ÉCONOMIE, EMPLOI ET TRAVAIL

JANVIER 2019

CYBERSÉCURITÉ : VERS LA RESPONSABILISATION DE L'ENSEMBLE DE LA CHAÎNE DE PRODUCTION

RENAISSANCE numerique

TABLE DES MATIÈRES

INTRODUCTION

Représentant plus de 95 % du tissu économique et près de la moitié des emplois salariés en France, les Très Petites Entreprises (TPE) et Petites et Moyennes Entreprises (PME) jouent un rôle essentiel dans le futur économique et social de notre pays.[1] [2] Cependant, force est de constater que les dirigeants de TPE-PME françaises ne considèrent pas – encore aujourd'hui – la révolution numérique, ses opportunités, son rôle dans la transformation organisationnelle des entreprises et des filières et les risques nouveaux qu'elle induit pour la sécurité de leurs activités, comme une priorité stratégique. La transformation numérique, mécaniquement, augmente la surface des attaques. Or, pour plus de la moitié de ces entrepreneurs, la transformation numérique ne comporte pas de risques et « *ne menace en rien leurs activités pour au moins les cinq prochaines années* ».[3] En 2017, 29 % des TPE-PME ayant été victimes d'une cyberattaque déclarent n'avoir rien changé à leur politique de sécurité.[4]

1 Les TPE sont des entreprises de moins de dix employés et qui font moins de 2 millions d'euros de chiffre d'affaires. Les PME, quant à elles, sont des entreprises de moins de 249 employés, dont le chiffre d'affaires représente moins de 50 millions d'euros et dont le bilan total est de moins de 43 millions d'euros.

2 Chiffres issus du Centre de documentation économie-finance du ministère de l'Économie, des Finances, de l'Action et des Comptes publics : https://www.economie.gouv.fr/cedef/chiffres-cles-des-pme

3 « Histoire d'incompréhension : Les dirigeants de PME et ETI face au digital », BPIFrance Le Lab, octobre 2017.

4 « Enquête Hiscox 2017 : ADN d'un entrepreneur », Hiscox, octobre 2017.

À l'heure où la problématique de la cybersécurité[5] n'a jamais été aussi vive, la table ronde « TPE-PME : Les nouveaux « chevaux de Troie » de l'économie numérique ? », organisée le 19 octobre dernier à l'occasion du mois européen de la cybersécurité par le think tank Renaissance Numérique, en partenariat avec Kaspersky Lab France et la Chambre de Commerce et d'Industrie de Paris Île-de-France, a été l'occasion d'interroger cette vision et les mesures visant à la dépasser.[6] Le paradoxe entre cette place névralgique au sein de l'économie française et cette faiblesse en matière d'appréhension des enjeux de cybersécurité pose une double problématique, à la fois quant à la vulnérabilité propre de ces entreprises face aux cyber risques et celle de leur responsabilité vis-à-vis du reste de la chaîne de production. Si cette problématique revêt un enjeu économique majeur, avec en ligne de mire le risque de paralysie de notre tissu économique, elle revêt également une dimension sociétale forte en termes de confiance dans la transformation numérique de notre société.

Au cœur de l'actualité avec les récentes attaques qui ont affecté de nombreuses entreprises françaises, non seulement de grandes entreprises telles que Renault en mai 2017[7], provoquant l'arrêt temporaire de sites de production, ou encore Saint-Gobain[8], estimant une perte de 250 millions d'euros sur ses ventes liées à la cyberattaque dont le groupe a été victime en juin 2017, mais également les TPE-PME, qui concentrent 80 % des cyberattaques en France[9], le débat sur les enjeux de cybersécurité s'inscrit aujourd'hui dans les priorités de l'État français et de l'Union européenne. Le récent « Appel de Paris pour la confiance et la sécurité dans le cyberespace » lancé par le Président de la République, Emmanuel Macron, lors du Forum sur la Gouvernance de l'Internet qui s'est tenu en novembre dernier, illustre cette attention publique. Cette problématique s'inscrit également dans le débat législatif européen. Le Règlement général sur la protection des données (RGPD), entré en vigueur en mai dernier, a ainsi permis aux entrepreneurs d'être sensibilisés à leur responsabilité en matière de protection des données et donc de sécurité. Plus récemment, la Commission européenne a proposé de créer « un cadre commun de certification de cybersécurité », présenté dans le cadre d'un « paquet cyber », un ensemble de mesures de lutte contre les cyber attaques à l'encontre des entreprises.

