Fleming Shi, 26 mars 2020* https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

C. LA CYBERMALVEILLANCE : UN RISQUE MORTEL

La perte partielle ou totale des ressources informatiques clés entraînant une rupture de service a pour plusieurs **conséquences cumulatives négatives** pour une entreprise : **perte financière directe** à la suite de ventes non réalisées pendant l'absence de service ; **atteinte à l'image** auprès des investisseurs, clients et opinion publique ; **risque légal** lié à une rupture contractuelle des engagements de la société et pénalités pour non-respect de ceux-ci ; **risque de perte de propriété intellectuelle** ou des données.

Une attaque informatique peut conduire une entreprise, et notamment une TPE ou PME, structurellement plus fragile, à disparaître.

Aux États-Unis, **50 %** des PME ayant eu tout leur système d'information bloqué plusieurs semaines à la suite d'une attaque informatique (généralement un rançongiciel), auraient fait faillite dans les 6 mois ayant suivi. D'autres études sont plus pessimistes : **80 %** des entreprises ayant perdu leurs données informatiques suite à une cyberattaque font faillite dans les 12 mois, selon une étude menée en 2019 par l'assureur britannique Hiscox[1].

Ces cyberattaques, de plus en plus ciblées, sont de plus en plus coûteuses, bien que le ministère de l'Intérieur estime que : *« l'évaluation du coût de la cybercriminalité reste encore un exercice complexe et repose pour l'instant sur des études évaluatives ou des sondages »*, le coût global d'une attaque informatique « *ne pouvant être précisé immédiatement* »[2].

L'impact financier des incidents informatiques est encore **mal connu** des entreprises elles-mêmes et seules 43 % d'entre elles peuvent en dresser une évaluation. L'impact concret est mieux connu et 59 % des cyberattaques provoquent un ralentissement voire un arrêt de la production, ou une indisponibilité du site Internet, des retards de livraison, une perte de chiffre d'affaires.

Aux États-Unis, une étude réalisée par le Ponemon Institute[3] en 2018 a estimé que le coût moyen d'un détournement de données serait de l'ordre

---

[1] *Hiscox a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5,569 professionnels en charge de la stratégie de cybersécurité de leur entreprise ont été contactés (plus de 1 000 personnes par pays pour le Royaume-Uni, les États-Unis et l'Allemagne, plus de 500 pour la Belgique, la France, l'Espagne et les Pays-Bas et plus de 300 pour la République d'Irlande). Les répondants ont rempli le questionnaire en ligne entre le 24 décembre 2019 et le 3 février 2020.*

[2] *« L'état de la menace liée au numérique en 2019 ».*

[3] *Le Ponemon Institute a été fondé en 2002 par le Dr Larry Ponemon et Susan Jayson. L'Institut mène des études sur des problèmes critiques affectant la sécurité des actifs informationnels et de l'infrastructure informatique, notamment une étude annuelle sur le coût des violations de données parrainé par IBM et l'étude annuelle sur les tendances du chiffrement désormais parrainée par n-Cipher, société du groupe Entrust Datacard figurant parmi les leaders mondiaux sur le marché des modules de sécurité matériels (HSM).*

de **3,62 millions de dollars,** alors qu'une étude de 2016[1] l'avait évalué en moyenne à 330 000 euros pour une entreprise de 1 000 salariés ou moins, et 1,3 million d'euros pour une entreprise de plus de 5 000 salariés.

Dans son étude consacrée en 2020 à 1 971 sociétés qui ont subi des cyber-incidents et des failles dans le monde, l'assureur britannique Hiscox évalue le **coût médian à 51 200 €, soit près de six fois le coût observé en 2019** (9 000 €), avec un **coût total de 1,6 milliard € contre 1,1 milliard € en 2019,** et un **nombre de société attaquées près de 33 % supérieur.**

En France, l'IFOP a évalué, en novembre 2018[2], que ces cyberattaques avaient **un coût inférieur à 10 000 euros** pour **64 % d'entre elles,** mais que **pour 14 %** d'entre elles, il s'élevait à **plus de 50 000 euros.**

---

1 *« Brèches de sécurité - quel est le coût réel pour votre business ? », NTT Com Security, octobre 2016.*

2 *« Les PME face aux enjeux de sécurité informatique », Étude IFOP du 5 au 9 novembre 2018 de nature quantitative auprès de 702 décideurs, réalisée pour Kaspersky et Euler Hermes.*

Source : « Cyberattaque : quel coût pour une TPE / PME ? » ;
Astrid Marie Pirson, directrice technique de la souscription Hiscox, 21 juillet 2020

Si les faillites de PME liées à une cyberattaque sont très peu documentées[1], « *les petites entreprises, plus vulnérables, courent le risque de*

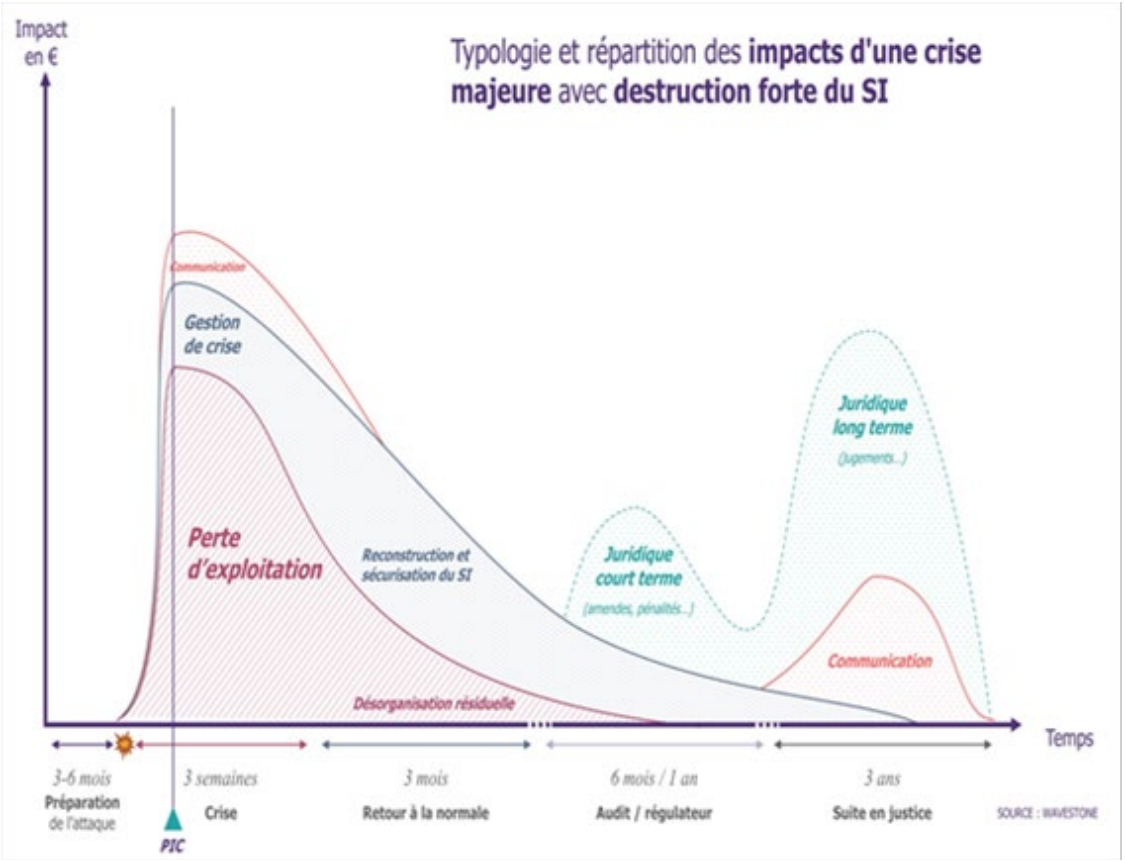
[1] *Selon le rapport Hiscox sur la gestion des cyber-risques, portant sur 8 pays en 2020 « Environ 63 % des entreprises de moins de dix salariés ont déclaré n'avoir subi aucun incident ni aucune faille. Toutefois, près de la moitié d'entre elles (49 %) n'ont pas de responsable de la cybersécurité et il pourrait ainsi y avoir des événements non pris en compte ». L'assureur a sollicité Forrester Consulting pour évaluer les capacités de gestion des cyber-risques des entreprises. Au total, 5 569 professionnels en charge de la stratégie de cybersécurité de leur entreprise ont été contactés (plus de 1 000 personnes par pays pour le Royaume-Uni, les États-Unis et l'Allemagne, plus de 500 pour la Belgique, la France, l'Espagne et les Pays-Bas et plus de 300 pour la République d'Irlande). Les répondants ont rempli le questionnaire en ligne entre le 24 décembre 2019 et le 3 février 2020. Le nombre de petites entreprises comptant moins de 250 salariés a été augmenté dans le panel, passant de 56 % à 60 %. Les entreprises de moins de neuf salariés représentent désormais 29 % du panel, contre 20 % l'an dernier. Les commerçants individuels représentent 10 % du total, contre 5 % l'an dernier. Les grandes (entre 250 et 999 salariés) et très grandes entreprises (1 000 salariés et plus) représentent toujours un total cumulé de 40 % du panel.*

subir des attaques et les moins bien préparées payent clairement le prix fort ».

Comme l'indique le schéma ci-dessus, au **coût direct** d'une cyberattaque s'ajoute le **coût indirect**, avec un délai de latence, qui déploie ses effets délétères parfois mortels pour l'entreprise.

« Les coûts engendrés par une crise cyber sont multiples, touchent de nombreuses dimensions et évoluent dans le temps. *Les enjeux financiers principaux de la vague initiale sont la perte d'exploitation dû à l'arrêt des systèmes, les frais de gestion de crise (expertise externe, mobilisation spécifique de collaborateurs, matériels, logiciels…), de communication et de gestion commerciale (communication interne ou avec les autorités, les clients, le grand public…). Les coûts engendrés par une crise cyber sont multiples, touchent de nombreuses dimensions et évoluent dans le temps. Dans les mois qui suivent, ces coûts de gestion de crise se transforment en coûts de désorganisation, par exemple dus à la perte d'efficacité du fait de systèmes non fonctionnels, de processus internes défaillants, de clients mécontents, puis en coûts de reconstruction et de sécurisation du système d'information.* ***Dans certains cas, en particulier pour les secteurs régulés ou si des données à caractère personnel ont été touchées, des coûts juridiques importants peuvent apparaître »[1].***

[1] *« Cybercrime : le ransomware, risque cyber numéro 1 », Gérôme Billois Partner cybersécurité et confiance numérique chez Wavestone et Marwan Lahoud, Président d'ACE Capital Partners, Blog de l'Institut Montaigne, 15 mars 2021.*



Source : « Cybercrime : le ransomware, risque cyber numéro 1 »,
Gérôme Billois Partner cybersécurité et confiance numérique chez Wavestone et
Marwan Lahoud, Président d'ACE Capital Partners,
Blog de l'Institut Montaigne, 15 mars 2021.

D. UNE PRISE DE CONSCIENCE INÉGALE DE LA CYBERMENACE

1. Un déni jusqu'en 2018 malgré les mises en garde

En 2018 encore, les entreprises françaises étaient dans le déni quant à l'importance et à l'impact du phénomène, constatait CCI France[1]. Une enquête[2] conduite auprès des dirigeants d'entreprises constatait que le thème de la cybersécurité « ***ne semble pas être à l'ordre du jour des inquiétudes des dirigeants*** » : 24 % d'entre eux déclarent que les risques liés à la cybersécurité de leur entreprise les préoccupent, soit un chiffre en recul de 16 points par rapport à octobre 2017, et 76 % se disent peu ou pas préoccupés.

---

1 *« Pérenniser l'entreprise face au risque cyber. De la cybersécurité à la cyberrésilience », CCI France, septembre 2020.*

2 *Grande consultation des entrepreneurs (enquête OpinionWay pour CCI France, La Tribune et Europe 1) effectuée, en partenariat avec cybermalveillance.gouv.fr, un focus sur la perception du risque cybersécurité dans les entreprises, en fonction de leur taille et de leur secteur d'activité.*

Néanmoins, les dirigeants de PME (entreprises de 10 salariés ou plus) étaient nettement plus conscients (62 % déclarant être préoccupés), que les dirigeants de TPE (0 à 9 salariés) se déclarant à 79 % peu ou pas préoccupés. La taille de l'entreprise joue donc un rôle considérable sur la perception du risque cyber par son dirigeant.

Seuls ces derniers ont été interrogés dans cette enquête. Ils ne se préoccupent du sujet qu'une fois l'entreprise victime ou qu'un incident leur a été remonté, ou estiment encore que « *la cybersécurité relève de la problématique technique et donc du ressort du DSI ou du RSSI (quand il y en a un) davantage que de la gouvernance de l'entreprise* ».

La forme de la cybercriminalité était également mal perçue : si les dirigeants identifiaient assez bien les menaces issues de malveillances, celles issues de la négligence des employés étaient totalement mésestimées.

La cybersécurité était, il y trois ans, loin d'être considérée comme « l'affaire de tous » et pour CCI France : « *les résultats de cette consultation ne prêtent pas forcément à l'optimisme. Ils montrent seulement qu'il reste beaucoup à faire en matière de pédagogie et de prévention en cybersécurité, et qu'une solution technologique n'apportera jamais de réponse parfaite à une problématique qui reste avant tout humaine* ».

Pourtant, **les parties prenantes du sujet de la cybersécurité** (ANSSI, AMRAE[1], fédérations professionnelles, prestataires de services informatiques et conseils spécialisés en risque cyber…) **ont multiplié les signaux d'alerte en direction des entreprises.**

DE MULTIPLES « WARNING » DE LA CYBERSÉCURITÉ EN 2017-2020 :

« La gestion du risque numérique en entreprise », AMRAE, février 2014 mise à jour janvier 2018 ;

« Guide d'hygiène informatique », publié en 2017, par l'ANSSI, proposant 42 mesures et ayant pour objectif d'accompagner les responsables de la sécurité des systèmes d'information ;

Lancement de la plate-forme « cybermalveillance.gouv.fr » le 30 mars 2017 par le groupement d'intérêt public ACYMA permettant d'apporter une assistance aux victimes de cyber-malveillance, et de sensibiliser le public aux enjeux de la sécurité et de la protection de la vie privée ;

MOOC « SECNUMACADEMIE », plate-forme de formation à la sécurité numérique de l'ANSSI, ouverte à tous et gratuite ;

Guide de sensibilisation de la FFA à destination des TPE/PME, « *Anticiper et minimiser l'impact d'un cyberrisque sur votre entreprise : TPE, PME, vous êtes concernées !* », publié en mai 2017 ;

[1] *Association pour le management des risques des assurances de l'entreprise.*

« *Le guide de la cybersécurité pour les experts-comptables* » mis en ligne en septembre 2018 par le Conseil supérieur de l'ordre des experts-comptables ;

« *Pérenniser l'entreprise face au risque cyber* », étude coproduite par la CCI Paris-Île-de-France et CCI France, septembre 2020 ;

Guide de cybersécurité à destination des dirigeants de TPE, PME et ETI de « bonnes pratiques et réflexes à adopter en cas de cyberattaques », rédigé par Bpifrance et Cybermalveillance.gouv.fr, mai 2021

2. Une prise de conscience en 2020

Avec les cyberattaques qui ont visé en 2020 et début 2021 des hôpitaux ou des centres de production de vaccins pendant la pandémie de la Covid-19, la cybersécurité est devenue un sujet grand public.

« *La prise de conscience du risque cyber commence à faire son chemin chez les dirigeants de TPE, PME et ETI* » ont constaté Bpifrance et Cybermalveillance.gouv.fr dans leur guide de mai 2021.

Les dirigeants d'entreprises intègrent désormais ce risque de façon croissante.

Selon le dernier panorama mondial des entreprises d'un assureur[1], **la part moyenne du budget informatique allouée à la cybersécurité a progressé de 63 % de 2020 à 2021 et les dépenses moyennes de cybersécurité ont plus que doublé en deux ans**, passant de 1,31 millions (2019) à 1,84 millions (2020) puis 2,95 millions (2021).

Dans une étude[2] sur la cybersécurité des « grosses » PME, de 250 à 500 salariés, en mai 2020, CISCO[3] a souligné qu'elles étaient presque aussi nombreuses à révéler des violations de données que les grandes entreprises (59 % contre 62 %) et a estimé qu'elles avaient renforcé leur sécurité puisque si 40 % des PME avaient subi « *une interruption de plus de huit heures suite à leur faille de sécurité la plus importante* » en 2018, elles n'étaient plus que 24 % en 2020. Elles sont 94 % à actualiser régulièrement ou constamment les infrastructures de cybersécurité, 72 % à effectuer des chasses aux menaces[4],

---

1 *Rapport Hiscox sur la gestion des cyber-risque, du 17 avril 2021 : https://www.hiscox.fr/courtage/sites/courtage/files/documents/21486%20-%20Hiscox%20Cyber%20Readiness%20Report%202021%20-%20France.pdf*

2 *« Dix mythes non justifiés sur la cybersécurité des PME ». https://www.cisco.com/c/dam/global/fr_fr/products/security/pdf/2020_cisco_smb-cybersecurity-report_fr.pdf*

3 *Fondée en 1984, cette entreprise informatique américaine était spécialisée, à l'origine, dans le matériel réseau (routeurs et commutateurs ethernet), et depuis 2009 dans les serveurs. Elle a renforcé ses activités dans la sécurité informatique après 2015.*

4 *Le « Threat Hunting » est un exercice de sécurité proactif qui vise à trouver et à déloger les attaquants qui ont pénétré un système informatique sans déclencher d'alerte.*

et elles testent régulièrement leur plan de réponse aux incidents[1]. Elles forment et sensibilisent massivement (à hauteur de 84 %) leurs salariés, et ce de manière obligatoire.

Cependant, **d'autres études[2] relativisent cette prise de conscience**. La cybersécurité resterait un sujet exclusivement **technique** et n'intéresserait les dirigeants que lorsqu'il est **trop tard**.

Si 82 % des dirigeants métiers ou IT en entreprise estiment que les cyber-menaces se sont aggravées au cours des deux dernières années, la cybersécurité reste un sujet exclusivement (21 % des répondants) ou principalement (41 %) du ressort de la DSI. Si 85 % des répondants estiment que les conseils d'administration se préoccupent davantage de cybersécurité qu'il y a deux ans, c'est uniquement lorsqu'il y a un important incident (comme une grosse fuite de données). 11 % voient encore la cybersécurité comme une question de conformité réglementaire ! Seuls 15 % des dirigeants admettent qu'il existe un impact technique et économique du sujet et 4 % comme un sujet essentiellement économique.

Seulement 44 % des répondants ont constaté un intérêt du conseil d'administration pour les exercices de cybersécurité. Toutefois, les cadres dirigeants s'intéressent davantage à la cybersécurité : très fortement pour 58 % des répondants, de façon appropriée pour 31 %. De même, les décisions stratégiques tiennent fortement (57 %) ou réellement (34 %) compte de la cybersécurité.

Il est avéré en tout état de cause que **la cybersécurité varie de façon décroissante selon la taille de l'entreprise, pour des raisons de coûts, de temps et de ressources humaines.**

« *Pour autant, peu d'actions concrètes sont mises en œuvre pour prévenir le risque cyber au sein de leur entreprise* », constate, en mai 2021, Bpifrance et Cybermalveillance.gouv.fr, qui pointent trois causes :

- « *une connaissance superficielle du risque cyber qui les conduit souvent à mésestimer les enjeux et à déléguer à leur équipe informatique considérant qu'il ne s'agit que d'un problème technique* ». Quand ils en ont conscience, les dirigeants ont tendance à se focaliser sur la menace externe émanant de groupes de cybercriminels motivés par l'argent, alors que les menaces externes issues de l'environnement de l'entreprise (fournisseurs, clients, partenaires) et internes (employés, consultants, etc.) sont nettement sous-estimées ;

---

[1] *45 % tous les six mois, 36 % tous les ans, 12 % tous les deux ans. Par ailleurs 56 % des PME appliquent des correctifs chaque jour ou chaque semaine comme 58 % des grandes entreprises.*

[2] *L'étude « Cybersecurity in the C-suite and Boardroom » réalisée par le cabinet ESG (Enterprise Strategy Group) sur la commande de Trend Micro, est basée sur une enquête réalisée en ligne auprès de 365 cadres dirigeants métiers ou IT de tous secteurs d'entreprises situées en Amérique du Nord (États-Unis et Canada) ou en Europe de l'Ouest (Royaume-Uni, France et Allemagne) entre le 28 septembre 2020 et le 24 octobre 2020.*

- « *le manque de solutions clé-en-main et une offre cyber qui est orientée vers des grands groupes* », les solutions disponibles sur le marché n'étant pas toujours bien adaptées aux dirigeants de PME et ETI qui ont du mal à se les approprier ;
- « *le coût perçu d'un investissement en cybersécurité joue un rôle dissuasif* » alors que la perte de valeur en cas d'attaque peut se révéler bien plus élevée.

3. Un enjeu majeur de la responsabilité de l'entreprise

a) La cybersécurité dans la notation financière

Les grandes agences de notation américaines intègrent le risque cyber dans leur notation financière. Dans un communiqué du 24 novembre 2015, Moody's prévenait que : « *nous n'intégrons pas explicitement le risque de cyberattaques dans notre analyse de crédit en tant que principal moteur de notation. Mais dans tous les secteurs, notre analyse fondamentale du crédit comprend de nombreux scénarios de tests de résistance, et un cyber-événement, comme d'autres risques d'événements, pourrait être le déclencheur de ces scénarios de crise. La gravité et la durée d'un cyber-événement réussi seront essentielles pour déterminer tout impact de crédit* »[1].

Cette position de Moody's intervenait après qu'une autre agence de notation, Standards & Poors, ait publié en septembre 2015 un rapport contenant un avertissement similaire pour le secteur bancaire : « *S&P pourrait émettre une révision à la baisse si une banque semblait mal préparée à faire face à une cyberattaque ou à la suite d'une violation causant des dommages importants à la réputation d'une banque ou entraînant des pertes financières substantielles ou des dommages juridiques* »[2].

Un marché de la cybernotation s'est développé, dominé par des agences américaines. La plus importante des agences de notation spécialisées qui se sont créées après 2015 est Bitsight, devant SecurityScoreCard. En France, la start-up Cyrating, incubée à ParisTech Entrepreneurs, créée en 2018, est la première agence européenne de notation.

La notation en matière de cybersécurité rencontre toutefois certaines limites et participe à l'affaiblissement de la souveraineté économique.

---

[1] « *Moody's Warns Cyber Risks Could Impact Credit Ratings. Stresses the Importance of Defenses, as Well as Breach Prevention Response* », *Marianne Kolbasuk McGee, Bank Info Security, 24 novembre 2015.*

[2] « *S&P's Cybersecurity Warning: Late to the Game Rating Agency Threatens to Downgrade Banks Over Security Shortcomings* », *Mathew J. Schwartz, Bank Info Security, 30 septembre 2015.*

Conformité et sécurité ne vont pas nécessairement de pair. Une organisation peut être conforme sans pour autant atteindre un niveau de sécurité satisfaisant. Aborder la sécurité uniquement à travers le prisme de la conformité à des normes peut avoir pour objectif premier de se couvrir jurdiquement. La notation s'appuie presque intégralement sur des analyses de vulnérabilités, sans tenir compte du contexte spécifique de l'entreprise et de son exposition aux risques. L'approche par les risques, individualisée, **couplant audit interne et externe, reste donc indispensable** et permettra de combiner une analyse précise des vulnérabilités techniques mais aussi humaines et organisationnelles de l'organisation et une vision à 360° du contexte externe (menaces).

La notation peut être, dans certains cas, contre-productive pour l'entreprise : « *mal comprise, une bonne note donne un faux sentiment de sécurité au COMEX n'aidant pas le directeur de la sécurité de l'information à obtenir le budget nécessaire au maintien de son SMSI (Système de Management de la Sécurité de l'Information). À l'inverse, une mauvaise note orientera les budgets vers un projet permettant de paraître plus sécurisé. L'effet pervers serait la priorisation de la protection des systèmes informatiques au détriment de la protection de l'information* »[1].

Les évaluations effectuées par les algorithmes utilisés par ces agences peuvent également susciter la **méfiance**. Ces notations peuvent être perçues comme très **intrusives** par les entreprises qui, en règle générale, ne peuvent pas refuser d'être notées. Avoir la capacité d'influencer le classement des entreprises signifie potentiellement pouvoir influencer le choix d'un prestataire. « *La domination du marché de la conformité par des agences américaines place celles-ci en position d'arbitre leur permettant de collecter et de traiter des données sensibles sur les entreprises non américaines* »[2].

Or, comme le prédisait dès le 27 décembre 2017 la CCI des Hauts-de-France, « ***tôt ou tard, toutes les entreprises auront des notations sur leur sécurité informatique*** »[3]**.**

b) La cybersécurité comme élément de responsabilité numérique des entreprises

Outre la notation financière, la notation ESG (environnement, société, gouvernance) **comporte également une référence à la cybersécurité, qui constitue une dimension essentielle de la gouvernance de l'entreprise** mais également de **la responsabilité sociétale** des entreprises sous l'angle de la protection contre le vol des données. Le cyberrisque était la principale

---

1 *« L'autonomie stratégique face au cyber-rating », École de Pensée sur la Guerre Économique, Jean-Michel Barbier, 8 juin 2020.*

2 *Observatoire du monde cybernétique, Lettre n°61, avril 2017.*

3 *https://hautsdefrance.cci.fr/actualites/cybersecurite-tot-tard-serez-notes/*

préoccupation ESG des investisseurs institutionnels en 2019[1]. Les entreprises qui s'adaptent constamment à l'évolution des cyberattaques et qui veillent à rendre compte de leurs efforts aux investisseurs se démarqueront dans un contexte où les investisseurs sont de plus en plus soucieux des questions de cybersécurité.

Alors que la cybersécurité est créatrice de valeur en ce qu'elle créée pour l'entreprise des externalités positives, celles-ci et « *en particulier les TPE et les PME, ont encore du chemin à parcourir pour dépasser la conformité et la lier à leur engagement sociétal global* » a ainsi constaté la Plateforme RSE[2] dans son rapport de juillet 2020 proposant de créer une « *responsabilité numérique de l'entreprise* » (RNE), s'intégrant dans la responsabilité sociétale de l'entreprise (RSE). Les fonds d'investissement et les banques ont un alignement d'intérêt à ce que les entreprises qu'ils financent soient matures en termes de cybersécurité de manière à préserver les sommes investies.

La transformation numérique qui impacte, aujourd'hui, toutes les entreprises, demeure peu intégrée dans les enjeux de la RSE – et inversement – et les deux mondes s'ignorent encore. Pourtant, la protection des données devrait s'inscrive comme un critère supplémentaire de la politique RSE. **La responsabilité numérique est un risque qui doit s'intégrer dans le référentiel RSE existant**. La Plateforme RSE préconise, à cet effet, d'inclure « *pour les entreprises concernées, dans leurs déclarations de performance extra-financière des indicateurs portant sur leurs politiques de protection des données* ».

Aller au-delà semble prématuré. En effet, une notation publique, par exemple lors de l'annonce d'une levée de fonds, au moment où l'entreprise dispose de trésorerie, accroîtrait le risque d'une cyberattaque. Comme le souligne Bpifrance : « *il serait dangereux pour une entreprise de publier un score de cybersécurité faible dans le cadre d'une DPEF[3] car cela en ferait une cible de choix pour les cybercriminels* »[4].

4. Un enjeu d'harmonisation européenne

L'inclusion de la cybersécurité dans la notation financière des entreprises nécessite une harmonisation de leur certification.

Pour assurer la sécurité de leurs informations sensibles, les entreprises peuvent s'appuyer sur la famille de normes ISO/IEC 27000.

---

1 *Sondage auprès de 800 entreprises sur les placements responsables effectué en 2019 par RBC, la Banque Royale du Canada.*

2 *La Plateforme nationale d'actions globales pour la responsabilité sociétale des entreprises (Plateforme RSE) réunit depuis 2013 les parties prenantes de la RSE en France : entreprises, partenaires sociaux, organisations de la société civile, réseaux d'acteurs, chercheurs et institutions publiques.*

3 *Déclaration de performance extra-financière.*

4 *Réponse au questionnaire de la Délégation aux entreprises du Sénat, 1er juin 2021.*

ISO/IEC 27001, norme la plus connue de cette catégorie qui n'en compte pas moins d'une douzaine, spécifie les exigences relatives aux systèmes de management de la sécurité des informations (SMSI). Elle vient d'être récemment complétée, en février 2021, par la spécification technique ISO/IEC TS 27110, « *Sécurité de l'information, cybersécurité et protection de la vie privée – Lignes directrices relatives à l'élaboration d'un cadre en matière de cybersécurité* », élaborée en collaboration avec la Commission électrotechnique internationale (IEC), pour « *créer, ou perfectionner, un système de protection robuste contre les cyber-attaques* ».

Ces référentiels privés permettent aux entreprises d'obtenir une certification publique de cybersécurité.

Le règlement européen du 17 avril 2019, intitulé « *Cybersecurity Act* »[1], marque une véritable avancée pour l'autonomie stratégique européenne avec la définition d'un **cadre européen** de certification de cybersécurité, essentiel pour renforcer la sécurité du marché unique numérique européen. En effet, à l'heure actuelle, la certification de cybersécurité relève strictement des autorités nationales qui peuvent exister ou non au sein des pays de l'Union, sans qu'aucun cadre européen n'établisse d'exigences minimales. En France, la certification de sécurité des produits dans ce domaine est réalisée sous l'autorité de l'ANSSI[2].

LA CERTIFICATION FRANÇAISE EN MATIÈRE DE CYBERSÉCURITÉ

« Le schéma français offre deux types de certification, une certification de sécurité de premier niveau (CSPN) et une certification dite « critères communs » (CC). Tandis que la certification CC répond à un standard international doté de sept niveaux d'assurance de plus en plus élevés, la certification CSPN a été élaborée par l'ANSSI pour fournir une solution de certification répondant à un risque plus modéré, et mettant en jeu une évaluation moins exhaustive.

Ces deux types de certification engagent notamment le type de laboratoire d'analyse technique, nommé Centre d'évaluation de la sécurité des technologies de l'information (CESTI), qui pourra mener l'évaluation. Pour une évaluation CC, le CESTI devra avoir été lui-même accrédité par le Comité français d'accréditation (le Cofrace) à l'aune de standards internationaux, et agréé par l'ANSSI. Pour une évaluation CSPN, le laboratoire devra simplement bénéficier d'un agrément de l'ANSSI.

L'ANSSI exerce un contrôle continu sur les évaluations. Si ce contrôle est gratuit, les

---

[1] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité)*

[2] *Voir sur ce sujet le rapport d'information de la commission des affaires européennes du Sénat n° 458 (session ordinaire 2017-2018) du 20 avril 2018 sur la cybersécurité dans l'Union européenne, de M. René Danesi et Mme Laurence Harribey.*

frais d'évaluation d'un produit par un CESTI sont à la charge du commanditaire de l'évaluation. Il convient de souligner que dans d'autres pays, comme en Allemagne, le contrôle par l'autorité nationale (en l'occurrence, le BSI) peut entraîner des frais ».

Source : rapport d'information de la commission des affaires européennes de l'Assemblée nationale, n°2415 du 14 novembre 2019, sur l'avenir de la cybersécurité européenne, de M. Éric Bothorel.

E. UNE COURSE DE VITESSE ENTRE CYBERATTAQUE ET CYBERPROTECTION

En Europe, plus de neuf entreprises sur dix utilisent une mesure de cyberprotection mais une sur deux n'a pas de solution satisfaisante pour la protection des données.

Une étude conduite par Dell en 2019[1] souligne que cette protection est faible même si elle recourt à l'IA (64 %), aux applications natives au *cloud* (60 %) ou à des applications *Software as a Service* (SaaS).

Une étude récente[2], conduite en avril 2021, a souligné que si neuf entreprises sur dix estiment qu'il est essentiel de se prémunir contre les attaques informatiques, **une entreprise sur deux ne sécurise pas ses postes de travai**l et **une sur trois n'utilise même pas d'antivirus. La prise de conscience ne se concrétise pas encore par une prévention efficace, le budget** alloué à la cybersécurité ne dépassant pas **1 000 euros** par an pour **six entreprises françaises sur dix.**

Selon Eurostat[3], la mesure de cybersécurité la plus couramment utilisée par les entreprises européennes est la mise à jour des logiciels ou des systèmes d'exploitation (87 %), suivie de l'authentification par mot de passe fort (76 %), de la sauvegarde des données dans un lieu ou un nuage séparé (76 %) et du contrôle d'accès au réseau (65 %). Moins de la moitié des entreprises ont déclaré conserver des fichiers journaux pour analyse après un incident de sécurité (45 %) et utiliser un réseau privé virtuel (VPN) (42 %). Les entreprises ont moins souvent utilisé des techniques de cryptage pour les données, les documents ou les courriers électroniques (38 %), des tests de sécurité (35 %), l'évaluation des risques (33 %) et l'identification et l'authentification des utilisateurs par des méthodes biométriques (10 %).

---

[1] https://www.delltechnologies.com/en-us/collaterals/unauth/infographic/products/data-protection/global-data-protection-index-2020-snapshot.pdf

[2] *Étude menée entre le 31 mars et le 2 avril 2021 par l'Ifop pour la société de conseil en cybersécurité F-Secure auprès d'un échantillon national représentatif de 500 "professionnels". 75 % des entreprises interrogées avaient moins de 10 salariés.*

[3] *Eurostat (2020), « ICT Security in Entrerprises », étude citée par le rapport de la Plateforme RSE sur la Responsabilité numérique des entreprises.*

Or, le niveau de cybersécurité des entreprises doit être rapidement et fortement augmenté avant l'arrivée de l'internet des objets (IoT)[1], qui va étendre de façon exponentielle la surface d'exposition au cyberrisque, **et de l'ordinateur quantique**[2] qui va démultiplier les capacités d'intrusion.

Les questions d'interopérabilité, de sécurité et de pérennité des équipements, ajoutées à la crise sanitaire et aux difficultés de production et d'approvisionnement qu'elle a engendrées, ont provoqué un ralentissement du déploiement des objets connectés qui devaient être 50 milliards en 2020, alors que l'on en dénombre 9,4 milliards aujourd'hui.

Toutefois, de plus en plus d'objets, d'appareils et de périphériques sont connectés à internet : webcams, installations de traitement de l'eau, alarmes, éoliennes, lecteurs de plaques d'immatriculation, téléviseurs intelligents, installations industrielles sensibles telles que des centrales électriques, raffineries, ou encore des réacteurs nucléaires...

Avec ce déploiement, **les cybercriminels auront une infinité de possibilités d'infecter les systèmes via les objets connectés**, comme l'a montré l'attaque conduite dès 2016 aux États-Unis contre *DYN Managed DNS*[3], au moyen notamment d'un code source mis à disposition en ligne. Plus de 100 000 objets connectés ont été infectés, dont des caméras publiques dont le contrôle avait été pris à distance par le logiciel malveillant nommé *MIRAI*.

En 2017, à la sortie de l'iPhone X, Apple se vantait d'avoir créé un système de reconnaissance faciale extrêmement robuste. Une semaine plus tard, et pour un coût ne dépassant pas les 150 $, une entreprise de cybersécurité vietnamienne *Bkav* réussissait à créer un masque capable de duper l'application…

Cependant, face à ce déploiement, **l'Intelligence Artificielle** (IA) pourrait changer la donne en matière de cybersécurité en analysant des quantités massives de données sur les risques afin d'accélérer les temps de réponse et de renforcer les opérations de sécurité qui resteront toujours sous-dimensionnées en ressources humaines ou technologiques. Des sociétés, comme IBM avec *IBM QRadar® Advisor with Watson*, proposent déjà des solutions d'informatique cognitive, un type avancé d'intelligence artificielle. Celles-ci tirent parti de diverses formes d'intelligence artificielle, y compris

---

[1] *Décrits dans la note scientifique n°1 de l'Office parlementaire d'évaluation des choix scientifiques et technologiques de mars 2018 : https://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2018_0013_note_objets_connectes.pdf*

[2] *Décrit dans la note scientifique n°15 de l'Office parlementaire d'évaluation des choix scientifiques et technologiques de juillet 2019 : http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2019_0069_note_ordinateurs_quantiques.pdf*

[3] *Service informatique de l'entreprise informatique américaine éponyme.*

les algorithmes d'apprentissage automatique et les réseaux d'apprentissage en profondeur, qui deviennent plus forts et plus intelligents au fil du temps.

Or, **IA et sécurité des données doivent être rendues compatibles**. En effet, « *lancées dans une course effrénée de développements de nouveaux produits, services ou fonctionnalités, les entreprises peuvent juger le déploiement d'outils sécuritaires comme une perte de temps et une source de coût à court terme voire même les considérer comme un obstacle à l'utilisation de techniques de machine learning ou d'Intelligence Artificielle, ceux-ci nécessitant d'accéder à de grands volumes de données* »[1]. Le chiffrement de bout-en-bout, grâce auquel les données ne peuvent être lues que par l'expéditeur et le destinataire de l'information, s'il rend illisible les informations, et renforce la sécurité, interdit également toute possibilité d'exploiter ces données ou même de lancer une recherche sur celles-ci. Les entreprises ne peuvent donc plus utiliser ces technologies indispensables à leur compétitivité et leur rapidité de commercialisation des offres.

Malheureusement, l'**IA est également utilisée par les cybercriminels**. En mars 2019, une entreprise allemande s'est fait dérober 220 000 euros en étant dupée par une voix artificielle imitant celle de son dirigeant, lui demandant d'effectuer un virement sur le compte d'un fournisseur hongrois. L'interlocuteur aurait en réalité été une voix synthétique, créée par un logiciel de génération de voix basé sur l'Intelligence Artificielle.

Plusieurs autres formes de ***Deepfake***[2] peuvent être ainsi utilisées dans le cadre de cyberattaques visant les entreprises comme le *face-swapping*, qui remplace dans une vidéo le visage d'une personne par celui d'une personne ciblée à partir de sa photo ; le *deepfake lip-synching*, qui, dans une vidéo, adapte les mouvements du visage d'une personne ciblée à partir d'un fichier audio d'une autre personne et permet de lui faire prononcer le discours contenu dans le fichier audio en question sans qu'elle ne l'ait prononcé ; le *deepfake puppetry*, qui génère une vidéo d'une personne ciblée à partir d'une vidéo d'acteur fournie en entrée, créant une vidéo dans laquelle la cible reproduit un discours joué par l'acteur[3].

Ces techniques sont **à la portée de tous** car le boom du *Machine Learning* conduit à la fois à des algorithmes de plus en plus performants,

---

[1] *« Peut-on concilier IA et sécurité des données ? », Timothée Rebours, ZDNet, 12 mars 2021.*

[2] *Mot-valise formé à partir de* deep learning *(« apprentissage profond ») et de* fake *(« faux »), c'est une technique de synthèse multimédia reposant sur l'intelligence artificielle. Elle peut servir à superposer des fichiers audio ou vidéo existants sur d'autres fichiers vidéo (par exemple le changement de visage d'une personne sur une vidéo) ou audio (par exemple reproduire la voix d'une personne pour lui faire dire des choses inventées). Cette technique peut être utilisée pour créer des infox et des canulars malveillants.*

[3] *Un exemple célèbre de cette technique est une vidéo de Barack Obama énonçant un discours simulé par Jordan Peele, dans laquelle la gestuelle de l'ancien président est reproduite de manière extrêmement réaliste.*

mais également à une généralisation de l'accès à ces algorithmes, à l'instar d'applications grand public comme Lyrebird (application gratuite de *Deepfake audio*) ou Zao (application chinoise de *face-swapping* commercialisée durant l'été 2019). Ces applications, créées dans un objectif de divertissement, représentent un nouvel outil performant, accessible et facile d'utilisation pour des cybercriminels.

« *Il ne fait aucun doute que les attaques utilisant ce type d'applications augmenteront dans les prochaines années. Fraude au président, atteinte à l'image, création de fausses preuves juridiques, contournement d'authentification biométrique : les cas d'usages envisageables sont nombreux et effrayants* », prédit Wavestone[1].

[1] *Dans son étude de 2019 : « Intelligence Artificielle et cybersécurité : protéger dès maintenant le monde de demain ».*

II. UN ÉTAT CONSACRANT DES MOYENS INSUFFISANTS À LA CYBERSÉCURITÉ DES TPE ET PME

A. UN DISPOSITIF RÉGALIEN DE CYBERPROTECTION COMPLEXE

Un récent rapport d'information[1] fait au nom de la commission des affaires européennes et de la commission des lois du Sénat, du 9 juillet 2020, a présenté le dispositif de lutte contre la cybercriminalité.

1. Un dispositif de lutte contre la cybercriminalité à la recherche d'une constante coordination

En France, l'accès au dispositif public s'effectue par **cybermalveillance.gouv.fr** qui a enregistré **en 2020** une hausse de fréquentation de **+ 155 %,** toutes victimes confondues. Parmi elles, ce sont plus de **10 000 entreprises** qui sont venues y chercher de l'assistance à la suite d'une attaque. Ce dispositif est pour l'instant **peu connu de la grande majorité des entreprises.**

Il vient compléter **PHAROS** (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), site web créé en 2009 par le Gouvernement pour permettre aux internautes de signaler des contenus et comportements illicites repérés en ligne et qui s'adresse au grand public, et le site **Signal Spam**, pour les pourriel (spam).

Derrière ce **guichet unique**, interviennent ensuite plusieurs acteurs publics :

- Au sein de la gendarmerie, le **centre de lutte contre les criminalités numériques** (C3N) est chargé de piloter la lutte contre la cybercriminalité ;
- Au sein de la direction centrale de la police judiciaire (DCPJ) du ministère de l'intérieur, a été créée une **sous-direction en charge de la lutte contre la cybercriminalité** (SDLC) ;
- À la préfecture de police de Paris, existe également une unité de police judiciaire spécialisée dans la lutte contre la cybercriminalité : la **Brigade de lutte contre la cybercriminialité** (BL2C) -ancienne brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI)- compétente pour les affaires relevant de l'accès ou du maintien frauduleux dans un système de traitement automatisé des données (STAD).

Aux côtés de ces trois acteurs, la cellule **Cyberdouane** de la direction nationale du renseignement et des enquêtes douanières (DNRED), le service de traitement du renseignement et d'action contre les circuits financiers

---

[1] *Rapport n°613 (2019-2020) de Mme Sophie Joissains et M. Jacques Bigot.*

(**Tracfin**) et le **service national des enquêtes** (SNE) de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) du ministère de l'Économie peuvent être saisis de dossiers en lien avec la cybercriminalité.

Au sein du ministère de la Justice enfin, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris disposent d'une **compétence concurrente nationale**[1] en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et d'atteintes aux intérêts fondamentaux de la Nation (ce qui peut couvrir des hypothèses de cyber-sabotage). Cette juridiction nationale chargée de la lutte contre la criminalité organisée (**JUNALCO**) est confiée, au sein du parquet, à la **section J3**.

Les rapporteurs et le président de la Délégation aux entreprises du Sénat se sont successivement rendus dans les locaux du C3N le 13 avril, de la SDLC et du BL2C le 28 avril.

Ce dispositif public, éclaté et difficile à lire pour les entreprises, présente certaines caractéristiques originales :

- **Un équilibre entre centralité de la compétence technique et la proximité**, avec la possibilité de déposer plainte dans les gendarmeries et commissariats dans les territoires, malgré l'absence de dépôt de plainte en ligne (le projet Thésée du ministère de la Justice n'étant pas encore opérationnel). **Le projet de création de CERT[2] régionaux va dans le bon sens car il faut des capteurs de terrain** ;
- **Une répartition originale des compétences police-gendarmerie non en fonction de la localisation de l'infraction (critère territorial) mais en fonction de la famille de cyberattaque (de rançongiciel) à traiter (critère fonctionnel) :** c'est en effet le Parquet (la section J3) qui répartit le traitement des plaintes entre le C3N, l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), et la Sous-direction de lutte contre la cybercriminalité de la police nationale et dispose de la Brigade de Lutte contre la Cybercriminalité (BLCC) de la Préfecture de police de Paris (qui conserve toutefois une compétente territoriale, pour Paris et petite couronne : 75, 92, 93 et 94). Cette répartition des compétences par famille de

---

1 *Depuis la loi n°2019-222 du 23 mars 2019 et la circulaire du 17 décembre 2019.*

2 *Un **CERT (Computer Emergency Response Team)**[2] a pour tâches la centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ; le traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques ; l'établissement et la maintenance d'une base de données des vulnérabilités ; la prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ; la coordination éventuelle avec les autres entités : opérateurs et fournisseurs d'accès à Internet, CERT nationaux et internationaux.*

cyberattaque impose une **neutralité de la taille de l'entreprise**, qu'elle soit une TPE, une PME ou une grande entreprise, dans le traitement judiciaire de la cyberattaque ;

- **Une coopération européenne qui fonctionne bien** et qui permet la création d'équipes communes d'enquête (ce qui ne serait pas possible en France, faute de cadre juridique de partage de l'information), ainsi qu'une **coopération public–privé,** avec les opérateurs privés numériques (via le CLUSIF ou le CESIN). La DCPJ a signé récemment, le 13 janvier 2021, une convention de partenariat avec le cabinet de conseil Wavestone[1], afin de partager l'information à des fins de prévention comme de remédiation. De même, la Direction générale de la sécurité intérieure (DGSI) travaille depuis 2015 avec la startup Palantir[2] afin d'établir une cartographie des réseaux criminels et terroristes, bien qu'une alternative française soit possible selon Thalès[3] ;
- **Une capacité de projection de forces d'intervention sur le terrain** à même de rassurer un dirigeant d'entreprise qui « *ne comprend pas ce qui lui arrive* », est confronté à un « *ennemi invisible* ». La priorité d'une PME attaquée n'est pas de déposer plainte, « *compte-tenu de l'état de sidération de la victime* », qui, le plus souvent, ignore les compétences numériques de la Gendarmerie. L'expertise numérique acquise par la Gendarmerie change son image auprès des dirigeants d'entreprise lorsqu'ils se rendent compte qu'elle est capable de les aider à sauver leur entreprise.

---

[1] *Cabinet de conseil indépendant, le cabinet Wavestone accompagne les entreprises et administrations dans la sécurisation de leur transformation numérique depuis les phases stratégiques, jusqu'à la déclinaison opérationnelle et dispose de 600 consultants répartis dans le monde. Il propose également des prestations de réponse en urgence à incidents de sécurité et de gestion de crises en cas de cyberattaques. À cette fin, il a mis en place un centre de réponse à incident, pôle d'expertise dans la lutte contre la cybercriminalité : le CERT-Wavestone (CERT-W) alliant expertises fonctionnelles, sectorielles et techniques, première, et actuellement la seule équipe en France ayant reçu la qualification de* « Prestataire de Réponse à Incident de Sécurité (PRIS) » *délivré par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) décision n°1443 du 29/06/2020. D'autres sont en cours de qualification : Airbus CyberSecurity SAS, AMOSSYS, Capgemini Technology Services / Sogeti ESEC, Intrinsec, LEXFO, Orange Cyberdéfense, THALES SIX GTS France SA.*

[2] *La société fondée en 2004 par Peter Thiel, cofondateur de PayPal et conseiller de Donald Trump, Alex Karp et Nathan Gettings, entrée à la Bourse de New York fin septembre 2020 et valorisée à près de 13 milliards d'euros, est un partenaire stratégique du gouvernement américain (NSA, CIA, FBI, forces armées...). Dès sa création, le fonds d'investissement de la CIA, In-Q-Tel, a investi deux millions de dollars dans la start-up. Son logiciel d'analyse de données est développé à partir d'un outil utilisé par PayPal pour détecter les flux financiers douteux.*

[3] *« Une alternative française au logiciel d'analyse de données de Palantir est possible, d'après Thales », Alice Vitard, L'Usine digitale, 26 octobre 2020.*

2. Une justice trop démunie face à une cybercriminalité industrialisée

À l'issue des déplacements et des auditions effectuées par la Délégation aux entreprises du Sénat, et notamment de sa table-ronde du 15 avril 2021, , **plusieurs enseignements peuvent être soulignés.**

Il est indispensable de renforcer les moyens humains et budgétaires. Le pôle du Parquet avec trois magistrats mériterait notamment d'être étoffé. Paradoxalement, ce n'est **pas une solution suffisante** car « *les cybercriminels pourraient noyer la procédure judiciaire en lançant 10 000 attaques quotidiennes nécessitant autant d'actes d'instruction judiciaire* ».

Un exemple des **limites actuelles des outils juridiques pour lutter efficacement contre la cybercriminalité** est l'affaire Vinnik. Ce dernier n'a pu être condamné que sur le fondement d'incriminations classiques.

RANÇONGICIEL LOCKY : VINNIK RELAXÉ DES FAITS DE CYBERCRIMINALITÉ MAIS CONDAMNÉ POUR BLANCHIMENT

« *Le tribunal correctionnel de Paris a relaxé lundi Alexander Vinnik des faits de cybercriminalité liés au rançongiciel Locky mais l'a condamné pour blanchiment organisé à cinq d'emprisonnement et 100 000 € d'amende. Le parquet avait requis dix ans et 750 000 €.*

Dossier emblématique de la section cybercriminalité du parquet de Paris, le dossier Locky, du nom de ce rançongiciel qui a fait plus de 5 000 victimes dans le monde entre 2016 et 2018, vient d'être au trois quarts balayé par la 13e chambre du tribunal correctionnel de Paris. L'unique prévenu de cette affaire, Alexander Vinnik, un Russe de 41 ans, a été relaxé de treize des quatorze chefs de prévention.

Si, lors du procès, le ministère public l'a dépeint comme le « chef d'orchestre » de ce rançongiciel, le tribunal semble l'avoir plutôt considéré comme un deuxième, si ce n'est un troisième soliste. Quant aux autres membres de l'orchestre, personne ne connaîtra leur partition, l'enquête ne les ayant jamais identifiés.

Le tribunal n'a donc pas retenu l'extorsion de fonds en bande organisée, l'association de malfaiteurs et toutes les infractions liées à la cybercriminalité comme l'accès frauduleux dans tout ou partie d'un système de traitement automatisé de données.

En revanche, ce citoyen russe de 41 ans est condamné pour blanchiment en bande organisée commis entre le 1er janvier 2016 et le 25 juillet 2017, le tribunal considérant qu'il y avait « suffisamment d'éléments à charge en procédure » montrant son implication dans des opérations de blanchiment « des sommes issues des infractions au rançongiciel Locky » via la plateforme de cryptomonnaie Btc-e.

Apparu en 2016, le rançongiciel Locky a touché près de 5 700 personnes dans le monde, dont 183 en France. Une pièce jointe était adressée par mail à des particuliers, des entreprises ou collectivités locales. Une fois ouverte, le logiciel malveillant cryptait les données informatiques. En échange d'une rançon payable en bitcoin, les victimes recevaient une clé de déchiffrement permettant de récupérer les données.

Les rançons ont alimenté plusieurs comptes avant d'en abonder deux autres sur la plateforme Btc-e liés à Alexander Vinnik. Ces fonds en bitcoin ont ensuite été convertis en monnaie fiduciaire avant de disparaître dans la nature. Selon l'accusation, l'enquête aurait permis d'établir qu'Alexander Vinnik aurait reçu 76 % des rançons payées par l'ensemble des victimes de ce rançongiciel, soit un peu plus de huit millions de dollars.

Cette plateforme a été fermée le 15 juillet 2017 à la demande des autorités américaines, le jour de l'interpellation en Grèce de M. Vinnik qui y passait des vacances en famille. Il a été remis à la France en janvier 2020.

Le tribunal a condamné M. Vinnik à verser près de 35 000 € de dommages et intérêts à sept parties civiles et en a débouté dix-neuf autres. Sa défense réfléchit à un appel. Tout comme le parquet de Paris ».

Source : Dalloz actualité, Pierre-Antoine Souchard, 8 décembre 2020.

Pour lutter efficacement contre la cybercriminalité, les services de cyberprotection ont besoin de conserver les données relatives au trafic et à la localisation d'un réseau de communication[1]. Ce recueil fait l'objet de 40 000 demandes par an.

Alors que le droit français impose aux opérateurs de télécommunication de conserver pendant un an toutes les données de connexion des utilisateurs pour les besoins du renseignement et des enquêtes pénales, la Cour de Justice de l'Union européenne avait fortement limité la possibilité d'imposer aux opérateurs la conservation des données de connexion[2].

Qualifiée dans un récent rapport de l'Assemblée nationale[3] de « *difficulté majeure* » pour la lutte contre la cybercriminalité, et de « *holdup jurisprudentiel* », cette jurisprudence a toutefois été désamorcée par le Conseil d'État qui a estimé, dans un récent arrêt d'Assemblée *French Data Network* du 21 avril 2021, que **la conservation généralisée aujourd'hui imposée aux**

---

[1] *Ces données, parfois appelées « métadonnées » pour les distinguer de celles qui portent sur le contenu des échanges, comprennent trois catégories :*
- *les données d'identité, qui permettent d'identifier l'utilisateur d'un moyen de communication électronique (par exemple les nom et prénom liés à un numéro de téléphone ou l'adresse IP par laquelle un utilisateur se connecte à internet) ;*
- *les données relatives au trafic, parfois appelées « fadettes », qui tracent les dates, heures et destinataires des communications électroniques, ou la liste des sites internet consultés ;*
- *les données de localisation, qui résultent du « bornage » d'un appareil par l'antenne relais à laquelle il s'est connecté.*

[2] *Dans ses jurisprudences Digital Rights Ireland et Seitlinger, 8 avril 2014 puis Tele2 Sverige et Watson e.a. 21 décembre 2016, Ministerio fiscal 2 octobre 2018.*

[3] *Rapport d'information n°3069 du 10 juin 2020 sur l'évaluation de la loi du 24 juillet 2015 sur le renseignement.*

opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale[1].

B. UN DISPOSITIF CENTRÉ SUR LES CYBERRISQUES LES PLUS GRAVES

La **Stratégie de la France en matière de défense et de sécurité des systèmes d'information**, rendue publique en **février 2011** par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), se concentre sur le renforcement de la « *cybersécurité des infrastructures vitales nationales* », qu'elle coordonne.

La cybersécurité opérationnelle est assurée par un réseau de CERT (*Computer Emergency Response Team*), organismes chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous.

L'article L.1332-1 du code de la défense[2] et l'article 22 de la loi n° 2013-1168 du **18 décembre 2013** relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale peuvent imposer des obligations aux **entreprises d'importance vitale**, à leurs frais, comme la mise en œuvre de « ***systèmes qualifiés de détection*** *des événements susceptibles d'affecter la sécurité de leurs systèmes d'information* ».

Le quatrième objectif de la **stratégie nationale pour la sécurité du numérique**, du **16 octobre 2015**, lie rattrapage de la numérisation des PME et progrès de leur sécurité numérique : « *En 2015, la part des entreprises françaises et singulièrement des PME-PMI utilisant largement le numérique n'est que dans la*

---

[1] *Le Conseil d'État a estimé que, pour les infractions pénales, la solution suggérée par la CJUE de conservation ciblée en amont des données n'est ni matériellement possible, ni – en tout état de cause – opérationnellement efficace. En effet, il n'est pas possible de pré-déterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise. Toutefois, la méthode de « conservation rapide » autorisée par le droit européen peut à ce jour s'appuyer sur le stock de données conservées de façon généralisée pour les besoins de la sécurité nationale, et peut être utilisée pour la poursuite des infractions pénales.*

S'agissant de la distinction établie par la Cour entre la criminalité grave et la criminalité ordinaire, pour laquelle elle n'admet aucune conservation ou utilisation de données de connexion, le Conseil d'État rappelle que le principe de proportionnalité entre gravité de l'infraction et importance des mesures d'enquête mises en œuvre, qui gouverne la procédure pénale, justifie également que le recours aux données de connexion soit limité aux poursuites d'infractions d'un degré de gravité suffisant.

[2] *Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.*

moyenne des pays européens. Le rattrapage de ce retard doit s'accompagner d'une meilleure sécurisation de la vie numérique des entreprises et en premier lieu d'une meilleure sécurité de leurs systèmes d'information. Il en va de notre compétitivité et donc de nos emplois ».

Toutefois, dans la **Revue stratégique de cyberdéfense du 12 février 2018**, les entreprises ne sont qu'indirectement évoquées et le cyberrisque concernant les TPE et PME n'est pas traité en tant que tel. En dehors de ces considérations générales, le dispositif public est centré sur les entreprises les plus sensibles et la sécurité des systèmes d'information des **opérateurs d'importance vitale (OIV),** dont le nombre exact et l'identité sont tenus secrets.

Si le rapport de la commission d'enquête du Sénat sur le devoir de souveraineté numérique **d'octobre 2019**[1] notait avec satisfaction : « *l'intégration fin 2018 d'une* ***dimension sécurité numérique dans la plateforme FranceNum*** *destinée à accompagner les TPE/PME dans leur transformation numérique avec un volet dédié à la sécurité numérique (sensibilisation au risque cyber et mise en relation avec des prestataires)* », celui-ci se borne à renvoyer, sur le site FranceNum, au guide de la cybersécurité pour les experts-comptables publié en septembre 2018 par le Conseil supérieur de l'ordre des experts-comptables. Seules 59 réponses sont apportées par ce site à l'occurrence « cybersécurité des PME » dont plusieurs renvoient au site « Pensez Cybersécurité » mis en ligne fin 2018 par le Gouvernement du Canada…

L'État porte ainsi une attention soutenue à la sécurité numérique « globale » comme en témoigne la loi n° 2019-810 du **1er août 2019** visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, qui soumet à autorisation l'installation de certains équipements sous la responsabilité des opérateurs de télécommunications et a également pour objectif de soutenir leur implication dans la sécurité de leurs réseaux « *dont la criticité est absolue* »[2].

L'ANSSI et le Secrétariat général de la défense et de la sécurité nationale (SGDSN) avaient également élaboré un **plan Vigipirate « Objectifs de cybersécurité »**[3], publié le **27 février 2014**, qui est principalement destiné aux collectivités territoriales et aux « *opérateurs non-OIV* » (opérateurs d'importance vitale), qui englobe donc potentiellement toutes les entreprises quelle que soit leur taille. Il expose les objectifs de cybersécurité et les recommandations à respecter pour sécuriser les systèmes d'information d'une entité. Ces objectifs sont organisés selon sept familles d'activités

---

1 *Rapport n° 7 (2019-2020) de M. Gérard Longuet, du 1er octobre 2019*

2 *Avis n° 569 (2018-2019) de M. Pascal Allizard, fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, du 12 juin 2019.*

3 *Voir : https://www.ssi.gouv.fr/uploads/2014/10/20140310_Objectifs_de_cybersecurite_document_public.pdf*

propres à la sécurité des systèmes d'information : la gouvernance, la maîtrise des risques, la maîtrise des systèmes, la protection des systèmes, la gestion des incidents, l'évaluation et la relation avec les autorités.

Très complet, il n'est cependant accessible qu'aux entreprises qui maîtrisent déjà le risque cyber et sont dotées d'une direction de la sécurité des services d'information étoffée. Quand bien même, **certains objectifs assignés sont ambitieux et sans doute hors de portée des grandes PME ou même ETI** comme l'indiquent ces quelques exemples :

- *« l'entité dispose de la documentation à jour de tous les systèmes d'information et composants dont elle est responsable, de manière à pouvoir intervenir plus facilement sur ses systèmes en cas d'incident » ;*
- *« l'entité maîtrise ses systèmes d'information sur tout leur cycle de vie » ;*
- *« Les systèmes d'information sont conçus et développés selon une architecture sécurisée ».*

Globalement, **les TPE et PME, comme les ETI qui ne sont pas identifiées comme d'importance vitale, ne sont pas assez bien cyberprotégées par ce dispositif public.**

Il convient de **combler un vide du dispostif public** qui assure une cybersécurité satisfaisante aux opérateurs d'importance vitale, grâce à l'ANSSI, mais **ne couvre pas suffisamment les TPE-PME** malgré la création récente du dispositif cybermalvaillance.gouv.fr, encore trop peu connu.

Or, ces catégories d'entreprises sont également devenues des cibles « faciles », à mesure du renforcement de la cyberprotection des ETI et grandes entreprises.

III. UNE CYBERSÉCURITÉ DIFFICILEMENT ACCESSIBLE AUX TPE ET PME

A. UN RISQUE CROISSANT D' « EFFET DOMINO » POUR LES ENTREPRISES

Face à la multiplication des cyberattaques, **les grandes entreprises et les ETI ont pris des mesures de défense compliquant la tâche des cybercriminels**. En particulier, les stratégies de sauvegarde et de reconstruction efficace des systèmes informatiques rendent le blocage des systèmes moins pertinent pour faire payer la rançon.

Les cybercriminels font des études de marché sur leurs cibles. Lorsque celles-ci ont atteint un niveau supérieur de protection, ils réorientent des attaques sophistiquées via leurs sous-traitants plus fragiles en termes de cybersécurité. **Une meilleure cyberdéfense des grandes entreprises a eu comme contrepartie de détourner la cybercriminalité vers les plus petites entreprises plus vulnérables.**

Cette évolution a reporté le risque vers les PME et TPE fournisseurs ou sous-traitantes. L'accès à distance au système d'information de l'entreprise augmente sa surface d'attaque en ouvrant de nouvelles portes. Les attaques ciblant la *supply-chain* utilisent le maillon faible qu'est le réseau interne d'un fournisseur ou d'un sous-traitant, moins bien sécurisé, pour s'introduire dans le système d'information de la grande entreprise. Une interconnexion mal sécurisée entre sites peut favoriser la propagation de malware et produire un « **effet domino** » sur l'ensemble du système d'information.

C'est la raison pour laquelle Tech in France et le Syntec demandent[1] : « ***d'être de plus en plus exigeant*** *envers les entreprises sur les minima de sécurité. Les grands donneurs d'ordre doivent avoir des exigences vis-à-vis des prestataires et des fournisseurs et pour cela, les certifications et normes certifiées par l'ANSSI sont utiles*[2] ».

De même, la Confédération des petites et moyennes entreprises (CPME) estime[3] que **la cybersécurité « *n'est pas hors de portée des TPE et PME* »** qui peuvent privilégier, pour des raisons de coût, l'externalisation soit « *auprès de leur prestataire informatique habituel soit, si celui-ci n'en pas la compétence, auprès d'un prestataire spécialisé en cybersécurité ou labellisé Expert Cyber* ».

---

[1] *Dans leurs propositions conjointes : « Crise Covid-19 et relance de l'économie », mai 2020.*

[2] *Le rapport note toutefois que : « certaines entreprises, sans être certifiées ou labellisées par l'ANSSI, garantissent une grande qualité de produit, et des niveaux de performance comparables à ceux des produits validés par l'ANSSI ».*

[3] *Réponse du 24 mars 2021 au questionnaire de la Délégation aux entreprises du Sénat.*

B. UN MANQUE DE CULTURE DE LA CYBERSÉCURITÉ

1. Le salarié, un maillon souvent faible de la cybersécurité de l'entreprise

a) Près d'une fois sur deux

Près d'un incident sur deux[1] est imputable au facteur humain comme en a témoigné un chef d'entreprise à la table-ronde organisée par la Délégation aux entreprises le 25 mars 2021 :

> **M. Jean-Charles Duquesne, membre du Mouvement des entreprises de taille intermédiaire (METI), directeur général de la Normandise : «** *Mon entreprise a été victime d'une attaque. On croit toujours que ces attaques visent Safran ou d'autres acteurs stratégiques - ma société fabrique des aliments pour chiens et chats ! Elle emploie 700 personnes, compte 120 millions d'euros de chiffre d'affaires, propose ses produits via la grande distribution ou sous ses propres marques sur un site internet. (…) Notre taille implique, surtout avec la crise, une utilisation massive des mails - lesquels constituent une porte d'entrée pour les attaques. Nous avons eu trois jours de perturbation, même si la production n'a pas été touchée, grâce à notre sensibilité au risque cyber. Le plus gros impact a été un investissement de 100 000 euros pour que cela ne se reproduise pas ; 70 personnes ont aussi été mises en congé de trois heures à trois jours.*
>
> *(…) Après l'attaque que nous avons subie, nous avons développé une solution permettant d'envoyer des mails pourris à l'ensemble de nos salariés, pour savoir s'ils cliquaient sur les pièces jointes.* ***Tout le monde avait été sensibilisé par l'attaque. Eh bien, un mois seulement après, 34 % des salariés sont tombés dans le piège. La pédagogie est basée sur la répétition****... ».*

Ce manque de cyberculture n'est pas une question de génération. Si la « génération Y »[2], considérée comme naturellement plus à l'aise que les générations précédentes avec les nouvelles technologies, est une forte consommatrice de numérique et est donc la plus exposée aux cyberattaques, **ses connaissances en termes de cybersécurité ne sont cependant pas suffisantes** d'après les résultats d'un sondage[3] : 82 % des répondants ignorent ce qu'est un pare-feu, 76 % indiquent ne pas connaître ce qu'est un malware, 73 % ne comprennent pas le terme VPN et 71 % n'arrivent pas à définir le terme HTML. Toutefois, ils connaissent les notions de virus (65 %), cookies (65 %) et bande passante (49 %).

---

[1] *Selon «* The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within *» de Kapersky Daily, 46 % des piratages et incidents de cybersécurité résultent d'une négligence ou d'un manque de formation.*

[2] *Elle désigne toutes les personnes nées entre 1980 et 2000. Cette génération représente environ 23 % de la population française et 32 % au niveau mondial.*

[3] *Réalisé pour le compte de l'éditeur en sécurité Specops Software qui a interrogé 2 445 personnes ayant entre 20 et 40 ans.*

Dans ce panel, parmi les 67 % qui ont été piratés, seul un tiers (39 %) a déclaré savoir quoi faire et comment y faire face. En outre, 61 % ont admis qu'ils ne savaient pas s'ils devaient lancer une analyse antivirus, changer leurs mots de passe ou jeter leur ordinateur portable. En outre, 73 % des personnes qui ont été piratées disent qu'elles n'ont pas changé ou ne changeraient pas leur comportement pour éviter que cela ne se reproduise (27 % le feraient), tandis que 92 % des sondés ne savent pas comment utiliser un VPN, 81 % a déclaré pouvoir ouvrir et exécuter des gestionnaires de tâches, 77 % ne pas savoir exécuter une analyse antivirus, 71 % une recherche en mode incognito, 66 % une suppression de l'historique des recherches de leur ordinateur. Cependant, 57 % peuvent résoudre avec succès les problèmes liés à leur appareil.

La cybersécurité est encore trop perçue comme **une contrainte supplémentaire** par les collaborateurs et **le fonctionnement en silos** du management d'un certain nombre d'entreprises ne favorise pas toujours ce travail d'équipe puisqu'une collaboration minimaliste ne permet pas de diffuser de façon efficace une culture partagée.

Certaines TPE et PME estiment qu'elles ont peu de risque d'être victimes d'incidents cyber, notamment lorsqu'elles **externalisent** la maintenance de leur système d'information et l'hébergement de leurs données auprès de prestataires dans le cloud, sans avoir conscience des risques problématiques associés à ce choix.

Certaines PME ont par ailleurs **de mauvais réflexes de cybersécurité :** « *La cybersécurité ne peut se résumer à l'achat d'un firewall à la FNAC* » estime ainsi Oliver Wild de l'AMRAE[1], « *La cybersécurité la plus efficace est homogène, évolutive en permanence, constante, et s'adapte aux priorités de l'entreprise* ».

b) Une culture à renforcer : quelques pistes

La culture de la cybersécurité doit donc être implantée dans l'entreprise.

Elle aurait pu se développer avec le RGPD, mais **le manque d'équipes qualifiées en interne** a freiné ce travail de déploiement d'une politique récurrente d'information sur les risques informatiques.

En outre, l'acculturation des salariés en matière de cybersécurité nécessite une forte implication non seulement de la direction mais aussi du *middle management*, ce qui implique de **placer en permanence l'utilisateur final et ses besoins au centre des préoccupations**. C'est par les usages au quotidien que la cybersécurité en entreprise sera la plus efficace.

Comme une sécurité informatique efficace repose sur **trois piliers** : les produits et les services de sécurité, les processus et les personnes, le

[1] *Audition du 18 mars 2021.*

simple fait d'augmenter le budget alloué aux outils n'est pas une réponse suffisante face à la multiplication des menaces de plus en plus sophistiquées. **Chaque salarié dispose de la clé de la cybersécurité de son entreprise.**

Cette diffusion d'une culture de la cybersécurité peut être ludique, afin de s'implanter plus efficacement, à l'instar du « chocoBLAST »[1] : quand un collaborateur d'une entreprise laisse son poste ouvert alors qu'il n'est pas à son poste, il se fait « hacker » sa boite e-mail et doit payer sa tournée de viennoiseries aux équipes.

Par ailleurs, le **6 mai** est aussi la **Journée internationale du mot de passe.** Cet élément de sécurité fait toujours office de porte d'entrée idéale pour les cybercriminels chez les victimes y compris parmi les entreprises de cybersécurité.

Ainsi, un mot de passe simple et exposé en ligne pourrait être le point de départ de l'une des plus grandes opérations de cyberespionnage de l'histoire[2] : « *Non seulement les identifiants étaient exposés sans protection, mais en plus ils étaient risibles. Le nom d'utilisateur « solarwinds.net » et le mot de passe, « solarwinds123 », avaient de quoi horrifier n'importe quel responsable de sécurité. Choisissez votre adjectif : faible, simple à deviner, et surtout indigne d'une entreprise qui fournit des organisations sensibles comme le gouvernement américain. La députée Katie Porter a donc demandé aux dirigeants de commenter ce raté colossal dans la sécurité du groupe* ».

Même des cybercriminels qui étaient parvenus à accumuler des millions de données dérobées sur un serveur auraient oublié de protéger ce butin d'une grande valeur, auquel n'importe qui pouvait accéder ![3]

En analysant le contenu de bases de données compromises en 2020, soit environ 275 millions, le gestionnaire de mots de passe NordPass a publié la liste des 200 mots de passe les plus courants sur Internet : « 123456 » truste le haut du classement. Ce mot de passe a été ainsi retrouvé plus de 2,5 millions de fois dans les bases scannées. On retrouve dans le top 10 sa suite logique (« 123456789 ») mais aussi « password », « 111111 », « qwerty » ou encore « abc123 »[4].

Les entreprises pourraient organiser le 6 mai de chaque année une sensibilisation de leurs salariés à cet élément de sécurité trop facilement attaquable.

---

[1] *Voir les « règles du jeu » : https://www.chocoblast.fr/reglement/*

[2] *Selon « Les dirigeants de SolarWinds accusent un stagiaire de la fuite du mot de passe « solarwinds123 », François Manens, Cyberguerre, 1er mars 2021.*

[3] *« Même les cybercriminels ne sécurisent pas correctement leurs bases de données (volées) » François Manens, Cyberguerre, 6 mai 2021.*

[4] *« Voici la liste des 200 mots de passe les plus utilisés en 2020 (et c'est le désarroi) », Benjamin Bruel, Clubic, 19 novembre 2020.*

2. Éducation et formation à la cybersécurité : des progrès mais peut mieux faire

Aujourd'hui, les usages du numérique sont traités au collège dans le cadre du programme d'enseignement moral et civique (EMC) et de l'éducation aux médias et à l'information (EMI), ainsi qu'en mathématiques et technologie.

Au lycée, la cybersécurité figure explicitement dans le programme d'EMC. L'enseignement de « Sciences numériques et technologie » fait d'ores et déjà partie du tronc commun en seconde, où les questions de sécurité et de confidentialité sont traitées. En première et en terminale générale, la spécialité « Numérique et des sciences informatiques » (NSI) vise l'appropriation des fondements de l'informatique pour préparer les élèves à une poursuite d'études dans l'enseignement supérieur. En outre, le cadre de référence des compétences numériques et la certification délivrée en fin de cycle 4 (collège) et de cycle terminal (lycée) comprend plusieurs domaines parmi lesquels « Protection et sécurité ».

La rénovation récente du BTS « Services informatiques aux organisations » (SIO) par l'arrêté du 29 avril 2019, dont la première rentrée a eu lieu en 2020 et la première session d'examen en 2022, est un premier signal positif pour la formation de technicien en cybersécurité, celle-ci constituant l'un des blocs de compétences à valider pour le diplôme.

Enfin, un master « Informatique, traitement de l'information, réseaux de transmission » a été créé. Selon le site France Compétences, cette certification[1], accessible aux personnes ayant un Bac + 4/5 en informatique, ou issue d'une filière juridique ou détenteur d'un Bac + 2 avec une expérience professionnelle dans le domaine, n'a pas encore trouvé de débouché.

Ses objectifs de certification visent à permettre au candidat de réaliser des diagnostics des systèmes d'information pour chercher les points faibles du système, trouver des solutions pour lutter contre les failles pour protéger et sécuriser les données de l'entreprise, mettre en place des processus de sécurité et les actualiser en fonction des nouvelles technologies.

La certification couvre les principales compétences permettant à un consultant en cybersécurité d'auditer en amont comme en aval les systèmes d'information intranet et extranet pour déceler d'éventuelles failles de

---

[1] ***Code(s) nomenclature des spécialités de formation (NSF) :***
- *326 : Informatique, traitement de l'information, réseaux de transmission*

Formacode(s) :
- *31006 : sécurité informatique.*

sécurité et autres vulnérabilités. **Ces compétences sont rares**[1], ne serait-ce qu'en raison de l'évolution exponentielle des méthodes et outils de protection mis en œuvre.

L'ÉDUCATION AU NUMÉRIQUE : L'EXEMPLE ISRAËLIEN

« Le National Cyber Bureau (NCB) pousse pour améliorer l'éducation dans les sciences numériques.

Le budget de l'éducation passe de 6,9 milliards de dollars en 2010 à 11,8 milliards de dollars en 2019. Les filières liées à la cybersécurité bénéficient d'initiatives publiques. Six centres de recherche universitaires sont dédiés spécifiquement à cette matière. L'interdisciplinarité est favorisée par rapport à un simple enseignement technologique, avec l'intervention régulière d'experts de sciences humaines.

Le NCB joue un rôle aussi déterminant pour agrandir le vivier des jeunes Israéliens pouvant intégrer la cyberindustrie. L'enseignement de l'informatique et de la programmation débute dès le collège dans les zones les plus privilégiées. Les examens de fin d'études dans l'enseignement secondaire présentent des options dans ces matières. Des tournois inter-écoles de hacking sont même organisés. Des recruteurs parcourent en outre les zones défavorisées pour identifier les talents potentiels qui pourraient intégrer les unités militaires. D'une manière générale, les jeunes montrant des dispositions particulières sont encadrés et reçoivent une instruction adaptée en informatique ou cybersécurité selon leur niveau ».

Source : « La cyberpuissance israélienne. L'essor inachevé de la start-up nation ? », études de l'Ifri, Novembre 2020.

[1] *Les compétences visées par cette certification sont :*

- *Maîtriser une séquence d'audit du système d'information.*
- *Maîtriser l'ensemble des assets à surveiller.*
- *Ordonnancer, piloter et coordonner un projet de sécurisation d'un système.*
- *Fédérer et animer une équipe projet.*
- *Sécuriser des données de l'entreprise.*
- *Actualiser les processus de sécurité en fonction des nouvelles technologies et maîtriser les tests d'intrusion.*
- *Vérifier le système protégé.*

Les compétences numériques sont définies par le Cadre de référence européen DigComp. **L'une des compétences numériques de PIX,** plateforme en ligne d'évaluation et de certification de la maîtrise du numérique au lycée, et compte 5 domaines et 16 compétences numériques, **concerne la protection et la sécurité** :

4. Protection et sécurité

4.1. Sécuriser l'environnement numérique

Sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données (avec des logiciels de protection, des techniques de chiffrement, la maîtrise de bonnes pratiques, etc.).

THÉMATIQUES ASSOCIÉES

Attaques et menaces ; Chiffrement ; Logiciels de prévention et de protection ; Authentification ; Sécurité du système d'information ; Vie privée et confidentialité

4.2. Protéger les données personnelles et la vie privée

Maîtriser ses traces et gérer les données personnelles pour protéger sa vie privée et celle des autres, et adopter une pratique éclairée (avec le paramétrage des paramètres de confidentialité, la surveillance régulière de ses traces par des alertes ou autres outils, etc.).

THÉMATIQUES ASSOCIÉES

Données personnelles et loi ; Traces ; Vie privée et confidentialité ; Collecte et exploitation de données massives

Enfin, deux labels ont été élaborés en collaboration entre l'ANSSI et l'Éducation nationale :

- **CyberEdu** (www.cyberedu.fr) : ce projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la défense et la sécurité nationale en 2013, a pour objectif d'introduire les notions de cybersécurité dans l'ensemble des formations en informatique de France.

Les établissements qui souhaitent valoriser la prise en compte de la dimension cyber/ SSI dans leurs formations non spécialisées peuvent faire une demande, gratuite, de labellisation auprès de l'association CyberEdu.

La labellisation est attribuée aux établissements qui dispensent un cours de sensibilisation à la cybersécurité pour les formations informatiques généralistes de niveau licence (ou équivalent) ou pour les formations de niveau master (ou équivalent) et intègrent des modules relatifs à la cybersécurité dans les cours relatifs aux réseaux, développements logiciels et systèmes d'exploitation.

Ce label n'est toutefois pas destiné aux formations de spécialistes en sécurité des systèmes d'information, qui sont labellisés par SecNum*edu*. CyberEdu reste « *un indicateur qui ne constitue pas une approbation à l'ensemble d'une formation* ».

L'ANSSI a passé un marché avec l'Université européenne de Bretagne, qui regroupe 28 établissements d'enseignement supérieur et de recherche, et Orange pour la réalisation de livrables correspondants à cette sensibilisation.

- **SecNum*edu*** *:* apporte aux étudiants et employeurs l'assurance d'une formation dans le domaine de la sécurité du numérique répondant à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine (établissements d'enseignement supérieur, industriels…).

Le label s'appuie sur un référentiel de labellisation, dont l'élaboration a été pilotée par l'ANSSI avec la contribution d'industriels, d'écoles, du **Pôle d'Excellence Cyber (PEC)** et du ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche. Il est attribué pour une durée de 3 ans renouvelable et permet à la formation qui en bénéficie de figurer au catalogue SecNumedu de l'ANSSI.

Ce programme de labellisation de formations est ouvert à tout établissement d'enseignement supérieur répondant à l'un des quatre critères : les formations universitaires délivrant un grade de Licence ou Master ; les formations d'ingénieur dont le diplôme est reconnu par la Commission des Titres d'Ingénieurs (CTI) ; les Mastères spécialisés reconnus par la Conférence des Grandes Écoles (CGE) ; les certifications de niveau I et II inscrites au Répertoire national des certifications professionnelles (RNCP).

L'ANSSI propose également un programme de labellisation pour les **formations continues courtes** : S**ecNum*edu*-FC**, et 70% du programme de cette formation est consacrée à la sécurité du numérique. La formation, inscrite au Répertoire Spécifique de France Compétences et/ou la formation, se déclare conforme à un cahier des charges reconnu par l'ANSSI.

Le déploiement de l'enseignement de la cybersécurité dans toutes les formations supérieures du numérique reste cependant trop lent et trop partiel. La cybersécurité doit y être intégrée « par défaut ».

Dans ce sens, la Commission supérieure du numérique et des postes, dans son avis n°2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique, prône que des enseignements portant sur la sécurité numérique et la cybersécurité soient intégrés systématiquement et rapidement dans tous les cursus de formation aux métiers du numérique « *Les principes de sécurité par conception, d'architecture sécurisée et de sécurité d'exploitation doivent s'imposer dans les formations de tous niveaux aux métiers du numérique. Cette recommandation est formulée tant pour la formation initiale que pour la formation continue* ».

Il est important par ailleurs de « *ne pas séparer le sous-jacent de la sécurité : pour intégrer le réflexe cyber et la security by design, il faut développer la cybersécurité dans les formations d'ingénieur et de développeur* » selon le président de l'association[1], **sans créer une filière spécifique car le sujet doit demeurer transversal.**

La formation initiale et continue prend donc mieux en compte la nécessité de développer dès l'enfance une culture en matière de cybersécurité. Ces efforts paraissent cependant encore insuffisants à l'aune de la pénurie de ressources humaines dans ce secteur en croissance et en manque criant de compétences.

C. UNE PÉNURIE DE RESSOURCES HUMAINES

1. Une pénurie mondiale de compétences en matière de sécurité informatique

La pénurie de ressources et compétences en matière de cybersécurité est mondiale. Dès lors, **ce handicap est particulièrement aggravé pour les TPE PME** pour lesquelles la ressource humaine devient pratiquement inaccessible.

Ainsi, **70 % des entreprises dans le monde manquent de spécialistes en sécurité informatique et il faudrait en former 4 millions pour répondre aux besoins du marché**, selon une étude récente réalisée avant la pandémie de la Covid-19[2]**. Cette pénurie est en forte croissance** puisqu'une autre étude de 2018 l'estimait à environ 3 millions[3].

Cette pénurie est corroborée par l'étude *IT Skills and Salary Report** de Global Knowledge de novembre 2020[4], qui estime que 78 % des décideurs informatiques mondiaux font face à des lacunes critiques en matière de compétences.

Avant la pandémie de la Covid-19, 45 % des entreprises considéraient que le déficit de compétences dans ce domaine s'est aggravé au cours des dernières années, 48 % que la situation n'a pas changé, tandis que 7 % seulement affirmaient que la situation s'est améliorée.

---

1 *Audition de M. Olivier Levillain, 20 mai 2021.*

2 *Étude conduite par l'Enterprise Strategy Group et l'Information Systems Security Association (ISSA) auprès de 327 professionnels du domaine (principalement basés en Amérique du Nord) entre fin 2019 et début 2020.* ***Cette enquête est toutefois essentiellement nord-américaine*** *: 92 % des répondants à l'enquête résidaient en Amérique du Nord, 4 % venaient d'Europe, 3 % d'Asie et 1 % d'Amérique centrale et du Sud.*

3 *ONG de professionnels de la sécurité chargée de certifier des professionnels de la sécurité de l'information, en fournissant les certifications SSCP et Certified Information Systems Security Professional (CISSP).*

4 *Étude construite sur les réponses de plus de 9 500 professionnels de l'informatique dans 159 pays.*

Le manque de candidats qualifiés freine les recrutements et les évolutions de carrière sont quasi-inexistantes après l'intégration dans l'entreprise : 68 % des professionnels de la cybersécurité interrogés ont déclaré qu'ils n'avaient pas de plan de carrière bien défini et peu de perspectives d'évolution dans ce domaine.

Ils peinent aussi bien à trouver un mentor qu'à obtenir des certifications en cybersécurité, ou entreprendre des stages dans ce domaine. En conséquence, les professionnels de la cybersécurité « *se débrouillent souvent dans leur carrière sans grande orientation, sautant d'un emploi à l'autre et améliorant leurs compétences à la volée plutôt que de manière systématique* ».

L'enquête révèle également que **de nombreux salariés travaillent dans la cybersécurité sans disposer de connaissances complètes en la matière.** Ainsi, 63 % des répondants ont un parcours professionnel dans cette spécialité qui date de moins de trois ans. Ils sont par ailleurs 76 % à avoir commencé dans l'informatique avant de passer à la cybersécurité. Or, les intéressés estiment qu'il faut entre trois à cinq ans (39 % des réponses) pour développer de véritables compétences en cybersécurité, tandis que 22 % avancent une période située entre deux à trois ans et 18 % affirment que l'acquisition de connaissances dépasse les cinq ans. Pour les employeurs, cela signifie que les professionnels de la cybersécurité de premier niveau doivent être considérés comme des investissements à long terme, et non comme des spécialistes de la résolution immédiate de problèmes.

Enfin, certains cadres exécutifs estiment ne pas avoir d'idée précise de la politique de sécurité informatique de leur entreprise, de sorte que « *les RSSI et autres cyber-leaders au sein d'une organisation doivent assumer des rôles de plaidoyers voire de formateurs afin de développer le potentiel de leurs équipes* ».

Au déficit de compétences en cybersécurité s'ajoute le fait que les entreprises **ne mesurent pas à leur juste valeur l'intérêt de sécuriser l'information.**

2. Une pénurie qui aggrave la fragilité des PME en cybersécurité

La France n'échappe pas à cette **pénurie mondiale**.

En janvier 2020, Pôle Emploi[1] comptabilisait 775 577 salariés dans le secteur numérique, dont 58 % dans l'informatique, 19 % dans les télécommunications, 9 % dans l'édition des logiciels ou encore 7 % dans le commerce et l'industrie.

Le numérique s'impose ainsi comme un secteur de recrutement en expansion et dont le taux d'embauche est 2,4 fois plus élevé que dans les autres secteurs. Dans les prochaines années, Pôle Emploi estime que ce sont 191 000 postes qui seront à pourvoir d'ici 2022.

---

[1] *« Les métiers du numérique : quelles opportunités d'emploi ? », Pôle Emploi, janvier 2020.*

La pénurie en compétences constitue l'une des faiblesses de la cybersécurité également pointée par l'Alliance pour la confiance dans le numérique dans son rapport annuel de 2020 : « *bien que la France ne souffre pas de retard en matière de formation à la cybersécurité, la croissance est telle dans ce secteur que les compétences sont* ***difficiles à trouver****. Les premières embauches de développeurs spécialisés dans un domaine spécifique de la cybersécurité (PKI, cryptographie, etc.) est* ***quasiment impossible****. Les entreprises sont contraintes d'embaucher dans le meilleur des cas des développeurs formés à la cybersécurité dans son ensemble, voire des ingénieurs généralistes qui seront formés en interne* ».

La concurrence mondiale est telle que les talents français sont attirés par de meilleures rémunérations à l'étranger, en particulier en matière de *deep learning* : « *les entreprises françaises (en particulier les PME), ont du mal à s'aligner sur les salaires offerts par les grands acteurs américains qui proposent en général* ***des salaires supérieurs de 10 % à 30 % à compétences égales*** ».

L'observatoire de la Grande école du numérique (GEN) a pour sa part analysé, en février 2021, les besoins en compétences numériques dans les 13 régions de la France métropolitaine[1]. L'étude souligne que, malgré un nombre de projets de recrutements importants sur les métiers numériques, « ***les régions peinent à recruter*** *: entre 60 % et 80 % des recrutements sont jugés difficiles dans ces métiers dans l'ensemble des régions* », alors même que ces métiers sont porteurs : « *ce sont les métiers de Développeur (fullstack, devOps), Technicien télécom et Chef de projet web qui se retrouvent sur le podium des métiers recherchés, suivis par le Digital business developper et l'Installateur réseaux* ».