En s'intéressant aux actions menées sur le terrain, tant par la puissance publique que par les acteurs privés en matière d'accompagnement des TPE-PME, cette note s'attache ainsi à questionner les conditions de mise en œuvre du processus de sécurisation de l'ensemble des acteurs de la chaîne de production.

5 La cybersécurité consiste en l'« *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'il rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.* » Source ANSSI : https://www.ssi.gouv.fr/entreprise/glossaire/c/

6 La table ronde s'est tenue à Paris et a réuni :

- Adrienne Charmet, Chargée de mission Relations institutionnelles au sein du dispositif Cybermalveillance.gouv.fr ;
- Tanguy de Coatpont, Directeur général de Kaspersky Lab France ;
- Henri Isaac, Maître de conférences, PSL Université Paris-Dauphine et Président de Renaissance Numérique ;
- Annabelle Richard, Avocate associée chez Pinsent Masons ;
- Joël Thiery, Membre élu, référent Intelligence économique et cybersécurité, CCI Paris Ile-de-France.

Cette note s'inspire librement des échanges lors de cette conférence pour porter le point de vue de Renaissance Numérique.

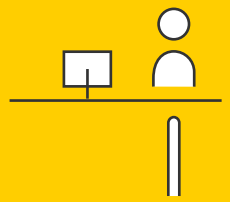
7 « Renault touché par la cyberattaque de niveau mondial, des sites de production à l'arrêt », *LeMonde.fr* avec *AFP* et *Reuters*, mai 2017.

8 « Saint-Gobain a fait l'objet d'une cyberattaque », *LeFigaro.fr* avec *AFP*, juin 2017.

9 « Les entreprises françaises face aux cyber-attaques », Denjean & Associés, décembre 2016.

PARTIE 1

DES INITIATIVES PUBLIQUES ENCORE LIMITÉES POUR PALLIER LE « FOSSÉ » DES TPE-PME EN MATIÈRE DE CYBERSÉCURITÉ



Majoritaires au sein du tissu économique français, les TPE-PME pâlissent d'un retard en termes de maturité numérique, ayant pour conséquence une sécurité lacunaire de leurs systèmes d'information. Bien que l'administration et les politiques publiques accusent elles-mêmes une prise de conscience tardive en la matière, les récentes initiatives de l'État illustrent une volonté de pallier ce « fossé » et restent précurseurs au sein de l'Union européenne.

UNE FAIBLE MATURITÉ NUMÉRIQUE DES TPE-PME

Alors que la transformation numérique offre aux entreprises un levier de croissance, elle induit de nouveaux risques aux conséquences économiques, juridiques et réputationnelles conséquentes. Le retard des TPE-PME en termes de cybersécurité est à rattacher à leur retard plus global en matière de transformation numérique. Selon le dernier indice relatif à l'économie et à la société numériques d'Eurostat, la France demeure relativement mal placée en termes de maturité numérique de ses TPE-PME[10]. 87 % des dirigeants de ces entreprises ne considèrent pas encore la transformation numérique comme nécessaire à la survie de leur activité, « *le temps pour digitaliser leur entreprise n'étant pas venu* ».[11] Dans les TPE-PME, la structure de prise de décision ne facilite pas l'appréhension de ces transformations. Il s'agit en effet de structures très resserrées autour du chef d'entreprise, ce dernier intégrant ainsi une grande partie des compétences. Or, il est difficile d'exceller dans tous les domaines. Au-delà de ce manque de compétences, le facteur temps du chef d'entreprise joue également un rôle important, ces enjeux se retrouvant relégués « à plus tard », entrainant un « réveil » à rebours, une fois le sinistre déclaré.

10 « Indice relatif à l'économie et à la société numériques 2018 - Rapport par pays : France », Commission européenne, 2018.

11 « Histoire d'incompréhension : Les dirigeants de PME et ETI face au digital », BPIFrance Le Lab, octobre 2017.