Cette pénurie constitue une puissante incitation à externaliser la gestion des bases de données et, plus globalement, la cybersécurité de l'entreprise.

D. UN RECOURS CROISSANT AU CLOUD

1. Un remède à l'insuffisance des ressources internes de cybersécurité : l'infogérance

En France, en 2016, 17 % des sociétés de 10 salariés ou plus avaient acheté des services de *cloud computing* contre 12 % en 2014 selon l'INSEE[2]. La tendance s'est depuis accentuée puisque selon Eurostat[3], les activités liées à la sécurité des TIC étaient réalisées par des **fournisseurs externes dans les deux tiers** des entreprises européennes. Cette proportion est identique pour les PME.

---

[1] *« Les besoins en compétences numériques dans les régions » – 4 février 2021.*

[2] *« Cloud computing, big data : de nouvelles opportunités pour les sociétés », INSEE Première, n°1643, mars 2017.*

[3] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises

La sécurisation des données peut inclure le chiffrement de bout en bout (*encryption end-to-end*), la microsegmentation (technique de sécurité des réseaux qui permet aux architectes de la sécurité de diviser logiquement le centre de données en segments de sécurité distincts) ou encore la mise en place d'un réseau privé virtuel (VPN - *Virtual Private Network*).

L'infogérance[1] est cependant toujours un risque comme le souligne dès décembre 2010 l'ANSSI, dans un guide sur l'externalisation des systèmes d'information[2] et notamment d'une messagerie d'entreprise ou d'une suite bureautique auprès d'un prestataire d'informatique en nuage : « *les informations échangées ou traitées par ce biais (pièces jointes, agendas des décideurs, etc.) peuvent revêtir un caractère «sensible», et sont susceptibles d'intéresser la concurrence (intelligence économique)* », en recommandant, « *en l'absence de cadre juridique international adapté à l'informatique en nuage* », « *de s'assurer que les données à caractère personnel restent localisées sur des serveurs exclusivement situés dans l'Union européenne – voire en France – et de prévoir les moyens de contrôle de cette obligation* », ce que l'évolution de l'économie numérique n'a pas permis d'assurer.

Un **Plan d'Assurance Sécurité** (PAS) précise la liste exhaustive des équipements et des programmes concernés par la maintenance informatique ainsi que l'assistance sur site et la récupération des données en fin de contrat, y compris celles confiées à des sous-traitants (clause de réversibilité). Ces derniers sont qualifiés par l'ANSSI comme « *le maillon faible de la chaîne de cybersécurité* », dont le recours doit être encadré[3].

Mettant en exergue le fait que « *passer au cloud, c'est entamer une transformation numérique favorisant la croissance de l'entreprise* », le site public FranceNum, portail de la transformation numérique des entreprises, renvoie au dossier du 11 février 2019 du magazine Capital.fr : Pourquoi le cloud devient un passage obligé pour les entreprises ?

Cependant, les PME, et plus encore les TPE, n'ont toujours pas les ressources pour réaliser un tel plan.

2. Un déséquilibre des relations contractuelles dans le cloud au détriment des PME

La cybersécurité dans le cloud diffère juridiquement et économiquement de l'acquisition d'un logiciel. L'acquisition d'un bien

---

[1] *Défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définis selon l'AFNOR (Norme Z 67801-1).*

[2] *https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf*

[3] *Voir, à cet égard : « Encadrez votre recours à la sous-traitance ! L'assurance : le partenaire d'une sous-traitance réussie TPE, PME, vous êtes concernées », FFA, janvier 2021.*

matériel de cybersécurité (logiciels) bénéficie de la garantie légale de conformité (article L.217-1 du code de la consommation), de la garantie légale des vices cachés (article 1641 du code civil) ou de la responsabilité du fait des produits défectueux. Son acquisition, sa maintenance en infogérance[1], relèvent du droit classique des relations contractuelles, faisant l'objet d'une abondante jurisprudence, et semble constitutive d'une relation équilibrée entre clients et fournisseurs.

En revanche, lorsqu'elles sont hébergées dans des plateformes appartenant à des GAFAM, les PME souffrent d'un déséquilibre des relations contractuelles.

Selon Eurostat, **14 % des entreprises européennes sont fortement dépendantes du *cloud* pour leur activité**, et celles-ci sont mal équipées pour faire face à la puissance monopolistique des fournisseurs de solutions de *cloud computing*. Cette situation est particulièrement vraie pour les PME : « *si 72 % des PME interrogées déclarent avoir l'intention d'en changer, 57 % déclarent avoir des difficultés à la faire. Cet effet de lock-in est lié à un manque de portabilité des données et de transférabilité, et heurte la capacité des organisations à choisir librement leur prestataire de service* », selon la Plateforme RSE[2].

Cette situation perdure malgré le **principe de libre circulation des données** établie par la Stratégie pour un Marché unique numérique lancée en mai 2015, déclinée par le règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[3], et les lignes directrices du 29 mai 2019[4] qui « *encourage les acteurs du secteur à élaborer, avec le soutien de la Commission, des codes de conduite fondés sur l'autorégulation concernant le changement de fournisseurs de services et le portage des données* ».

Des codes de conduite devaient être rédigés par les parties prenantes, l'un pour le marché du IaaS (*Infratructure As A Service*)[5] et l'autre pour le marché du SaaS (*Software As A Service*), par le « SWIPO Working Group » (SWItching cloud and POrting data), mis en place en avril 2018 et devaient être présentés en novembre 2019 mais aucun consensus n'a pu être trouvé. Le CIGREF a donc publié le **26 mai 2021** un **référentiel du cloud de**

---

1 *Le client externalise auprès d'un prestataire informatique la gestion et l'exploitation de tout ou partie de son système d'information (SI).*

2 *Rapport sur la responsabilité numérique des entreprises, juin 2020.*

3 *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1807&from=FR*

4 *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52019DC0250&from=EN*

5 *Le SaaS est l'une des quatre catégories principales de Cloud Computing, au même titre que l'Infrastructure en tant que service (IaaS), la Plateforme en tant que Service (PaaS), et le Desktop en tant que Service (DaaS). Parmi les principaux fournisseurs d'un logiciel SaaS, on retrouve Salesforce, Oracle, IBM, Intuit ou encore Microsoft.*

confiance[1]. Ce référentiel opérationnel a vocation à être également contractuellement exigible. Il n'est ni un label ni une certification.

Ce **coup d'arrêt du processus d'autorégulation du marché du cloud en Europe** est, pour le CIGREF, « *la conséquence d'une* ***asymétrie systémique*** *de compétences, de moyens et d'objectifs de certains grands fournisseurs mondiaux de services cloud d'une part, qui défendent le cœur de leur activité commerciale et leur capacité d'enfermement de leurs clients, et d'autre part ceux des utilisateurs dont le lobbying dans ce domaine n'est pas le métier* »[2]. Les principaux fournisseurs ont refusé d'intégrer les attentes des utilisateurs en matière de régulation du cloud, notamment en termes d'interopérabilité logicielle et de portabilité des licences logicielles.

Pour une TPE ou une PME, la relation dans le cloud est déséquilibrée en faveur des fournisseurs.

Si la contractualisation entre les PME et les opérateurs du *cloud* permet d'obtenir des garanties opérationnelles et de sécurité, les PME ne peuvent maitriser suffisamment cette évolution en raison de l'asymétrie des positions des acteurs de ce marché qui leur donne **un faible pouvoir de négociation.** Or, « *la décision de recourir au cloud n'est ni facilement réversible ni clairement neutre. Elle résulte d'une obligation opérationnelle de minimisation des coûts* » estime la Plateforme RSE dans son rapport précité.

Un rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies de juin 2020[3] confirme cette asymétrie.

Faute de contentieux (les différends ne se règlent pas devant la justice mais par transaction) mais en se fondant sur un rapport au Parlement européen[4] qui soulignait qu'« *une comparaison de quatre contrats pour des services d'informatique en nuage destinés au grand public révèle que les fournisseurs* ***déclinent toute responsabilité*** *en matière de disponibilité ou de fonctionnalité du service, et qu'ils* ***se prémunissent contre les éventuels dommages causés aux consommateurs*** », la mission a dressé le même constat en juin 2020 pour les contrats cloud destinés aux professionnels[5]. **Une telle**

---

1 https://www.cigref.fr/wp/wp-content/uploads/2021/05/20210526_Cigref_Referentiel-du-cloud-de-confiance_v.02.pdf

2 https://www.cigref.fr/wp/wp-content/uploads/2019/11/CP-SWIPO-Cigref-version-francaise-2019-11-25.pdf

3 *« La responsabilité des fournisseurs de systèmes numériques », juin 2020.*

4 *« L'informatique en nuage. Une vue d'ensemble des enjeux économiques et politiques », note du Service de recherche du Parlement européen, mai 2016.*

5 *« Il s'agit, dans tous les cas,* ***d'engagement de moyens*** *» et « le fournisseur* ***exclut toujours dans le contrat de réparer un quelconque préjudice*** *causé par l'indisponibilité du service ». Il s'agit généralement de «* ***contrats d'adhésion*** *que le client doit accepter en l'état (…) Les contrats comportent de nombreuses* ***clauses de non-responsabilité ou limitant l'indemnisation en cas de préjudice*** *au montant payé par le client pour son abonnement. La formulation de certaines clauses est* ***peu compréhensible :*** *elles sont écrites en majuscules, en employant des formulations commençant par « Sous réserve du droit applicable...» ce qui les rend*

apathie est surprenante alors que les cyberattaques dans le cloud n'ont cessé de croître.

Certes, les dispositions existantes, qu'il s'agisse du code civil[1], du code de la consommation[2] ou du code de commerce[3], pourraient être invoquées par les entreprises lésées. Or, **elles ne le sont pas**. Les **actions** engagées **en justice** sont le fait d'associations de consommateurs ou de la DGCCRF, notamment pour faire condamner (par l'Autorité de la concurrence) les GAFAM. Les entreprises préfèrent la discrétion de la transaction, et s'abstenir d'attraire leur fournisseur de cybersécurité en ligne devant la justice.

particulièrement absconses pour le non-juriste qu'est le consommateur ou le «petit» professionnel qui ne dispose pas de service juridique ».

[1] *L'article 1170 du Code civil (« Toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite ») vise ainsi à ce que le dispositif contractuel soit en accord avec l'engagement promis par le fournisseur. Sont ainsi visées les* ***clauses limitatives de responsabilité*** *par lesquelles le débiteur est peu incité à exécuter une obligation essentielle pour le créancier (pour un contrat d'hébergement dans le cloud, la limitation importante des pénalités dues en cas de non-respect de la qualité de service). L'article 1171 du Code civil (« Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite »), introduit la notion de* ***déséquilibre significatif*** *dans le droit commun des contrats.*

[2] *Avec la notion de* ***clauses abusives*** *de l'article L.212-1.*

[3] *Avec la notion de* ***pratique restrictive de concurrence*** *de l'article L.442-1-I.*

IV. UN ENCOURAGEMENT AU DÉVELOPPEMENT D'UN ÉCOSYSTÈME DE LA CYBERSÉCURITÉ

A. UNE FORTE AMBITION PUBLIQUE EN MATIÈRE DE CYBERSÉCURITÉ

1. Un moteur de développement économique

a) Un marché en pleine expansion dans le monde

Le marché mondial de la cybersécurité était, en 2019, d'environ 106 milliards de dollars (dont 47 milliards pour les services de sécurité, comme les services d'intégration et de conseil, la formation à la cyber et l'éducation, 38 milliards pour les dépenses en logiciels, et 21 milliards pour les dépenses en matériel), soit une forte hausse de 10,7 % par rapport à l'année précédente, alors qu'il ne pesait que 75,5 milliards de dollars en 2016.

Il devrait franchir les 116 milliards en 2020 et dépasser les **151 milliards de dollars en 2023. Il augmenterait donc de plus de 420 % en quatre ans !**

La cybersécurité est à la fois une menace pour les entreprises et une opportunité de développer un marché porteur de produits et de services de sécurité numérique.

b) Un marché créant une importante valeur ajoutée en France

Selon l'édition 2020 de l'Observatoire de la confiance numérique, la cybersécurité et la sécurité numérique réalisent **en France 13 milliards d'euros de chiffre d'affaires**[1], avec 8,8 % de croissance entre 2018 et 2019, dégage 6,1 milliards d'euros de valeur ajoutée et employait 67 000 personnes.

Elle est **fortement exportatrice**, avec 12,4 milliards d'euros réalisés à l'international et 4,4 milliards de chiffre d'affaires à l'exportation. Elle crée **6,1 milliards de valeur ajoutée** et emploie 67 000 salariés.

---

[1] *Le chiffre d'affaires est réparti entre « Cybersécurité » (produits / logiciels et services) à hauteur de 57 % et 43 % pour la « Sécurité Numérique » (identité numérique, systèmes et sous-systèmes électroniques de confiance).*

Non seulement l'industrie de sécurité est la filière industrielle qui a **la croissance la plus forte**[1] avec le **plus fort taux de valeur ajoutée** (près de 43 %), mais la cybersécurité constitue le segment de cette filière qui tire la dynamique du secteur[2].

Les produits électroniques de sécurité correspondent à 44 % du chiffre d'affaires total de la filière de sécurité, soit près de la moitié. Or, alors qu'une grande partie des étapes de production en amont de la chaine de valeur de l'industrie électronique française est réalisée en Asie, ce phénomène ne s'applique que peu au segment de la sécurité qui maintient les étapes de la production en France en raison de sa proximité avec les secteurs régaliens. D'autres filières françaises se concentrent plus fortement sur des activités d'intégration en amont de la chaîne de valeur et sur des activités d'ingénierie pure (design, développement, etc.). Étant donné qu'une grande partie de la chaîne de valeur de l'industrie électronique de sécurité est réalisée depuis la France, le taux de valeur ajoutée augmente.

Enfin, la cybersécurité dans son ensemble correspond à près de 25 % du CA total de la filière de sécurité en 2018. Or, les services de cybersécurité mais également les produits de cybersécurité impliquent une très grande partie de travail humain hautement qualifié (développement de logiciels, etc.), et correspondent donc à un taux de valeur ajoutée très élevé.

L'offre française est fortement exposée à la **concurrence mondiale**. Le poids des acteurs étrangers est estimé à 30 %à 40 % du marché français si on inclut les services. Les acteurs dominants sont concentrés dans quelques pays (en particulier États-Unis et Israël).

Associée jusqu'ici à l'idée de contraintes et de dépenses, la cybersécurité doit être considérée aujourd'hui comme un atout compétitif et un investissement productif. **Un comportement cybersécurisé devient un critère de sélection pour les clients** soucieux à l'idée de confier des données personnelles, voire sensibles, à une entreprise.

---

[1] *Près de 6 % pour la période 2013-2016.*

[2] *En termes de valeur ajoutée, la filière industrielle de sécurité se place à la 11ème place des industries manufacturières françaises (sur 15), entre la filière bois et la filière électronique. En termes d'emploi, la filière industrielle de sécurité se place à la 10ème place des industries manufacturières françaises (sur 15), entre l'industrie chimique et l'industrie des équipements électriques. Étant donné la croissance de l'industrie française de sécurité, celle-ci devrait dépasser en valeur ajoutée la filière Bois, papier et imprimerie ainsi que l'industrie pharmaceutique dans un horizon proche.*

2. Les atouts de la France dans le marché de la cybersécurité

La France dispose d'atouts en matière de cybersécurité.

La France est en effet aujourd'hui **la quatrième nation la mieux armée en matière de cybersécurité derrière les États-Unis, Israël et la Grande-Bretagne.**

a) Des atouts technologiques

La France dispose d'atouts de premier plan pour pérenniser son avance technologique et économique, notamment dans trois domaines :

- **L'Intelligence Artificielle**, l'apprentissage automatique (***machine learning)*** et l'apprentissage profond (***deep learning)***[1]. Les GAFAM installent des centres de recherche à Paris et débauchent de nombreux talents français, leur proposant des rémunérations plus attractives. Du côté de la R&D publique, l'INRIA met en place des équipes mixtes composées à la fois d'informaticiens spécialisés dans le *deep learning* et de mathématiciens fondamentaux. Ces équipes sont dédiées en particulier aux stratégies de défense et d'attaque via le *deep learning* ;
- La France fait historiquement partie des leaders mondiaux de **cryptographie** et maintient sa position ;

---

[1] ***Le Machine learning*** *(apprentissage automatique) est la technologie la plus ancienne et la plus simple. Elle s'appuie sur un algorithme qui adapte lui-même le système à partir des retours faits par l'humain. La mise en place de cette technologie implique l'existence de données organisées. Le système est ensuite alimenté par des données structurées et catégorisées lui permettant de comprendre comment classer de nouvelles données similaires. En fonction de ce classement, le système exécute ensuite les actions programmées. Il sait par exemple identifier si une photo montre un chien ou un chat et classer le document dans le dossier correspondant. Après une première phase d'utilisation, l'algorithme est optimisé à partir des feedbacks du développeur, qui informent le système des classifications erronées et lui indiquent les bonnes catégories.*

Le ***Deep learning*** *(apprentissage profond) n'a pas besoin de données structurées. Le système fonctionne à partir de plusieurs couches de réseaux neuronaux, qui combinent différents algorithmes en s'inspirant du cerveau humain, permettant au système de travailler à partir de données non structurées. Cette approche est particulièrement adaptée pour les tâches complexes, lorsque tous les aspects des objets à traiter ne peuvent pas être catégorisés en amont. Le système identifie lui-même les caractéristiques discriminantes des données, sans avoir besoin d'une catégorisation préalable. Il n'a pas besoin d'être entraîné par un développeur. Il évalue lui-même le besoin de modifier le classement ou de créer des catégories inédites en fonction des nouvelles données. Tandis que le Machine learning fonctionne à partir d'une base de données contrôlable, le Deep learning a besoin d'un volume de données bien plus considérable et disposer de plus de 100 millions d'entrées pour donner des résultats fiables. Par ailleurs, la technologie nécessaire pour le Deep learning est plus sophistiquée. Elle exige plus de ressources et s'avère nettement plus coûteuse : elle n'est donc pas intéressante, du moins à l'heure actuelle, pour une utilisation de masse par les entreprises.*

- Dans la **technologie post-quantique**[1] (dont cryptographie), la France se maintient dans le « top trois » mondial. D'ici une dizaine d'année, les ordinateurs quantiques devraient atteindre des stades opérationnels. La cryptographie post-quantique est donc l'un des sujets de recherche les plus critiques pour la France.

La France est également en bonne position en *blockchain* et en sécurisation des objets connectés. Si la France dispose notamment de près de 1 000 chercheurs académiques affectés à temps plein à des thématiques de cybersécurité, l'Alliance pour la confiance numérique regrette que « *la recherche publique souffre cependant du peu d'effectifs dédiés au Big data* ».

b) Des start up dynamiques mais souvent rachetées pendant leur croissance

Selon M. Philippe Vannier, Président de l'Alliance pour la Confiance Numérique (ACN)[2], cette filière[3] se caractérise par : « *le dynamisme du taux de croissance annuel qui oscille chaque année autour de 10 %, l'apport de ce secteur au reste de l'économie avec un taux de valeur ajoutée supérieur à tous les autres domaines, ainsi que la qualité du tissu économique national composé à la fois de grands groupes leaders mondiaux, de PME-ETI très solides, de nombreuses start-up agiles et innovantes ainsi que d'une recherche académique de pointe* »[4].

Selon le « *radar 2019 des start-up en cybersécurité en France* » publié par Wavestone, **le nombre de start-up en cybersécurité a également augmenté de 18 % depuis janvier 2018** et les levées de fonds ont significativement progressé. Choisissant d'innover dans des domaines matures de la cybersécurité telle que la sécurité de la donnée, la gestion des identités et des accès ou encore la gestion des vulnérabilités, les start-up françaises misent de manière croissante sur l'international.

---

[1] *Voir à ce sujet la note n°18 de l'Office parlementaire d'évaluation des choix scientifiques et technologiques de juillet 2019 : http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2019_0071_note_cryptographies_quantiques_postquantiques.pdf*

[2] *Elle fédère les principaux acteurs français et européens de la confiance numérique, représente la filière auprès des pouvoirs publics. À ce titre, elle est membre de la FIEEC et participe aux travaux du Comité Stratégique de Filière des industries de sécurité.*

[3] *Elle comporte, selon l'ACN, la « Cybersécurité proprement dite », qui correspond à la sécurisation interne des systèmes numériques et associe les services (conseil, conception, mise en place, exploitation, formation), et les logiciels et solutions, destinés aux marchés professionnels (État et secteur public, installations critiques, entreprises, PME) et grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc.) et la « Sécurité Numérique », c'est-à-dire les produits et solutions électroniques de mise en œuvre de systèmes numériques pour instaurer la confiance dans le monde extérieur : gestion des identités, gestion des accès, biométrie, transactions, communications numériques, objets et véhicules connectés, processus industriels et logistique, transports, réseaux, villes intelligentes, etc. Les produits de sécurité numérique sont des produits matériels (cartes à puce, documents, lecteurs, etc.) ou des équipements (gestion des accès, biométrie, détection, localisation, communication, etc.).*

[4] *Introduction au rapport annuel de l'Observatoire de la filière de la Confiance Numérique, édition 2020.*

D'après l'Observatoire de la confiance numérique de 2019, la France comptait, en 2018, 2 088 entreprises dans le domaine, dont 65 grandes entreprises, 75 entreprises de taille intermédiaire et 636 PME et 1 355 micro-entreprises. L'offre en matière de cybersécurité est donc **très fragmentée** (63 % des entreprises de la confiance numérique font moins de 2 millions d'euros de chiffre d'affaires).

La France compte **des leaders mondiaux** sur les segments de la sécurité numérique (Thales, Airbus D&S, Atos), de la gestion des identités et des accès (Thales, Idemia, IN Groupe), des services de cybersécurité (Thales, Atos, Orange Cyberdefense, Cap Gemini, Sopra Steria), et de la sécurisation des paiements (Atos). Entreprise lilloise, Vade Secure est le leader mondial de la protection des messageries face aux menaces sophistiquées véhiculées par les e-mails, notamment le *phishing*, et les *malwares* avec plus de 1 milliard de boîtes aux lettres protégées dans 76 pays.

La France comporte également des start-up dynamiques et innovantes.

Les plus innovantes dans le domaine de la cybersécurité se voient récompensées par des prix décernés dans le cadre du Forum International de la Cybersécurité, organisé conjointement par la Gendarmerie nationale et CEIS, société de conseil en stratégie et en management des risques, avec le soutien de la Région Hauts-de-France. Le prix est parrainé par Atos, avec le soutien du CESIN.

Certaines de ces start-up sont regroupées dans le réseau FIRST (French Industrials for Resilience, Security & Trust).

QUELQUES PÉPITES FRANÇAISES DE LA CYBERSÉCURITÉ

CybelAngel, *spécialiste de la détection des fuites de données de grands groupes, détecte les menaces en-dehors du périmètre de l'entreprise et les résout avant qu'elles ne causent des dégâts en scannant chaque jour 3 milliards de pages qui échappent à Google. Créée en 2011, elle a fait son entrée dans le Next 40, ayant pour clientes la moitié des entreprises du CAC 40.*

Citalid : *Pionnier de la quantification et du pilotage du risque cyber en Europe, le logiciel Citalid évalue dynamiquement l'exposition financière des entreprises aux menaces informatiques. Capable de simuler l'impact de chaque investissement sur la réduction du risque, il permet aux décideurs de rationaliser leur arsenal cyber et d'assurer leur risque résiduel de façon optimale.*

Olvid *est une messagerie instantanée unique, dont la sécurité ne repose plus sur les serveurs mais uniquement sur la cryptographie. Nous apportons la preuve mathématique de l'inviolabilité des communications. Résultat : une application aussi facile d'usage que WhatsApp, sans fuites de données, qui ne collecte aucune donnée personnelle et dans laquelle l'usurpation d'identité est impossible.*

Oxibox *est une solution de cyber-résilience, garantissant la capacité de retour à la normale des systèmes informatiques après une cyberattaque en quelques minutes. Avec un déploiement simple, rapide et compatible avec tous les environnements, nous rendons les sauvegardes invisibles et incorruptibles par les ransomwares.*

TheGreenBow. *Avec plus d'un million et demi d'utilisateurs à travers le monde, TheGreenBow est le logiciel Client VPN le plus éprouvé. Disponible sur plusieurs plateformes, il permet d'établir des connexions sécurisées aussi bien pour des postes nomades, que pour des accès extranet de type télétravail ou des applications gouvernementales.*

Vates *est l'éditeur français de solutions de virtualisation open source. L'entreprise développe son propre hyperviseur basé sur Xen, XCP-ng, et sa solution d'administration et de backup de machines virtuelles, Xen Orchestra. Vates investit massivement dans le durcissement et la sécurisation de son hyperviseur et exporte massivement son expertise en Europe et dans le monde.*

Seela *est une plateforme de e-learning permettant la réalisation de parcours de formation dans les domaines des réseaux, du SI et de la Cybersécurité notamment au travers son accès à la CyberRange d'Airbus CyberSecurity.*

RESCO Courtage *est un courtier en assurance spécialisé dans les risques Sécurité, Sûreté et Cyber. Expert en protection des entreprises, sa mission est de conseiller les entreprises et de rechercher avec réactivité et discrétion, les meilleures solutions d'assurance face aux actes de malveillance et à la cybercriminalité.*

Source : FIRST

Cet écosystème est extrêmement dynamique et évolue rapidement. De nombreuses « pépites » françaises de la French Tech sont rachetées par les géants du numérique, lors des levées de fonds, faute de la disponibilité d'un financement français.

Pour certains experts[1], **«** *avec leurs données et leurs algorithmes, les géants d'Internet peuvent détecter les menaces concurrentielles et racheter les start-ups qui peuvent devenir leurs rivales. Ils peuvent également manipuler les marchés qu'ils hébergent, par exemple en faisant réagir rapidement leurs algorithmes afin que les concurrents n'aient aucune chance de gagner des clients* »[2].

[1] *« Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy » Ariel Ezrachi de l'Université d'Oxford, et Maurice Stucke de l'Université du Tennessee, 2016.*

[2] *Rapport de la Plateforme RSE sur la responsabilité numérique des entreprises, 2020.*

B. UN PARTENARIAT PUBLIC-PRIVÉ APPELÉ À S'APPROFONDIR

1. La stratégie publique de développement du marché de la cybersécurité

Contrepartie de l'impossibilité de cyberprotéger toutes les PME et TPE, **la stratégie de l'État vise à encourager le développement d'un écosystème de la cybersécurité** : « *à l'horizon 2025, l'objectif assigné à cette stratégie est l'atteinte d'un chiffre d'affaires de 25 Md€ pour la filière (soit un triplement du chiffre d'affaires actuel), le doublement des emplois dans le secteur en passant de 37 000 à 75 000 emplois et l'émergence de trois licornes françaises en cybersécurité* », selon les annonces gouvernementales du 18 février 2021.

LES ACTIONS DE STRUCTURATION DE L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ

Appel à projets (AAP) visant à soutenir le développement de briques technologiques critiques (2021/2022)

La stratégie d'accélération cyber prévoit de consacrer un total de 400 M€, dont 200 M€ de financements publics, pour des projets de recherche et développement cofinancés avec les acteurs privés de la cybersécurité. Les thématiques visées seront dévoilées progressivement, les levées de dossiers afférentes étant prévues tout au long des années 2021 et 2022.

Lancement des programmes et équipements prioritaires de recherche (PEPR)

Co-pilotés par le CNRS, l'INRIA et le CEA, ils ont vocation à financer la recherche amont et à soutenir l'excellence scientifique française.

Soutien aux projets du Campus Cyber (2021/2022)

Le Campus Cyber constituera à partir du 4ème trimestre 2021 le lieu totem de la cybersécurité en France. La stratégie d'accélération cyber prévoit 100 M€, dont 50 M€ de financements publics issus du 4ème Programme d'Investissement d'Avenir (PIA4), pour des projets collaboratifs entre les membres du Campus.

Appel à manifestation d'intérêt (AMI) « Sécuriser les territoires » (lancé le 18/03/2021), puis appel à projets (AAP) (2021)

La stratégie d'accélération cyber prévoit de soutenir la mise en place de démonstrateurs de cybersécurité visant une collectivité locale, un ou plusieurs établissements de santé et un port. Ouvert du 18/03/21 au 16/06/21, l'AMI vise à sélectionner les structures qui accueilleront les démonstrateurs. Les AAP sélectionneront les entreprises qui les développeront. 40 M€, dont 20 M€ de financements publics du PIA4, sont dédiés à ce projet.

Renforcement du niveau de sécurité de l'État (2021/2022)

La stratégie d'accélération a prévu d'attribuer à l'Anssi (Agence nationale de la sécurité des systèmes d'information) un budget complémentaire de 136 M€ destiné à renforcer la cybersécurité des organismes critiques de la sphère étatique. Le pilotage est assuré par l'Anssi.

Mise en place d'une journée « autonomie et sécurité numérique » (2021)

Cet événement est destiné à mettre en relation des acheteurs publics et des directeurs de la sécurité de l'information d'organismes publics avec des PME et des startup françaises du secteur de la cybersécurité. Il permettra de mieux faire connaitre aux premiers les solutions proposées par les seconds.

Mise en place d'un « observatoire des métiers et des qualifications de la sécurité du numérique » (2021/2022)

Cet observatoire analysera les besoins en compétences et l'adéquation avec les formations existantes pour le secteur de la cybersécurité.

Conclusion du Grand Défi cyber, soutenu par le PIA4

AMI pour la création d'un startup studio spécialisé en cybersécurité pour aider à la création de startup cyber et amener des financements dès l'amorçage ;

Plusieurs AAP pour la mutualisation et la valorisation des données d'intérêt cyber ;

Lancement de la tranche 2 des axes verticaux du Grand Défi.

La cybersécurité et la sécurité de l'Internet des objets est l'une des cinq priorités du contrat stratégique de la filière « industries de sécurité » du 29 janvier 2020, avec la sécurité des grands évènements et des Jeux Olympiques de Paris 2024, l'identité numérique, les territoires de confiance et le numérique de confiance. Il s'agit de *« positionner l'industrie française comme **leader mondial** de la cybersécurité et de la sécurité de l'IoT »*.

L'objectif est ambitieux. Il compte **quatre axes** :

- L'axe 1, « *Faire de la France une terre de cybersécurité* », consiste à mettre en place les dispositifs destinés à rendre le grand public plus averti des risques cyber, renforcer l'attractivité des métiers de la cybersécurité et de la France, et assurer des capacités d'enseignement et de formation nécessaires à tous les niveaux.
- L'axe 2, « *Mobiliser les territoires* », vise à dynamiser les énergies et les intelligences disponibles sur l'ensemble de nos territoires pour coordonner les initiatives locales, et contribuer à leur mise en cohérence en réponse aux besoins de cybersécurité de la filière, et des bassins industriels français.-
- L'axe 3, « *Forum État Industrie Utilisateurs* », projette de créer un outil de dialogue et d'actions coordonnées entre l'État, l'industrie et les utilisateurs afin d'échanger sur les besoins, le cadre réglementaire, les contraintes et les opportunités générées par l'environnement international dans le secteur de la cybersécurité.
- L'axe 4, « *Doter la France d'une offre de rang mondial* », consiste à développer en bonne collaboration des démonstrateurs, prototypes et projets susceptibles de hisser l'industrie de cybersécurité française aux premiers rangs de l'offre mondiale.

- L'axe 5, « *Déployer des actions structurantes pour l'écosystème dans le cadre du campus cyber* », fait le lien entre le contrat stratégique de filière et le campus cyber, qui aura une vocation très opérationnelle, à la différence du forum qui sera une instance stratégique. Le campus pourra mettre en place des actions du contrat de filière.

2. Un Pôle d'excellence cyber en Bretagne

La cybersécurité suppose une vaste coalition des acteurs publics et privés et la conjugaison de leurs efforts.

Elle existe déjà **en Bretagne** au sein du **Pôle d'excellence cyber** qui relie industriels, établissements d'enseignement, laboratoires de recherche, startups et PME.

Initié en 2014 par le ministère des Armées et par le Conseil régional de Bretagne avec une portée nationale et un objectif de rayonnement international, le Pôle d'excellence cyber s'appuie sur le tissu académique et industriel régional ainsi que sur des partenaires nationaux ou d'autres territoires.

Le Pôle d'excellence cyber a pour mission de stimuler le développement de l'offre de formation cyber (initiale, continue, supérieure), de la recherche académique cyber, et de la base industrielle et technologique de cybersécurité, avec une attention particulière portée aux PME-PMI innovantes, y compris à l'export. Il répond ainsi à trois enjeux majeurs, au profit de la communauté nationale de cyberdéfense et de cybersécurité : des compétences nécessaires pour répondre aux besoins de développement de la filière, une offre de recherche en adéquation avec les besoins du ministère et des industriels, des produits et services de confiance.

Il regroupe actuellement une trentaine de membres actifs : douze grands groupes (Airbus Cyber Security, Bertin IT, Capgemini, DCI, EDF, La Poste, Naval Group, Nokia, Orange, Sopra Steria, Thales), des PME et plus d'une quinzaine de laboratoires, d'universités et d'écoles d'ingénieurs

Il accompagne également les entreprises dans la définition d'offres, de services et de stratégies intégrant la cybersécurité. Enfin, il aide les startup et PME développant des produits innovants à grandir et se développer.

Ce pôle régional sera prochainement complété par un Campus Cyber à la Défense.

3. Le futur Campus Cyber à la Défense

Lancé le 16 juillet 2019, le rapport de Michel Van Den Berghe[1] sur la faisabilité d'un « Campus Cyber » dédié aux enjeux du numérique doit se concrétiser à l'automne 2021. Ce « *lieu totem de la cybersécurité* » rassemblera les principaux acteurs nationaux et internationaux du domaine. Il permettra en particulier d'accueillir sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de la formation, des acteurs de la recherche et des associations afin de renforcer les synergies.

Le Campus Cyber prévoit de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. Des déclinaisons de Campus en région sont prévues dans les années à venir. À ce jour, plus de 60 acteurs, issus d'une pluralité de secteurs d'activité, ont indiqué leur volonté de participer au Campus.

Il devra promouvoir l'excellence française en matière de cybersécurité, en fédérant les talents et les acteurs du secteur dans un lieu commun, autour de projets d'innovation, faciliter les projets multipartites et développer les communs de la sécurité et de la confiance numériques.

Le Campus Cyber est fondé sur **quatre piliers** :

- **Les opérations** : favoriser le partage de données pour renforcer la capacité de chacun à maitriser le risque numérique (détection, capacités de veille, réponse aux incidents, mise en commun de la connaissance sur la menace) ;
- **La formation :** soutenir la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiant(e)s, personnel en reconversion…) afin de favoriser une montée en compétence globale de l'écosystème (programmes communs, partage de ressources) ;
- **L'innovation** : développer les synergies entre les acteurs publics et privés (industriels, start-up et centres de recherche) pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique ;
- **L'animation** : proposer un lieu ouvert, vivant, dédié à la programmation d'événements innovants, propice aux échanges et à la découverte des évolutions (conférence, webinaires, showroom, jobdating, etc.).

Le pilotage opérationnel du Campus Cyber sera assuré par une Société par Actions Simplifiée (SAS), actuellement en cours de création, détenue à **51 % par le secteur privé** (industriels, PME, start-up) et **49 % par le secteur public.**

Le Campus cyber sera **localisé à La Défense dans la tour « Eria »** avec une possible extension dans les prochaines années sur le plateau de

[1] *https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport.pdf et audition du 11 mars 2021.*

Satory, à Versailles (78), afin de répondre à certains besoins spécifiques d'acteurs industriels.

En tant qu'acteur central de l'écosystème de la cybersécurité en France, l'ANSSI s'investit dans ce projet pour soutenir et participer à sa création. Si les capacités et l'engagement de l'État demeurent essentiels, le renforcement du niveau de sécurité numérique dépendra aussi de l'association étroite des différents acteurs nationaux, publics et privés, pour pleinement garantir la sécurité de la transformation numérique.

C. UN OBJECTIF DE LONG TERME : LE CLOUD SOUVERAIN

1. L'enjeu du cloud

La transition numérique des entreprises est confrontée à un dilemme. L'hébergement de leurs données sur des serveurs d'entreprises non-européennes, les expose à **des risques judiciaires et industriels**. Cet hébergement est **toutefois une condition de leur croissance**.

L'ENJEU ÉCONOMIQUE DU CLOUD SOUVERAIN

Le cloud permet à ses utilisateurs de confier la gestion de leurs données et de leurs systèmes d'information à un tiers. Ce tiers est un fournisseur de services qui, sur un principe de location, met à la disposition de ses clients ses capacités hardwares et/ou softwares. Il se charge notamment d'assurer la sécurité et le bon fonctionnement des ressources informatiques qu'il héberge. C'est ce qu'on appelle l'infogérance.

Les données hébergées par un prestataire sont stockées au sein de centres de données, ou datacenters. L'utilisateur y accède alors grâce au réseau Internet (ou à un intranet dans le cas de clouds particuliers). Aujourd'hui, compte tenu de la vitesse de circulation des données sur les réseaux, les datacenters ne doivent plus impérativement se situer à proximité des utilisateurs. Ils peuvent être implantés de l'autre côté du globe sans que cela n'entrave le fonctionnement d'un cloud. Datacenters, utilisateurs et prestataires peuvent alors dépendre d'États différents. Et c'est là que le bât blesse.

Un prestataire se doit de garantir la confidentialité des données hébergées sur son cloud. Certains gouvernements disposent toutefois d'une législation leur permettant d'accéder aux données. Cette accessibilité devient un enjeu de souveraineté lorsque les données en question émanent de citoyens ou d'organisations d'un autre État. L'autorité de ce dernier sur ses propres données n'est effectivement pas reconnue, du moins n'est pas respectée. En outre, en accédant aux données d'un État tiers, un gouvernement accède à des ressources qui ne lui appartiennent pas et dont l'exploitation présente une grande valeur stratégique et économique.

« Le cloud souverain et la stratégie géopolitique française : 3 questions à Clotilde Bômont »
Sciencespo.fr, 21 décembre 2020.

Par ailleurs, l'enjeu économique est crucial : « *comment permettre aux acteurs européens de capter ce marché en forte croissance tout en favorisant un cloud souverain et en permettant aux entreprises, administrations publiques et particuliers d'accéder aux meilleures technologies ?* »[1].

En effet, le marché du cloud s'établissait **en 2020 à 270 milliards** de dollars (contre 233,4 milliards en 2019), soit quasiment deux fois plus qu'en 2016.

La croissance du cloud doit s'accélérer. En 2021, le marché devrait atteindre plus de 332 milliards de dollars, 400 milliards de dollars en 2022 et même **plus de 1000 milliards de dollars en 2024 !**

2. Une souveraineté numérique perdue

Le marché mondial de l'industrie du stockage des données (le *cloud)* est **dominé par quatre acteurs américains qui possédaient 65 % de parts de marché fin 2020 :** Amazon (33 %), Microsoft (18 %), Google (9 %), Alibaba (5 %), IBM (5 %), Salesforce (3 %), Tencent (2 %), Oracle (2 %), NTT (1 %) et SAP (1 %).

En Europe, il a enregistré une croissance de 27 % par an entre 2017 et 2019, est estimé à 53 milliards d'euros en 2020 et **devrait atteindre 300 à 500 milliards d'euros d'ici 2027-2030[2].**

Si **les États-Unis dominent** le marché des services applicatifs (*SaaS* ou *Software as a service*), et le marché européen du cloud, avec trois acteurs majeurs (les « hyperscalers »), qui captent, sur le marché de l'Infrastructure en tant que Service (IaaS), **70 % de parts de marché** : Amazon avec AWS (53 %), Microsoft avec Azure (9 %) et Google Cloud (8 %). Cependant, les spécialistes du cloud et les opérateurs télécoms européens gagnent progressivement de l'importance sur leurs marchés nationaux. Ainsi OVHcloud et Deutsche Telekom se classent troisième et quatrième dans leur pays sur les marchés infrastructures et plates-formes. On peut également citer en France : Atos, Orange Business Services ou encore Outscale.

En France, Amazon occupait, en mai 2020, 30 % du marché, Microsoft 20 % et OVHcloud dépassait 10 %. Amazon représente plus de trois fois la taille d'OVHcloud en termes de revenus dans le cloud d'infrastructure en France.

---

[1] *« Le cloud, un marché d'envergure à capter pour la France et l'Europe », Patrick Randall, Les Numériques, 24 mai 2021.*

[2] *Livre blanc KPMG, avril 2021. Ce Livre blanc a été construit à partir de données et de ressources émanant d'une variété de sources, dont plus de 250 entretiens avec des décideurs publics et privés européens. L'étude a été menée sur une période de 8 semaines entre janvier et mars 2021 et réalisée grâce au soutien et à la contribution active d'InfraNum, ainsi que de Talan, OVHcloud et Linkt.*

OVHcloud, entreprise fondée en 1999, s'est développée dans ce secteur à la fin des années 2010. Elle propose des prestations de cloud public et privé, des serveurs dédiés, de l'hébergement mutualisé, du *housing* (ou colocation), de l'enregistrement de noms de domaines, de la fourniture d'accès Internet et fibre, ainsi que de la téléphonie sur IP.

La société affirme desservir plus d'un million et demi de clients, en s'appuyant sur un réseau de 23 *datacenters*[1] répartis entre l'Europe, l'Amérique du Nord et l'Asie-Pacifique. L'entreprise, qui a déployé son propre réseau de fibre optique à travers le monde, revendique une capacité totale de 20 Tbit/seconde et plus de 260 000 serveurs physiques hébergés, soit l'un des plus grands parcs mondiaux de serveurs.

Le 10 novembre 2020 OVHcloud a annoncé avoir signé un partenariat stratégique avec Google, permettant à OVHcloud d'accéder à la technologie Anthos, une solution d'exploitation cloud à destination des entreprises, que l'entreprise française exploitera avec ses équipes et ses propres infrastructures.

Cette domination suscite des craintes en Europe, notamment sur la protection des données sensibles des entreprises depuis l'adoption du ***Cloud Act*** aux États-Unis en 2018.

Un usage abusif de cette législation à des fins d'espionnage économique et industriel a été évoqué. Dans la pratique, les demandes concernant les entreprises seraient extrêmement rares. Selon une experte : « *il paraît donc difficile de prévoir ce qu'un juge américain déciderait s'il devait mettre en balance une demande de communication de données d'une personne morale française fondée sur le Cloud Act avec les lois françaises de blocage ou sur le secret des affaires. Force est de constater que sur le plan des données non personnelles, la législation française (et européenne) peine à apporter un gage de sécurité suffisant* »[2].

Cette dépendance manifeste est devenue un objet de débat public depuis que **l'État a choisi Microsoft pour l'hébergement des données médicales des Français** (*Health Data Hub*). Le professeur Didier Sicard, ancien président du Comité consultatif national d'Éthique et spécialiste des données de santé, a ainsi considéré[3] que : « *On offre aux Américains une richesse nationale unique au monde* », compte tenu des ambitions des GAFAM en matière d'assurance de santé[4].

---

[1] *Centre de données, c'est-à-dire un lieu et un service regroupant des équipements constituants du système d'information d'une ou plusieurs entreprise(s) : ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc...*

[2] *« Le "Cloud Act", trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique », Laura Brincourt, DiploWeb.com, 16 mai 2021.*

[3] *Dans une tribune de l'Obs du 23 juin 2020.*

[4] *« Ces données sont une mine d'or pour les GAFAM, qui veulent désormais investir le domaine prudentiel. En effet, ces entreprises ne souhaitent pas directement devenir des acteurs du soin. Ce*

Sénateurs[1] et députés[2] se sont saisis de la question, avec une mission d'information en cours à l'Assemblée nationale sur la souveraineté numérique.

De même, la **DGSI** (Direction Générale de la Sécurité Intérieure) a choisi la société **Palantir**, initialement financée par la CIA, pour traiter les données de **l'antiterrorisme** en France.

Un émoi comparable a été provoqué par le **choix d'Amazon par Bpifrance** pour deux services. Le premier est l'hébergement des attestations des prêts garantis par l'État (PGE), une aide mise en place depuis mars 2020 pour soulager la trésorerie des entreprises. Le second est lié à une tournée dédiée à l'entreprenariat, organisée par Bpifrance, qui se déroulera au cours de l'été 2021, durant lequel l'entreprise proposera des modules de formation sur la numérisation des PME.

Or, pour la première application, l'entreprise candidate au PGE doit notamment fournir des renseignements sur son chiffre d'affaires hors taxe de 2019, la masse salariale annuelle constatée et le montant de l'emprunt demandé, qui constituent des informations stratégiques de l'entreprise.

L'invalidation[3], le 16 juillet 2020, du *Privacy Shield*, négocié entre 2015 et 2016, qui autorisait les entreprises européennes à transférer des données personnelles en outre-Atlantique, en reconnaissant que la législation américaine offrait les mêmes garanties que le droit européen, a créé une situation juridique fragile et délicate[4].

La sécurisation du cloud est un enjeu majeur, la moitié des entreprises prévoyant d'y transférer toutes leurs données d'ici deux ans[5].

---

secteur nécessite des investissements beaucoup plus risqués sur le long terme. Leur objectif sera plutôt d'utiliser les données qu'elles ont pu acquérir et leur capacité de traitement de ces données pour modéliser les risques liés à la santé de chaque individu et ainsi optimiser les profits de leurs services d'assurances. Le secteur de l'assurance devient l'une des cibles prioritaires des grands acteurs industriels des technologies. Ainsi, Verily, entreprise détenue par Alphabet, la maison-mère de Google, vient d'annoncer que le groupe se lançait dans le secteur de l'assurance santé avec sa nouvelle division Coefficient », « Au-delà du « sovereignty-washing *» : 3 questions à Bernard Benhamou sur le cloud souverain en France », Sciencespo.fr, 2 septembre 2020.*

[1] *Proposition de résolution n° 576 du 26 juin 2020 du Sénat, tendant à la création d'une commission d'enquête sur la protection des données de santé, présentée par Mme Nathalie Goulet.*

[2] *« Souveraineté numérique : lettre à Emmanuel Macron » par un collectif de députés et de professionnels de la tech », La Tribune, 9 mars 2021.*

[3] *Au motif que les programmes de surveillance américains ne sont pas compatibles avec les principes du Règlement général sur la protection des données (RGPD) et permettent aux autorités américaines d'avoir un accès très large aux données traitées par les entreprises alors que les citoyens européens n'ont pas de recours effectifs aux États-Unis leur permettant de maîtriser pleinement leurs données personnelles.*

[4] *Le Health Data Hub a mandaté le 11 janvier 2021 le cabinet d'avocats parisien DLA Piper pour évaluer les conséquences juridiques de cette décision selon NextImpact, 2 février 2021.*

[5] *Étude Oracle/KPMG « Cloud threat report 2020 » menée auprès de 750 professionnels de la cybersécurité et de l'informatique en France et dans le monde entier.*

Près de 90 % des entreprises utilisent des logiciels en mode SaaS (Software as a Service) et 76 % utilisent aujourd'hui du IaaS (Infrastructure as a Service).

Toutefois, **les professionnels de la cybersécurité craignent qu'une approche fragmentée de la sécurité des données et des services mal configurés n'altèrent les nouveaux modèles de sécurité dans le cloud**. « *Seuls 8 % des responsables sécurité informatique (RSI) déclarent comprendre parfaitement le modèle de sécurité à responsabilité partagée des services cloud. Alors que les entreprises transfèrent plus que jamais des charges de travail critiques vers le cloud, cette forte croissante de la consommation de cloud a créé des zones d'ombres avec des équipes IT et des fournisseurs de services cloud qui cherchent à comprendre leur degré de responsabilité quant à la sécurité des données* » selon Oracle.

Ces professionnels se méfient des fournisseurs de services cloud ; 80 % d'entre eux craignent que ceux avec lesquels ils traitent ne deviennent des concurrents sur leurs propres marchés. Une forte majorité (75 %) considère le cloud public comme étant mieux sécurisé que leurs propres datacenters. Pourtant, 92 % d'entre eux ne pensent pas que leur entreprise soit bien préparée pour adopter correctement les services du cloud public.

L'origine de ces inquiétudes repose en partie sur le maintien d'anciens modèles de sécurité qui sont devenus inadaptés car les systèmes en place, très souvent mal configurés, restent constamment confrontés à de nouvelles failles de sécurité.

3. Une volonté européenne de reconquête de la souveraineté dans le cloud

Le Sénat a exprimé cet objectif de **souveraineté européenne numérique** dans la Résolution européenne pour une cybersécurité robuste en France, qu'il a adoptée le 26 mai 2018[1]. Il a alors appelé à une : « *véritable politique industrielle européenne dans le domaine de la cybersécurité, susceptible de renforcer la souveraineté européenne dans le monde numérique* », objectif explicité dans le rapport de la commission d'enquête du Sénat sur le devoir de souveraineté numérique - n°7 (2019-2020) de M. Gérard Longuet - du 1er octobre 2019. L'Assemblée nationale conduit actuellement une mission d'information de la conférence des Présidents sur la souveraineté numérique nationale et européenne.

« *Le projet d'un cloud Souverain répond à des considérations politiques d'indépendance technologique et de sécurité, mais aussi à des considérations économiques et industrielles.* ***Laisser des entreprises étrangères acquérir un savoir-faire industriel dans le domaine du cloud tout en empêchant les acteurs européens de se développer et d'évoluer afin d'apporter une***

[1] *N°109 (2017-2018).*

alternative compétitive constitue une erreur critique » estime le Secrétaire général de l'Institut de la Souveraineté Numérique[1].

Les autorités européennes sont désormais engagées dans cette voie. Le commissaire européen au marché intérieur, M. Thierry Breton, a ainsi déclaré le 20 août 2020 que : « *ce qui fait le succès de l'Internet, c'est son caractère mondial. En ce qui nous concerne nous, Européens, nos données, c'est ce que nous avons de plus précieux en matière industrielle. J'ai toujours dit que je souhaitais que* ***les données des Européens soient traitées, stockées et processées en Europe*** **».** La construction d'un cloud européen souverain est une œuvre de longue haleine.

4. Des occasions manquées : une politique publique non maîtrisée de reconquête de la souveraineté dans le cloud

La volonté de retrouver la souveraineté des données est régulièrement évoquée en France depuis 2010. **Cependant, les actes n'ont pas suivi les discours**, ce qui est **emblématique de l'insuffisance maîtrise d'une politique publique dans un domaine pourtant incontestablement stratégique**.

Dans un premier temps, l'État a soutenu, en 2011, le « **Projet Andromède** », proposé par Orange, Thales et Dassault Systèmes. Cependant, dès s**eptembre 2012, un** désaccord entre Dassault Système et Orange aboutit à la création de deux entreprises. D'un côté, Orange et Thalès lancent **Cloudwatt**. De l'autre, Dassault Systèmes est rejoint par SFR et Bull pour former **Numergy. Les deux tentatives sont des échecs et ferment en 2020.**

L'État a peiné à se doter d'une stratégie claire, cohérente et continue. Ces errements sont détaillés en annexe.

Dans un effort de clarification, une circulaire a déterminé, en 2018, **trois offres de *cloud* organisées en cercles** :

- Le premier s'appuie sur un *cloud* interne à l'État, fonctionnant sur une base OpenStack, pour des données, des traitements et des applications sensibles et pour répondre à des besoins régaliens d'infrastructures numériques ;
- Le deuxième repose sur un *cloud* dédié, développé par un partenaire industriel mais adapté pour les besoins de l'État d'une sensibilité moindre, mais nécessitant un certain niveau de pérennité ;
- Le troisième définit quant à lui le recours à des offres génériques de *cloud* externe de prestataires extérieurs.

---

[1] *« Au-delà du «* sovereignty-washing *» : 3 questions à Bernard Benhamou sur le cloud souverain en France », Sciencespo.fr, 2 septembre 2020.*

Il n'en demeure par moins que **cette stratégie publique peine à suivre les évolutions rapides du marché**. C'est ainsi que, dans le rapport de la commission d'enquête du Sénat sur le devoir de souveraineté numérique du 1er octobre 2019, « *la **nécessité d'anticiper** le changement majeur à venir pour le stockage des données informatiques, à savoir le **passage de 80 % des données stockées dans le cloud à 80 % des données stockées en edge computing***[1]*, ou « informatique en périphérie » en raison du développement exponentiel des objets connectés (tels que les montres, les enceintes et les assistants connectés ou encore les véhicules autonomes, etc...)* » est souligné. Le rapport appelle l'État **à se doter dès maintenant d'une stratégie claire** sur cette nouvelle technologie.

5. Un ralliement pertinent de la France au projet GAIA-X

Initiative franco-allemande, GAIA-X ne vise pas à créer une entreprise superpuissance capable d'offrir les mêmes services que les géants américains, mais plutôt à construire une **infrastructure européenne des données**. Concrètement, le projet prendra la forme d'une **entité de gouvernance qui édictera de grands principes de sécurité, d'interopérabilité et de portabilité des données permettant à des entreprises de proposer leur offre de service compatible avec GAIA-X.**

Ce projet a reçu le soutien **l'*European Cloud User Coalition***, une coalition de 13 banques européennes[2] qui veulent établir de nouveaux standards sur le stockage des données.

Le 9 décembre 2020, le **French GAIA-X Hub** a été lancé. Il est animé par le CIGREF (Club informatique des grandes entreprises françaises), une association à but non lucratif composée d'un réseau de grandes entreprises et administrations publiques françaises, et à ses partenaires, le pôle de compétitivité Systematic Paris-Région[3] et l'Académie des technologies. Il regroupe plus de 150 grandes entreprises et organismes français de tous les secteurs d'activité.

---

[1] *Architecture de technologie d'information distribuée qui se caractérise par une puissance de traitement décentralisée. Le* edge computing *permet de traiter des données de façon directe par le périphérique qui les produit (ou par un ordinateur local). Il n'est, dès lors, plus nécessaire de transmettre les données à un centre de données distant afin de pouvoir les traiter. Par rapport au* cloud computing*, cela revêt trois principaux avantages provenant justement de l'absence de transmission du point d'émission des données au point de stockage et de traitement : une réduction du temps de latence du traitement de l'information, un meilleur niveau de sécurité et une réduction des coûts.*

[2] *Parmi les banques qui prennent part au projet : l'italien Unicredit, les banques néerlandaises ING et KBC, les autrichiennes Erste Bank et Bawag, la Swedbank de Suède et l'irlandaise Allied Irish Banks. L'initiative remonte à 2019 et part du groupe bancaire allemand Commerzbank.*

[3] *Systematic, pôle européen des « Deep Tech », rassemble et anime depuis sa création en 2005, une communauté de près de 900 membres adhérents, dont près de 600 start-ups, PME et ETI, 140 grands groupes, 140 académiques, un collège des investisseurs et un collège d'une vingtaine de collectivités.*

Pour le lancement, un binôme composé par l'hébergeur français **OVHcloud** et la société appartenant à Deutsche Telekom **T-Systems** collabore pour créer une plateforme qui sera la base du lancement des futurs prototypes.

Cette nouvelle orientation de la stratégie acte le fait que le secteur privé a pris une avance non rattrapable : « *alors que les investissements colossaux et les économies d'échelle dont bénéficient les géants du numérique américains et chinois rendent improbable la naissance d'un leader unique sur le territoire national, une stratégie axée sur un catalogue de solutions complémentaires, la collaborations entre experts de différents segments du marché et la portabilité des données permet aux acteurs soucieux de localiser leurs données dans des data centers européens d'avoir recours aux services de plusieurs entreprises "compatibles" avec Gaia-X* » selon un expert[1] qui estime que la réussite de cette stratégie fondée sur l'interopérabilité entre différents acteurs économiques européens, « *dépendra de deux facteurs déterminants en matière de souveraineté numérique : notre vigilance vis-à-vis des choix technologiques qui seront opérés dans le cadre de cette initiative et la mise en place d'une politique cohérente quant à l'usage des clouds souverains et non-souverains dans l'espace public européen* ». Il faudra également **faire coopérer des entreprises européennes et non européennes parfois concurrentes au-delà des 22 membres fondateurs.**

Ce projet est ainsi ouvert aux acteurs américains du cloud au travers de leurs filiales européennes : Google Cloud (via Google Ireland), AWS (via Amazon Europe Core S.a.r.l au Luxembourg), Azure (via Microsoft NV). Ou encore Cisco, Bit4id, Oracle Corporation, Palantir Technologies, Salesforce, Snowflake. On recense également **les acteurs chinois** Alibaba Cloud et Haier Cosmo IoT Ecosystem Technology.

Selon M. Alban Schmutz, de Gaia-X : « *Gaia-X est ouvert à tous ceux qui acceptent les principes définis par les Policy Rules, y compris les acteurs américains. Ils peuvent alors entrer dans les groupes techniques, participer à l'architecture et proposer des services. En revanche, ne peuvent être élues au Board que des organisations ayant leur siège social mondial en Europe*. ».

« *Les acteurs américains du cloud sont bienvenus et leurs connaissances des services cloud peuvent être utiles aux instances techniques qui élaborent les API et les services de base du métacloud européen, mais ils n'auront pas voix au chapitre en matière de gouvernance et de valeurs européennes* » [2] en matière de gestion des données privées, d'ouverture, de réversibilité des services et de possibilité de changer de fournisseur.

---

[1] *« Le cloud souverain est de retour : généalogie d'une ambition emblématique de la souveraineté numérique en France », Sciencespo.fr, 20 juillet 2020 par Pierre Noro.*

[2] *« Microsoft, Google, Amazon sont officiellement membres de Gaia-X », Loïc Duval, News Informatique, 19 novembre 2020.*

6. Une nouvelle « stratégie nationale pour le cloud »

Dans la conférence de presse présentant la Stratégie nationale pour le cloud, le 17 mai 2021, M. Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance a imputé à l'échec des premières tentatives de réappropriation du cloud au fait que : « *nous n'avions pas tenu compte ni des réalités technologiques, ni des attentes des entreprises ni de celle des administrations* ».

La stratégie publique actuelle vise donc à faciliter l'émergence d'un marché de confiance du *cloud*, c'est-à-dire à proposer aux entreprises ainsi qu'à la puissance publique des offres diversifiées, performantes et sécurisées. Ces travaux ont vocation à promouvoir les offres *cloud* européennes se différenciant par leur niveau de confiance.

Elle se fonde sur le double constat, d'une part du caractère « *désormais incontournable pour les entreprises* » et du caractère non moins incontournable de la domination du cloud par des « *acteurs internationaux dont certains sont soumis à des lois à portée extraterritoriale* ».

Pour la première fois est reconnue de façon explicite par l'État que « *les entreprises se retrouvent souvent* ***dépendantes*** *de leur fournisseur cloud* », qui peut imposer des conditions de sortie très complexes.

Cette stratégie, qui décline le projet Gaïa X, repose sur **trois piliers** :

- Un **label cloud de confiance**, démarche de promotion du visa de sécurité SecNumCloud, déjà évoqué, qui doit garantir la réversibilité, l'interopérabilité, la transparence et la portabilité, conditions définies dans le projet Gaïa X. Pour autant, ce label ne va pas aussi loin que l'avait demandé le CIGREF dans un communiqué de presse du 2 février 2021, souhaitant : « *le développement de dispositions légales incitant les entreprises ayant recours au cloud à renforcer la protection de leurs données sensibles, et des traitements associés, en les confiant aux fournisseurs cloud dont les offres seraient conformes à un référentiel de confiance, auditable et maîtrisé* »[1]. Lors de la conférence de presse du 17 mai 2021, son président a estimé qu'il fallait également « *clarifier les régimes juridiques auxquels les fournisseurs de service cloud sont soumis* »

- Une **doctrine** de la transformation numérique de l'État, **cloud au centre**, qui devient la méthode d'hébergement par défaut des services numériques de l'État.

  Le programme de formation continue des agents publics de la filière numérique comportera un volet cloud.

---

[1] https://www.cigref.fr/wp/wp-content/uploads/2021/02/@Cigref_communique_annee_zero_cloud_de_confiance_02022021.pdf

Chaque produit numérique manipulant des données sensibles comme des données économiques relatives aux entreprises françaises « *devra impérativement être hébergé sur le cloud interne de l'État ou sur un cloud industriel qualifié SecNumCloud par l'ANSSI et protégé contre toute réglementation extracommunautaire* ».

- Un **financement** par le PIA IV et France Relance[1] des projets industriels de développement de technologies cloud en France, les plus importantes étant également financées dans le cadre d'un Projet important d'intérêt européen commun (PIEEC)[2].

Par rapport à la doctrine des trois cercles de 2018, cette stratégie « *acte l'abandon de l'offre de compromis, dit de cercle 2, expérimentée par le ministère des Armées avec OVH, et qui ne s'est "pas beaucoup développée" a reconnu Amélie de Montchalin. Elle se contente de poursuivre les offres interministérielles dites de cercle 1 conçues et mises à disposition par Bercy et la Place Beauvau auprès des autres administrations (notamment pour les projets les plus sensibles) et renforce le cercle 3, c'est-à-dire le catalogue d'offres génériques et commerciales compilées par Capgemini depuis juillet 2020* » décrypte une analyse[3].

Comme pour le projet Gaïa X, **cette stratégie nationale ne ferme pas la porte aux opérateurs privés américains,** qui pourront proposer leur offre sous licences. Pour M. Bruno Le Maire : « *Le recours à des licences américaines dans le nucléaire n'a pas empêché la France de devenir une puissance souveraine dans ce domaine. L'objectif est de suivre la même approche avec le cloud* ». Il s'agit donc, comme l'a indiqué M. Bernard Duverneuil, président du CIGREF, de : « *maîtriser la dépendance dans la durée des clients vis-à-vis de leurs fournisseurs* »[4], ce qui est n'est pas une définition proche de celle de la souveraineté numérique. « *Il reste nécessaire de s'appuyer sur les technologies des hyperscalers*[5]*. Ce transfert de technologie et de compétence n'est pas dénué de risques et des précautions s'avéreront indispensable*s », a-t-il averti. Un référentiel de sécurité sera soumis à consultation publique par le CIGREF fin mai 2021.

---

[1] *Notamment via l'appel à manifestation d'intérêt « Développement et renforcement de la filière française et européenne du cloud », de Bpifrance, ouvert jusqu'au 17 mai 2021.*

[2] *Un PIEEC n'est pas un programme de financement de l'Europe, mais une notification à l'Union européenne. En effet, ce mécanisme autorise les pouvoirs publics des États membres à financer des initiatives au-delà des limites habituellement fixées par la réglementation européenne en matière d'aides d'État. Les opérateurs économiques participants doivent, entre autres, démontrer un projet de leadership technologique et la volonté de coopérer avec d'autres leaders européens de l'innovation sur le secteur concerné dans le but de développer l'ensemble de la chaîne de valeur sur le territoire européen.*

[3] *Acteurs publics 7 avril 2021 et 17 mai 2021.*

[4] *https://www.economie.gouv.fr/cloud-souverain-17-mai*

[5] *Par extension de l'hyperscale, traitement informatique massif, généralement pour le big data ou le cloud computing, désigne les grands fournisseurs de solutions cloud : AWS, Microsoft et Google.*

L'Europe et les GAFAM sont condamnés à s'entendre. La première ne peut priver ses entreprises de solutions innovantes et efficaces en matière de cybersécurité ; les seconds ont intérêt à établir des partenariats au sein du marché européen très lucratif. Dans ce sens, ils seront de plus en plus enclins à **réserver à leurs entreprises clientes l'exclusivité des clés de déchiffrement des données stockées dans leur *cloud* sans qu'eux-mêmes puissent y avoir accès**, ce qui rendrait impossible le décryptage par les autorités locales, même en cas de coopération juridique forcée du prestataire de *cloud.*

Cette stratégie ne détermine pas l'évolution du marché européen du cloud qui pourrait, selon le Livre blanc de KPMG, suivre un certain nombre de **scénarios**, au nombre de **cinq** :

1. Le **cloud comme bien commun**, **avec une interopérabilité volontaire accrue** entre les services de cloud, voire une fédération des acteurs autour d'écosystèmes cloud sectoriels communs.
2. La **montée en puissance des acteurs européens**, permise par l'émergence de nouveaux segments de marché ; *edge computing*, développement de l'intelligence artificielle, notamment dans le secteur industriel ; offres souveraines, etc...
3. L'instauration d'une **puissante vague réglementaire**, notamment avec la création d'une Autorité de régulation du cloud, une réglementation plus stricte des pratiques commerciales, une interopérabilité forcée entre les opérateurs imposée par le régulateur et une réglementation accrue de l'innovation basée ou dérivée du cloud.
4. Une **européanisation des opérations des grands acteurs non-européens du cloud**, soumis à des réglementations assurant à l'Europe une création de valeur effective régionalement, et un respect strict des réglementations européennes.
5. Une **séparation fonctionnelle ou structurelle** des activités cloud des autres activités des opérateurs de cloud, avec notamment la création d'entités légales distinctes, dans la logique des appels aux discussions actuelles sur les Big Tech aux États-Unis.

L'avenir du cloud européen pourrait être la combinaison de ces scénarios à des horizons variés. Le cabinet avertit qu'à défaut de changements significatifs par rapport à la situation actuelle : « *si la domination des "hyperscalers" venait à se renforcer, l'Europe pourrait perdre de 20 à 50 % de l'impact économique estimé du marché du cloud computing* ». La création de 350 000 emplois et 170 milliards d'euros d'investissement en Europe sont en jeu.

L'annonce, le 27 mai 2021, de la création par Capgemini et Orange de la société « Bleu », qui permettra de mettre en commun leur savoir-faire, en partenariat avec Microsoft, est une première concrétisation de cette

stratégie. Elle créée un fournisseur de services cloud français répondant aux besoins des organisations soumises à des exigences particulières en termes de sécurité, de confidentialité et de résilience, telles que définies par l'État français, opérant exclusivement sous juridiction française et européenne.

D. UN DROIT DE LA COMMANDE PUBLIQUE FREINANT L'ÉMERGENCE DE L'ÉCOSYSTÊME DE LA CYBERSÉCURITÉ

Pour déployer ces atouts et faire éclore l'écosystème de la cybersécurité tant promu par le discours public, encore faut-il s'en donner les moyens en favorisant les start-ups par la commande publique.

Or, « *si la France possède de très bons ingénieurs qui inventent des produits de cybersécurité innovants, nous sommes de mauvais commerciaux pour les vendre* », estime malheureusement M. Erwann Keraudy, CEO de la start-up CybelAngel, qui déclare : « *je ne veux ni subvention publique ni aide de l'État mais des contrats avec les institutions publiques bien que leur maturité est incomplète, leurs budgets insuffisants et on rencontre l'obstacle du droit de la commande publique. Il est paradoxal que mon entreprise travaille davantage avec le gouvernement britannique qu'avec le gouvernement français* »[1].

Ainsi, et comme le souligne l'ACN, **le développement de l'excellence de la filière française de cybersécurité doit se traduire par une politique publique d'achat de solutions de cybersécurité françaises** : « *de nombreux acteurs de la filière de la Confiance Numérique relèvent une absence dommageable de culture d'achat de produits français, aussi bien de la part des entreprises que des administrations. Cette absence de culture d'achat de produits français a naturellement conduit les entreprises et les administrations françaises à se tourner vers des offres étrangères sur la période 2013-2019. En effet, dans un contexte général de stagnation de la croissance et d'austérité budgétaire des services publics, le premier critère d'achat s'avère souvent être le prix. Or, les acteurs américains et chinois sont souvent plus compétitifs que les français sur le seul critère du prix (notamment en raison d'économies d'échelles plus importantes et d'une sous-traitance plus forte dans des pays à faibles coûts salariaux). En plus de pénaliser les acteurs français de la filière, l'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France lorsque les acheteurs sont des organismes publics, des OIV (Opérateur d'Importance Vitale), et/ou des OSE (Opérateur de Service Essentiel)* ».

Sa pleine réussite, qui déterminera la future autonomie des entreprises françaises, dépendra d'un **portage politique constant et de haut niveau** ainsi que de la **remise en question des orientations actuelles de la commande publique**. C'est dans ce domaine que **l'interventionnisme politique du XXIème siècle doit se réinventer.**

---

[1] *Audition du 6 mai 2021.*

UTILISER LA COMMANDE PUBLIQUE POUR RÉUSSIR UN *CLOUD* SOUVERAIN

Il faut avoir conscience que l'interventionnisme américain est leur secret le mieux gardé. Tout en érigeant la figure de l'entrepreneur dans son garage comme le symbole de l'innovation américaine et en proclamant les vertus du libre-échange, l'État américain exerce un protectionnisme fort, appuyant des industries clés en fonction de leur caractère stratégique. Beaucoup de technologies américaines ont d'abord été développées dans un environnement (ou avec un soutien) militaire. La commande publique peut ensuite prendre le relais pour accompagner l'élaboration d'applications civiles de ces technologies. Comme l'a écrit Mariana Mazzucato dans *The entrepreneurial State*, toutes les technologies qui ont fait du premier iPhone un *smartphone* ont été financées, à un moment ou à un autre, par l'État américain.

Au-delà même de la problématique du *cloud* souverain, on ne peut envisager la souveraineté numérique sans se mettre en ordre de marche pour orienter la commande publique, comme nous le réclamons, avec un *Small Business Act* en France et en Europe, et dans le même temps bloquer les interventions extérieures potentiellement toxiques. En effet, si nous ne faisons rien pour soutenir des entreprises nationales et européennes afin de développer un écosystème industriel compétitif indépendant vis-à-vis des filières industrielles américaines et chinoises, la dérive que nous subissons sera inéluctable. Une stratégie défensive fondée uniquement sur le droit ne suffira pas à protéger notre souveraineté et enrayer ni la dynamique actuelle de dépendance vis-à-vis des industriels extra-européens, ni la vassalisation politique, sociale et économique qu'elle va entraîner dans les années à venir.

Source : « Au-delà du « sovereignty-washing » : 3 questions à Bernard Benhamou sur le cloud souverain en France », Sciencespo.fr, 2 septembre 2020.

V. METTRE LA CYBERSÉCURITÉ À LA PORTÉE DES TPE ET PME

A. RENDRE LA CYBERPROTECTION PUBLIQUE PLUS ACCESSIBLE AUX TPE ET PME

1. Faciliter l'accès des TPE et PME aux solutions de sécurité numérique

a) Offrir aux entreprises un numéro d'appel en cas de cyberattaque

En Israël, État très exposé à la guerre numérique et qui a également constaté en 2020 une augmentation de 50 % des actes de cybermalveillance[1], la cybersécurité est « *le secteur le plus privilégié par les politiques publiques* »[2]. C'est **le premier pays au monde à avoir instauré un numéro d'urgence pour les victimes d'actes de cybercriminalité.** Toute entreprise qui suspecte une attaque peut appeler le 119 gratuitement 24 heures sur 24, 7 jours sur 7, et entrer en contact avec des spécialistes.

En France, le site cybermalveillance.gouv.fr renvoie vers le numéro d'aide aux victimes du ministère de la Justice mais qui n'est destiné qu'aux particuliers.

Il manque toutefois de visibilité puisque, selon l'enquête CCI France de févier 2021[3], seulement 24 % des dirigeants d'entreprise ont entendu parler du dispositif. La connaissance de la plateforme apparait d'autant plus lacunaire que 14 % déclarent en avoir entendu parler, mais ne pas bien voir de quoi il s'agit et **76 % n'en ont simplement jamais entendu parler**. La connaissance de la plateforme est à peine meilleure dans les entreprises comptant plus de 10 salariés : 29 % de notoriété, contre 23 % dans les entreprises plus petites.

Une **campagne de promotion en direction des entreprises** permettrait de mieux identifier cybermalveillance.gouv.fr comme dispositif de cyberprotection. Au sein de cette plateforme**, un service d'urgence pourrait être dédié exclusivement aux entreprises**. Il pourrait être composé **d'étudiants** disposant des compétences numériques adéquates et effectuant leur **service civique**. Ces derniers pourraient être encadrés par la réserve citoyenne de cyberdéfense (RCC), branche de la réserve citoyenne nationale créée en 2016. Elle a pour vocation à intervenir principalement non seulement sur les réseaux du ministère des Armées mais également au profit des opérateurs d'importance vitale (OIV), des administrations et de leurs

---

[1] « An increase of about 50% in reports to the 119 center of INCD on cyber incidents in 2020 », *Israel National Cyber Directorate, 31 janvier 2021.*

[2] *« La cyberpuissance israélienne. L'essor inachevé de la start-up nation ? », études de l'Ifri, novembre 2020.*

[3] *Étude réalisée du 12 au 18 février 2021 par OpinionWay, auprès d'un échantillon de 608 dirigeants d'entreprise.*

sous-traitants et mène des actions de sensibilisation et d'information, sans rôle opérationnel en cas de cyberattaque de grande ampleur.

Proposition n°1 : Promouvoir davantage le dispositif cybermalveillance.gouv.fr auprès des entreprises et dédier un service d'urgence aux entreprises ; des étudiants disposant des compétences numériques adéquates pourraient y effectuer leur service civique.

b) Assurer une meilleure connaissance du cyberrisque

Il n'existe pas à ce jour en France d'organisme, privé ou public, dont la mission serait de collecter et d'anonymiser les incidents cyber afin de produire des statistiques qui pourraient être partagées avec tous les acteurs.

Ainsi qu'il a été dit, **toutes les entreprises ne portent pas plainte** après une cyberattaque et les pouvoirs publics n'ont pas une vision exhaustive de la cybermenace.

De même, **l'obligation de notification à la CNIL** pour les victimes d'incident cyber, en cas d'atteinte à la sécurité des données ou des systèmes d'information, a été étendue depuis le 25 mai 2018 à toutes les entreprises ayant des activités de traitement des données. Mais elle **est loin d'être respectée**, bien qu'elle soit lourdement sanctionnable[1] et a été lourdement sanctionnée[2], d'autant que le recours à un prestataire pour la gestion des données n'exonère pas la société de son obligation de garantir la sécurité des données traitées pour son compte.

Les établissements de santé ont déjà une obligation de signalement des incidents de sécurité des systèmes d'information[3].

Cette absence de base de données fiable prive l'ensemble des acteurs économiques d'une source d'information qui **contribuerait à une prise de conscience accrue du risque cyber.** Elle prive également les assureurs d'un outil de travail essentiel pour modéliser les risques cyber.

---

[1] *Les violations des dispositions concernant la sécurité des données peuvent être sanctionnées par une amende administrative d'un maximum de 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.*

[2] *Les sociétés Dailymotion et Uber ont été sanctionnées par la CNIL, en juillet et décembre 2018, pour manquement à la sécurité des données de leurs clients, à des amendes respectives de 50 000 € et de 400 000 €.*

[3] *Article L.1111-8-2 du code de la santé publique : « Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'État. Un décret définit les catégories d'incidents concernés et les conditions dans lesquelles sont traités les incidents de sécurité des systèmes d'information ». Le décret d'application n°2016-1214 du 12 septembre 2016 précise que les incidents graves de sécurité des systèmes d'information du secteur santé doivent être signalés sans délai à compter du 1er octobre 2017.*

L'anonymisation de ces déclarations, des victimes comme des attaquants, permettrait d'une part aux entreprises victimes de préserver leur capital relationnel, leur image de marque, et, d'autre part, de mettre en échec les stratégies de communication des cybercriminels. Ces derniers les intègrent en effet de façon croissante afin d'effrayer les entreprises, « *ce qui maximise les chances des cyberassaillants d'être payés par leurs futures victimes lors de leurs prochains forfaits* »[1] comme il a été souligné lors de l'attaque, en mai 2021, par le groupe de cybercriminels DarkSide des réseaux de Colonial Pipeline, oléoduc alimentant le nord-est des États-Unis[2].

Un même souci de confidentialité devrait animer une réflexion sur la publicité des appels d'offre des collectivités locales pour souscrire une assurance de leurs risques cyber.

L'une des missions du GIP « ACYMA » devait être justement : « *la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié* », qui n'a pas encore été créé. **Cette proposition l'y encourage**, en associant le privé et le public.

Proposition n°2 : Ouvrir un guichet de recueil anonymisé des cyberattaques frappant les entreprises, afin de disposer de statistiques fiables.

c) Créer des équipes régionales de réponse afin de mieux protéger les PME

Entre le dispositif Cybermalveillance.gouv.fr adressé aux TPE et les PME ou ETI qui sont considérées comme opérateurs d'importance vitale et cyberprotégés à ce titre par l'ANSSI, **le dispositif public devrait être complété pour mieux protéger les PME** par le déploiement territorial de plusieurs **équipes de réponse aux incidents informatiques (CSIRT - *Computer Security Incident Response Team*)** dans les **Régions**, avec le soutien de ces dernières.

Plusieurs des schémas régionaux de développement économique, d'internationalisation et d'innovation (SRDEII) évoquent le numérique, mais ce volet devrait être précisé afin que **les Régions puissent investir dans la cybersécurité, en déclinant territorialement les CSIRT.**

Dans le même sens, la commission supérieure du numérique et des postes dans son avis n°2021-03 du 29 avril 2021 portant recommandations dans le domaine de la sécurité numérique préconise que la création des

---

[1] *« 5 choses à savoir sur Darkside, le groupe de cybercriminels qui prend en otage le pétrole américain », Nicolas Richaud, Les Echos, 11 mai 2021.*

[2] *« Five signs ransomware is becoming an industry », Roman Dedenok, Kapersky Daily, 16 avril 2021.*

CSIRT en région soit l'occasion de **fédérer localement les acteurs de la sécurité numérique, de les faire travailler en réseau, et de sensibiliser l'écosystème public et privé à ces problématiques**. « *Ce campus hébergerait le CSIRT incubé par l'ANSSI et serait notamment un véritable relais de gouvernance régional pour l'ANSSI, au service de tous les départements d'une même région pour un maillage territorial efficace. La création de ces campus régionaux pourrait s'appuyer sur l'article L.4251-13 du Code général des collectivités territoriales portant nouvelle organisation territoriale de la République, et être inscrite dans les schémas régionaux de développement économique, d'innovation et d'internationalisation* ».

Cet investissement des Régions dans la cybersécurité permettrait **une sensibilisation des collectivités locales,** lesquelles sont à la fois **insuffisamment averties du cyberrisque et totalement démunies pour s'en protéger,** malgré deux publications récentes qui leur sont spécifiquement adressées :

- un guide « Sécurité numérique des collectivités locales » rédigé par l'ANSSI, en mars 2020 ;
- un guide de « sécurité numérique pour les petites et moyennes collectivités locales », en décembre 2020, réalisé par le Pôle d'excellence cyber, résultant d'un partenariat entre la Région Bretagne et le commandement de la cyberdéfense (COMCYBer).

Dans le cadre du plan France Relance, l'ANSSI bénéficie d'une enveloppe de **136 millions d'euros** pour renforcer la cybersécurité de l'État et des territoires sur la période 2021-2022[1]. L'objectif est d'élever durablement le niveau de cybersécurité de l'État, des collectivités, des établissements de santé et des organisations au service des citoyens, tout en développant le tissu industriel français de cybersécurité. Cette somme doit servir au co-financement des CSIRT régionaux.

Engagées dans une transformation numérique profonde, autant pour répondre à des obligations réglementaires qu'au souci de rendre un meilleur service aux citoyens, la dépendance croissante des collectivités territoriales aux systèmes d'information, couplée à l'hétérogénéité de la taille des communes crée une **fragilité**, soulignée dans la Revue stratégique de cyberdéfense de 2018[2].

Il faut aider les collectivités territoriales à se cybersécuriser en privilégiant les acteurs de proximité de la cybersécurité, ce qui suppose

---

[1] *Voir le document : https://www.ssi.gouv.fr/uploads/2021/02/anssi-france_relance-cybersecurite_proteger_services_publics_et_collectivites_territoriales.pdf*

[2] *Voir le guide « Sécurité numérique des collectivités locales » rédigé par l'ANSSI en mars 2020 : https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf*

une adaptation du droit de la commande publique, comme développé ci-après.

« *La maturité des collectivités locales est incomplète, les budgets sont insuffisants et elles ne disposent pas des compétences humaines en capacité de rédiger des appels d'offres. Malgré l'assouplissement par le décret de 2018 sur les marchés innovants*[1]*, le droit de la commande publique constitue un frein* » témoigne ainsi Erwan Keraudy, CEO de CybelAngel[2].

Afin de **cybersécuriser rapidement les collectivités locales**, tout en leur permettant l'acquisition de solutions nationales de cybersécurité, le décret de 2018 doit être pérennisé dans le domaine de la cybersécurité.

Elles pourraient ainsi faire appel à des solutions de cybersécurité proposées par des start-up ou PME locales, afin de favoriser l'émergence de « l'écosystème de la cybersécurité ».

Proposition n°3 : Décliner dans les Régions des équipe de réponse aux incidents informatiques (CSIRT - *Computer Security Incident Response Team*), et inclure la cybersécurité dans les schémas régionaux de développement économique, d'internationalisation et d'innovation (SRDEII) afin de sensibiliser les collectivités locales.

d) Adapter le droit de la commande publique pour favoriser l'émergence de l'écosystème de la cybersécurité

Le marché des TPE et des PME est un marché de masse.

L'accès des entités publiques aux start-up de la cybersécurité que souhaite développer l'ÉtatÉtat passe par **un assouplissement des règles de la commande publique et de fonctionnement de l'Union des Groupements d'Achats Publics** (UGAP).

En effet, cette dernière a confié à *Specialist Computer Company France* (SCC France), acteur privé spécialiste de la transformation digitale des organisations[3], le marché relatif aux logiciels multi-éditeurs. Ce marché permet d'intégrer à l'offre de la centrale d'achat public les catalogues de plus de 800 éditeurs répondant à l'ensemble des besoins des DSI de l'État, des collectivités, et plus largement de celles de la sphère publique.

---

[1] *Le décret du 24 décembre 2018 portant diverses mesures relatives aux contrats de la commande publique crée une expérimentation de trois ans permettant aux acheteurs de passer des marchés négociés sans publicité ni mise en concurrence préalable pour leurs achats innovants d'un montant inférieur à 100.000 euros.*

[2] *Audition du 6 mai 2021.*

[3] *Suite à un accord-cadre lancé par l'UGAP en février 2012 et de la mise en concurrence en février 2017, renouvelé en 2019.*

Une PME française doit donc être référencée dans le catalogue établi par cette société britannique pour être proposée à des entités publiques françaises….

Par ailleurs, la commission supérieure du numérique et des postes dans son avis précité du 29 avril 2021, préconise d'étudier une modification de la directive 2014/25/UE du 26 février 2014 relative à la commande publique des opérateurs de réseaux, « *notamment pour permettre aux opérateurs de réseaux, dont les achats de produits et services de cybersécurité sont généralement soumis à cette directive, d'orienter leurs achats en la matière auprès de fournisseurs nationaux et européens. A minima, il conviendrait de définir que la cybersécurité entre dans le champ d'exclusion de l'application de la directive au profit des OIV (Opérateurs d'Importance Vitale) et OSE (Opérateurs de Services Essentiels) afin de leur permettre d'accéder à des solutions de confiance* ».

Proposition n°4 : Adapter le droit de la commande publique pour favoriser l'écosystème de la cybersécurité en :

- **pérennisant les dispositions du décret du 24 décembre 2018 permettant l'achat sans mise en concurrence[1], par les collectivités locales, de « services innovants » ;**
- **permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;**
- **étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité.**

2. Renforcer la cyberprotection publique des entreprises

a) Établir des plans de prévention des risques numériques

Il existe en France des plans de prévention des risques naturels (inondation, littoral, mouvement de terrain et multirisques), mais **aucun document public de prévention d'une attaque numérique systémique** qui ciblerait non seulement les opérateurs d'importance vitale mais toutes les entreprises, par une cyberattaque des grands fournisseurs informatique, qui, par rebond et se déployant dans la *supply chain* informatique, affecterait des dizaines de milliers de PME, voire de TPE.

[1] *Jusqu'à 100 000 euros HT.*

DÉFINITION D'UNE CYBERATTAQUE SYSTÉMIQUE VISANT LES ENTREPRISES

« Un risque est systémique quand une attaque est en mesure d'affecter un nombre important d'organisations simultanément via les systèmes qu'elles utilisent. Aujourd'hui, cela est possible du fait des technologies utilisées et des interconnexions croissantes entre les organisations et donc entre leurs systèmes informatiques.

Le premier facteur est ***une dépendance technologique forte****. Le fonctionnement de toutes les sociétés repose aujourd'hui sur le numérique. Or, le marché des systèmes d'exploitation et celui des microprocesseurs sont ainsi largement dominés par un tout petit nombre d'acteurs. L'adoption grandissante du cloud public par les entreprises participe également au risque systémique. Cela est dû au fait que les infrastructures cloud sont opérées en grande majorité par trois acteurs qui représentent à eux seuls plus de la moitié du marché des services d'infrastructures cloud. Cette situation crée une fragilité systémique : si une faille est détectée dans l'un de ces systèmes, elle peut être exploitée pour toucher un nombre considérable d'acteurs.* ***Cette menace est d'autant plus réelle que la plupart de ces systèmes ont été conçus sans intégrer la cybersécurité par défaut****. De plus, pour certaines entreprises, il est* ***difficile de suivre la cadence des mises à jour*** *développées par les éditeurs et fournisseurs, laissant ainsi les failles ouvertes.*

Le second facteur est ***une interconnexion croissante.*** *À mesure que les entreprises et les administrations encouragent la transversalité en interagissant de plus en plus entre elles, que les organisations ont régulièrement recours à des prestataires extérieurs pour accomplir des tâches spécifiques, et que les objets connectés s'immiscent dans notre quotidien, les opportunités d'attaques et les effets de propagation en cas d'intrusion augmentent. À l'échelle d'un pays, cette interconnexion des systèmes rend les conséquences d'une attaque potentiellement dramatiques. À l'échelle individuelle des organisations (opérateurs de service public, entreprises, ONG, petites et moyennes entreprises), elle* ***augmente les portes d'entrée*** *par lesquelles peuvent pénétrer les virus ».*

Source : « Cybermenace : avis de tempête », rapport de l'Institut Montaigne, novembre 2018.

Les grands fournisseurs d'accès, souvent en situation de monopole, sont régulièrement attaqués et **ne sont pas invulnérables** comme l'a montré la cyberattaque contre Microsoft Exchange début mars 2021, ayant affecté 60 000 entreprises.