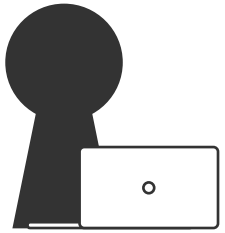
L'objectif est ainsi de permettre aux TPE-PME de se saisir de l'importance de la problématique tout en évitant une approche anxiogène qui pourrait avoir un effet contre-productif. Une étude récente de la Banque publique d'investissement (BPI) divise les dirigeants de PME et ETI en trois grandes catégories : les « Conquérants », les « Sceptiques » et les « Apprentis »[12]. La première catégorie, qui ne représente que 10 % de cette population, a une vraie compréhension des enjeux et s'est pleinement engagée dans la transformation numérique. Les « Sceptiques » représentent 38 % de cette population et considèrent que la transformation numérique ne les concerne pas, n'est pas un sujet prioritaire et qu'ils peuvent encore attendre avant de se lancer. Le reste des dirigeants, 52 %, est en exploration (les « Apprentis »). Ils ont à peu près saisi que la transformation numérique était un sujet important, mais ne savent pas par quel bout la prendre entre ses différents enjeux. Or, si les messages adressés à cette population considèrent ce nouvel espace comme essentiellement à risque, cela devrait les inciter à passer ce cap.

Le renforcement de la gestion des cyber risques par les TPE-PME ne pourra se faire qu'en adoptant une logique positive et constructive. Il s'agit de leur offrir les outils pour appréhender ces nouveaux risques. La transformation numérique, et derrière elle la cybersécurité, sont devenues un enjeu stratégique pour les entreprises. Au-delà de la maîtrise du caractère technique de ces risques - car nous ne serons pas tous demain des experts du *hacking* -, l'enjeu de la cybersécurité appelle à une évolution organisationnelle des entreprises. La vulnérabilité des TPE-PME face aux cyber menaces relève de la nécessité de faire évoluer non seulement leur culture numérique, mais également leur culture de gestion de crise.

Il existe une responsabilité partagée au sein des entreprises. Cela passe par la formation de l'ensemble des employés à la compréhension du rôle des systèmes d'information dans l'activité économique. Selon une étude menée par PwC auprès de 1000 patrons d'entreprises françaises, 34 % des incidents de sécurité en entreprise ont été déclenchés par des salariés.[13] Quel que soit leur poste, l'ensemble des salariés est concerné par les cyber menaces dont la variété ne cesse d'évoluer au gré de l'imagination des pirates (voir le tableau p. 12). Faire face aux cyber attaques nécessite donc que tous les employés, même les plus éloignés de l'utilisation des outils informatiques, y soient préparés. Par exemple, les agents communaux des espaces verts qui aujourd'hui utilisent des tablettes tactiles pour le comptage des plantes et leurs commandes, constituent tout autant des vulnérabilités pour les collectivités. Les auteurs de cyberattaques ne s'y trompent pas et ont su développer une certaine « ingénierie sociale » au travers de leurs attaques, en activant des leviers psychologiques pour embarquer leurs victimes. Un des exemples les plus courants est la « fraude au président », qui consiste à se faire passer pour le dirigeant de l'entreprise et touche fréquemment les secrétaires.

La sécurité informatique est un processus continu. Il doit en être de même pour la formation des employés. Pour être effective, cette sensibilisation doit s'installer dans la durée et passer par des mises en situation permettant à chacun d'appréhender les risques dans son quotidien.

Au-delà de l'anticipation et la réduction des risques, il est également important de mettre en place un certain nombre de mesures qui vont permettre de réagir efficacement une fois la crise survenue (avec des dispositifs de sauvegarde adéquats, etc.). La mise en application récente du RGPD a en cela constitué un « sursaut » intéressant, dont les effets seront à suivre dans la durée (voir à ce sujet l'encadré p. 18).



12 « Histoire d'incompréhension : Les dirigeants de PME et ETI face au digital », BPIFrance Le Lab, octobre 2017.

13 « Infographie : les salariés, première cause des incidents de cybersécurité », PwC, mars 2016.