Or comme l'a souligné l'étude précitée de l'Institut Montaigne : « *à l'heure où les systèmes sont de plus en plus interconnectés et où les réseaux sont de plus en plus imbriqués, la France, comme tous les pays, est susceptible d'être touchée par un "****ouragan cyber****" »*, provenant d'un acteur non-étatique, qui aurait dérobé directement ou indirectement des outils d'attaques développés par un État. Selon les scénarii, une telle cyberattaque d'ampleur, qui impacterait, par exemple, 15 000 PME, 12 grandes entreprises, dont quatre dans des secteurs stratégiques et quatre ministères, **coûterait entre 5 et 50 milliards d'euros**, pouvant affecter tout particulièrement les PME, moins

bien protégées, transformant cette cyberattaque « *en une véritable crise sociétale* ».

Un plan national de prévention des cyberrisques devrait être établi afin de coordonner la réponse des pouvoirs publics et des acteurs privés en cas d'attaque numérique systémique. En s'inspirant de l'entraînement de l'Estonie[1], des exercices civils de simulation de cyberattaque devraient être régulièrement organisés.

Proposition n°5 : Élaborer des plans nationaux de prévention des cyberrisques afin de coordonner la réponse des pouvoirs publics et des acteurs privés en cas d'**attaque numérique systémique** affectant une part significative des entreprises quelle que soit leur taille. En outre, des **exercices de simulation** devraient être **régulièrement organisés**.

b) Renforcer le dispositif public de cyberprotection des entreprises

(1) Fédérer public et privé pour renforcer la cyberprotection

Présenté le **18 février 202**1 pour répondre aux cyberattaques ayant visé des hôpitaux et la chaîne d'approvisionnement (*supply chain)* de la production de vaccins contre la COVID-19, le « ***plan à 1 milliard*** *d'euros pour renforcer la cybersécurité* » vise à « ***doubler les effectifs*** *de la filière d'ici à 2025* » en faisant émerger des « ***champions français*** *de la cybersécurité* ».

Les **objectifs clés fixés à l'horizon 2025** :

- multiplier par trois le chiffre d'affaires de la filière (passant de 7,3 milliards à 25 milliards d'euros) ;
- positionner la France par rapport à la concurrence internationale en doublant notamment les emplois de la filière (passant de 37 000 à 75 000) ;
- structurer la filière et repositionner la France par rapport à la concurrence internationale en nombre d'entreprises ;
- faire émerger trois licornes françaises en cybersécurité en s'appuyant sur les grandes start-up du secteur, et notamment celles membres du French Tech 120 ;
- diffuser une véritable culture de la cybersécurité dans les entreprises ;
- stimuler la recherche française en cyber et l'innovation industrielle (hausse de 20 % des brevets).

[1] *Le dernier exercice de cyberdéfense s'est tenu à Tallinn (Estonie) du 13 au 16 avril 2021. Il a réuni 2000 spécialistes occidentaux issus de 22 pays. Selon le scénario, une « Red Team » (attaquants) aurait déclenché une vaste série d'incidents cyber contre le « Berylia », un pays situé près de l'Océan Atlantique. L'attaque aurait visé les infrastructures critiques, dont le secteur de l'eau et le secteur financier, et les systèmes de communication militaires.*

Ce plan répond également à l'interpellation du CIGREF[1] du 18 novembre 2020, considérant inacceptable l'augmentation, en nombre et en intensité, des cyberattaques, constituant une menace croissante pour l'économie. Pour le CIGREF, « ***aucun autre secteur d'activité que celui du numérique n'accepterait de se développer dans un tel contexte de faiblesse du droit applicable et de quasi impunité des criminels*** ».

Or, **alors que les entreprises demandent à l'État de renforcer les moyens, notamment humains de la cyberprotection publique, celui-ci renvoie aux entreprises la responsabilité de construire un écosystème censé les protéger.**

Le milliard d'euros pour la cybersécurité ne peut consacrer 0 euro au renforcement du dispositif public des PME et TPE, même si la dotation supplémentaire de 136 millions en faveur de l'ANSSI est naturellement bienvenue.

Ce **malentendu** est d'autant plus flagrant que l'État proclame que « *à la fois essentielle à la souveraineté des États, à la pérennité du développement des entreprises et à la sécurité des citoyens, la cybersécurité est un enjeu majeur du XXIe siècle.* » , selon les propos de Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, tenus à l'occasion de la présentation de ce plan, sans se donner suffisamment les moyens de l'ambition qu'il affiche.

Or, selon deux experts de la cybersécurité des entreprises[2] : « ***Le domaine judiciaire est en difficulté pour s'attaquer au cybercrime, et ce pour de nombreuses raisons : de trop nombreux dossiers, un manque d'effectifs qualifiés, un code pénal peu adapté à la lutte contre le cybercrime****, des difficultés législatives liées à l'obtention et à la validité des preuves numériques, un cloisonnement entre les différents acteurs, un manque de ressources pour suivre les flux de monnaies virtuelles…*

L'action répressive sur la cybercriminalité est aujourd'hui limitée par deux facteurs à l'international comme en France : d'une part, ***les effectifs alloués et compétents sont trop rares, et ce à toutes les échelles*** *(la police judiciaire, la gendarmerie, Tracfin, Europol, Eurojust, et tout particulièrement la Justice). D'autre part,* ***l'arsenal technique est limité, avec un manque d'outils souverains et fonctionnels pour mener les enquêtes numériques*** *(citons entre autres la captation de preuves et le suivi des transactions de cryptomonnaies).*

---

[1] *Fondé en 1970, le CIGREF organise, anime, synthétise et diffuse la pensée collective de ses membres sur leurs principaux enjeux numériques. Il entretient des relations de dialogue avec leurs principaux fournisseurs afin de traiter collectivement les difficultés rencontrées. Il compte 150 adhérents, grandes entreprises et administrations publiques françaises représentant un chiffre d'affaires cumulé de 1 700 Md€, 9 millions de salariés, 200 000 employés internes dans l'IT et les systèmes d'information, pour une dépense annuelle de 50 Md€ dans les solutions et services numériques.*

[2] *« Cybercrime : briser la rentabilité », Gérôme Billois, Marwan Lahoud, Blog de l'Institut Montaigne, 16 mars 2021.*

À l'échelle nationale, nous devons également lever certaines barrières pour rattraper le retard accumulé. ***L'un des enjeux principaux est le manque de coopération entre les nombreuses institutions, en particulier entre la justice et les services de renseignement.*** *Un meilleur partage d'informations permettrait d'accélérer les enquêtes* ».

(2) Renforcer les moyens humains de la lutte contre la cybercriminalité

Cette insuffisance de moyens humains, qui est revenue régulièrement lors des auditions conduites par les rapporteurs, a été récemment soulignée par le Sénat, malheureusement sans que leur proposition soit suivie d'effet :

> ***« Le renforcement des moyens d'investigation apparaît indispensable pour faire face au développement de la criminalité dans l'univers numérique.***
>
> *Par priorité,* ***ce sont les moyens du parquet spécialisé qui mériteraient d'être considérablement augmentés****. Un effectif de trois magistrats pour traiter les affaires de dimension nationale et internationale et animer un réseau de référents est* ***notoirement insuffisant****. Les effectifs du parquet spécialisé mériteraient* ***d'être décuplés*** *pour être portés au niveau de ceux des grands États européens les plus engagés dans ce domaine.*
>
> *Si la spécialisation est nécessaire, elle ne doit pas être poussée à l'excès, compte tenu du caractère transversal de la cybercriminalité. Il est souhaitable que les équipes en charge de la cybercriminalité demeurent intégrées à des services de plus grande dimension afin que* ***des compétences variées puissent être mobilisées pour traiter une affaire*** ».
>
> *Source : Rapport d'information précité n° 613 (2019-2020) du 9 juillet 2020.*

La police, la gendarmerie et les magistrats doivent être mieux soutenus pour lutter à armes égales contre la cybercriminalité.

Les forces de sécurité publique recourent de façon croissante à des experts contractuels dont la rémunération doit être attractive, afin de les retenir dans un contexte, déjà évoqué, de pénurie mondiale d'ingénieurs qualifiés, et de surenchère avec le privé. **Les budgets publics doivent donc être renforcés pour mieux rémunérer ces cyberexperts contractuels**.

Le renforcement de la formation en cybersécurité est en cours depuis plusieurs années à l'École nationale de la magistrature, dont l'enseignement est largement numérisé. « *S'il n'y a pas d'enseignement spécifique dédié à la cybercriminalité, les* ***moyens d'investigation qui peuvent être utiles dans les dossiers relatifs à la cybercriminalité*** *sont présentés et notamment l'expertise informatique dans les* ***enseignements de la fonction de juge d'instruction*** »[1] mais la faiblesse du temps consacré (quelques heures) ne permet qu'une sensibilisation des futurs magistrats.

---

[1] *Réponse écrite de l'ENM au questionnaire de la Délégation aux entreprises, 17 mars 2021.*

Le renforcement de cette formation est indispensable « *non seulement pour avoir une vision et une connaissance des modes opératoires des délinquants qui sont de plus en plus sophistiqués, mais également pour gérer la dimension de coopération internationale. Cette formation doit également mettre l'accent sur les* ***techniques spéciales d'enquête*** *harmonisées par la loi de 2019, qui sont très encadrées juridiquement et qu'il convient de* ***sécuriser pour faire tenir les procédures****. Il s'agit plus particulièrement de l'enquête sous pseudonyme, de la géolocalisation, de la captation de données à distance* », selon Mme Myriam Quéméner, Avocat général près de la Cour d'Appel de Paris[1]. Compte tenu de l'évolution permanente de la cybercriminalité, cette formation doit être continue.

Il serait également nécessaire que les magistrats soient intégrés à la communauté cyber et participent aux think tanks et aux divers événements rassemblant les professionnels de la matière. La technicisation croissante de la cybercriminalité suppose également de **créer, non seulement au Parquet, mais également au Siège et à chaque degré de juridiction, un département cyber numérique étoffé, composé de magistrats et de cadres spécialisés**.

Enfin, le pôle spécialisé du Parquet de Paris doit être étoffé car les effectifs actuels, trois magistrats, sont notoirement insuffisants. La création d'un **Parquet national de lutte contre le cybercrime** pourrait être envisagée.

Proposition n°6 : Renforcer la réponse pénale à la cybercriminalité :

- **Développer la formation initiale et continue des magistrats en matière de cybercriminalité ;**
- **Augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ;**
- **Doter les forces de cybersécurité de moyens financiers adéquats ;**
- **Étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ;**
- **Créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité.**

(3) Adapter les procédures judiciaires pour lutter plus efficacement contre la cybercriminalité

Bien que le temps de la justice reste globalement trop lent en comparaison avec l'environnement extrêmement dynamique de la cybercriminalité, il n'existe pas encore de **procédure de « cyberréféré »** lui permettant d'accélérer ses interventions.

[1] *Audition du 15 avril 2021.*

Il convient en priorité de **mettre l'accent sur l'adaptation de la procédure pénale aux infractions numériques de masse.**

Ainsi, les infractions d'atteinte aux systèmes de traitement automatisé de données (STAD) ne sont pas mentionnées aux articles 706-73 et 706-73-1 du code de procédure pénale alors que les cybercriminels disposent des connaissances et des moyens techniques pour réduire leurs traces numériques, agir de façon anonyme notamment par l'utilisation de cryptoactifs.

Il est également nécessaire d'adapter les obligations pesant sur les opérateurs nationaux de télécommunications pour réduire le nombre de déplacements inutiles des forces de sécurité sous de faux prétextes ou d'escroquerie, qui sont générés par appels téléphoniques masquant le véritable numéro d'appel par un numéro de téléphone appelé ne correspondant pas à la réalité. Le numéro présenté reprend fréquemment le numéro géographique d'un commissariat de Police ou autre afin de tromper plus facilement son interlocuteur.

Ce « *spoofing* » est rendu possible notamment par l'utilisation de services internet dédiés à cette activité, qui émettent les appels, via des opérateurs internationaux. Le lien entre l'appel et le service internet est rendu très difficile par le fait que l'acheminement de l'appel à l'international transite par plusieurs opérateurs internationaux avant d'arriver sur le territoire. S'agissant d'appels provenant de l'étranger, les opérateurs nationaux n'ont pas d'obligation de vérification de l'adéquation entre l'opérateur acheminant l'appel et le numéro affiché.

Enfin, et d'une manière générale, **les difficultés sont récurrentes pour obtenir une preuve numérique** : les éléments constitutifs de l'infraction sont dématérialisés et extraterritorialisés ; l'absence de conservation des données ou l'utilisation de *Virtual Private Networks* (VPN) ou de TOR[1], destinés à préserver l'anonymat des utilisateurs du réseau, comme les outils de chiffrement, obligent les enquêteurs à multiplier les actes d'enquête pour retrouver l'auteur des faits.

Comme l'a souligné Myriam Quémener, avocate générale près la cour d'appel de Paris, « *la matière pénale renforce les exigences sur les enquêteurs qui devront pouvoir démontrer son origine et son authenticité aux avocats et aux magistrats. Le respect de la procédure d'accès à la preuve numérique est d'une importance fondamentale car elle permet de démontrer l'intégrité des données*

[1] ***TOR** (**T**he **O**nion **R**outer – le suffixe des domaines natifs de TOR .onion, étant devenu synonyme de liberté sur internet, TOR étant parfois surnommé « onionland ») est de loin la plus connue et la plus importante des portes d'entrée du Darknet (autrefois appelé « Arpanet »). Ce dernier est un ensemble de réseaux et de technologies utilisés pour partager du contenu numérique. Il est formé par l'ensemble des darknets et des outils associés de préservation de la confidentialité. Il permet un partage anonyme, chiffré, sans divulgation des adresses IPs de chacun, grâce à des protocoles spécifiques intégrant nativement des fonctions d'anonymisation. Le Darknet contient, entre autre, le darkweb.*

électroniques et d'expliquer la manière dont elles ont été obtenues en conformité avec les droits des parties »[1].

Il est donc nécessaire de **renforcer les échanges d'information avec les opérateurs privés** : « *Microsoft connaît mieux la cybersécurité des entreprises françaises que la cybersécurité publique nationale mais ne partage pas toujours cette information* », et de développer la **coordination avec le dispositif « Cybermalveillance.gouv.fr ».** S'agissant du secteur privé, le **rôle des opérateurs de réseau** pourrait être conforté. Il pourrait ainsi sensibiliser leurs clients à la cybersécurité, voire renforcer cette dernière, moyennant une majoration marginale du coût des abonnements.

La **place de l'ANSSI dans le dispositif pénal, et la répartition des rôles entre les investigations techniques et les investigations judiciaires, devraient être précisées** car l'essentiel est d'apporter des preuves[2], ce que seule l'ANSSI peut techniquement opérer. Sur ces deux éléments (coopération avec le privé et avec l'ANSSI), **une base législative au traitement et au partage de l'information doit être créée.**

Le **projet de loi relatif à la prévention d'actes de terrorisme et au renseignement**[3], en cours d'examen par l'Assemblée nationale, **renforce le partage d'information** mais **seulement en matière de terrorisme**.

Par ailleurs, **une proposition de loi de l'Assemblée nationale (n°2778), visant à renforcer la cybersécurité française,** a été déposée le 24 mars 2020 par M. Jean-Louis Thiériot (LR) et d'autres députés. Elle prévoit qu'en cas d'attaque informatique ou de pré-positionnement d'implants logiciels qui visent « *les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* », les services de l'État puissent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque. À cet effet, l'article unique vise à compléter l'article L.2321-2 du code de la défense. La notion de « potentiel économique » permet d'englober les cyberattaques contre les TPE et PME.

Proposition n°7 : Adapter les procédures pénales à la cybercriminalité et renforcer la coopération des institutions judiciaires avec l'ANSSI au-delà de la lutte contre le terrorisme.

---

1 *Audition du 15 avril 2021.*

2 *La question de l'accès à la preuve numérique dépasse d'ailleurs le cadre de la lutte contre la cybercriminalité : dans les affaires d'une certaine complexité, quelle qu'en soit la nature, les enquêteurs ont souvent comme premier réflexe d'exploiter des données de téléphonie mobile, de vidéosurveillance ou de solliciter des expertises informatiques, ce qui témoigne de la nécessité de sécuriser ces données.*

3 *N°4104 du 28 avril 2021.*

(4) Mettre à profit la Présidence française de l'Union européenne pour approfondir la coopération européenne en matière de lutte contre la cybercriminalité

Pour renforcer la coopération européenne dans la lutte contre la cybercriminalité, la présidence française de l'Union européenne (PFUE) au premier semestre 2022 devra être mise à profit pour porter ces différents sujets auprès des États-membres et des institutions, afin de renforcer la sécurité et la protection de l'espace numérique européen.

Des négociations sont actuellement en cours au niveau de l'Union européenne, dans le cadre du **paquet « e-evidence », afin d'harmoniser les règles de recueil de la preuve numérique** applicables à l'échelle européenne. Elles ont toutefois été ralenties par la crise sanitaire. Actuellement, la durée de conservation des données par chaque hébergeur n'obéit à aucune norme commune dans l'Union européenne. Ce recueil doit également garantir que la preuve n'a pas été falsifiée.

Par ailleurs, **une harmonisation de la position de l'Union européenne sur une vision plus offensive de la cybersécurité est nécessaire.**

L'interdiction juridique des perquisitions virtuelles ou de la fabrication et l'implantation d'éléments de neutralisation de logiciels malveillants dans des ordinateurs situés à l'étranger avait été évoquée dans le rapport du Sénat précité mais n'a toujours pas trouvé de réponse juridique satisfaisante.

Est-il permis d'apporter une modification, sans l'accord de leur propriétaire ni des États concernés, à des ordinateurs situés à l'étranger ?

Dans la résolution de l'affaire *REDATUP* en 2019, le C3N n'avait pas porté atteinte à un STAD puisque ce sont les ordinateurs contaminés qui se connectaient au serveur présent sur le territoire national, sans qu'il leur soit ordonné de réaliser de codes supplémentaires. Mais serait-il envisageable que des données plus intrusives soient envoyées vers les ordinateurs de particuliers ou d'entreprises à l'étranger, sans les en informer, dans le but de « nettoyer » ces machines, voire dans le but de neutraliser un *botnet* à distance ?

Sur ce sujet, le rapport du Sénat appelait à une « *réflexion européenne et internationale afin de définir les pratiques qui sont juridiquement acceptables et de prévoir des règles de bonne conduite dans les relations entre État*s ».

Elle pourrait déboucher dans les négociations (entamées depuis 2017) portant un deuxième protocole additionnel à **la convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, dite convention de Budapest**[1]**.**

[1] *Établie dans le cadre du Conseil de l'Europe, seul traité à portée universelle sur ce sujet. Son objectif principal est de poursuivre une politique pénale commune destinée à protéger la société de*

(5) Approfondir la coopération mondiale contre la cybercriminalité

Par ailleurs, **tant que le numérique reste dominé par les acteurs privés américains, une coopération juridique entre l'Union européenne et les États-Unis demeure la clé de voûte de la cybersécurité**.

Aux États-Unis, il n'existe pas d'obligation générale de conservation minimale des données pour une utilisation éventuelle par les services de police ou de justice. Malgré les coopérations existantes, « *le traitement des demandes (liées par exemple aux GAFAM Google, Amazon, Facebook, Apple, Microsoft), adressées par les autorités judiciaires françaises aux autorités judiciaires américaines, prennent parfois plusieurs semaines, hormis en cas d'urgence vitale, et peuvent ne pas aboutir, notamment lorsque la liberté d'expression, moins restrictive que l'analyse juridique de la France, est en jeu* »[1].

Un **mandat de négociation** a été confié à la Commission européenne pour organiser l'accès réciproque à la preuve électronique dans la relation avec les États-Unis, en application du *Cloud Act* américain. Quatre sessions de négociation ont eu lieu entre septembre 2019 et mars 2020. « *Toutefois, la Commission européenne lie la poursuite de ces négociations à celles du paquet « e-evidence », soulignant la nécessité de disposer de positions consolidées au niveau européen avant de poursuivre les discussions avec les États-Unis au-delà des aspects techniques relevant des États membres. Aucune nouvelle session de négociation n'a eu lieu depuis mars 2020* », selon une réponse ministérielle récente[2].

« *Les criminels utilisent des technologies rapides et modernes pour organiser leurs crimes et dissimuler les preuves. Une grande partie des données nécessaires pour traquer ces criminels sont conservées aux États-Unis ou par des compagnies américaines. Il est temps de travailler à un accord global entre l'Union européenne et les États-Unis pour accélérer l'accès de nos autorités judiciaires à ces preuves* », avait plaidé la commissaire européenne à la Justice, Vera Jourova, en février 2019.

Proposition n°8 : Accélérer les négociations européennes sur le paquet « *e-evidence* » et reprendre les négociations entre l'Union européenne et les États-Unis, afin d'approfondir la coopération internationale concernant la cybercriminalité.

---

la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et l'amélioration de la coopération internationale.

[1] *« Le droit pénal à l'épreuve des cyberattaques », Club des Juristes, avril 2021.*

[2] *Réponse du 8 décembre 2020 à la question n° 33267 adressée au Ministre de l'Europe du 20 octobre 2020 de Mme Marielle de Sarnez.*

B. DIFFUSER UNE CULTURE DE LA CYBERSÉCURITÉ DANS L'ENTREPRISE

Compte-tenu de la situation économique fragilisée des TPE et PME, les préconisations du CESIN imposant de nouvelles obligations aux entreprises n'ont pas été retenues[1].

Même si l'objectif recherché ne peut que susciter une approbation de principe, *rendre obligatoire* d'employer un expert en cybersécurité (à partir d'un certain seuil), un diagnostic flash de cybersécurité ou une formation des dirigeants dans ce domaine (laquelle conditionnerait toute forme de subvention aux entreprises dans le domaine numérique), n'est ni opportun ni souhaitable dans la perspective de reprise de l'activité économique de ces entreprises.

D'autres moyens d'atteindre cet objectif doivent donc être trouvés.

1. Renforcer l'« hygiène numérique » dans les entreprises

a) Introduire un volet de cybersécurité dans toute formation au numérique

Le niveau général « d'hygiène numérique » doit s'élever pour réduire l'impact potentiel d'une attaque sur l'entreprise.

Le renforcement des compétences numériques des salariés doit être une priorité des entreprises, tant le développement du télétravail pendant le confinement a révélé certaines faiblesses.

Selon une étude récente[2], **40 % des salariés ont amélioré leurs compétences numériques durant le confinement.** Cet enjeu inquiète car il creuse les inégalités entre les salariés. En effet, 60 % des interrogés craignent que l'automatisation, de plus en plus performante, mette en danger leur emploi, et 39 % d'entre eux que leur poste soit obsolète d'ici 5 ans. Par ailleurs, si 46 % des personnes interrogées qui détiennent un diplôme d'études supérieures indiquent que leur employeur offre beaucoup de possibilités concernant la montée en compétences digitales, ils sont seulement 28 % pour ceux titulaires d'un diplôme de niveau scolaire.

Pour évaluer ces compétences, des entreprises proposent des outils comme **le référentiel DiGiTT,** développé par Alternative Digitale et élaboré en collaboration avec des laboratoires de recherche (LIST, CNAM), Cette certification DiGiTT est **reconnue par l'État** en étant enregistrée au Répertoire Spécifique de France Compétences. Valable trois ans, elle est éligible au Compte personnel de formation.

---

1 *Contribution écrite de mars 2021.*

2 *L'étude « Hopes and Fears », menée au mois de février dernier par le cabinet d'audit PwC regroupe les réponses de 32 500 salariés dans 19 pays différents dont la France.*

Un volet de cybersécurité doit être systématiquement intégré à la définition, par les opérateurs de compétence (OPCO), des formations proposées. L'article L.6332-1 du code du travail prévoit que les OPCO doivent : « *assurer un service de proximité au bénéfice des très petites, petites et moyennes entreprises, permettant d'améliorer l'information et l'accès des salariés de ces entreprises à la formation professionnelle et d'accompagner ces entreprises dans l'analyse et la définition de leurs besoins en matière de formation professionnelle, notamment au regard des mutations économiques et techniques de leur secteur d'activité* ». Cet article pourrait être complété en précisant explicitement que cet accompagnement aux mutations techniques intègre une formation au numérique et à la cybersécurité.

Par ailleurs, l'article L.6111-2 du code du travail précise le contenu de la formation professionnelle tout au long de la vie en mentionnant : « *Les actions de lutte contre l'illettrisme et en faveur de l'apprentissage et de l'amélioration de la maîtrise de la langue française ainsi que des compétences numériques* ». Cet article pourrait être complété afin de préciser que l'apprentissage des compétences numériques doit comprendre celle de la cybersécurité.

Deux amendements en ce sens ont été déposés par le Président de la Délégation aux entreprises et les rapporteurs de la présente mission dans le projet de loi portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets, en cours d'examen au Sénat.

Cette mission pourrait être confiée aux CCI, dans le cadre de leur mission en faveur de la formation professionnelle – initiale ou continue – avec la formation aux enjeux environnementaux du numérique.

Proposition n°9 : Prévoir que les salariés doivent se voir proposer une formation professionnelle au numérique et à la cybersécurité.

b) Former davantage de professionnels de la cybersécurité

Selon le contrat stratégique de la filière « industries de sécurité » du 29 janvier 2020 : « *la filière arrive aujourd'hui plus ou moins à trouver les ingénieurs pointus dont elle a besoin et le nombre de places en master semble maintenant suffisant* ». En revanche, elle présente **un déficit d'étudiants aux niveaux Bac et Bac +2.**

L'un des objectifs de ce contrat est donc soit de créer de nouvelles formations courtes en cybersécurité (de niveaux 3, 4, 5 / BTS ou DUT Cyber) soit d'adapter les formations existantes (comme le BTS « Services informatiques aux organisations » précité) aux besoins des utilisateurs.

L'objectif est de **former 4 000 « opérateurs cyber » en 3 ans** sur les outils des éditeurs nationaux qui s'engagent à fournir les licences et les

tutoriels nécessaires. À titre de comparaison, Israël forme plus de 5 000 nouveaux lycéens par an à la cybersécurité.

Une campagne massive de publicité sur les métiers de la cybersécurité devrait accompagner cet effort.

Proposition n°10 : Déployer une campagne massive présentant les métiers de la cybersécurité, cofinancée par l'État et les acteurs privés du secteur.

2. Développer une « hygiène de la cybersécurité » dans les entreprises

a) Intégrer la cybersécurité dans la gouvernance de l'entreprise

Toutes les entreprises, y compris les TPE et PM, doivent organiser leur gouvernance pour organiser leur cyberrésilience.

En effet, l'augmentation des cyberattaques dépasse le cadre de la responsabilité de l'expert et doit devenir un projet d'entreprise impliquant l'ensemble de ses parties prenantes, et tout particulièrement les ressources humaines. La cyberrésilience transforme le modèle expert en modèle de management du risque.

Dès lors, selon CCI France, le sujet de la cybersécurité nécessite, à la fois, « ***une adhésion*** *de toutes les composantes de l'entreprise (directions, fonctions et collaborateurs) à la posture et à la stratégie adoptée en fonction de la cartographie des risques ;* ***une prise en compte de l'écosystème*** *(fournisseurs, clients et partenaires) dans cette gestion du risque et dans la construction d'une réponse pérenne ; et* ***une gouvernance*** *qui permet d'avoir des structures de décision agiles et réactives et de placer l'expertise de cyberprotection (RSSI) de façon appropriée dans l'organisation de l'entreprise* »[1]. Cependant, comme le constate cette étude, cette prise de conscience des dirigeants des TPE et PME est rendue plus difficile pour ces entreprises qui « *ne possèdent pas de Comex, voire de Direction des systèmes d'information (DSI) et encore moins de RSSI* ».

C'est la raison pour laquelle, pour implémenter la cybersécurité dans les TPE et PME, la **conviction et l'adhésion du dirigeant** sont les seules voies d'accès.

b) Mieux identifier le cyberrisque

Pour le réseau CCI France : « *les chefs d'entreprise considèrent le risque cyber comme un sujet technologique. Or, la plupart des cyberattaques provient des*

[1] *« Pérenniser l'entreprise face au risque cyber : de la cybersécurité à la cyberrésilience », CCI France, mai 2020.*

failles de la part des utilisateurs qui sont souvent considérés comme la « passoire » des hackers. Le risque cyber est donc un sujet humain ».

À ce titre, la gestion de la cybersécurité est de plus en plus considérée comme **un indicateur de la bonne gouvernance** de l'entreprise, et non plus uniquement comme un sujet technique relevant de la seule direction informatique.

Face à la multiplication des cyberattaques, et corrélativement, à l'augmentation des mesures de cybersécurité, le risque pour une entreprise à ne rien entreprendre de façon proactive et préventive dans ce domaine est de **perdre son statut de victime au profit d'une accusation de négligence**, qui contribuerait ainsi à la **détérioration importante de son image**.

C'est ainsi qu'avertissent deux experts[1] : « *Comme si les entreprises subissant une cyberattaque étaient encore vues comme des victimes ! **Ce temps-là est révolu : leurs publics leur reprochent désormais un manque de préparation**. Au-delà des pertes liées à l'arrêt de l'activité, d'autres dommages sont en effet à prendre en compte. C'est notamment l'image des sociétés victimes qui est souvent dégradée auprès des clients et partenaires à la suite d'une défaillance de sécurité. Une étude du cabinet PwC a d'ailleurs montré que **87 % des consommateurs sont prêts à rompre leur contrat avec une société qui affiche une faille informatique**. Même si les entreprises ne peuvent se prémunir à 100 % contre les risques de cyberattaques, ne rien faire n'est pas une option* ».

En raison de leur nombre, les TPE et PME ne pourront recevoir une aide et une protection publique comparable aux entreprises jugées d'importance vitale pour la vie économique de la Nation.

En raison de sa permanence, le cyberrisque doit être bien identifié et les PME comme les TPE doivent s'y préparer et s'organiser non seulement pour ne plus mettre en péril l'activité de l'entreprise mais aussi pour assurer la continuité d'activité, dans une logique de cyberrésilience.

La cyberprotection est de la responsabilité des entreprises. Elles peuvent toutefois être aidées par une certification et des experts.

c) Valoriser la certification en cybersécurité des entreprises

De plus en plus d'entreprises obtiennent et mettent en avant une certification de cybersécurité. Être certifié, c'est répondre à un cahier des charges donné par une norme établie par des organisations externes.

En matière de cybersécurité, les normes les plus connues de l'AFNOR[2] sont :

---

[1] *« Les entreprises démunies face à la multiplication des cyberattaques », La Tribune, 22 janvier 2020 Par Antoine Denry, directeur stratégie de H+K Strategies Paris, professeur au Celsa et à l'Université Panthéon-Sorbonne et Laurence Bault, directrice chez H+K Strategies Paris, et membre de l'AEGE, réseau d'experts en intelligence économique.*

[2] *https://certification.afnor.org/thematique/numerique*

- ISO 9001 : définit les critères d'un système de management en prônant une approche processus et l'amélioration continue ;
- ISO 27001 : mise en œuvre d'un système de management de la sécurité de l'information ;
- ISO 27005 : gestion des risques dans le contexte de la sécurisation des systèmes d'information.

Hors obligation sectorielle ou légale (par exemple le référentiel PCI-DSS pour les acteurs de la chaîne monétique des cartes de paiement), une certification n'est pas obligatoire. Même si une entreprise peut mettre en place un Système de Management de la Sécurité de l'Information répondant partiellement aux exigences exprimées, que le coût de la certification est moins élevé que celui d'une cyberattaque, que certains appels d'offres exigent de telles certifications, que celles-ci favorise l'amélioration continue et développe une culture commune au sein de l'entreprise, **la certification cybersécurité des entreprises n'est pas obligatoire.**

Elle est cependant prise en considération de façon croissante par les parties prenantes de l'entreprise, comme les investisseurs, les agences de notation (l'agence de notation Fitch l'intègre dans son évaluation des banques) ou les assurances.

d) Consolider la certification ExpertCyber

Deux types de certification co-existent : l'une publique et nationale, en cours de déploiement, une autre privée et internationale.

En matière de certification privée, plusieurs normes américaines sont proposées et deux chefs de file sont reconnus à l'échelle mondiale dans le domaine de la certification en matière de cybersécurité : (ISC)² et ISACA.

En matière de certification publique, le paysage est plus simple puisqu'un label unique et public a été lancé en mai 2020, **ExpertCyber**, développé par Cybermalveillance.gouv.fr, en partenariat avec les principaux syndicats professionnels du secteur : Fédération EBEN, Cinov Numérique, Syntec Numérique), la Fédération Française de l'Assurance et le soutien de l'AFNOR.

Peuvent être éligibles à la labellisation, pour une durée de deux ans, les entreprises de service informatique de toute taille, justifiant d'une expertise en sécurité numérique, adressant une cible professionnelle et assurant des prestations d'installation, de maintenance et d'assistance. Ce label permet d'être référencé sur www.cybermalveillance.gouv.fr.

L'examen de la candidature vise à déterminer plusieurs aspects. Après les vérifications d'ordre général sur la protection des données, est examinée la façon dont travaille l'entreprise via une étude de ses rapports de réponse à incident. Le processus de candidature se penche également sur les profils des employés de la société, notamment via un questionnaire de

compétences techniques sur les sujets de cybersécurité. Enfin, le dernier volet aborde la question du service client : la sensibilisation des clients à la cybersécurité en premier lieu, mais la transparence et la lisibilité des propositions commerciales seront aussi prises en compte.

Obtenir le label ExpertCyber permet au professionnel d'évaluer son expertise, ses bonnes pratiques et connaissances jugées nécessaires pour remplir ses missions auprès de ses clients. Il valorise son expertise, offre des garanties à ses clients, s'intègre dans une communauté d'experts.

Cette offre publique a comblé un vide qui doit profiter aux TPE et PME. Les visas de cybersécurité distribués par l'ANSSI ne s'adressaient qu'aux structures d'importance vitale. « *Ces prestataires ne vont pas intervenir sur les incidents mineurs qui peuvent toucher les PME, TPE et petites collectivités* », constatait Franck Giquel, responsable des partenariats de Cybermalveillance[1], lequel a été missionné pour que les entreprises de toutes tailles puissent accéder à une aide adaptée. Ce label permet de trier parmi les **1 600 prestataires** de proximité recensés sur le site Cybermalveillance qui jusqu'ici ne permettait que de présumer l'expertise en cybersécurité des entreprises.

Ce label doit également garantir une certaine qualité de l'accompagnement client, offrant aux assurances des listes d'acteurs de confiance capables de venir assister des TPE, PME ou petites collectivités, sur les questions de cybersécurité.

La construction d'une expertise de qualité est la condition pour rassurer les TPE et PME comme les assureurs. À terme, lorsque le label sera solidement installé, il est proposé qu'il devienne une condition de l'éligibilité au remboursement d'une cyberattaque par l'assurance.

Proposition n°11 : À terme, réserver l'éligibilité au remboursement d'une cyberattaque par les assurances aux entreprises ayant eu recours aux services des prestataires labellisés Expert Cyber.

C. INTERDIRE LE CARACTÈRE ASSURABLE DES RANÇONS À DES CYBERCRIMINELS

1. Une évaluation et un cadre incertains

En 2018, le marché mondial de la cyberassurance était estimé entre 3 et 3,5 milliards de dollars. Le marché américain capte 85 à 90 % de ces primes. L'Europe, quant à elle, ne représente encore que 5 à 9 % de ce

[1] *« À quoi va servir Expert Cyber, le nouveau label du gouvernement ? », François Manens, Cyberguerre, 22 mai 2020.*

marché, soit un montant maximum de 255 millions d'euros (300 millions de dollars) de primes.

Les pertes couvertes par de ces contrats d'assurance ne s'élevaient en 2019 qu'à environ 5 milliards de dollars, alors que le coût économique annuel de la cybercriminalité est estimé à plus de 700 milliards de dollars. En comparaison, les pertes économiques totales dues aux catastrophes naturelles et d'origine humaine s'élevaient à environ 140 milliards de dollars, dont 56 milliards de dollars assurés. Ces chiffres montrent le potentiel inexploité du marché de la cyber-assurance ; cette activité qui constituera dans la décennie à venir **l'un des principaux moteurs de croissance pour les assureurs des marchés développés**, où les branches traditionnelles, telles que l'assurance automobile ou habitation, sont largement saturées. En particulier, les primes de cyber-assurance pourraient augmenter de 20 à 30 % par an en moyenne, poussés notamment par la demande des petites et moyennes entreprises.

En France, en 2020, l'encaissement des primes d'assurance en cybersécurité s'élève à 130 millions d'euros alors que le marché de l'assurance non-vie représente, par comparaison, 59 milliards. Il est en forte progression puisque l'encaissement représentait 87 millions en 2019. Cependant, cette augmentation de 49 % est inférieure à la progression des **indemnisations versées qui ont été multipliées par trois en une année,** passant de 73 à 217 millions. Le ratio sinistres/primes a donc doublé, passant de 84 à 167 %[1]. Toutefois, ce bond est dû à seulement quatre sinistres de haute intensité concernant des grandes entreprises. Sans ces derniers, le volume de sinistralité eût été identique.

Le pourcentage d'entreprises ayant déclaré être assurées contre les incidents de sécurité augmente proportionnellement à la taille de l'entreprise. Si 87 % des grandes entreprises déclarent en avoir une, pour une couverture de 38 millions en moyenne ce qui est trop limité, seulement 8 % des ETI déclarent avoir souscrit à une telle assurance, pour une couverture moyenne de 8 millions[2].

Les PME, pour leur part, ignorent presque totalement les assurances du risque cyber. En 2020, seulement 362 des 140 000 PME réalisant entre 10 et 15 millions de chiffre d'affaires ont souscrit une telle assurance[3]. Leur taux de couverture est marginal avec seulement 0,0026 %... Le coût d'indemnisation pour une PME est de 40 000 euros en moyenne.

---

1 *Source : « Lumière sur la cyberassurance », AMRAE, mai 2021.*

2 *Idem.*

3 *L'étude précitée indique toutefois que : « ce chiffre est sans doute sous-estimé car elles peuvent aussi souscrire ce type de garanties auprès d'un agent général d'assurance, ou d'un courtier de proximité ».*

Les cyber-assurances prennent en charge trois risques :

- l'assistance à la gestion de crise ;
- l'évaluation des dommages sur les biens afin de reprendre une activité le plus rapidement possible ;
- l'atteinte à la confidentialité des données ou à la vie privée de tiers en cas de divulgation publique des données personnelles, dans le cadre du Règlement général sur la protection des données (RGPD).

Pour un assureur, **les PME n'ont pas le réflexe assurantiel en matière de cybersécurité**[1] : « *les PME se pensent trop souvent à l'abri du danger car elles ont déjà pris des mesures d'ordre technique (logiciels, pare-feu…) qu'elles estiment, à tort, imparables. Cela va prendre encore du temps pour que le réflexe cyber-assurance s'impose au sein des petites entreprises malgré mon rôle de conseil. Il est regrettable qu'une police d'assurance soit souscrite après que l'incident ait eu lieu, c'est pourtant mon quotidien* ». Par ailleurs, selon Oliver Wild de l'AMRAE[2], les PME « *se sont vues contraintes au saut numérique, auquel s'ajoute la nécessité d'un nouvel investissement financier et humain dans l'assurance cyber. Les PME doivent prendre conscience à la fois de leur dépendance numérique et de la nécessité de la sécurité numérique* ».

2. Un marché assurantiel risqué mais attractif

Les assureurs sont les premiers à s'interroger sur le caractère assurable du risque[3], lequel présente certaines spécificités.

En effet, un **cumul des engagements** est possible si un même événement est susceptible de causer de multiples sinistres au titre de diverses polices chez de multiples assurés à travers le monde : « *Si Google, Amazon ou OVH étaient touchés par un malware, que se passerait-il ? Si nous avons dix assurés qui sont hébergés par le même prestataire et que ce dernier connaît des difficultés de type cyber, nous pourrions avoir à payer dix fois la perte d'exploitation propre à chaque risque* » estime un autre assureur[4]. **Le cyberrisque doit par ailleurs être identifié de manière autonome** alors qu'actuellement des contrats traditionnels existants[5] peuvent couvrir des

---

1 *Julien Nelkin, Agent Général Aviva et gérant de JNK Assurances, Forbes, 29 septembre 2020.*

2 ***A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise est l'association professionnelle de référence des métiers du risque et des assurances en entreprise. Elle rassemble plus de 1500 membres appartenant à plus de 750 organisations privées ou publiques. Audition du 18 mars 2021.*

3 *Allianz Global Corporate & Specialty SE (AGCS), assureur en risques industriels et risques de spécialité du groupe Allianz, s'est ainsi associé en 2017 à la société américaine Cyence pour renforcer ses capacités d'analyse des cyber-risques à l'échelle mondiale.*

4 *Jérôme Chartrain, souscripteur cyber chez Allianz Global Corporate & Specialty (AGCS), Institut des Actuaires, 20 septembre 2018.*

5 *Dénommés « silent cover » ou « garanties silencieuses ».*

cyberrisques sans que ceux-ci aient été identifié comme tels ni pris en compte dans la tarification des contrats traditionnels par l'assureur.

Globalement, **le modèle assurantiel global n'est pas stabilisé**. Selon le président de l'AMRAE : « *avec un taux de couverture des entreprises et un volume de primes encore trop limités, les assureurs ne parviennent pas à trouver les conditions de la mutualisation indispensable au règlement des sinistres de forte intensité* »[1].

Si la cyberattaque est liée à un **risque de guerre**, elle est non assurable selon l'article L. 121-8 du Code des assurances[2]. Or, il est parfois difficile de distinguer une cyberattaque résultant d'un conflit et une simple attaque malveillante. Une rumeur de 'guerre informatique' pourrait bloquer l'indemnisation même si retrouver l'origine d'une attaque est actuellement pratiquement impossible. Inversement, la construction d'un régime assurantiel s'apparentant à celui des catastrophes naturelles en cas d'attaque systémique[3] pourrait **transférer l'indemnisation finale du préjudice à l'État**. Lorsque le fait générateur de la cyberattaque est le **terrorisme**, le mécanisme de la **co-réassurance assuré par le GAREAT**[4] s'applique dans les conditions suivantes :

- si la cyberattaque de nature terroriste provoque un dommage direct[5], le GAREAT couvre ces dommages ;
- si elle provoque une perte d'exploitation sans dommage direct, le GAREAT n'interviendra pas, même si le bien affecté par l'attaque est couvert en risque incendie ;
- si elle provoque une atteinte aux données, le GAREAT prend en charge le remplacement d'un support irrémédiablement corrompu et techniquement irréparable mais non si le support est techniquement réparable. Dans ces conditions, la restauration des données est en effet considérée comme la conséquence d'un dommage immatériel.

---

1 *« Lumière sur la cyberassurance », AMRAE, mai 2021.*

2 *« L'assureur ne répond pas, sauf convention contraire, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires. Lorsque ces risques ne sont pas couverts par le contrat, l'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère ; il appartient à l'assureur de prouver que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires ».*

3 *En juillet 2018, Stefan Golling, responsable de la souscription entreprise de Munich Re, déclarait ainsi que sa société ne voulait pas assurer certains aspects du cyberrisque à l'instar d'une « panne généralisée de réseaux externes, tels que l'électricité, les télécommunications ou l'infrastructure Internet ».*

4 *Groupement d'Intérêt Économique, créé fin 2001, dont l'objet est la mise en place d'un programme de réassurance au nom et pour le compte de ses adhérents dont il est mandataire, pour le transfert des risques de terrorisme dont la couverture est obligatoire en application de l'article L.126-2 du Code des assurances.*

5 *Par exemple, si un malware affecte le système de sécurité d'un process industriel, ce qui provoque un incendie et une perte d'exploitation.*

Rédigé en janvier 2018 au sein du Club des juristes mais avec le soutien de la Fédération française de l'assurance, le rapport « Assurer le risque cyber » estimait ainsi ce dernier « ***à la frontière de l'assurabilité*** », en raison de son coût croissant notamment avec un scénario de « **cyber-hurricane** »[1] qui « *pourrait atteindre des niveaux jamais atteints précédemment et mettre en danger la solvabilité d'un ou de plusieurs assureurs* ».

Cette inquiétude a conduit l'Autorité de contrôle prudentiel et de régulation, à lancer[2] un avertissement, en considérant que : « *si les contrats dédiés au cyber risque sont pour le moment peu développés, les organismes ne mesurent pas encore suffisamment leur exposition, notamment à travers les garanties implicites contenues dans les contrats en cours* ». Pour la Fédération française des assurances, la situation s'est depuis améliorée, et les entreprises d'assurance qui font partie du groupe de travail cyber de la FFA ont confirmé « *avoir réalisé un travail précis de l'exposition de leur portefeuille au risque cyber. Elles ont toutes travaillé sur l'identification de leurs expositions aux garanties non affirmatives, à la fois pour faire payer le juste prix du risque à leurs assurés, mais également et surtout afin de mieux maîtriser leurs cumuls d'engagements* »[3].

Certains acteurs majeurs de l'assurance, tel Swiss Re[4], affirment cependant que le cyberrisque **dépasse la capacité d'absorption du marché** et que ceux « *liés à des événements dommageables extrêmes ou catastrophiques, tels que la perturbation d'infrastructures ou de réseaux critiques, pourraient* ***demeurer inassurables*** » compte tenu de l'interdépendance des systèmes informatiques qui démultiplie les probabilités de propagation de certains types d'incidents cyber.

En outre, **ce marché pourrait être rapidement sélectif**, les assurances privilégiant les entreprises qui ont réalisé les analyses de leurs risques et mis en place des process de sécurisation numérique, et refusant d'assurer ou d'indemniser celles qui ont négligé leur cybersécurité.

Toutefois, le marché reste attractif et, pour sécuriser et gagner des clients, les **plateformes** pourraient proposer **directement** une assurance. Ainsi, l'alliance conclue en mars 2021 entre Google Cloud, Allianz Global Corporate and Specialty (AGCS) et Munich Re intègre des services de cyberassurance dans les services de *cloud computing*.

« Un manque cruel de données, des données peu fiables et un risque qui est toujours en train d'évoluer, stable ni du point de vue réglementaire, ni du point de

---

[1] *Incident cyber majeur, prenant par exemple pour cible des infrastructures critiques qui ont par nature une grande capacité de diffusion.*

[2] *Dans un communiqué du 12 décembre 2019.*

[3] *Réponse au questionnaire de la Délégation aux entreprises, 13 avril 2021.*

[4] *Deuxième société mondiale de réassurance après Munich Re.*

vue technique : le risque cyber est un casse-tête pour l'actuaire et les assureurs » selon un actuaire[1].

Les assureurs sont d'autant plus **prudents** que la cybersécurité est intrinsèquement difficilement assurable. **L'historique des sinistres, encore mal connu, leur manque** et rend difficile la fixation de leurs tarifs. L'évolution perpétuelle des cyberattaques rend les données historiques inaptes à prévoir les futurs risques. L'absence de déclaration systématique d'une cyberattaque affectant une entreprise entraîne une **sous-estimation de la sinistralité.** Enfin, **l'étendue du préjudice indemnisable est encore flou** : le cyberrisque, inclut-il, du point de vue assurantiel, la perte d'exploitation, le patrimoine immatériel de l'entreprise comme le risque d'image, et permet-il de couvrir les sanctions d'une entreprise qui n'a pas déployé une cybersécurité suffisante ou méconnu ses obligations légales de protection des données ? Permet-il également de couvrir le paiement d'une rançon ?

3. Une pratique qui nourrit un écosystème criminel

Le paiement de rançons par des entreprises victimes d'un rançongiciel nourrit cet écosystème criminel.

Selon un assureur[2], **16 % des entreprises attaquées dans le monde ont subi une attaque par rançongiciel et 58 % des entreprises concernées ont versé une rançon, soit pour récupérer des données, soit pour empêcher la publication d'informations sensibles.** Ce sont les entreprises américaines les plus promptes à payer puisque 71 % en auraient versé. Certains interlocuteurs relativisent cette pratique, et estiment que seules 5 % des entreprises auraient payé en 2020.

Payer attire également les répliques, de nouvelles attaques ciblant les entreprises qui ont payé. Pour le CERT : « *Si à court terme, payer la rançon est le moyen le plus simple et souvent le moins cher de recouvrer ses données, cela ne garantit en rien qu'une attaque de la part du même groupe cybercriminel ou d'un État de la menace rançongiciel autre ne surviendra pas un autre jour. L'éditeur de Sophos mentionnait dans un rapport de janvier 2018 que* ***la moitié des victimes de rançongiciels l'étaient plusieurs fois*** »[3].

Payer nourrit un écosystème trouble. Comme le souligne le CERT : « *certaines sociétés se sont également développées autour de ce paiement des rançons en proposant des services de négociation et de médiation entre la victime et l'attaquant. C'est le cas notamment de la société Coveware qui procède en toute*

---

[1] *Florian Pons, actuaire qualifié, ingénieur Supélec, est membre du groupe de travail Big Data et Cyber-risk de l'Institut des actuaires : « Cyberassurance : digérer la part de risques ». Institut des actuaires, 20 septembre 2018.*

[2] *Rapport Hiscox sur la gestion des cyber-risque, du 17 avril 2021, précité.*

[3] *« État de la menace rançongiciel à l'encontre des entreprises et institutions », 5 février 2020.*

transparence[1]*. Toutefois, certaines sociétés camouflent le fait qu'elles payent la rançon en prestations de déchiffrement des fichiers à l'aide d'expertise technique interne. Pire, certaines de ces sociétés ont également développé des liens parfois étroits avec des groupes cybercriminels, notamment GandCrab, afin d'accéder à des réductions des rançons. Cette gestion du risque par le développement d'une économie autour du paiement des rançons est un phénomène inquiétant. Il valide pleinement le modèle économique développé par les attaquants, les assurant d'un plus grand nombre de paiements des rançons ».*

4. Un paiement sans garantie de résultat

En cas de cyberattaque, dans la pratique, les entreprises consacrent en priorité leurs efforts à la restauration de leur système informatique. Elles sont nombreuses, notamment les PME, à vouloir payer une rançon pour le restaurer dans les meilleurs délais. Or, le paiement d'une rançon ne permet pas toujours d'obtenir le déchiffrement des données.

L'ANSSI recommande de ne pas payer la rançon, laquelle ne garantit pas à l'entreprise de pouvoir récupérer ses données :

> ***« Il est recommandé de ne jamais payer la rançon. Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux****. De plus, le paiement de la rançon n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels. Par ailleurs, l'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données) ».*
>
> *Source : « Attaques par rançongiciels, tous concernés comment les anticiper et réagir en cas d'incident ? », ANSSI , août 2020.*

Le Haut comité juridique de la place financière de Paris a été missionné en début d'année par la direction générale du Trésor pour apporter des recommandations à ce sujet. Il devrait rendre ses conclusions le 29 septembre 2021.

5. Une interdiction du caractère assurable des rançongiciels

Dans une directive publiée le 1er octobre 2020 par le ministère du Trésor américain[2], **le gouvernement des États-Unis** indique que **des**

---

[1] *La société américaine prétend que cette transparence contribue à la cybersécurité : « Nous pensons que les entreprises de récupération de données qui dissimulent leurs méthodes sont malhonnêtes et que les victimes méritent une expérience fondée sur l'honnêteté, la transparence et l'équité ».*

[2] *Publiée en annexe du présent rapport.*

sanctions pourront être envisagées, dans certaines conditions, pour les entreprises qui paient une rançon suite à une attaque de rançongiciel. Compte-tenu de la **portée extraterritoriale** que les États-Unis entendent donner à leur législation économique, notamment avec le *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* de mars 2018[1], les entreprises européennes et françaises sont potentiellement concernées dès lors qu'elles ont un rapport soit avec le marché ou la monnaie américaine, soit avec une procédure judiciaire américaine[2]. Cette recommandation **n'interdit cependant pas le paiement,** fréquemment pratiqué par les entreprises américaines.

Aucun pays dans le monde ne rend illicite le paiement d'une rançon et son caractère assurable, même si les autorités publiques font pression sur les entreprises pour ne pas les payer[3]. Les entreprises payent en ultime recours, lorsque leur survie est en jeu, ou lorsque l'intérêt national est impacté, tel a été le cas par exemple de l'alimentation énergétique du nord-est des États-Unis lors de l'affaire de l'oléoduc Colonial Pipeline. Dans ce dernier cas, l'autorisation des autorités publiques est sous-jacente.

En France, le paiement des rançons n'est pas actuellement interdit. « *Leur assurabilité est sujette à caution* » selon la Fédération française des assurances[4], qui « *réclame depuis de nombreuses années un éclaircissement sur l'assurabilité des rançons. Aucune position ni de l'ACPR, ni de la DG Trésor ni du législateur, n'est venue répondre à cette question. La seule réponse claire concerne le financement du terrorisme qui est interdit* »[5].

Un simple communiqué du ministère des Finances de décembre 2015 a en effet clairement prohibé « *les contrats d'assurance, dont l'objet est de garantir le paiement d'une rançon à* ***Daech****, comme à toute entité terroriste* » et pour encourager « *l'insertion de clauses dans les contrats d'assurance "kidnapping et rançon" excluant le remboursement ou le paiement d'une rançon, directement ou indirectement, via des intermédiaires, qui bénéficieraient à Daech* ». Cependant, il est souvent difficile de connaître l'auteur d'une cyberattaque et d'identifier l'origine terroriste ou non d'un incident. « *Sauf à pouvoir démontrer qu'un piratage a été réalisé par une organisation terroriste, il demeure un vide juridique quant à la légalité de l'assurabilité des rançons* » considère la FFA.

---

1 *Le CLOUD Act réaffirme la capacité du droit américain à s'appliquer, en matière numérique, peu importe le territoire. Il permet, en particulier à la justice américaine, munie d'un simple mandat, d'exiger auprès des entreprises technologiques établies aux États-Unis la transmission des données de communications d'un utilisateur stockées sur des serveurs appartenant ou étant opérés par l'entreprise, où qu'ils se trouvent, sans en informer l'individu en question.*

2 *Voir le rapport d'information de M. Philippe Bonnecarrère, fait au nom de la commission des affaires européennes du Sénat, n° 17 (2018-2019) du 4 octobre 2018, sur l'extraterritorialité des sanctions américaines.*

3 *M. Chrisitian Delcamp, Fédération Française de l'assurance , audition du 3 juin 2021.*

4 *« Assurer le risque cyber », rapport de janvier 2018.*

5 *Réponse au questionnaire de la Délégation aux entreprises, 13 avril 2021.*

Or, **les actifs numériques apparaissent comme une source croissante de financement du terrorisme**.

C'est pourquoi **l'ordonnance n°2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques** renforce la lutte contre l'anonymat des transactions en actifs numériques et tire toutes les conséquences de l'absence d'harmonisation du cadre européen en la matière en incluant les prestataires de services sur actifs numériques parmi les entités ayant **l'interdiction de tenir des comptes anonymes** et en confirmant l'obligation, introduite par la loi PACTE, d'enregistrement préalable pour les acteurs étrangers désireux de cibler le marché français en libre prestation de services. Ces mesures seront complétées par des dispositions réglementaires portées dans un décret sur le gel des avoirs qui permettront de renforcer significativement les obligations d'identification préalable dans le cadre des transactions occasionnelles réalisées par les prestataires de services sur des actifs numériques français. Ce cadre national particulièrement exigeant devrait être promu, dans les prochains mois, dans le cadre de la réforme européenne du dispositif réglementaire et de supervision de l'Union, aujourd'hui incomplet.

Dans cette logique, **interdire le caractère assurable des rançongiciels est une nécessité** bien que ce soit les entreprises les plus conscientes du cyberrisque qui sont les premières à s'assurer. On peut craindre en revanche qu'assurer un cyberrisque n'inciterait pas l'entreprise à prendre des mesures de cyberprotection adaptées. La nécessité d'une solvabilisation du marché de l'assurance doit également être prise en considération.

Cependant, interdire aux assureurs français de proposer ce type d'assurance créerait une distorsion de concurrence avec les autres assureurs européens qui y sont autorisés. **Cette interdiction devrait donc procéder d'un Règlement européen voire d'un amendement à la convention de Budapest de 2001**, qui est en cours d'actualisation. L'adhésion des États-Unis depuis 2007 à cette convention sur la cybercriminalité en fait l'instrument le plus adapté pour apporter une réponse coordonnée à cette question.

Cette interdiction devrait conduire à prohiber également **l'assurabilité des sanctions administratives** en cas en cas de violation de la réglementation sur la protection des données à caractère personnel, qui divise la jurisprudence comme la doctrine.

Proposition n°12 : Interdire l'assurabilité des rançongiciels et des sanctions administratives en cas en cas de violation de la réglementation sur la protection des données à caractère personnel, par un amendement à la convention de Budapest de 2001, par un Règlement européen, et par une disposition législative expresse dans le code des assurances.

D. DÉVELOPPER DIX OUTILS DE CYBERSÉCURITÉ ADAPTÉS AUX TPE ET PME

1. Offrir des outils sécurisés : la *security by design*

De nombreux interlocuteurs ont rappelé que les fabricants de logiciels ne sécurisaient pas suffisamment leurs produits. Il conviendrait donc de **renforcer la responsabilité des éditeurs de logiciels et des revendeurs sur le niveau de cybersécurité de leurs produits**.

Ce point ne figure pas, hélas, dans la directive NIS 2[1]. La réponse à cette question rappelle la difficulté d'établir la responsabilité des hébergeurs pour les contenus[2].

Dans ce sens, le rapport de la Cour des comptes, de février 2020, sur la lutte contre les contrefaçons suggère parallèlement de **renforcer les obligations juridiques des plateformes du commerce en ligne** afin de mieux lutter contre le commerce de contrefaçons.

a) 150 000 failles de sécurité recensées

Les failles de sécurité numérique sont recensées aux États-Unis dans un catalogue public répertoriant les vulnérabilités de sécurité[3], le ***Common***

---

[1] *Le 16 décembre 2020, **la Commission européenne** a présenté sa stratégie en matière de cybersécurité pour la décennie numérique, laquelle a pour ambition de « façonner l'avenir numérique de l'Europe ». Dans ce contexte, la Commission européenne a adopté une **proposition de révision de la directive NIS (dite NIS 2.0) et une proposition de directive sur la résilience des entités critiques**. Dans le cadre de ces deux propositions de directive, la Commission européenne élargit le champ d'application de la directive NIS en ajoutant de nouveaux secteurs d'activité en fonction de leur importance pour l'économie et la société et en prenant leur taille en considération. Ainsi, la distinction entre les opérateurs de services essentiels et les fournisseurs de services numériques serait-elle supprimée. En outre, les entités seraient réparties en deux catégories : entités essentielles ou entités importantes. Chacune de ces catégories étant soumise à des obligations spécifiques. La Commission européenne propose également de renforcer les exigences de sécurité suivant une approche par les risques. La proposition de directive NIS 2.0 introduit des dispositions plus précises sur le processus de notification des incidents, le contenu des rapports et les délais. Les propositions de la Commission européenne visent, par ailleurs, à harmoniser les régimes de sanction sur le territoire de l'Union européenne.*

Enfin, ces propositions s'intéressent plus particulièrement à la question de la sécurité des chaînes d'approvisionnement et aux relations avec les fournisseurs. En effet, les risques en matière de cybersécurité devront aussi être pris en compte dans ces contextes. Ainsi, sur le plan contractuel, ces propositions conduisent à renforcer notamment les clauses relatives à la sécurité et aux audits.

En dernier lieu, au niveau européen, la coopération opérationnelle est accentuée entre les États membres et l'European Union Agency for Cybersecurity (ENISA) notamment en matière de gestion de crises en matière de cybersécurité et d'identification des incidents de sécurité.

[2] *En témoigne la censure de la loi « AVIA » par le Conseil constitutionnel, par sa décision n° 2020-801 DC du 18 juin 2020.*

[3] *Une vulnérabilité de cybersécurité fait généralement référence à une faille dans le code logiciel qui permet à un attaquant d'accéder à un réseau ou un système. Les vulnérabilités exposent les*

Vulnerabilities and Exposures ou **CVE.** Il est alimenté par l'organisation à but non lucratif MITRE, et soutenu par le département de la Sécurité intérieure des États-Unis. Il fournit la base de données nationale sur les vulnérabilités (NVD) du gouvernement américain. Elle compte actuellement plus de **150 000 entrées**.

Un exemple bien connu de vulnérabilité de cybersécurité est la faiblesse Windows CVE-2017-0144 qui a ouvert la porte aux attaques de rançongiciel WannaCry via EternalBlue.

La base de données NVD recense **une hausse des vulnérabilités** : **18 362 en 2020**, contre 17 382 en 2019 et 17 252 en 2018[1]. La moitié des vulnérabilités des applications Web internes sont considérées comme à haut risque. Elles peuvent être découvertes à tout moment alors qu'elles sont anciennes : la faille CVE-1999-0517[2] découverte en 2020 datait de 1999.

Le principe semble même être que **la majorité des applications présentent des failles de sécurité.** Un rapport sur l'état de la sécurité logicielle, publié en octobre 2020[3], a révélé que plus des trois quarts (75,2%) des applications présentaient des failles bien que seules 24% d'entre elles soient considérées comme présentant des défauts de gravité élevée.

Selon le rapport qui fait autorité, *Edgescan's 2021 Vulnerability Statistics Report*[4], **même le cloud n'est pas invulnérable**. Début 2020, les chercheurs de Check Point CloudGuard, qui voulaient réfuter l'hypothèse selon laquelle les infrastructures cloud sont sécurisées, ont découvert et signalé des vulnérabilités critiques dans l'infrastructure Microsoft Azure.

Cependant, **toutes les vulnérabilités ne mènent pas forcément à une cyberattaque**. En effet, elles sont majoritairement rendues publiques et corrigées (*full disclosure*). Selon Orange Cyberdéfense[5], moins de 5 % des vulnérabilités publiées disposent d'un code d'exploitation final, lequel permettrait d'exploiter la vulnérabilité et rendrait possible une attaque. Ainsi, la **plupart** des vulnérabilités **ne sont pas exploitées**.

Mais, malgré la publication des failles, les cyberattaques perdurent car les mises à jour ne sont pas effectuées. Selon le rapport sur la cybersécurité 2021 de Check Point[6], 75 % des attaques ont profité de failles signalées en 2017 ou avant, et 18 % des attaques utilisaient des vulnérabilités

---

entreprises et les particuliers à une gamme de menaces, notamment les logiciels malveillants et les prises de contrôle de compte.

1 *« 25+ cyber security vulnerability statistics and facts of 2021 », Aimee O'Driscoll, Comparitech, 21 avril 2021.*

2 *Elle affecte le protocole SNMPv2 (Simple Network Management Protocol version 2), qui est utilisé pour gérer les périphériques et les ordinateurs sur un réseau IP.*

3 *https://www.veracode.com/state-of-software-security-report*

4 *https://info.edgescan.com/vulnerability-stats-report-2021*

5 *« Vulnérabilités : de quoi parle-t-on ? », 14 mars 2019.*

6 *https://www.checkpoint.com/downloads/resources/cyber-security-report-2021.pdf*

qui ont été révélées en 2013 ou avant. 26 % des entreprises restent vulnérables au rançongiciel WannaCry car elles n'ont pas encore corrigé la vulnérabilité qu'il exploite[1]. Environ 25 % des failles sont toujours ouvertes un an et demi après leur découverte. Selon le Ponemon Institute : « *60 % des victimes de cyberattaque ont déclaré l'avoir été en raison d'une vulnérabilité connue mais non corrigée* ». Cependant, une proportion encore plus élevée (62 %) a déclaré qu'elle n'était pas au courant des vulnérabilités de leur entreprise avant une violation.

Le temps de la correction des failles dépend du nombre d'analyses de cybersécurité : les entreprises qui effectuaient plus de 260 scans par jour ont corrigé 50% des défauts en 62 jours alors que ce délai a été porté à 217 jours pour les applications exécutant seulement 1 à 12 analyses par jour.

Lutter contre les failles et vulnérabilités des systèmes et des logiciels fait partie du quotidien des responsables informatiques. Il est nécessaire de se tenir informé des attaques en vogue et des failles découvertes.

Cependant, **le nombre de failles de sécurité va croître de manière exponentielle avec l'Internet des objets (IoT).** Pour une caméra de vidéosurveillance, il faut ainsi sécuriser à la fois l'objet connecté, mais également le protocole de communication avec lequel l'équipement échange sur le réseau et la cible d'enregistrement des images.

« *La Security by Design est à la fois un objectif et une philosophie. Elle n'est pas inatteignable. Mais elle n'est pas non plus définitive. Il y a donc des méthodes pour s'approcher d'un optimum* » estime Stéphane de Saint Albin, vice-président d'Hexatrust, l'association qui fédère des entreprises françaises spécialisées en cybersécurité[2].

Deux initiatives pourraient toutefois renforcer la *security by design* : l'introduction d'une « garantie logicielle » d'une part, des « hackathon »[3] rendant publics les failles de sécurité, d'autre part.

b) L'insuffisante garantie de mise à jour des logiciels de sécurité

Des avancées existent dans ce domaine mais elles ne concernent que les consommateurs et non les entreprises.

---

1 https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-corporate-networks-2020/

2 *« Security by Design : les règles à suivre pour les équipements de sécurité connectés », Info Protection, 11 juin 2020.*

3 *Terme issu de l'anglais hack (s'introduire dans un système) et du français marathon imaginé par les communautés de développeurs regroupés au sein du mouvement Free Open Source Software.*

LA GARANTIE LOGICIELLE DE MISE À JOUR

① La directive 2019/770/UE du 20 mai 2019 relative à la fourniture de contenus et services numériques et la directive 2019/771/UE du 20 mai 2019 concernant certains aspects des contrats de vente de biens prévoient désormais **l'obligation pour le vendeur de fournir des mises à jour, y compris de sécurité, qui assurent le bon usage des produits pendant une période raisonnable**.

Lors de la discussion de la loi n°2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire, le Sénat avait introduit la notion de « garantie logicielle » imposant aux fabricants de smartphones et de tablettes de proposer des mises à jour correctives du système d'exploitation, compatibles avec tous les modèles de leur gamme, jusqu'à dix ans après leur mise sur le marché.

Les députés ont sensiblement allégé cette disposition en la remplaçant par un dispositif d'information. Le producteur doit d'abord informer le vendeur de la durée au cours de laquelle les mises à jour des logiciels restent compatibles avec un usage normal de l'appareil, c'est-à-dire un usage qui « *[réponde] aux attentes légitimes du consommateur* ». Ensuite, le vendeur « *met ces informations à disposition du consommateur* ». En séance, les députés ont ajouté une information sur les mises à jour nécessaires au maintien de la conformité des biens comportant des éléments numériques. Le vendeur doit informer le consommateur des modalités d'installation de ces mises à jour « de façon suffisamment claire et précise ». Le consommateur peut les refuser. Le vendeur doit alors expliquer les conséquences de ce refus pour être déchargé de sa responsabilité en cas de défaut de conformité lié à la non-installation des mises à jour. Ces dispositions sont complétées par une obligation de fourniture des mises à jour dans un délai raisonnable. Ce délai « *ne peut être inférieur à deux ans* ».

② La directive 2019/770/UE du 20 mai 2019 a été transposée par la loi n°2020-1508 du 3 décembre 2020, portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière. L'article 1er révise certaines modalités de la garantie légale de conformité des biens et instaure une **garantie analogue pour les produits numériques**.

La durée de la garantie légale de conformité sera fixée à deux ans pour les biens comportant des éléments numériques. Elle pourra être supérieure à deux ans lorsque le contrat prévoit la fourniture de contenus ou de services numériques pendant une période supérieure à deux ans. Pendant ce délai, le consommateur aura droit à la réparation ou au remplacement du bien (ou à la mise en conformité du contenu/service numérique) et ce, sans frais, sans inconvénient majeur et dans un délai raisonnable ne pouvant dépasser 30 jours. À défaut, il pourra obtenir une réduction du prix ou la résolution du contrat.

Elle prévoit certaines obligations spécifiques aux éléments numériques qu'ils fassent l'objet d'un contrat de fourniture ou qu'ils relèvent des caractéristiques essentielles d'un bien connecté. Il s'agit en particulier du **droit à recevoir des mises à jour** nécessaires au maintien de la conformité, du **droit de refuser les éventuelles modifications** (*upgrades*) intervenant après la fourniture ou encore du **droit de récupérer** les contenus utilisés en cas de résolution du contrat.

Les sanctions en cas de non- respect de ces modalités sont renforcées.

Toutefois, **ces garanties ne concernent pas les entreprises, mais seulement les consommateurs personnes physiques**, dans la mesure où il agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole (selon l'article liminaire du code de la consommation).

③ La proposition de loi sénatoriale visant à réduire l'empreinte environnementale du numérique en France, n 27, du 12 octobre 2020, adoptée par le Sénat le 12 janvier 2021 est en cours d'examen à l'Assemblée nationale.

Son article 8 complète la transposition de la directive 2019/770/UE. Le Sénat avait imposé que le vendeur veille à **fournir les mises à jour, y compris des celles de sécurité, non nécessaires à la conformité du bien séparément des mises à jour nécessaires à la conformité du bien**, de façon à permettre au consommateur, s'il le souhaite, de n'installer que les mises à jour nécessaires à la conformité du bien. La version adoptée en commission du développement durable et de l'aménagement du territoire[1] est moins exigeante. Elle prévoit que le vendeur ne pouvant être seul responsable de la fourniture des mises à jour logicielles, celui-ci doit **veiller à ce que le consommateur soit informé et reçoive les mises à jour** non nécessaires à la conformité du bien séparément des mises à jour nécessaires à la conformité du bien.

Le vendeur aurait **une obligation d'information et de vérification de la bonne réception des mises à jour, et non de fourniture de ces mises à jour**.

Une adaptation, pour les entreprises, de cette garantie logicielle serait opportune.

Dans cet objectif de renforcement de la sécurité par défaut, 16 grandes entreprises mondiales ont signé la « ***Charter of Trust*** »[2], laquelle fournit à ses membres une vision harmonisée de la sécurité tout au long de la chaîne d'approvisionnement numérique et a défini 12 exigences minimales concernant la cybersécurité des chaînes d'approvisionnement.

c) Rendre publiques les failles de sécurité avec le hacking éthique

Ces failles de sécurité sont tellement nombreuses que les principales entreprises du numérique rémunèrent ceux qui les détectent :

- Le programme de récompense de vulnérabilité de **Google** a versé 6,7 millions de dollars en récompenses en 2020 et 28 millions de dollars depuis 2010. 662 chercheurs de 62 pays ont reçu des primes en 2020, la plus grande récompense s'élevant à 132 500 dollars.

- **Microsoft** a indiqué en août 2020 qu'elle avait payé 13,7 millions de dollars en primes de bogues au cours des 12 derniers mois, soit plus du

[1] *Rapport n°4196 du 26 mai 2021. La proposition de loi a été examinée en séance publique le 10 juin 2021.*

[2] *https://www.charteroftrust.com/*

double du montant que Google a payé en 2019. Au total, 327 chercheurs ont reçu un prix, le plus important s'élevant à 200 000 dollars.

- **Facebook** indiquait en novembre 2020 que depuis le lancement de son programme en 2011, la société a reçu plus de 13 000 rapports et attribué 6 900 primes, celles de 2020 totalisant près de 2 millions de dollars. Environ 17 000 rapports ont été reçus et plus de 1 000 primes ont été attribuées. Sa prime la plus élevée à ce jour est de 80 000 dollars.

Ce « **piratage éthique** »[1] a été **légalisé en France** par la **loi du 7 octobre 2016** pour une République numérique. Elle a introduit dans le code de la défense un article L2321-4[2], visant à sécuriser ceux qui signalent une faille informatique découverte par leurs soins. Cependant, **cette protection des lanceurs d'alerte en cybersécurité n'est pas totale**, comme l'a montré le licenciement « pour faute grave » d'un employé de Dedalus France – « *leader européen en matière de solutions logicielles de Santé* » – qui avait alerté les autorités pour faire colmater une faille importante en urgence au sein de l'AP-HP, victime d'une cyberattaque[3].

Il existe même une certification en hacking éthique[4] décernée par le EC-Council américain.

Afin de sensibiliser les éditeurs de logiciels au renforcement de la *security by design*, **un hackathon de la cybersécurité pourrait être organisé par l'ANSSI**, qui rendrait ainsi publiques les failles de sécurité, notamment pour les logiciels entrant sur le marché.

Un hackathon désigne un rassemblement d'informaticiens durant plusieurs jours en vue de collaborer sur des sujets de programmation informatique pointus et innovants. Il serait entièrement dédié à la cybersécurité des entreprises (mais pourrait être ultérieurement décliné pour les établissements de santé et collectivités locales), organisé annuellement, et

---

[1] *Les hackeurs éthiques sont des experts en sécurité informatique qui ne s'introduisent dans les systèmes informatiques qu'après une mission explicite. En raison du consentement de la « victime », cette variante de piratage est considérée comme éthiquement justifiable. L'objectif du piratage éthique est de découvrir les faiblesses des systèmes et infrastructures numériques.*

[2] *Ainsi rédigé :*

« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

[3] « Un leader européen des données de santé licencie un lanceur d'alerte pour faute grave » *Jean-Marc Manach, Next Impact, 2 octobre 2020.*

[4] *https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/*

les vainqueurs verraient leurs investigations récompensées par une certification renforcée de « Cyber Expert ».

Cet évènement pourrait être organisé **tous les 30 novembre**[1], qui est, depuis 1988, la **journée mondiale de la cybersécurité**[2].

Proposition n°13 : Afin de renforcer la *security by design* :

- **étudier l'extension aux entreprises de la « garantie logicielle » concernant les mises à jour de sécurité ;**
- **organiser, avec le support de l'ANSSI, un « hackathon de la cybersécurité » des entreprises, lors de la journée mondiale de la cybersécurité, le 30 novembre.**

2. Développer l'accompagnement des dirigeants de PME à la cybersécurité

Les organisations professionnelles, comme la CPME, les réseaux professionnels, tel CCI France, ou Bpifrance, qui peut financer jusqu'à 50 % d'une mission d'audit de cybersécurité pendant 10 jours, accompagnent déjà les dirigeants de PME pour les sensibiliser à cet enjeu.

Les experts-comptables et les commissaires aux comptes (CAC) sont de plus en plus sensibilisés au rôle primordial d'alerte qu'ils doivent tenir en matière de lutte contre la cybercriminalité[3]. Après les directions des systèmes d'information, ils représentent les **premières vigies** face aux cyberattaques subies par leurs clients. Ils jouent un rôle essentiel d'alerte et de conseil par un regard extérieur dans la prévention à la cybersécurité.

Cette obligation professionnelle résulte à la fois :

- de la norme d'exercice professionnel (NEP) 240[4], qui demande au commissaire aux comptes d'être acteur dans la détection de fraude interne ou externe (conformément à cette obligation de moyen, le commissaire aux comptes doit tout mettre en œuvre pour s'assurer qu'il n'y a pas de fraudes avérées) ;

---

[1] *Le 31 mars est par ailleurs la journée mondiale de la sauvegarde des données informatiques.*

[2] *Une initiative similaire a été proposée dans une tribune signée par 11 députés « Pour la création de la journée mondiale des White Hats (hackers éthiques) », L'Opinion, 12 Janvier 2021.*

[3] *« Les professions comptables vigies en matière de cybersécurité », Anne Moreaux, Les Affiches Parisiennes, 26 juin 2018.*

[4] *La norme d'exercice professionnel 240 qui correspond à l'adaptation de la norme ISA 240 a été homologuée par arrêté du 10 avril 2007. Elle a fait l'objet d'amendements de conformité et a été homologuée par arrêté du 21 juin 2011.*

- de la NEP 570[1], qui lui confie un rôle d'alerte en cas de menace pour la continuité d'exploitation de l'entreprise auditée ;

- l'audit légal des petites entreprises (ALPE), qui comprend un rapport sur les risques financiers, comptables et de gestion dans lequel figure une appréciation des risques de cybersécurité en application de la NEP 911[2].

En tant que principaux partenaires de l'entreprise, ils n'abordent pas la cybersécurité comme un sujet de technique informatique, mais sous l'angle du management du risque, donc de gouvernance et de protection du bilan de l'entreprise. En cas de cyberattaque, le commissaire aux comptes peut ainsi réaliser également une analyse critique de la procédure de sauvegarde et suivre son incidence sur les comptes de l'entité, ou encore s'assurer du suivi correct de l'après-attaque.

Le champ de conseil au numérique des experts-comptables a été étendu par la loi PACTE du 22 mai 2019, **dans toutes les entreprises y compris celles qui n'ont pas l'obligation de faire certifier les comptes, en se faisant assister par des cyberexperts.**

Après une campagne de sensibilisation des PME, la Compagnie nationale des commissaires aux comptes a présenté en février 2019, l'outil « **CyberAUDIT** », afin de favoriser l'intervention des commissaires aux comptes dans les entreprises en matière de cybersécurité.

Le rôle des deux professions n'est cependant pas simple à distinguer en matière de cybersécurité. Dans un entretien récent[3], M. Jean Bouquot, alors président de la Compagnie nationale des commissaires aux comptes (CNCC) indiquait : « *En matière de cybersécurité, de certification d'une situation financière ou de critères extra-financiers, nous retrouvons potentiellement l'expert-comptable dans des missions proches. Pour bien distinguer les deux, il faut comprendre que dès lors qu'il s'agit d'auditer une situation financière par exemple, c'est le commissaire aux comptes qui intervient. Dès lors qu'il y a une dimension de conseil ou une dimension de construction de la situation financière, par exemple, la mission est en principe celle de l'expert-comptable* ».

Comme la loi le permet désormais, et comme le rapport de l'Institut Montaigne de 2018 le préconise[4], les réseaux des métiers du chiffre (experts-comptables et commissaires aux comptes) doivent être **mobilisés pour réaliser un diagnostic cybersécurité annuel,** avec un cahier des charges construit avec les autorités publiques, qui doit être communiqué directement aux dirigeants à titre d'information avec les recommandations de base pour couvrir les risques. Ce **référentiel indicatif** renforcerait la culture de la cybersécurité dans l'entreprise, en sensibilisant les dirigeants de PME, et de

---

1 *La norme d'exercice professionnel 570 a été homologuée par arrêté du 26 mai 2017.*

2 *La norme d'exercice professionnel 911 a été homologuée par arrêté du 6 juin 2019.*

3 *Interview de Compta On Line du 6 juillet 2020.*

4 *« Cybermenace, avis de tempête », de novembre 2018)*

l'entreprise, en valorisant celles qui ont un niveau satisfaisant. Il permettrait également de **mieux identifier le commissaire aux comptes comme acteur de l'audit du cyberrisque**. Ce dernier est souvent le meilleur allié du RSSI dans l'entreprise, en convainquant le chef d'entreprise de la nécessité de consacrer des moyens financiers appropriés à la cybersécurité.

Cela implique **d'augmenter le niveau de compétence des métiers du chiffre sur la cybersécurité** et de **faire primer le rôle d'alerte et de sensibilisation sur une expertise technique en matière de cybersécurité**.

Proposition n°14 : Construire un référentiel accessible aux TPE et PME pour renforcer la certification en matière de cybersécurité.

3. Sensibiliser les TPE et PME à la responsabilité en cascade

Le fait que les TPE et PME puissent constituer une porte d'entrée dans les systèmes d'information des ETI ou grandes entreprises dont elles sont sous-traitantes, doit les inciter puissamment à s'investir dans la cybersécurité.

Si elles ne le font pas, l'omission dans la mise en place de mesures de sécurité suffisantes pourrait caractériser une **faute par abstention** susceptible d'engager la **responsabilité civile** de l'entreprise ou de son dirigeant, sur le fondement de l'article 1383 du code civil, qui énonce que « *chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ». L'entreprise qui n'aura pas pris des mesures de sécurité raisonnables pour protéger son serveur contre une infection informatique virale sera de toute évidence négligente au sens de cette disposition.

Outre cette règle générale, la loi la n°2017-399 du 27 mars 2017 relative au **devoir de vigilance** des sociétés mères et des entreprises donneuses d'ordre impose aux grandes entreprises un contrôle des sous-traitants notamment en matière de cyberrisque, par l'intermédiaire du plan de vigilance. Celui-ci doit identifier les risques et prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes, résultant des activités « *des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie* »[1], la sous-traitance étant définie comme l'exercice d'une influence dominante sur une entreprise en vertu d'un contrat ou de clause statutaire.

Ainsi, les TPE et PME peuvent être la cible d'attaques par rebond et être tenues **responsables** des dommages causés à des tiers tout en étant elles-

[1] *Articles L. 225-102-4 et 5 du Code de commerce*

mêmes **victimes**, lorsque l'entreprise dont le réseau est interconnecté avec un sous-traitant afin de permettre des opérations à distance.

Peuvent être personnellement reprochés au dirigeant d'une entreprise la négligence ou l'insuffisante préparation, un manquement à l'obligation d'assurer la sécurité des données ou un défaut de notification de la violation de données aux autorités de contrôle et aux personnes concernées. Les dirigeants de TPE et PME ne peuvent souvent pas déléguer cette compétence, faute de collaborateurs disposant de l'expertise nécessaire. Leur assurance responsabilité civile peut parfois ne pas suffire.

La cybersécurité est donc aussi et de plus en plus **un risque juridique**[1].

Pour les directions juridiques des entreprises, seule la conformité juridique (74 %) dépasse désormais la cybersécurité et la confidentialité des données (46 %), suivies par l'éthique de l'entreprise, l'évaluation des risques et les fonctions liées aux affaires gouvernementales, dans l'ordre des priorités juridiques[2].

« *Cette menace devrait se traduire par un intérêt accru pour les assurances cyber et pour la responsabilité des dirigeants des entreprises visées par ce nouveau régime* » estime l'étude de janvier 2018 « Assurer le risque cyber » du Club des Juristes.

Proposition n°15 : Sensibiliser les dirigeants des PME sur leur responsabilité personnelle en cas de cyberattaque de la chaîne d'approvisionnement dont ils sont partie prenante.

4. Utiliser l'assurance pour inciter les entreprises à se cybersécuriser

Le marché de la cyberassurance n'est pour le moment pas mûr.

Jusqu'à présent, le marché de l'assurance peut répondre aux besoins des assurés sans qu'il ait besoin d'un système de co-réassurance.

Cependant, comme l'avertit la Fédération française de l'assurance : « *Lors du renouvellement des contrats des grandes entreprises au 1er janvier 2021 des problèmes de capacités ont pu apparaitre. Cela s'explique notamment par des facteurs exogènes au marché de l'assurance cyber. Après une période de 15 ans de*

---

[1] *Le CESIN avait publié en septembre 2016 un « guide de la cybersécurité pour les dirigeants d'entreprise ».*

[2] *Etude « CLO Survey » par l'Association of Corporate Counsel. « La responsabilité en matière de cybersécurité au cœur des priorités des directions juridiques », Anne Moreaux, Affiches parisiennes, 5 mai 2021.*

marché favorable aux assurés, le marché des risques d'entreprises connait depuis 18 mois un resserrement fort de ces conditions de souscription tant en termes de franchises, de capacités et de tarification. La couverture des risques cyber connait cette même évolution, d'où des difficultés de placement de cette couverture sur certains grands comptes. Des facteurs inhérents à ce marché expliquent également ce durcissement des conditions de souscription. L'accélération des attaques cyber favorisée par le confinement (télétravail, e-commerce) mais également la plus forte sensibilité au risque systémique en raison de la crise sanitaire et son impact sur les pertes d'exploitation sans dommage direct ont entrainé une revue des contrats d'assurance»[1].

Si le contrat stratégique de la filière « industries de sécurité » du 29 janvier 2020 évoque : « *une couverture assurantielle du Risque IT pour tous, qui viendrait financer les dommages et la remédiation en cas d'incident. Pour explorer cette piste, l'État pourrait réunir les assureurs pour réfléchir à la création d'un tel fonds* », **une couverture assurantielle obligatoire des entreprises concernées par une cyber-attaque serait contre-productive car elle entrainerait une déresponsabilisation des entreprises face au cyberrisque.**

Comme, on l'a vu, le niveau d'exigence en matière prévention cyber est loin d'être acquis pour de nombreuses entreprises. Rendre obligatoire une assurance entrainerait un surcoût parfois excessif pour des TPE et PME, de plus, dans un temps réduit et alors que l'exposition à des attaques n'est pas forcément élevée.

Pour la Fédération française des assureurs, une telle assurance obligatoire serait « *un carcan à la liberté contractuelle qui ne serait pas adaptée à l'hétérogénéité du cyberrisque* » et **pourrait entrainer la sortie de ce marché d'assureurs alors qu'il est nécessaire de les y maintenir, voire de les y attirer**.

L'incitation fiscale serait plus adaptée avec un mécanisme de déduction fiscale réservée aux TPE et PME pour mieux se prémunir du cyberrisque.

En janvier 2019, une enquête de la CPME ne recensait que 17 % d'entreprises de moins de 50 salariés assurées contre les attaques informatiques. La CPME souligne pourtant que l'assurance « *pourrait constituer un bon moyen de prévention si les cyberassureurs n'assuraient pas le paiement de rançongiciels dans leur cadre contractuel* »[2]. Il faut **utiliser l'outil assurantiel** pour inciter les entreprises et notamment les TPE et PME à adopter des solutions de cybersécurité, ce qui suppose de **réunir trois conditions** :

- Une meilleure compréhension du risque, donc la connaissance la plus exhaustive possible des sinistres (cf proposition n°2) ;

---

[1] *Réponse au questionnaire de la Délégation aux entreprises du 13 avril 2021.*

[2] *Réponse au questionnaire de la Délégation aux entreprises du 24 mars 2021.*

- L'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label ExpertCyber ;
- La création d'une agence de cybernotation européenne, ou française, utilisant les référentiels de l'ANSSI (ou de l'ENISA), afin de se dégager d'un marché de la notation financière américanisé.

Proposition n°16 : Affermir le marché de l'assurance en matière de cybersécurité par :

- **une meilleure compréhension du risque, en ayant la connaissance la plus exhaustive possible des sinistres ;**
- **l'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label ExpertCyber ;**
- **la création d'une agence de cybernotation européenne, utilisant les référentiels de l'Agence européenne chargée de la sécurité des réseaux et de l'information –ENISA-, ou française, utilisant ceux de l'ANSSI.**

5. Mutualiser l'expertise en cybersécurité avec des tiers de confiance

La mutualisation de l'expertise est la réponse à la **course de vitesse** engagée entre, d'une part, la croissance exponentielle des cyberattaques, et, d'autre part, la formation à la cybersécurité. L'ambition de passer de 37 000 à 75 000 emplois dans la filière dans les cinq ans pour pouvoir contrer les cybermenaces comme le développement d'une filière française de cybersécurité, une « *base industrielle et technologique de cyberdéfense* », risquent en effet de ne pas suffire.