TYPOLOGIE DES CYBER MENACES[14] [15]

Classification	Menace	Méthode et conséquences sur l'entreprise
Collecte d'information	*Malware* (Programme malveillant)	Reprogrammation de matériel permettant l'installation d'informations malveillantes dans les logiciels et disques durs
Collecte d'information	*Botnets* (Intrusion des serveurs)	Prise de commande et de contrôle des serveurs et ordinateurs infectés
Collecte d'information	Déni de service	Accès aux documents et serveurs de l'entreprise bloqués par la déconnexion à distance des routeurs
Collecte d'information	*Phishing* (Hameçonnage)	Récupération de données par l'ouverture et/ou la réponse à un mail qui appâte en imitant des références familières à la victime[16]
Collecte d'information	*Spam*	Infection de l'ordinateur et arrêt de fonctionnement par ouverture d'un mail ou d'une pièce jointe contenant des documents corrompus ou programmes malveillants
Divulgation d'actifs	Manipulation d'accès physiques à des cyber ressources	Dégâts physiques, vols, pertes de stockages d'information, et arrêt de responsivité des équipements et réseaux
Divulgation d'actifs	Menace de l'intérieur	Mauvais usages des outils et/ou des canaux d'exploitation, par les agents et employés, accidentels ou intentionnels, qui peuvent entraîner la fuite/perte de données
Exploitation des vulnérabilités	*Web-based attack* (Défiguration Web)	Infection du serveur par l'accès à des URLs malveillants ou de pages web compromises
Exploitation des vulnérabilités	« Kits d'exploit »	Infection du serveur par l'utilisation d'un programme inspectant les vulnérabilités de l'environnement ciblé pour installer un programme malveillant adapté grâce à des liens corrompus

14 « Cybersécurité : les 10 menaces les plus courantes expliquées ! », *Leptitdigital.fr,* novembre 2016. https://www.leptidigital.fr/technologie/liste-cybermenaces-9721/

15 « Cybersécurité : les cybermenaces dont il faut se méfier en 2018 », Ecoles IPI, janvier 2018. http://www.ipi-ecoles.com/cybermenaces-2018/

16 Selon les premières observations de la plateforme Cybermalveillance.gouv.fr, le hameçonnage représente 13 % des menaces auxquelles sont confrontées les entreprises, ce qui en fait la première cyber menace pour les professionnels. Il est suivi des botnets qui représentent 12 % de ces menaces. Cependant, ces chiffres doivent être interprétés avec précaution, le dispositif n'étant encore qu'au démarrage de la collecte de données via la mise en place de son observatoire.

UNE VOLONTÉ ÉTATIQUE EN DEVENIR

La prise de conscience en matière de cybersécurité n'a pas été tardive que pour les entreprises. Elle l'a également été pour la puissance publique. Alors que le cadre juridique est aujourd'hui opérant pour faire face aux enjeux post-attaques, c'est dans la phase de préparation que les politiques publiques peinent encore à aider les entreprises à être en capacité d'anticiper ces menaces et en réduire les risques. Notons également que même post-attaque la résolution judiciaire n'est pas aisée, les acteurs de ces attaques étant souvent basés à l'étranger et la chaîne de responsabilité étant particulièrement difficile à démontrer.

Jusqu'alors, les politiques et initiatives publiques s'étaient majoritairement concentrées sur la sécurisation des infrastructures, des services de l'État et des « Opérateurs d'Importance Vitale » (OIV)[17], comme l'illustre la création en 2009 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI est l'autorité de régulation en ce domaine. Comme Guillaume Poupard, directeur général de l'ANSSI, l'évoque, « *les grands parlent aux grands* »[18], l'attention des décideurs politiques s'attardant ainsi tout d'abord sur la sécurité des systèmes d'information des grandes entreprises. Cela s'ex-

17 Il s'agit d'entreprises ou d'établissements jugés comme stratégiques pour le fonctionnement du pays.

18 « Cybersécurité : *"Certains États et entreprises nous apprécient faibles"* », Interview de Guillaume Poupard, directeur général de l'ANSSI, *LaTribune.fr*, octobre 2017.

plique en partie par le caractère extrêmement hétérogène des TPE-PME qui complexifie la politique publique en la matière et appelle à moins de rigidité.

Les particuliers et TPE-PME ne sont apparus au cœur des priorités que depuis peu. À partir de 2015, une réflexion a été lancée avec une assez large consultation. En quelques années, les moyens qui leur ont été consacrés par les politiques publiques se sont développés.