Pour les TPE et PME, la mise en réseau des RSSI est recommandée par CCI France.

Elle l'est également par l'ANSSI, pour les communes, dans le guide que l'agence a publié récemment avec le concours de l'AMF en novembre 2020[1].

De multiples services de cybersécurité peuvent être externalisés et mutualisés, depuis l'analyse des vulnérabilités, la surveillance des menaces, la gestion et le support des équipements de sécurité et, plus récemment, les solutions d'EDR (*Endpoint Detection & Response*)[2].

---

[1] *Il recommande de : « regrouper plusieurs structures communales et/ou départementales à l'échelle d'un centre unique de ressources intitulé « Centre de ressources numériques territorial (CRNT) » participe concrètement à offrir une performance de services renforcée tout en optimisant les moyens financiers disponibles ».*

[2] *Catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information.*

Cette mutualisation peut s'opérer dans le cadre des **groupements d'employeurs,** dont la base juridique est le titre III de la loi n° 2011-893 du 28 juillet 2011 pour le développement de l'alternance et la sécurisation des parcours professionnels.

Les groupements d'employeurs prennent la forme d'une association ou d'une société coopérative qui ne poursuit aucun bénéfice commercial mais a comme objectifs, d'une part, de recruter des salariés pour les mettre à disposition des entreprises adhérentes, sans que celles-ci supportent la charge d'un emploi permanent, et d'autre part, d'apporter aide et conseils aux entreprises adhérentes en matière de gestion des ressources humaines.

Le groupement est l'employeur unique des salariés. Il s'assure du paiement des salaires et des charges. Ensuite, il re-facture la rémunération des salariés aux entreprises, majorée d'un montant destiné à couvrir ses frais de fonctionnement.

Le groupement d'entreprises bénéficie des aides publiques en matière d'emploi et de formation professionnelle dont auraient profité ses entreprises adhérentes si elles avaient embauché directement les personnes mises à leur disposition.

Une telle entité regrouperait des entreprises partageant le même « paysage numérique », c'est-à-dire dont les systèmes de sécurité informatiques sont proches.

Cependant, les données à cybersécuriser étant extrêmement confidentielles, les experts concernés devront faire preuve d'une **déontologie renforcée.** Ils pourraient avoir le **statut de tiers de confiance** afin de garantir l'interopérabilité de la cybersécurité qu'ils assurent auprès d'une entreprise avec les autres tiers de confiance numérique afin de garantir la capacité de continuité et de réversibilité de service au-delà de leur intervention.

Ces obligations juridiques pourraient être définies, au-delà de la matière fiscale[1], en associant à sa définition la Fédération nationale des tiers de confiance du numérique[1].

---

[1] *« L'article 68 de la loi n° 2010-1658 du 29 décembre 2010 de finances rectificative pour 2010 a instauré la mission de tiers de confiance. Le dispositif de tiers de confiance défini par l'article 170 ter du code général des impôts (CGI) autorise les contribuables assujettis à l'obligation de dépôt d'une déclaration annuelle de revenus (BOI-IR-DECLA), qui sollicitent le bénéfice de déductions de leur revenu global, de réductions ou de crédits d'impôts, à remettre les pièces justificatives des charges correspondantes à un tiers de confiance choisi parmi les membres des professions réglementées d'avocat, de notaire ou de l'expertise comptable et ayant signé avec l'administration fiscale une convention individuelle. La mission du tiers de confiance, ainsi que les droits et obligations de chaque partie, sont définis par un contrat ou une lettre de mission conclu entre le tiers de confiance et son client ou adhérent agissant au nom du foyer fiscal. Les conditions d'application de ce nouveau dispositif sont précisées dans le décret n° 2011-1997 du 28 décembre 2011. Le terme générique de « profession réglementée de l'expertise comptable » est utilisé pour désigner les experts-comptables, les sociétés d'expertise comptable et les associations de gestion et de comptabilité » source : site du BOFIP.*

Proposition n°17 : Faciliter la mise en réseau des responsables de sécurité des services informatiques (RSSI) pour les PME par la constitution de groupements d'employeurs, ayant un statut de tiers de confiance.

6. Simplifier l'offre destinée aux PME et TPE

Face aux cyberrisques, les entreprises ont du mal à gérer leur propre complexité et celle des solutions de cybersércurité.

Pour la complexité interne, il leur est conseillé de dresser régulièrement un inventaire de leurs systèmes en place, supprimer les outils en double et remplacer les solutions autonomes par des applications inter-systèmes afin que les équipes informatiques puissent bénéficier d'une vue d'ensemble des vulnérabilités de l'infrastructure IT leur permettant de simplifier la gestion des risques. En découle généralement une réduction des coûts, puisqu'une solution unifiée est souvent moins chère qu'un ensemble de technologies en silo dotées de fonctionnalités trop nombreuses ou redondantes. « *Pour relever ces défis, les entreprises doivent rationaliser l'administration de leurs règles de sécurité. La meilleure approche consiste à recourir à une solution de gestion centralisée des règles, capable d'offrir à l'équipe IT une parfaite visibilité et un meilleur contrôle sur l'ensemble du réseau et de lui signaler automatiquement toute infraction, allégeant considérablement sa charge de travail* », estime un expert[2].

Voici ce que recommande l'ANSSI : « *lors de la conception, les interfaces et la complexité du système devraient être limitées au maximum afin de limiter l'introduction de vulnérabilités lors de l'implémentation* »[3].

L'automatisation des réponses, notamment grâce au recours à l'IA, pour contrer les cyberattaques est la réponse à l'augmentation exponentielle de leur volume. En 2017, 11 % des entreprises subissaient plus de 100 000 alertes quotidiennes. Elles étaient 17 % en 2020.

Pour la complexité externe, si les entreprises investissent davantage dans la cybersécurité, le risque est d'acquérir un trop grand nombre d'outils, ce qui réduit l'efficacité de la sécurité de leur système d'information.

Le recours au multicloud, qui domine désormais, complique la cybersécurité car les données et applications sont désormais basées sur

---

1 *https://fntc-numerique.com/fr/accueil.html*

2 *« La complexité est l'ennemi de la sécurité. Comment les entreprises peuvent-elles continuer à moderniser leurs architectures réseau sans augmenter leur exposition aux cybermenaces ? », Erwan Jouan, Les Echos, 13 février 2018.*

3 *« La cybersécurité des systèmes industriels – mesures détaillées », janvier 2014.*

différentes plateformes, *data centers* et zones, dans un vaste choix de langues, cadres et systèmes de stockage par le biais de différentes techniques[1].

Selon une étude[2], 86 % des entreprises utilisent jusqu'à **une vingtaine de solutions de sécurité** et 20 % (+8 points depuis 2017) estiment cette multiplicité comme une grande difficulté.

Selon d'autres études, les organisations déploient en moyenne **entre 45 outils** de cybersécurité pour protéger leurs réseaux et systèmes d'information[3] **et plus de 50 solutions** (pour 78 % des entreprises), voire plus de 100 (pour 37 %)[4] !

Or, cette multiplication d'outils affaiblit la cyber-résilience. Ainsi, l'opportunité de détecter des cyberattaques baisserait de 8 %, et celle d'y répondre de 7 %, chez les organisations qui s'appuient sur plus de 50 outils, par rapport à celles qui utilisent une quantité plus modérée de solutions et services dédiés à la sécurité informatique.

Comme l'estime la Plateforme RSE dans son étude de 2020 sur la responsabilité numérique des entreprises, cette « ***dispersion des technologies n'est pas sans risque*** ». Comme 80 % des entreprises ont fait appel en 2019 à plusieurs fournisseurs de protection des données, elles « *risquent de connaitre 5 fois plus de coûts engendrés par des pertes de données, 2 fois plus de coûts engendrés par des temps d'immobilisation de leurs données et elles sont 1,7 fois plus susceptibles d'avoir des difficultés à récupérer leurs données après une cyberattaque que celles qui utilisent un seul fournisseur* ».

Un cabinet d'experts[5] prodigue certains **conseils** pour atténuer ce risque :

- *« Une entreprise de cybersécurité pourrait vous bluffer avec des termes très techniques et une campagne marketing impressionnante, mais examinez les tests indépendants ;*
- *Une entreprise qui se contente d'installer des logiciels et que vous ne revoyez plus par la suite ne répond certainement pas à vos besoins ;*
- *Une société qui prétend être spécialisée dans un domaine, sans offrir d'autres produits complémentaires ou une assistance, ne peut pas fournir la protection qui vous convient ;*

---

1 *HTTP, événements, gRPC, WebSockets…*

2 *La sixième édition annuelle du baromètre Cisco 2020 CISO Benchmark Report est basée sur une enquête menée auprès de 2 800 professionnels de la sécurité de 13 pays à travers le monde.*

3 *« Cyber Resilient Organisation Report » IBM Security et Ponemon Institute Etude conduite auprès de plus de 3400 professionnels IT et sécurité ont été interrogés par le.*

4 *Étude Oracle/KPMG « Cloud threat report 2020 » menée auprès de 750 professionnels de la cybersécurité et de l'informatique en France et dans le monde entier.*

5 *Les « Conseils de cybersécurité destinés aux petites entreprises », Kaperski.*

- *En cas de menace détectée ou de difficulté à sauvegarder vos fichiers, il faut une entreprise capable d'offrir une assistance irréprochable, qui aide à appréhender les menaces, à trouver des solutions et à simplifier la cybersécurité ;*
- *Ciblez les entreprises qui offrent une gamme complète de solutions de sécurité, notamment celles dont vous pourriez avoir besoin à l'avenir* ».

D'autres prônent une **solution globale**. Ainsi, le rapport précité de l'Institut Montaigne de novembre 2018 recommande : « *la création et à la souscription d'offres cybersécurité pour les TPE/PME/ETI, en particulier des offres de connectivité réseau intégrant par défaut des mesures de sécurité de base (nettoyage du trafic), des offres d'applications métier (ex. ERP) sécurisées par défaut et des offres de cyberassurance, incluant des services en cas d'incidents* ».

Proposition n°18 : Développer l'offre d'un « package » simplifié de solutions de cybersécurité aux TPE et PME.

7. Rétablir l'égalité des relations contractuelles dans le cloud au profit des PME

a) L'inaccessible preuve de la faute

La responsabilité pour faute est inaccessible au client d'un contrat de service de cyberprotection en ligne, qui est un contrat avec obligation de moyens, car il **ne peut rapporter la faute** du fournisseur de service de sécurité en ligne.

Pour des prestations exécutées à distance, il est impossible au client de scruter le comportement des agents du fournisseur pour s'assurer de leur diligence et de leur compétence. Les traces techniques pouvant aider à prouver la faute du fournisseur ne sont pas accessibles au client. Quand bien même elles le seraient, la technicité requise pour les expertiser est hors de portée du client. Il n'existe pas, dans le secteur informatique, de référentiels de bonnes pratiques à l'instar des documents techniques unifiés (DTU) du BTP permettant de définir des comportements professionnels-types.

Lorsque ce client est une TPE ou PME « profane », pour lequel le contrat n'entre pas dans le champ de son activité principale (par exemple un bijoutier qui achète un service de comptabilité en ligne), la mise en œuvre de cette responsabilité est impossible.

b) Des propositions multiples mais parfois peu réalistes.

Dans ce contexte, un rapport du Conseil général de l'économie, de l'industrie, de l'énergie et des technologies sur « *La responsabilité des fournisseurs de systèmes numériques* », de juin 2020, préconise d'instaurer, par la loi :

- soit des **obligations accessoires** aux contrats de service en ligne, à l'instar des 18 « *régimes spécifiques des contrats ayant un objet particulier* » que le code de commerce a institué[1],
- soit **un régime de responsabilité sans faute**, à l'instar du régime de responsabilité légale du fait des produits défectueux, des dommages causés par les fuites ou rejets d'hydrocarbures, ou des dommages causés par l'énergie nucléaire.

Il propose également :

- de **faire bénéficier les « petites entreprises » d'une protection contre les clauses abusives** dès lors que le professionnel est profane, c'est-à-dire que le contrat (de cyberprotection) n'entre pas dans le champ de son activité principale ;
- **d'exiger, dans les clauses des contrats de cybersécurité dans le cloud, l'expression « en droit local »** afin de ne pas « *introduire toute une série d'exclusions limitant sa responsabilité ou le droit à indemnisation du cocontractant, même lorsque le droit français, par exemple, interdit une telle exclusion, sans que cette rédaction soit pour autant contestable devant un tribunal* » ;
- d'imposer une **sécurité par défaut** dans la mise en œuvre de tout produit ou service numérique, afin de proposer une protection efficace et automatique « *dès la mise en marche du produit ou à la première connexion* » ;
- **d'instaurer la gratuité des mises à jour de sécurité**, même en l'absence d'abonnement aux évolutions fonctionnelles du produit ou du service numérique ;
- **d'instaurer l'obligation de fournir les mises à jour de sécurité, pendant 5, voire 10 ans après la fin de commercialisation du produit numérique.**

Afin de **ré-équilibrer les relations** entre clients (particuliers ou professionnels) et fournisseurs de services en ligne et pour une réparation plus facile des dommages rencontrés dans l'usage de ces services, **deux pistes** pourraient être envisagées :

- **instaurer par la loi des obligations accessoires** aux contrats de service en ligne et comporter un accord sur les niveaux de service (SLA) pour la disponibilité du service et le délai maximum de réponse à une sollicitation du support client. La modification substantielle d'une fonctionnalité ou sa disparition doivent être annoncées avec un délai suffisant pour permettre au client la mise en place d'une solution de contournement économiquement acceptable ;
- **instaurer une responsabilité sans faute** du fournisseur dans les contrats de service en ligne. Cette obligation pourrait n'être applicable qu'à des

[1] *Notamment les « contrats de services de communications électroniques » ou les « services accessibles par l'intermédiaire des opérateurs de communications électroniques ».*

fournisseurs présentant une surface financière suffisante et un délai de prescription (6 mois par exemple) pourrait être défini au-delà duquel la recherche de responsabilité du fournisseur n'est plus possible afin de faciliter l'assurabilité du risque.

Cependant, imposer une obligation de résultat à la fourniture d'un service de cybersécurité n'est pas réaliste. La cyberprotection absolue n'existe pas. Par ailleurs, elle peut démotiver les efforts de l'entreprise d'implanter une culture de cybersécurité et faciliter son externalisation illusoire.

c) Étendre le champ de protection du Code de la consommation

Pour la Fédération française des assurances, créer une obligation de résultat rendrait la mise en jeu de la responsabilité quasi-automatique et *« dans le contexte très spécifique des attaques malveillantes, les entreprises victimes d'une cyberattaque deviennent dès lors automatiquement responsables des conséquences dommageables de cette attaque. (…) L'avantage de l'obligation de moyens est notamment d'apprécier les mesures de prévention mises en œuvre par l'entreprise plutôt que de créer une responsabilité automatique qui in fine pourrait s'avérer plus déresponsabilisant en termes de cybersécurité. Modifier le régime de responsabilité civile aurait également pour conséquence de créer des distorsions de concurrence entre acteurs français et acteurs étrangers relevant d'une autre législation, freinant le développement de l'innovation en France »*[1].

En revanche, **comme les TPE et PME doivent être considérées comme de petits professionnels profanes dès lors que le numérique n'entre pas dans le champ de leur activité principale[2], la protection de l'article L.212-1 du Code de la consommation sur les clauses abusives[3]**

---

[1] *Réponse au questionnaire de la Délégation aux entreprises du 13 avril 2021.*

[2] *Au sens de l'article L 221-3 du code de la consommation :* « Les dispositions des sections 2, 3, 6 du présent chapitre applicables aux relations entre consommateurs et professionnels, sont étendues aux contrats conclus hors établissement entre deux professionnels dès lors que l'objet de ces contrats n'entre pas dans le champ de l'activité principale du professionnel sollicité et que le nombre de salariés employés par celui-ci est inférieur ou égal à cinq ».

[3] *« Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat.*

Sans préjudice des règles d'interprétation prévues aux articles 1188, 1189, 1191 et 1192 du code civil, le caractère abusif d'une clause s'apprécie en se référant, au moment de la conclusion du contrat, à toutes les circonstances qui entourent sa conclusion, de même qu'à toutes les autres clauses du contrat. Il s'apprécie également au regard de celles contenues dans un autre contrat lorsque les deux contrats sont juridiquement liés dans leur conclusion ou leur exécution. L'appréciation du caractère abusif des clauses au sens du premier alinéa ne porte ni sur la définition de l'objet principal du contrat ni sur l'adéquation du prix ou de la rémunération au bien vendu ou au service offert pour autant que les clauses soient rédigées de façon claire et compréhensible.

Un décret en Conseil d'État, pris après avis de la commission des clauses abusives, détermine des types de clauses qui, eu égard à la gravité des atteintes qu'elles portent à

devrait leur être accordée en matière de cybersécurité. Le seuil de cet article, fixé à cinq, pourrait être relevé afin de mieux protéger les PME.

En invoquant ce dispositif, la TPE ou PME n'aurait pas à prouver le caractère abusif de la clause litigieuse, contrairement au droit commun de l'article 1171 du code civil[1].

Cette proposition rejoint les objectifs de la directive 2018/197265 du 11 décembre 2018 établissant le code des communications électroniques européen, qui étend aux microentreprises, aux petites entreprises et aux organisations à but non lucratif le bénéfice de certaines dispositions prévues pour les consommateurs (sur les modalités de l'information contractuelle, sur la durée maximale des contrats et sur les offres groupées). Ces entités sont en effet considérées comme étant dans une situation comparable à celle des consommateurs en termes de pouvoir de négociation.

Proposition n°19 : Accorder aux TPE et PME, dont le champ de l'activité principale n'est pas le numérique, la protection de l'article L212-1 du Code de la consommation sur les clauses abusives pour les contrats conclus en matière de cybersécurité.

8. Assurer la cybersécurité à l'entrée du cloud et mieux en prendre en considération les PME dans les normes de cybersécurité du cloud

En Grande-Bretagne, Amazon Web Services (AWS) propose un dispositif qui configure l'environnement cloud aux normes de sécurité publiques.

Ce « ***Quick Start*** » configure un environnement cloud Amazon Web Services (AWS) qui se conforme aux « Principes de sécurité dans le cloud » du *National Cyber Security Centre* (NCSC) et aux contrôles de sécurité critique du *Center for Internet Security* (CIS).

---

l'équilibre du contrat, doivent être regardées, de manière irréfragable, comme abusives au sens du premier alinéa. *Un décret pris dans les mêmes conditions, détermine une liste de clauses présumées abusives ; en cas de litige concernant un contrat comportant une telle clause, le professionnel doit apporter la preuve du caractère non abusif de la clause litigieuse.*

Ces dispositions sont applicables quels que soient la forme ou le support du contrat. Il en est ainsi notamment des bons de commande, factures, bons de garantie, bordereaux ou bons de livraison, billets ou tickets, contenant des stipulations négociées librement ou non ou des références à des conditions générales préétablies ».

[1] *« Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite.*

L'appréciation du déséquilibre significatif ne porte ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation ».

Le modèle Quick Start configure automatiquement les ressources AWS et déploie une application Web multiniveau basée sur Linux. Il n'y a pas besoin, pour l'entreprise utilisatrice, d'appliquer un référentiel complexe. La matrice des contrôles de sécurité de Quick Start est complétée par un audit permanent de cybersécurité également automatisé (AWS Config).

Un tel schéma a été déployé également aux États-Unis, en Espagne, Canada, Suède, Inde, Corée du Sud et Singapour.

Lors de son audition[1], M. Julien Grouès, directeur général d'Amazon Web Services (AWS) France, a indiqué **la disponibilité de l'opérateur privé pour élaborer, avec l'ANSSI, le même dispositif en France**, lequel « *apporterait aux TPE et PME une grande facilité d'usage en les exonérant de l'obligation de s'assurer si leur entrée dans le cloud répond aux spécificités de cybersécurité publique* » Ce transfert de sécurité serait un modèle de simplicité, d'efficacité et de conjugaison intelligente du privé et du public.

Cette solution serait naturellement **appliquée à tous les fournisseurs d'offre cloud.**

Par ailleurs, une **convergence franco-allemande** pour sécuriser le cloud pourrait donner un **nouvel élan à la cybersécurisation des PME**.

Un label franco-allemand avait été lancé en 2016, *European Secure Cloud*, en coopération avec l'homologue allemand de l'ANSSI, le *Bundesamt für Sicherheit in der Informationstechnikle (BSI)*. Il est basé sur 15 règles techniques et organisationnelles communes entre SecNumCloud et le catalogue allemand **Cloud Computing Compliance Controls Catalog (C5)**[2]. Malheureusement, cette action n'a pas été suivie des effets attendus : l'ANSSI n'a certifié que trois acteurs locaux de petite taille à ce jour. Tous les acteurs concernés déplorent cette lenteur qui entrave les actions si utiles de certifications, en particulier en matière d'exportation.

Cette convergence franco-allemande sur les normes pourrait être enrichie d'une **approche commune** afin de **mieux prendre en considération les PME dans le schéma européen de certification de cybersécurité pour les services cloud** qui doit uniformiser le marché.

En effet, si le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, évoque la nécessité de : « *prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin que*

---

[1] *Audition du 15 avril 2021.*

[2] *Programme d'attestation de l'Office fédéral de la sécurité des technologies de l'information (BSI du gouvernement allemand), afin d'aider les organisations à démontrer leur sécurité opérationnelle face aux cyber-attaques courantes lorsqu'elles utilisent des services cloud dans le cadre des « recommandations de sécurité pour les fournisseurs de cloud » du gouvernement allemand.*

les réseaux et systèmes d'information, les réseaux de communication, les produits, services et appareils numériques utilisés par les citoyens, les organisations et les entreprises – depuis les petites et moyennes entreprises (PME), jusqu'aux opérateurs d'infrastructures critiques – soient mieux protégés contre les cybermenaces », il manque des mesures concrètes pour traduire cet objectif pour ce qui concerne les PME.

Proposition n°20 : Étudier la faisabilité :

- **d'une part, d'une solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI ;**
- **d'autre part, d'une approche commune franco-allemande en faveur d'une meilleure prise en considération des PME dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA.**

9. Instituer un crédit d'impôt pour inciter les entreprises à se numériser en toute sécurité

a) Une demande récurrente du Sénat

Depuis 2018, le Sénat propose de créer un dispositif d'aide massif pour aider les TPE-PME à se numériser, avec un volet de formation à la cybersécurité ou d'acquisitions de solutions de cyberprotection.

Une proposition d'un **dispositif de soutien à la modernisation numérique du commerce de détail et à la formation numérique des commerçants**, est évoquée dans le rapport d'information, fait au nom de la Délégation aux entreprises et de la Délégation aux collectivités territoriales, (n° 526 (2017-2018) de MM. Rémy Pointereau et Martial Bourquin, déposé le 30 mai 2018). Ce **crédit d'impôt** avait deux objets :

- d'abord, favoriser la formation au numérique des artisans et commerçants de détail pour faciliter leur initiation aux techniques commerciales sur internet, aux méthodes d'animation commerciale et d'accueil ;

- ensuite, leur permettre de réduire de 50 % et à hauteur de 5 000 € le coût d'équipement en appareils numériques en vue de commercialiser via le e-commerce.

Cette proposition a été traduite dans **l'article 9 de la proposition de loi sénatoriale portant Pacte national de revitalisation des centres-villes et centres-bourgs** n° 460 (2017-2018) du 20 avril 2018.

Elle a été reprise dans la **recommandation n° 5** du rapport d'information de Mme Pascale GRUNY, fait au nom de la délégation aux entreprises « *Accompagnement de la transition numérique des PME : comment la*

France peut-elle rattraper son retard ? » (n° 635 (2018-2019) - 4 juillet 2019) *:* « créer un crédit d'impôt à la formation et à l'équipement au numérique pour les artisans et commerçants de détail ».

Elle a été également reprise comme Mesure 12 du rapport de la commission des affaires économiques du Sénat sur la plan de relance (n° 535 (2019-2020) du 17 juin 2020) : « *mettre en place un « crédit d'impôt à la numérisation des PME » à destination des chefs d'entreprise et des salariés, prenant en charge notamment une partie des dépenses de formation, d'équipement, de création de site internet, de services annexes (comme en matière de cybersécurité), et articulé avec la pérennisation du suramortissement pour la numérisation des PME industrielles proposé par les pilotes de la cellule « Industrie ».*

Elle s'est traduite par un amendement[1] **au projet de loi de finances rectificative adopté par le Sénat le** 17 juillet 2020, mais rejeté par l'Assemblée nationale.

Ce crédit d'impôt aurait incité les PME à former leurs dirigeants et leur personnel à l'utilisation des outils et équipements numériques (formation au commerce électronique, à l'utilisation des biens et logiciels numériques comme les machines de production à commande numérique ou les logiciels de conception, formation à l'utilisation des équipements acquis grâce au crédit d'impôt ainsi créé).

Dans sa réponse, défavorable, le Gouvernement a prétendu que l'existence de onze opérateurs de compétences agréés (OPCO) chargés d'accompagner la formation professionnelle, de financer l'apprentissage et d'aider les branches à construire leur certification professionnelle en la matière, suffisait à satisfaire cet objectif.

Or, les PME ont besoin d'un coup de pouce individualisé.

b) Les limites des aides gouvernementales à la numérisation

Cette logique est d'ailleurs celle du Plan d'Investissement dans les Compétences qui vise à former un million de jeunes et un million de demandeurs d'emploi peu qualifiés et à accélérer la transformation de la formation professionnelle, pour un coût de de **15 milliards d'euros** entre 2018 et 2022.

Le **volet numérique** du Plan rendu public le **4 avril 2018** se fixe un objectif de **10 000 formations aux métiers du numérique** pour accélérer l'accès des jeunes et des demandeurs d'emploi « bac ou infra bac » vers les professions du secteur du numérique qui expriment de forts besoins de recrutement. Il prend la forme d'une nouvelle « aide au projet d'inclusion de compétences numériques » pour toutes les entreprises, avec une prise en charge du coût de la formation jusqu'à 8 € par heure, sous un plafond de 800 heures annuelles, et la rémunération du demandeur d'emploi.

---

[1] *n°277 rect. sexies.*

L'avis de la commission des affaires économiques du Sénat au projet de loi de finances pour 2021 (n° 139 (2020-2021) du 19 novembre 2020) souligne que l'**importance de la numérisation des PME semble enfin actée par l'exécutif,** notamment avec **l'aide forfaitaire de 500 euros**, à destination des entreprises fermées administrativement, afin de couvrir une partie des coûts liés au lancement d'une activité en ligne.

Or, cette dernière a **une portée limitée** :

- son périmètre est circonscrit aux entreprises contraintes administrativement de fermer et n'ayant aucune présence sur internet (sans que ne soient indiqués les critères pour qualifier cet aspect) soit seulement 120 000 entreprises, dans l'hypothèse où l'enveloppe est entièrement consommée, pourront en bénéficier, sur 3 millions de PME ;
- il s'agit d'une aide financée par un redéploiement ponctuel de crédits depuis le Fonds de solidarité, crédits qui devraient ensuite être reversés vers le Fonds en 2021. Il ne s'agit donc pas d'une ouverture nette de crédits, mais d'une baisse temporaire des fonds dédiés à la compensation de perte d'activité ;
- enfin, elle ne concerne pas la participation des entreprises à la formation au numérique des salariés, qui devrait pourtant être reconnue comme une contribution à une mission d'intérêt général.

Un amendement au projet de loi de finances pour 2021[1], avait donc été présenté, le 3 décembre 2020, par M. Serge Babary, au nom de la commission des affaires économiques, reprenant la proposition sénatoriale de crédit d'impôt. Il n'a pas été retenu.

c) Créer un crédit d'impôt « cybersécurité » pour les TPE et PME

La sensibilisation, les diagnostics de numérisation, et la formation-accompagnement sous forme de « conseils » ne saurait suffire. En effet, au-delà des problématiques de formation ou de diagnostic, le **coût financier** que représente le virage numérique, surtout pour les plus petites entreprises, est un frein majeur à leur numérisation. Ce coût est d'autant plus rédhibitoire **que les PME devront également, à la sortie du confinement, affronter d'autres dépenses**, comme consacrer leur trésorerie à la reconstitution de leurs stocks.

Le risque est donc réel que les PME aient une bonne connaissance de leurs insuffisances numériques, grâce aux diagnostics, tout en ne disposant pas des moyens financiers d'y remédier.

Ce volet financier de la numérisation des PME reste un angle mort de cette politique publique, alors même qu'il est le plus attendu.

---

[1] *N° II-606 rectifié (portant article additionnel après l'article 42).*

En outre, la multiplication des outils (diagnostics, formations individuelles ou collectives, conseils, chèque numérique) et des acteurs (site du ministère, réseaux consulaires, régions et communes, entreprises privées, France Num, plateformes locales), créé un fort **besoin de simplicité et de clarté** exprimé par les entrepreneurs. Un dispositif fiscal simple, à leur main, aiderait à réellement faire « décoller » la politique de numérisation.

La politique des « petits pas » en la matière ne saurait suffire, tant le retard accumulé est important. Il faut **changer de braquet** et permettre un **choc d'offre de formation au numérique**.

Ainsi, lors de la présentation du contrat stratégique de la filière « industries de sécurité » en février 2020, il était proposé que l'État s'engage à « *inciter à un renforcement des dispositifs de financement de la cybersécurité* ».

L'État ne peut à la fois enjoindre aux TPE et PME de se numériser et ne pas leur donner les moyens financiers d'y procéder en toute sécurité.

Proposition n°21 : Mettre en place un crédit d'impôt à destination des TPE et PME, prenant en charge une partie des dépenses d'équipement et de formation des chefs d'entreprise et des salariés à la cybersécurité.

10. Créer un « cyberscore » de la cybersécurité des solutions numériques

Dans sa séance du **22 octobre 2020**, le Sénat a adopté, à l'unanimité des présents, une **proposition de loi** pour la **mise en place d'une certification du niveau de cybersécurité des plateformes numériques destinées au grand public**, présentée par M. Laurent Lafon et plusieurs de ses collègues du groupe Union centriste.

Le Gouvernement a partagé cet objectif. Il a toutefois présenté des aménagements sur la mécanique du diagnostic qui « *ne peut reposer que sur l'entreprise elle-même, car les plateformes changent très souvent d'algorithmes, à un rythme souvent hebdomadaire, de sorte qu'un système d'audit ou de diagnostic par un tiers serait inopérant en pratique. Par conséquent, les opérateurs doivent être considérés comme responsables des informations qu'ils affichent et s'assurer qu'elles restent exactes à chaque mise à jour de leur logiciel* ».

Les ajouts proposés par le Gouvernement ont concerné également le champ d'application du dispositif, afin de le restreindre, dans un premier temps, aux plateformes de taille mondiale, « *soit les acteurs auprès desquels il est le plus important d'intervenir* ».

Enfin, le Gouvernement ne s'est pas montré favorable à la modification du code de la commande publique pour préciser que la nature et l'étendue des besoins à satisfaire par un marché public sont déterminés en

prenant en compte « *les impératifs de cybersécurité* »[1]. En effet, à la différence d'un critère comme celui du développement durable, qui est susceptible de concerner tous les marchés, le critère de la cybersécurité ne saurait porter que sur les achats de prestations informatiques. Le Gouvernement a considéré que : « *le principe fondamental d'égalité devant la commande publique, qui impose de ne formuler d'exigence en termes d'expression des besoins, de critères de choix et de clauses d'exécution qu'en lien avec l'objet du marché, serait totalement bafoué* », et le Sénat a souscrit à cette analyse.

Pour certains députés[2], cette initiative sénatoriale « *contribuerait à combler ce déficit de connaissance et à donner l'opportunité aux utilisateurs de faire un choix éclairé* » bien qu'un « *prérequis indispensable* » doive être mis en œuvre : « *une vaste campagne de sensibilisation permettant à tous nos concitoyens d'être pleinement conscients que les choix qu'ils font en matière de services numériques ont des conséquences pour eux-mêmes et pour la société en général, sur nos emplois, notre recherche, notre indépendance, nos valeurs, nos communications, en un mot sur notre monde de demain, en France et en Europe... Nous, acteurs du numérique, appelons à lancer dans les meilleurs délais – en partenariat avec l'État et les régions – une vaste campagne de sensibilisation pour que chacun privilégie dès à présent les applications et services numériques de confiance, protecteurs de nos données* ».

Ainsi, et même limitée aux plateformes numériques destinées au grand public, ce qui confèrerait une large audience, cette disposition doit permettre une sensibilisation du grand public à la cybersécurité, dont les entreprises pourraient indirectement profiter.

Proposition n°22 : Afin de sensibiliser les citoyens à la cybersécurité, instaurer un « cyberscore » des plateformes numériques destinées au grand public.

---

[1] *La commission des affaires économiques du Sénat avait émis, dans son rapport (n° 38 (2020-2021) de Mme Anne-Catherine Loisier, déposé le 13 octobre 2020)* « des réserves sur l'opportunité d'une telle insertion », *mais la commission avait* « adopté cet article sans modification en raison de l'accord entre groupes politiques relatif à l'examen des propositions de loi ».

[2] *« Dans la crise actuelle, les acteurs publics doivent encourager les citoyens à opter pour les solutions numériques souveraines ! » Chronique signée par Thomas Fauré, président de Whaller, Philippe Latombe, député de Vendée, Jean-Michel Mis, député de la Loire et membre du Conseil national du numérique, Philippe Lenoir et Pascal Voyat, cofondateurs de Mailo, Journal du Net, 10 mars 2021.*

EXAMEN EN DÉLÉGATION

La Délégation aux entreprises s'est réunie le jeudi 10 juin 2021 pour l'examen du présent rapport. À l'issue de la présentation, le débat suivant s'est engagé :

« ***M. Serge Babary, président***. – *Je remercie les rapporteurs pour ce remarquable travail, très dense et précis. Je signale la présence, dans les départements, de cybergendarmes qui seront des référents numériques dans les gendarmeries. J'ouvre le débat sur vos conclusions.*

M. Christian Klinger. – *La cybercriminalité est un phénomène nouveau et récent, notamment le rançonnage, et les forces de police et de justice manquent de moyens adéquats pour l'affronter. Il faut en priorité y affecter des ressources humaines. La coopération européenne ne doit-elle pas s'élargir à international ? Nous sommes en effet confrontés à une cybercriminalité sinon d'État du moins encouragée par certains d'entre eux, qui favorisent avec bienveillance un cyberespionnage à des fins industrielles et commerciales ? Autre question, la technologie de l'ordinateur quantique sera-t-elle plus protectrice ?*

M. Sébastien Meurant. – *Le phénomène est récent mais s'accélère. Il faut en effet renforcer le pôle cyber du Parquet de Paris, qui a une compétence nationale mais comprend seulement trois magistrats. La prise de conscience de la dimension et de la spécificité de la cybercriminalité existe au niveau national des forces de sécurité, que ce soit la police ou la gendarmerie. Sur le terrain, dans nos territoires, la situation est plus contrastée. Les dispositifs de cyberprotection des entreprises ne sont pas suffisamment connus. Il existe des formations des forces de sécurité mais pas de « ruissellement » pour apporter des réponses adéquates. Nous avons pu visiter le C3N, centre de lutte contre les criminalités numériques, service à compétence judiciaire nationale, qui regroupe l'ensemble des unités du pôle judiciaire de la Gendarmerie nationale traitant directement de questions en rapport avec la criminalité et les analyses numériques. Il jouit du savoir-faire militaire de la gendarmerie et s'occupe de la sécurité nationale. La coopération internationale, européenne et américaine, est en effet nécessaire car le cybercrime n'a pas de frontière. Il est particulièrement difficile d'apporter la preuve numérique et d'agir sur des ordinateurs infectés par des réseaux criminels situés à l'étranger, sans l'accord de l'entreprise concernée ou la coopération de l'État dans lequel ils se situent. Nous ne sommes pas naïfs et savons que certains de ces réseaux sont soutenus par certains États malveillants, pour des motifs géopolitiques.*

Quant à l'ordinateur quantique, c'est une version moderne de la course entre le bouclier et l'épée. Il devrait permettre une meilleure cyberprotection, mais cette technologie peut aussi être utilisée par les cybercriminels pour démultiplier leurs forfaits. C'est une course et la protection doit être en avance.

M. Rémi Cardon. – *Le déploiement dans les régions d'équipes de réponse aux incidents informatiques, après l'inauguration du Cybercampus, doit faciliter l'accès des PME à la cyberprotection tout en sensibilisant les collectivités locales.*

On a constaté une forte augmentation de la fréquentation du site cybermalveillance.gouv.fr, mais sans une croissance corrélative des dépôts de plaintes car les acteurs de la cybersécurité publique ne sont pas suffisamment connus. Il faut une montée en compétence des forces de cybersécurité afin de recevoir, orienter et traiter correctement les plaintes selon les catégories de logiciels à l'origine de la cyberattaque. Le temps de l'appropriation de cette compétence est cependant long.

Mme Annick Billon. – *Tous les territoires sont concernés par la cybercriminalité. En Vendée, l'entreprise PRB, de production de revêtements de façade pour le bâtiment, a été victime d'un rançongiciel la semaine dernière. Cette entreprise, connue pour être un des sponsors de bateaux du Vendée Globe, a renvoyé ses 650 salariés chez eux le temps des réparations informatiques. Je suis donc persuadée que les propositions de la Délégation aux entreprises vont rencontrer un grand écho partout en France métropolitaine et en outre-mer ! Un parquet national spécialisé a été créé : la cybercriminalité pourrait-elle être également traitée par un parquet européen ? Quelle est la position des assurances sur le risque de 700 milliards d'euros ? Le Cybercampus de la Défense est-il suffisant compte-tenu du fait que 43 % des PME ont été victimes. Une déclinaison territoriale n'est-elle pas nécessaire ?*

M. Rémi Cardon. – *Un parquet européen serait à la fois pertinent et complexe à mettre en place tant les stratégies des États sont différentes. Il permettrait cependant de mettre de la cohérence et de la performance dans la réponse pénale à la cybercriminalité, comme l'a indiqué le directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).*

Pour les assureurs, le risque cyber est un nouveau marché prometteur compte-tenu de la saturation des autres risques. Nous présentons une proposition forte, interdire le caractère assurable des cyberrançons, sans interdire toutefois leur paiement lorsque des emplois et des vies humaines sont menacées, notamment dans le domaine de la santé et des cliniques privées. Il faut un message fort et politique. Les cybercriminels procèdent à des études de marché de leurs victimes et dressent des bilans financiers.

L'ouverture du Cybercampus permettra de fédérer les forces publiques et privées de lutte contre la cybercriminalité mais le déploiement régional des équipes de réponse permet d'apporter une réponse de proximité aux entreprises. L'articulation entre ces deux niveaux est encore floue et la coordination devra se préciser. Nous devrons faire le point à l'automne lorsque le Cybercampus sera opérationnel. Les sénateurs ont une responsabilité pour sensibiliser les territoires sur ce sujet.

M. Sébastien Meurant. – *Il existe une très bonne coopération internationale, y compris avec l'Afrique. Les institutions judiciaires proposent des solutions rapides et nationales car il faut apporter une réponse efficace. Localement, il faut une maturité qui n'est pas encore présente.*

Le modèle du cybercampus est Israël et, dans une moindre mesure, les États-Unis. Il associe grandes entreprises et start-up, avec un ticket d'entrée de

l'ordre de 10 000 euros. Il créé une émulation vertueuse, pour faire grandir les start-up en licornes. Une déclinaison territoriale régionale est nécessaire, de même qu'une formation minimale de toutes les forces de sécurité qui doivent être déployés dans les territoires.

S'agissant des assureurs, ils sont divisés. C'est un nouveau marché aux États-Unis. Pour certains, le cyberrisque est un nouveau marché, mais le risque reste mal connu des actuaires. Sur le caractère assurable des rançongiciels, nous avons auditionné le Haut comité juridique de la place financière de Paris qui a été missionné en début d'année par la direction générale du Trésor pour apporter des recommandations à ce sujet. Il devrait rendre ses conclusions le 29 septembre 2021. Il a été très prudent. Par ailleurs, si des cyberattaques se déploient pendant un conflit, si un État est le cyberattaquant, l'État sera-t-il assureur en dernier recours ? Il existe encore beaucoup d'interrogations, car le sujet reste encore nouveau.

Enfin, la coopération internationale se fonde sur la convention de Budapest sur la lutte contre la cybercriminalité, à laquelle les États-Unis sont partie. Elle date de 2001, alors que le premier virus informatique est apparu en 1989. S'agissant du parquet européen, il ne fonctionne que depuis début novembre 2020. Il doit donc monter en puissance avant que ses compétences ne soient étendues à d'autres sujets que les infractions pénales portant atteinte aux intérêts financiers de l'Union européenne.

***M. Martin Lévrier**. – Comme pour la pandémie que nous venons de traverser, le meilleur des remèdes à la cybercriminalité est la prévention et donc l'hygiène numérique. Ne faudrait-il pas une incitation fiscale à la formation à la cybersécurité des entreprises ?*

***M. Rémi Cardon**. – Cette prévention doit commencer dès le plus jeune âge et l'Éducation nationale doit mobiliser ses ressources humaines pour former au numérique et à la dimension de la cybersécurité, car il faut apprendre à vivre avec internet. Or, les entreprises manquent de compétences. La filière doit se développer aussi dans l'enseignement supérieur.*

La prise de conscience des entreprises est parfois tardive. Elles ont également besoin d'auditer leurs outils informatiques afin de repérer les failles. Nous proposons un crédit d'impôt afin de prendre ceci en charge.

Les centres régionaux de réponse informatique conduiront sans doute les régions à s'impliquer davantage dans ce domaine, qui aurait pu être un enjeu des élections régionales !

***M. Sébastien Meurant**. – La question n'est pas de savoir si une entreprise va être cyberattaquée mais quand. L'hygiène numérique est davantage une question comportementale qu'un sujet financier, et la cybersécurité est à la fois collective et individuelle. Nous proposons cependant, et à nouveau, un crédit d'impôt pour inciter les entreprises à renforcer leurs outils de cybersécurité ainsi qu'un cyberscore des plateformes numériques destinées au grand public, comme le Sénat l'a voté en octobre 2020, pour sensibiliser tous les citoyens qui doivent l'être, dès l'école, notamment avec le cyberharcèlement. La cybersécurité nous concerne tous, les sénateurs y compris : regardons comment nous gérons nos mots de passe !*

***Martine Berthet**. – Plusieurs questions déjà posées ont évoqué les sujets que je voulais aborder. La cybersécurité peut menacer des vies lorsqu'elle s'attaque aux hôpitaux comme, récemment, celui d'Albertville, voire perturber les systèmes de déclenchement des avalanches. Ce sujet est d'une grande ampleur, et le chiffre que vous avez cité, la cybercriminalité étant au niveau de la troisième économie mondiale après les États-Unis et la Chine, impressionne.*

Vous avez évoqué les métiers de la cybersécurité. Sont-ils réservés à des formations de niveau bac +2, rapides à obtenir ? Comment intéresser les jeunes et quelles sont les filières ?

***M. Rémi Cardon**. – Il existe en effet une pénurie d'ingénieurs, citée à chaque audition. L'enseignement supérieur doit se mobiliser pour accroître l'offre de formation pour cette filière essentielle. Mais la culture de cybersécurité des étudiants des grandes écoles, en dehors des filières informatiques, doit également se renforcer. Les métiers de la cybersécurité recrutent des profils très divers, très loin du stéréotype du jeune « geek » à capuche ! Ces derniers peuvent d'ailleurs trouver un débouché professionnel à leur passion.*

***M. Sébastien Meurant**. – Cette pénurie est mondiale, ce qui explique les difficultés de recrutement, d'autant que les salaires sont plus attractifs aux États-Unis. Ceci pose la question de la rémunération des experts contractuels des forces de cybersécurité, qui demeurent dans nos forces de police car ils n'ont pas que des motivations financières. Les formations en bac +2 offrent des débouchés mais manquent de demandes. Il s'agit de métiers d'avenir, bien rémunérés, qui ont du sens, sont accessibles dès le niveau bac et pas seulement à une élite mathématique, et qui doivent être davantage féminisés. Il faut décentraliser la cybersécurité dans les territoires pour renforcer l'attraction de ces métiers.*

***M. Daniel Salmon**. – La question de la cybersécurité des hôpitaux publics pose la question de la vulnérabilité de notre société comme de l'insuffisance des moyens de l'hôpital. Elle souligne la nécessité de la sauvegarde manuelle et, plus généralement, de la capacité humaine à gérer ces cyberattaques pour garantir la résilience de ces entités.*

***M. Sébastien Meurant**. – La liste des hôpitaux cyberattaqués est impressionnante. La réaction de l'AP-HP a été rapide, grâce à la capacité de garder, dans la mémoire humaine des médecins, les patients soignés pour des infections de longue durée.*

Mais ces attaques soulignent la nécessité de renforcer la sécurité du cloud car on ne peut pas aller en arrière. La numérisation de la santé est un processus irréversible et présente des avantages. On opère avec des robots, on effectue des imageries par résonance magnétique (IRM) qui sont des process numérisés et dématérialisés. Il faut des procédures de sauvegarde solides car les cyberattaques posent des questions de vie ou de mort comme on l'a vu avec la panne d'Orange, qui a affecté les numéros téléphoniques d'urgence.

Comme vient de le souligner M. Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui publie ce matin son rapport annuel, les cybercriminels ont compris que les attaques contre des

hôpitaux publics étaient vaines car ils ne peuvent pas payer de rançons et l'ANSSI s'attend à voir le nombre de cyberattaques diminuer.

***M. Rémi Cardon**. – Les cliniques privées sont dans une situation différente. Elles sont des cibles de choix, les cybercriminels calculant leurs demandes de rançons en fonction de leur bilan financier. Lorsqu'elles sont cyberattaquées, leur résilience dépend de leur rapidité de réaction et de sauvegarde et récupération des données. À cet égard, il faudra s'interroger à l'avenir sur le niveau de protection de Health Data Hub, hébergé chez Microsoft.*

***M. Serge Babary, président**. – Je vous remercie pour ces précisions et soumets les conclusions du rapport à votre approbation. Ne relevant aucune opposition, je constate que le rapport est approuvé à l'unanimité par la Délégation aux entreprises.* »

GLOSSAIRE

APT (Advanced Persistent Threats)	Type de piratage informatique furtif et continu ciblant une entité spécifique, généralement une organisation pour des motifs d'affaires ou un État pour des motifs politiques ;
Big Data	Désigne les ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour générer de la valeur, et qui dépassent en général les capacités d'une seule et unique machine ;
BlockChain	La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ;
Botnet	Réseau de programmes informatiques connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches ;
BtoB (Business to Business)	Ensemble des activités commerciales nouées entre deux entreprises ;
Cloud	Processus consistant à utiliser des serveurs informatiques distants au travers des réseaux internet ;
Crime-as-a-service (CaaS)	« Kits » et autres services packagés développés par un criminel professionnel ou un groupe de criminels qui sont ensuite proposés à la vente ou à la location à d'autres criminels, généralement moins expérimentés ;
Darknet	Partie du réseau Internet accessible seulement par des logiciels qui anonymisent les données des utilisateurs ;

DSI	Directeur (ou direction) des services informatiques ;
GAFAM	Acronyme des principales entreprises du web : Google, Apple, Facebook, Amazon et Microsoft ;
GIP-ACYMA	Groupement d'Intérêt Public « Action contre la Cybermalveillance » ;
Hacker	Utilisateur d'un ordinateur ou d'un réseau qui recherche les moyens d'en contourner les protections logicielles et matérielles par jeu, sans intention de nuire, contrairement à un « pirate informatique » ;
Hardware	Éléments matériels d'un système informatique ;
HTML	Langage informatique utilisé pour la création de pages web, permettant notamment de définir des liens hypertextes ;
IA	L'Intelligence Artificielle est « l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence humaine ». Elle correspond donc à un ensemble de concepts et de technologies plus qu'à une discipline autonome constituée ;
IaaS (Infrastructure as a Service)	Forme de Cloud qui offre des ressources informatiques au sein d'un environnement virtualisé par le biais d'internet ou d'une autre connexion ;
Logiciels EDR	Logiciel qui se fonde sur une technologie émergente de détection des menaces sur les « EndPoints » (ordinateurs, serveurs) ;

Malware	Logiciel malveillant développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté ;
Phishing	Pratique qui consiste à récupérer des informations personnelles d'un internaute. Le terme est la contraction des mots anglais *fishing* pour pêche et *phreaking* pour le piratage de lignes téléphoniques ;
Proxy	Serveur relais qui, sur Internet, stocke les données en vue de faciliter leur accès ;
Ransomware	Logiciel malveillant de rançon qui prend en otage des données personnelles ;
RSSI	Responsable de la sécurité des systèmes d'information ;
SaaS (Software as a Service)	Modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur ;
Sécurité « by design » ou « Security by design »	Système de sécurité directement intégré dans le code source d'une application ou d'un site web ;
Shadow IT	Terme qui désigne les systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information ;
Software	Logiciel ;
Spam	Envoi répété d'un message électronique, souvent publicitaire, à un grand nombre d'internautes sans leur consentement ;

Supply Chain	Chaîne d'approvisionnement ;
URL	Adresse d'un site ou d'une page sur Internet ;
VPN	Un réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics ;
Zero Trust	Modèle de sécurité informatique qui repose sur le principe qu'aucun utilisateur n'est totalement digne de confiance sur un réseau.

ANNEXES

Annexe 1 L'exemple des recommandations de cybersécurité du réseau des CCI, septembre 2020

Annexe 2 L'avis sur « les risques potentiels de sanctions pour faciliter les paiements de rançongiciel » du Département du Trésor des États-Unis, octobre 2020

Annexe 3 La résolution européenne du Sénat sur la lutte contre la cybercriminalité du 14 août 2020

Annexe 4 L'écosystème du cybercrime
« Cybercrime : plongée dans l'écosystème », Gérôme Billois, Marwan Lahoud, Blog de l'Institut Montaigne, 15 mars 2021.

Annexe 5 Le premier échec d'un cloud public souverain français 2010-2019

Annexe 6 Les errements d'une stratégie publique du cloud

ANNEXE 1

L'EXEMPLE DES RECOMMANDATIONS DE CYBERSÉCURITÉ DU RÉSEAU DES CCI

SEPTEMBRE 2020

1) À destination des dirigeants de TPE :

1. Rendre la thématique cyber et ses enjeux accessibles et intelligibles aux TPE
2. Activer le levier de la cyberassurance pour faire entrer les TPE dans une prise de conscience
3. Guider les dirigeants de TPE par des rencontres « one-to-one » (avec des conseillers CCI par exemple)
4. Concevoir et proposer des diagnostics TPE de cyberrésilience et des tests d'intrusion (en lien avec l'ANSSI et la Gendarmerie nationale)
5. S'appuyer sur les écosystèmes locaux d'échanges entre entreprises (type Plato) pour accompagner les TPE dans la sensibilisation et la protection des systèmes d'information et des interconnections

2) À destination des PME/ETI :

1. Inciter les entreprises à pratiquer des tests d'intrusion, des diagnostics et des crash-tests pour devenir résilients face au risque cyber (tout comme on réalise des tests de sécurité incendie)
2. Organiser une prise en main de la problématique cyber par palier : prise de conscience (coaching) pour le dirigeant, entraînement (training) pour l'adjoint direct en charge du risque cyber (DRH, DAF, etc.) et formation pour les salariés de l'entreprise selon la taille de celle-ci
3. Activer le levier de la certification et de l'audit pour faire entrer les PME dans un degré de conscience cyber plus élevé
4. Inciter les entreprises à réviser leurs contrats d'assurance pour y inclure le risque cyber ou en vérifier la clause (soutenir la démarche de l'Autorité de contrôle prudentiel et de résolution - ACPR) dans sa proposition de clarification de la position des compagnies d'assurance et de redescendre tous leurs contrats sur des bases de couverture du risque cyber)
5. Faire une large campagne sur la mise à niveau des standards (obligations réglementaires) et des outils (mises à jour logicielles et configuration) de cybersécurité ; les normes et certifications peuvent être obligatoires mais donnent surtout accès à des marchés pour la plupart des ETI
6. Faciliter la mise en réseau des RSSI pour les PME par la conclusion de partenariats de mutualisation des ressources et d'informations afin de pallier la pénurie de talents : la lutte contre des cybermenaces sophistiquées nécessite, d'abord et avant tout, des processus matures et des professionnels de la sécurité efficaces et dédiés 24h/24, 7j/7

7. Mutualiser les expériences d'entreprises en matière de cyberrésilience et changer la culture du secret qui entoure l'attaque cyber (qu'elle ait ou non aboutie)
8. Fédérer des écosystèmes d'échange d'expérience à l'échelle industrielle (sur le modèle du Cluster Security Valley)

Source : « Pérenniser l'entreprise face au risque cyber – De la cybersécurité à la cyberrésilience », CCI France, septembre 2020

ANNEXE 2

L'AVIS SUR « LES RISQUES POTENTIELS DE SANCTIONS POUR FACILITER LES PAIEMENTS DE RANÇONGICIEL » DU DÉPARTEMENT DU TRÉSOR DES ÉTATS-UNIS[1]

1ER OCTOBRE 2020

L'Office of Foreign Assets Control (OFAC) du Département américain du Trésor publie cet avis pour mettre en évidence les risques de sanctions associés aux paiements de rançongiciel liés aux activités malveillantes activées par le cyberespace. La demande de paiements de rançongiciel a augmenté pendant la pandémie de COVID-19, car les cyberacteurs ciblent les systèmes en ligne sur lesquels les Américains comptent pour continuer à faire des affaires. Les entreprises qui facilitent les paiements de rançongiciel aux cyberacteurs au nom des victimes, y compris les institutions financières, les sociétés de cyber-assurance et les entreprises impliquées dans la criminalistique numérique et la réponse aux incidents, encouragent non seulement les futures demandes de paiement de rançongiciel, mais peuvent également risquer de violer les réglementations de l'OFAC. Cet avis décrit ces risques de sanctions et fournit des informations pour contacter les agences gouvernementales américaines compétentes, y compris l'OFAC, s'il y a une raison de croire que le cyber-acteur exigeant le paiement d'un rançongiciel peut être sanctionné ou avoir un lien de sanctions.

Contexte des attaques de rançongiciel

Le rançongiciel est une forme de logiciel malveillant (« malware ») conçu pour bloquer l'accès à un système informatique ou à des données, souvent en chiffrant des données ou des programmes sur des systèmes informatiques pour extorquer des paiements de rançon aux victimes en échange du déchiffrement des informations et restaurer l'accès des victimes à leurs systèmes ou données. Dans certains cas, en plus de l'attaque, les cyberacteurs menacent de divulguer publiquement les fichiers sensibles des victimes. Les cyberacteurs exigent alors un paiement de rançongiciel, généralement via une monnaie numérique, en échange d'une clé pour décrypter les fichiers et restaurer l'accès des victimes aux systèmes ou aux données. Ces dernières années, les attaques de rançongiciel sont devenues plus ciblées, sophistiquées, coûteuses et nombreuses. Selon les rapports sur la criminalité Internet 2018 et 2019 du Federal Bureau of Investigation, il y a eu une augmentation annuelle de 37% des cas de rançongiciel signalés et une augmentation annuelle de 147% des pertes associées de 2018 à 2019. Alors que les attaques de rançongiciel sont menées contre de grandes entreprises, de nombreux rançongiciel les attaques ciblent également les petites et moyennes entreprises,

[1] *« Cet avis est purement explicatif et n'a pas force de loi. Il ne modifie pas les autorités statutaires, les décrets ou les règlements. Il n'est pas destiné à être, ni ne doit être interprété comme, complet ou comme imposant des exigences en vertu de la loi américaine, ou traitant d'une autre manière des exigences particulières en vertu de la loi applicable. L'avis invite à consulter les dispositions juridiquement contraignantes citées pour les autorités judiciaires compétentes. Cet avis se limite aux risques de sanctions liés aux ransomwares et ne vise pas à aborder plus largement les problèmes liés aux efforts de collecte de renseignements sur les cybermenaces des praticiens de la sécurité de l'information ».*

agences gouvernementales locales, hôpitaux et districts scolaires, qui peuvent être plus vulnérables car ils peuvent avoir moins de ressources pour investir dans la cybersécurité (…).

Les paiements de rançongiciel avec un lien de sanctions menacent les intérêts de sécurité nationale des États-Unis

Faciliter un paiement de rançongiciel qui est exigé à la suite d'activités cybernétiques malveillantes peut permettre aux criminels et aux adversaires ayant un lien de sanctions de profiter et de faire progresser leurs objectifs illicites. Par exemple, les paiements de rançongiciel versés à des personnes sanctionnées ou à des juridictions sanctionnées de manière globale pourraient être utilisés pour financer des activités contraires aux objectifs de sécurité nationale et de politique étrangère des États-Unis. Les paiements de rançongiciel peuvent également encourager les cyberacteurs à se livrer à de futures attaques. De plus, payer une rançon aux cyber-acteurs ne garantit pas que la victime retrouvera l'accès à ses données volées.

Faciliter les paiements de ransomware pour le compte d'une victime peut enfreindre les règlements de l'OFAC

Sous l'autorité de l'International Emergency Economic Powers Act (IEEPA) ou du Trading with the Enemy Act (TWEA), les ressortissants américains sont généralement interdits de s'engager dans des transactions, directement ou indirectement , avec des individus ou entités (« personnes ») figurant sur la liste des ressortissants spécialement désignés et des personnes bloquées (liste SDN) de l'OFAC, d'autres personnes bloquées et celles couvertes par des embargos de pays ou de région (par exemple, Cuba, la région de Crimée en Ukraine, Iran, Corée du Nord et Syrie). De plus, toute transaction qui entraîne une violation de l'IEEEPA, y compris les transactions par une personne non américaine qui amène une personne américaine à violer les sanctions fondées sur l'IEEEPA, est également interdite. Il est également généralement interdit aux personnes américaines, où qu'elles se trouvent, de faciliter les actions de personnes non américaines, qui ne pourraient pas être effectuées directement par des personnes américaines en raison de la réglementation des sanctions américaines. L'OFAC peut imposer des sanctions civiles pour les violations de sanctions fondées sur la responsabilité stricte, ce qui signifie qu'une personne soumise à la juridiction américaine peut être tenue civilement responsable même si elle ne savait pas ou avait des raisons de savoir qu'elle s'engageait dans une transaction avec une personne qui est interdite en vertu les lois et règlements relatifs aux sanctions administrés par l'OFAC.

Les Directives d'application des sanctions économiques de l'OFAC (Directives d'application) fournissent plus d'informations sur l'application par l'OFAC des sanctions économiques américaines, y compris les facteurs que l'OFAC prend généralement en compte pour déterminer une réponse appropriée à une violation apparente. En vertu des Directives d'application, en cas de violation apparente des lois ou réglementations américaines sur les sanctions, l'existence, la nature et l'adéquation d'un programme de conformité aux sanctions est un facteur que l'OFAC peut prendre en compte pour déterminer une réponse d'application appropriée (y compris le montant des sanctions civiles, sanction pécuniaire, le cas

échéant).

De manière générale, l'OFAC encourage les institutions financières et autres entreprises à mettre en œuvre un programme de conformité basé sur les risques pour atténuer l'exposition aux violations liées aux sanctions. Cela s'applique également aux entreprises qui interagissent avec des victimes d'attaques de rançongiciel, telles que celles impliquées dans la fourniture de services informatiques, d'assurance, criminalistique numérique et réponse aux incidents, et services financiers pouvant impliquer le traitement des paiements de rançon (y compris les institutions de dépôt et les services monétaires). En particulier, les programmes de conformité aux sanctions de ces entreprises devraient tenir compte du risque qu'un paiement de rançongiciel puisse impliquer un SDN ou une personne bloquée, ou une juridiction totalement sous embargo. Les entreprises impliquées dans la facilitation des paiements de rançongiciel au nom des victimes devraient également se demander si elles ont des obligations réglementaires en vertu des règlements du Financial Crimes Enforcement Network (FinCEN).

En vertu des directives d'application de l'OFAC, l'OFAC considérera également le rapport complet d'une entreprise sur une attaque de rançongiciel à l'intention des forces de l'ordre comme un facteur atténuant important pour déterminer un résultat d'application approprié si la situation est ultérieurement déterminée à avoir un lien de sanctions. L'OFAC considérera également la coopération complète et opportune d'une entreprise avec les forces de l'ordre pendant et après une attaque de rançongiciel comme un facteur atténuant important lors de l'évaluation d'un éventuel résultat d'application de la loi.

Politique de licence de l'OFAC

Les paiements de rançongiciel profitent aux acteurs illicites et peuvent saper les objectifs de sécurité nationale et de politique étrangère des États-Unis. Pour cette raison, les demandes de licence impliquant des paiements de rançongiciel exigés à la suite d'activités malveillantes activées par le cyberespace seront examinées par l'OFAC au cas par cas avec une présomption de refus.

Les victimes d'attaques par rançongiciel doivent contacter les agences gouvernementales compétentes

L'OFAC encourage les victimes et les personnes impliquées dans la lutte contre les attaques de rançongiciel à contacter immédiatement l'OFAC si elles estiment qu'une demande de paiement par rançongiciel peut impliquer un risque de sanctions. Les victimes doivent également contacter le Bureau de la cybersécurité et de la protection des infrastructures critiques du Département du Trésor des États-Unis si une attaque implique une institution financière américaine ou risque de perturber considérablement la capacité d'une entreprise à fournir des services financiers critiques.

ANNEXE 3

LA RÉSOLUTION EUROPÉENNE DU SÉNAT SUR LA LUTTE CONTRE LA CYBERCRIMINALITÉ DU 14 AOÛT 2020

Extraits

(…) Le cyberespace est dépourvu de frontières, ce qui constitue un défi pour les autorités répressives et judiciaires en matière d'enquêtes et de poursuites pénales, comportant un risque élevé d'impunité ; considère par conséquent que les cybercrimes doivent être traités dans le cadre de la coopération judiciaire en matière pénale, avec l'appui du réseau judiciaire européen en matière de cybercriminalité ;

(…) La lutte contre la cybercriminalité exige une coopération internationale efficace permettant de promouvoir la sécurité et la stabilité du cyberespace ; considère que l'amélioration de cette coopération requiert la ratification de la convention de Budapest par l'ensemble des États membres de l'Union européenne et la conclusion dans les meilleurs délais des négociations sur le deuxième protocole additionnel à cette convention ; souhaite le renforcement de la coopération entre l'Union européenne et le Conseil de l'Europe dans la lutte contre la cybercriminalité, dans le respect de leur mandat respectif ;(…) L'Union européenne doit s'organiser pour poursuivre plus efficacement les cybercriminels ; constate que la territorialité de la loi pénale constitue encore trop souvent un obstacle aux poursuites, en particulier lorsque les cybercrimes impliquent plusieurs États membres ; demande par conséquent la conduite d'une réflexion approfondie sur les voies et moyens d'une extension du champ de compétences du Parquet européen à la lutte contre la cybercriminalité ; est conscient qu'une telle évolution ne pourra intervenir, le cas échéant, que si plusieurs conditions sont réunies, en particulier l'unanimité au Conseil européen, le respect du principe de subsidiarité et le fonctionnement probant du Parquet européen dans son champ initial de compétences ; estime en effet que la centralisation au Parquet européen du traitement des affaires transfrontalières de cybercriminalité permettrait une plus grande intégration du fonctionnement de l'Union européenne face à des menaces grandissantes.

ANNEXE 4

L'ÉCOSYSTÈME DU CYBERCRIME

« Cybercrime : plongée dans l'écosystème », Gérôme Billois, Marwan Lahoud, Blog de l'Institut Montaigne, 15 mars 2021.

Toute attaque nécessite un premier accès au système d'information de la cible. Concrètement, l'objectif du cybercriminel est d'avoir le contrôle d'au moins un ordinateur connecté au réseau de l'organisation. Pour répondre à ce besoin, des groupes spécialisés dans la découverte et la revente d'accès aux réseaux d'organisations publiques ou privées ont fait leur apparition sur les marchés clandestins. La vente s'effectue généralement via un service tiers (forum en ligne ou sur le *dark web*) afin d'éviter tout contact direct entre les criminels et les revendeurs d'accès.

Ces revendeurs réalisent des campagnes d'hameçonnage (des courriels frauduleux) ou des scans massifs des réseaux, pour trouver des failles dans les sites web ou les systèmes d'accès distants. Une fois les vulnérabilités identifiées, ils s'introduisent dans les machines ciblées pour mettre en place des accès à distance qui pourront être utilisés dans la durée. Ces accès sont ensuite revendus au plus offrant.

Il est courant de retrouver sur le marché noir des accès datant de six mois et pour des prix allant de quelques centaines à plus de 150,000 dollars. Le montant varie en fonction de la qualité des accès. Il sera élevé si les accès permettent de s'infiltrer sur les réseaux les plus critiques au sein d'organisations susceptibles de payer des rançons élevées ou de dérober des données particulièrement sensibles et confidentielles.

Pour conduire les attaques, les cybercriminels ont ensuite besoin de serveurs - anonymes et protégés - pour héberger leurs outils d'attaques et masquer leurs traces, notamment si des autorités sont sur leur piste. Pour répondre à ce besoin, il existe de nombreux hébergeurs peu regardant sur les activités de leurs clients, appelés "*bulletproof hosting services*". On peut en distinguer deux catégories : ceux qui possèdent et opèrent leurs propres infrastructures physiques, et ceux qui détournent et revendent des offres de fournisseurs classiques, tout en camouflant les activités de leurs clients finaux, les cybercriminels.

Des groupes spécialisés dans la découverte et la revente d'accès aux réseaux d'organisations publiques ou privées ont fait leur apparition sur les marchés clandestins. Un rapide tour d'horizon des dernières attaques par *ransomware* montre l'augmentation massive du recours à des plateformes de *Ransomware-as-a-Service*. Ces cartels du cybercrime fournissent à leurs affiliés des outils d'attaque ainsi que divers services (de négociation, de récupération des paiements…). Ils garantissent trois choses : que ces outils ne seront pas détectés par les mécanismes de protection standards ; que le chiffrement des données sera efficace ; et que les victimes pourront, après paiement de la rançon, retrouver leurs données. Ils assurent également un support technique. Pour arriver à ce

niveau de service, les plateformes disposent d'effectifs dédiés. Le groupe REvil mentionne par exemple une équipe de 10 développeurs.

Contre ces outils et services "*de qualité*", les plateformes cybercriminelles prélèvent une partie des montants rançonnés en guise de paiement. Les rémunérations prélevées par ces plateformes sont variables : 20 % pour Netwalker et jusqu'à 70 % pour d'autres groupes.

L'externalisation d'une partie des cyberattaques a permis à des cybercriminels moins expérimentés de mener des attaques plus complexes et ambitieuses et de démultiplier les gains pour les plateformes. Ainsi, la conduite de l'attaque est prise en charge par une équipe de cybercriminels affiliés, tout en étant fortement assistée par le cartel de *Ransomware-as-a-Service*.

Lorsqu'un cybercriminel devient affilié à une telle plateforme, sa tâche est facilitée. Il ne s'occupe pas de développer un rançongiciel et une interface permettant de piloter l'attaque, ni de gérer la négociation et la collecte de la rançon. Toutefois, ces affiliés sont chargés de l'intrusion - via les accès achetés précédemment -, du vol de données permettant de faciliter la négociation et du déploiement du *ransomware*.

Les relations sur ce type de plateforme sont avant tout fondées sur la confiance entre le vendeur (la plateforme) et l'acheteur (le cybercriminel qui va conduire l'attaque). Les cybercriminels affiliés doivent d'abord faire leurs preuves sur des attaques basiques, avant de gagner la confiance nécessaire pour mener des opérations plus ambitieuses.

Une fois la cyberattaque menée à bien, les cybercriminels ont en leur possession une rançon payée en cryptomonnaies, la plupart du temps en Bitcoins. Même s'il existe des cryptomonnaies plus confidentielles, comme Monero, la popularité du Bitcoin en fait un choix privilégié encore aujourd'hui. Dans un premier temps, les cybercriminels doivent s'assurer que la rançon n'est pas tracée pour remonter jusqu'à eux. Pour cela, ils font appel à des Bitcoins mixers, qui permettent de mélanger les Bitcoins de la rançon avec des Bitcoins "*propres*". Ces derniers appartiennent à des personnes faisant appel à ces mêmes plateformes pour conserver leur anonymat lors de transactions en Bitcoins. La cyberattaque menée à bien, les cybercriminels ont en leur possession une rançon payée en cryptomonnaies.

Enfin, les cybercriminels doivent trouver un moyen pour blanchir l'argent et le retrouver physiquement dans leur porte-monnaie. Pour ce faire, ils font par exemple appel à des groupes spécialisés dans le blanchiment ayant recours à des passeurs d'argent, ou "*money mules*", pour sortir l'argent du pays et le transformer en espèces. Pour recruter les passeurs, les cybercriminels abusent de la confiance de personnes relativement naïves à travers des arnaques, telles que des fausses offres d'emploi, ou encore en faisant du chantage. D'après le spécialiste en cybersécurité Brian Krebs, le coût du blanchiment est estimé à 50 % des profits générés et la plupart du temps externalisés.

ANNEXE 5

LE PREMIER ÉCHEC D'UN CLOUD PUBLIC SOUVERAIN FRANÇAIS 2010-2019

2009 - Constatant le développement spectaculaire du secteur, l'idée d'un cloud souverain germe au sein de l'État

Janvier 2010 - Première mention dans un discours public : « *les Nord-Américains dominent ce marché, qui constitue pourtant un enjeu absolument majeur pour la compétitivité de nos économies, pour le développement durable et même, j'ose le dire, pour la souveraineté de nos pays* », Discours du Premier ministre François Fillon sur le haut débit et de l'économie numérique, 18 janvier 2010, Vélizy.

2011 - Une ébauche de partenariat public-privé avec Orange, Thales et Dassault Systèmes voit le jour sous le nom de « **Projet Andromède** », avec pour objectif de combiner les expertises des trois entreprises en matière de télécommunications et de cybersécurité afin de donner naissance à un géant français à même de garantir l'indépendance et la souveraineté de l'industrie française. Le projet Andromède est inclus dans la première vague des investissements d'avenir, avec 135 millions d'euros d'investissements prévus.

Septembre 2012 - Suite à un désaccord entre Dassault Système et Orange deux entreprises voient le jour. D'un côté, Orange et Thalès lancent **Cloudwatt**. De l'autre, Dassault Systèmes est rejoint par SFR et Bull pour former **Numergy**. L'État devient actionnaire minoritaire à 33% dans les deux startup, grâce à deux investissements de 75 millions d'euros issus du Fonds national de Sécurité Numérique, géré par la CDC.

Octobre 2012 - L'État français mise donc sur une concurrence et une complémentarité vertueuse entre ses deux nouveaux champions, comme le rappelle Fleur Pellerin, ministre déléguée à l'Économie numérique, en octobre 2012 **: « *Le gouvernement a décidé de soutenir deux projets «cloud» de taille critique face à la concurrence nord-américaine. La volonté de l'État est de privilégier l'effet de levier plutôt que la concentration des efforts sur un seul projet. L'émulation ne peut apporter que des bénéfices* ».**

2013-2014 - Les deux jeunes pousses **peinent à atteindre leurs objectifs**. Elles sont issues d'entreprises non-spécialistes du cloud, elles ne bénéficient pas des économies d'échelle qu'aurait permises une mutualisation de leurs ressources, et elles développent toutes les deux des produits sur OpenStack, une infrastructure en licence libre qui ne leur confère qu'un avantage concurrentiel limité. De plus, Cloudwatt adopte un positionnement commercial ambigu, proposant des offres pour les utilisateurs individuels avant même le lancement de services pour les entreprises. Alors que le projet Andromède tablait originellement sur 597 millions d'euros de chiffre d'affaires en 2015, Cloudwatt ne franchit pas la barre des 2 millions en 2014. Numergy fait à peine mieux avec 6 millions d'euros. AWS engrangeait 4,6 milliards de dollars la même année.

Mars 2015 - Dans l'espoir de redresser la barre, Orange rachète les parts de Thalès et de la CDC pour devenir l'unique propriétaire de Cloudwatt. SFR emboîte le pas l'année suivante avec le rachat complet de Numergy. De son côté, l'État

accepte l'échec de sa stratégie d'investissement direct, profitant de cette porte de sortie pour affirmer que des 150 millions d'euros initialement prévus à l'investissement, seule la moitié aurait été dépensée.

23 mars 2018 - Le directeur de l'activité data centers et cloud chez SFR Business, Eric Jacoty, explique dans une interview pour l'Usine Nouvelle, que Numergy ne faisait plus partie de la stratégie de cloud public de SFR.

Juillet 2019 - Par un simple email aux utilisateurs de ses services qu'Orange annonçait la fermeture de Cloudwatt, programmée pour janvier 2020.

Source : « Le cloud souverain est de retour : généalogie d'une ambition emblématique de la souveraineté numérique en France », Siencespo.fr Pierre Noro 20 juillet 2020.

ANNEXE 6

LES ERREMENTS D'UNE STRATÉGIE PUBLIQUE DU CLOUD

Septembre 2013 - Le gouvernement présente les 34 plans de la Nouvelle France Industrielle. Ce programme, porté par le ministre de l'Économie, du Redressement productif et du Numérique, Arnaud Montebourg, doit permettre d'identifier les priorités de politique industrielle pour la France et les marchés mondiaux particulièrement porteurs. Le *cloud computing* figure parmi les 34 plans. Il fait l'objet d'une dizaine de mesures dont la feuille de route est validée en juin 2014.

18 juin 2015 - Le *cloud* est complètement absent de la *Stratégie numérique du gouvernement* présentée le 18 juin 2015 par le Premier ministre, Manuel Valls. La consultation nationale, pilotée par le Conseil national du numérique et prélable à l'élaboration de cette stratégie, mentionne le *cloud* essentiellement en traitant d'un usage personnel et individuel de la technologie.

Février 2015- L'ANSSI lance le label « Secure Cloud » qui vise à évaluer les garanties de sécurité proposées par un prestataire, et, en juillet 2015, est mis à disposition un guide de bonnes pratiques sur l'utilisation du *cloud* par les collectivités territoriales.

Octobre 2015 – L'ANSSI évoque le *cloud* dans sa *Stratégie nationale pour la sécurité du numérique* seulement en référence aux travaux de certification de sécurité pour l'informatique en nuage, communs avec l'Allemagne.

Mai 2016 – Le programme « *Nouvelle France Industrielle : construire l'industrie française du futur* », lancé le 18 avril 2015 et présenté en mai 2016, aborde le *cloud* sous l'entrée « Économie des données ». En ligne directe avec le plan *cloud computing* de 2013, les projets menés dans ce cadre sont toujours sous la direction de Thierry Breton et d'Octave Klaba, rejoints par Gérard Roucairol, président de Teratec.

Mai 2016 - L'étude prospective *Technologies clés 2020*, conduite tous les cinq ans par la Direction générale des entreprises (DGE), cherche à déterminer les technologies stratégiques des cinq à dix années à venir. Le *cloud* est deux fois plus présent dans l'édition de 2015 que dans celle de 2011.

2017 - Aucune mention du *cloud* dans la *Revue stratégique de défense et de sécurité nationale*.

Févier 2018 - La *Revue stratégique de cyberdéfense* consacre au *cloud* une section entière et pointe les dangers pour la souveraineté nationale. S'il était question en 2010-2014 de « renforcer » la souveraineté nationale, ce sont désormais les menaces portées à la souveraineté qui sont mises en exergue.

8 novembre 2018 - Le cabinet du Premier ministre adresse à tous les services étatiques une circulaire présentant la doctrine d'utilisation de l'informatique en nuage de l'État. Le *cloud* y est présenté comme une « *évolution structurelle* » des systèmes d'information (SI) qui « *permet des gains importants d'efficacité* ». Dans les

représentations, il devient alors un composant essentiel de la transformation numérique de l'État. Le déploiement d'une solution hybride, qui mêle *cloud* privé et *cloud* public, est imaginé. **Cette première stratégie française cohérente en matière de *cloud computing* ne compte que trois pages. Contrairement au projet Andromède, il s'agit cette fois, en structurant et réunissant les besoins de l'État en matière d'informatique en nuage, de construire la demande et non plus l'offre**.

Février 2019 – Dans son discours d'inauguration du 8e *datacenter* d'Equinix, Bruno Le Maire, ministre de l'Économie et des Finances, évoque le besoin de protéger les données du CLOUD Act et le concept de « *cloud* de confiance » fait son apparition. Baptisé ensuite « *cloud* national stratégique » il pourra faire l'objet d'un partenariat franco-allemand. OVHcloud et Outscale, filiale de Dassault Systèmes, sont mandatées pour formuler des propositions dans ce sens avant la fin 2019.

Octobre 2019 – Le rapport du Sénat sur la souveraineté numérique d'octobre 2019 explique que le *cloud* de confiance permettra de « *proposer aux entreprises ainsi qu'à la puissance publique des offres diversifiées, performantes et sécurisées* ». Il y est précisé que, « *contrairement au projet de "cloud souverain" [...], l'initiative vise, dans un marché qui a aujourd'hui atteint une bonne maturité, à s'appuyer sur des fournisseurs et des offres déjà exposés au marché* ».

4 juin 2020 - L'État français rejoint l'initiative allemande Gaia-X dessinée en octobre 2019 et abandonne l'idée de créer "ex-nihilo" une nouvelle entreprise soutenue par la puissance publique et des grandes entreprises, pour se tourner vers la formation d'une infrastructure européenne articulée autour d'un organisme de gouvernance et de coordination chargé d'émettre des standards de sécurité, d'interopérabilité et de portabilité des données. Gaia-X concrétise une lente transformation de la stratégie nationale de *cloud* souverain en promouvant un écosystème reposant sur de nombreuses entreprises capables de proposer des offres complémentaires et interopérables pour répondre aux besoins effectifs des entreprises et de la sphère publique

Source : D'après « Le cloud computing : de l'objet technique à l'enjeu géopolitique. Le cas de la France » Clotilde Bômont, Amaël Cattaruzza, Hérodote 2020/2-3 (N° 177-178).

LISTE DES DÉPLACEMENTS

Mardi 13 avril 2021

Centre de lutte contre les criminalités numériques (C3N) situé à Pontoise

- **Général de division Patrick Touron**, commandant le Pôle Judiciaire de la Gendarmerie Nationale ;

- **Colonelle Fabienne Lopez**, chef du Centre de Lutte contre les Criminalités Numériques du Service Central de Renseignement Criminel de la Gendarmerie Nationale ;

- **Général de brigade Éric Freyssinet**, chef du Pôle National de Lutte contre les cybermenaces de la Direction des Opérations et de l'Emploi à la Direction Générale de la Gendarmerie Nationale.

Mercredi 28 avril 2021

Sous-Direction de Lutte contre la Cybercriminalité (SDLC) de la police judiciaire nationale, situé à Nanterre

- **Mme Catherine Chambon**, contrôleur général de la Police nationale, commissaire général de police, sous-directrice de la lutte contre la lutte contre la cybercriminalité ;

- **M. Nicolas Guidoux**, commissaire divisionnaire, adjoint à la sous-directrice de la lutte contre la cybercriminalité ;

- **M. François Beauvois**, commissaire de police, chef de la division de l'anticipation et de l'analyse ;

- **M. Eric Reverdito**, brigadier-chef de police, chef du groupe des techniques spécialisées d'enquête.

Brigade de Lutte contre la Cybercriminalité (BL2C) de la préfecture de police de Paris, situé à

- **M. Éric Francelet**, commissaire divisionnaire, chef de la Brigade de lutte contre la cybercriminalité ;

- **M. Francis Humbert**, commandant de police, chef de groupe enquêtes ;

- **M. Laurent Bovis**, major exceptionnel de police, chef du Laboratoire d'investigation opérationnelle du numérique ;

- **M. Florent Cudennec**, brigadier de police, chef de groupe enquêtes.

LISTE DES PERSONNES AUDITIONNÉES

Jeudi 18 février 2021

- *Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) :* **Mme Mylène Jarossay**, présidente.

- *Alliance pour la Confiance Numérique (ACN) :* **M. Philippe Vannier**, président.

Jeudi 4 mars 2021

- *Tech In France :* **M. Pierre-Marie Lehucher**, président, et **Mme Nolwenn Le Ster**, présidente du comité Cybersécurité et *Head of* Cybersecurity, cloud infrastructure services France, Capgemini.

- *Hexatrust :* **M. Jean-Noël de Galzain**, président.

Jeudi 11 mars 2021

- *Club de la sécurité de l'information français (CLUSIF) :* **M. Jean-Marc Grémy**, vice-président.

- *: Cybercampus :* **M. Michel Van Den Berghe**, ancien président de *Orange Cyberdéfense*.

Jeudi 18 mars 2021

- *Association pour le management des risques et des assurances de l'entreprise (AMRAE) :* **M. Oliver Wild**, président.

Jeudi 25 mars 2021

Table ronde « *Quelle cybersécurité pour les ETI-PME-TPE ?* » :

- *CCI France* : **M. Joël Thiery**, élu à la CCI Paris-Île-de-France, et **M. Philippe Clerc**, conseiller expert pour les études et la prospective ;

- *Confédération des petites et moyennes entreprises (CPME)* : **M. Marc Bothorel**, membre de la Commission numérique de la CPME, chef d'entreprise, et **Mme Delphine Borne**, juriste au sein de la direction des affaires économiques, juridiques et fiscales ;

- *Fédération du e-commerce et de la vente à distance (FEVAD)* : **Mme Sabah Doudou**, directrice conseil ;

- *Mouvement des entreprises de France (MEDEF)* : **M. Christian Poyau**, co-président de la Commission Mutations Technologiques & Impacts sociétaux et co-fondateur et président-directeur général de Micropole, et

M. Guillaume Adam, directeur affaires européennes et numérique, FIEEC (Fédération des industries électriques, électroniques et de communication) ;

- *Mouvement des entreprises de taille intermédiaire (METI)* : **M. Rémi Bottin**, directeur synergies et développement du Groupe Bessé, **M. Jean-Charles Duquesne**, directeur général de la Normandise, et **Mme Florence Naillat**, adjointe au délégué général du METI.

Jeudi 25 mars 2021

- *Commission nationale de l'informatique et des libertés (CNIL) :* **Mme Sophie Nerbonne**, directrice à la direction de la conformité, et **M. Bertrand Pailhes**, directeur des technologies et de l'innovation.

- *Secrétariat général pour l'investissement :* **M. William Lecat**, coordinateur national de la stratégie d'accélération cybersécurité.

Jeudi 8 avril 2021

- *Fédération française de l'assurance (FFA) :* **M. Stéphane Pénet**, directeur général adjoint, **M. Christophe Delcamp**, directeur adjoint, et **Mme Anne-Marie Papeix**, responsable RC médicale, RC et environnement à la direction des assurances dommages et de responsabilité.

- *Wavestone :* **M. Gerome Billois**, partner.

Jeudi 15 avril 2021

Table ronde « *La cybersécurité des ETI-PME-TPE : la réponse des pouvoirs publics* »

- *Agence nationale de la sécurité des systèmes informatiques (ANSSI)* : **M. Guillaume Poupard**, directeur général

- *Délégué ministériel aux partenariats, aux stratégies et aux innovations de sécurité (DPSIS)* : **M. Michel Cadic**, délégué adjoint

- *Groupement d'intérêt public ACYMA (GIP ACYMA)* : **M. Jérôme Notin**, directeur général

- *Tribunal judiciaire de Paris* : **Mme Johanna Brousse**, vice-procureur, chef de la section J3, Lutte contre la cybercriminalité

Jeudi 15 avril 2021

- *Amazon Web Services :* **M. Stephan Hadinger**, senior manager Solutions Architecture et porte-parole en France, **M. Julien Groues**, directeur général.

- *Cour d'appel de Paris :* **Mme Myriam Quéméner**, avocat général près la Cour d'appel de Paris, docteur en droit.

Jeudi 6 mai 2021

- *CybelAngel :* **M. Erwan Keraudy**, CEO, **Mme Camille Charaudeau**, VP Product Strategy, **Mme Pauline Apretna**, responsable Commerciale France .

- *Thales :* **M. Marc Darmon**, président du Conseil des industries de confiance et de sécurité (CICS)

Jeudi 20 mai 2021

- *CyberEdu :* **M. Olivier Levillain**, président.

- *French industrials for resilience, security & Trust - First :* **M. François Feugeas**, président de l'association First et président d'Oxibox et **M. Sébastien Garnault**, président de Garnault & associés

Jeudi 27 mai 2021

- *BPI France :* **M. Pascal Lagarde**, directeur exécutif, en charge de en charge de l'international, de la stratégie, du développement et des études, **M. Guillaume Calin** (direction de la stratégie et du développement), et **M. Vivien Pertusot**, directeur adjoint de BPIFrance Le Lab

- *Club informatique des grandes entreprises françaises (CIGREF) :* **M. Jean-Claude Laroche**, vice-président et directeur des systèmes d'information de ENEDIS

Jeudi 3 juin 2021

- *France Stratégie – Plateforme RSE pour les rapports de juillet 2020 et d'avril 2021 de la Plateforme RSE consacrés à la responsabilité numérique des entreprises :* **Mme Bettina Laville**, animatrice, et **Mme Ghislaine Hierso**, co-rapporteure, 4D / Les Petits Débrouillard.

- *Haut Comité Juridique de la Place de Paris (HCJP) :* **M. Gérard Gardella**, secrétaire général, et **M. Christian Delcamp**, directeur juridique du Crédit agricole

CONTRIBUTIONS ÉCRITES

- *Conscio Technologies :* **M. Michel Gérard**, président & directeur général

- *Cyberwatch :* **M. Maxime Alay-Eddine**, président

- *The Green Bow :* **M. Stéphane Miège**, conseiller pour la cybersécurité

- *Mail in black :* **Thomas Kerjean**, CEO

- *Bien Commun Advisory :* **M. Antoine Boulay**, président

- *Garnault & Associés :* **M. Sébastien Garnault**, président

- *Eurosagency :* **M. Fabrice Laffargue**, conseiller sénior

- *Fédération EBEN :* **Mme Delphine Cuynet**, directrice générale

- *Digital SME France :* **M. Amandine Laveau Zimmerle**, présidente

- *Hia Secure :* **M. Philippe Dieudonné**, partner et fondateur

- *Oracle :* **M. Matis Pellerin**, director, public policy & government affairs (directeur, relation publique et affaires gouvernementales)