Parmi ces initiatives, l'ANSSI a « incubé » un dispositif d'assistance aux victimes de cyberattaques, la plateforme Cybermalveillance.gouv.fr[19], devenue aujourd'hui le groupement d'intérêt public (GIP) ACYMA. La plateforme est née d'un constat, celui de l'augmentation des attaques sur des acteurs qui n'étaient jusque-là pas pris en compte par les pouvoirs publics : les particuliers, les TPE-PME et les collectivités territoriales.

Elle se distingue par un modèle de décision et de financement multi parties prenantes, regroupant des acteurs publics et privés ; ce qui lui permet d'être plus agile. Ces acteurs sont répartis en quatre collèges :

- le collège des « étatiques », représentant l'État, dont le Premier ministre (SGDSN, ANSSI), le ministère de l'Économie et des Finances, le ministère de la Justice, le ministère de l'Intérieur et le Secrétariat d'État chargé du numérique ;
- le collège des « utilisateurs », représentant les associations et confédérations de potentielles victimes, comme CCI France, Consommation, logement et cadre de vie (CLCV), la Confédération des petites et moyennes entreprises (CPME), l'Association e-Enfance, etc. ;
- le collège des « prestataires », représentant les entreprises prestataires de proximité pouvant aider à la réparation des systèmes d'informations des victimes (Cinov-IT, Conseil National du Logiciel Libre (CNLL), la fédération Entreprises du Bureau et du Numérique (Eben), le Syntec Numérique) ;
- le collège des « offreurs de solution », tels que la Fédération Française des Assurances, Orange Cyberdéfense, Kaspersky Lab France, Microsoft, MMA, etc.

19 Plateforme Cybermalveillance : https://www.cybermalveillance.gouv.fr

Lancée en octobre 2017, la plateforme développe trois axes d'actions principaux :

- L'assistance, en offrant à la victime des conseils pour comprendre pourquoi et comment elle a pu être victime d'une cyberattaque, par des contenus accessibles au plus grand nombre, et en mettant en relation la victime avec des prestataires de proximité susceptibles de réparer ses systèmes ;
- La sensibilisation, en développant des campagnes grand public afin de sensibiliser sur les conséquences des cyberattaques et les moyens de les prévenir (à venir) ;
- L'observation de la menace, en développant des « parcours de victimes » dans le but de voir apparaître des tendances chiffrées et de les analyser afin de mieux prévenir et adapter les réponses aux attaques.

Ce dernier axe de travail a permis en un an de recenser 30 000 « parcours de victimes », dont un tiers émanant d'entreprises, à mettre en regard de seulement 5 000 plaintes recensées par le Ministère de l'Intérieur. Bien que les résultats soient encore préliminaires, car les initiatives récentes et les moyens financiers et humains restreints[20] [21], les données chiffrées que recense l'observatoire permettront, à plus long terme, de faire évoluer et améliorer la compréhension du sujet, d'anticiper les tendances et adapter les actions et la politique publique pour y faire face. Elles permettront à l'État d'avoir ses propres données, indépendantes des entreprises du secteur qui sont aujourd'hui les premiers acteurs à avoir une lecture fine de ces enjeux grâce aux informations qu'elles recueillent. En cela, ces nouvelles données intéressent également d'autres acteurs à l'instar des assureurs qui se sont associés à la plateforme.

Des initiatives publiques plus générales sur la transformation numérique des TPE-PME tendent également à intégrer l'enjeu de la cybersécurité. On peut notamment citer France Num, la plateforme lancée par Mounir Mahjoubi, alors Secrétaire d'État chargé du numérique auprès du Premier Ministre, au mois d'octobre dernier.[22] Cette plateforme a notamment pour objectif

20 Le budget prévisionnel pour l'année 2019 est de 2,5 millions d'euros, 25 % émanant de la sphère publique et 75 % de la sphère privée. « Lancement du dispositif national d'assistance aux victimes d'actes de cybermalveillance », ANSSI, dossier de presse, mai 2017. https://www.ssi.gouv.fr/uploads/2017/05/dossier-presse-lancement-cybermalveillance-gouv-fr.pdf

21 Le dispositif Cybermalveillance.gouv.fr ne compte que huit employés.

22 Plateforme France Num : https://www.entreprises.gouv.fr/numerique/france-num

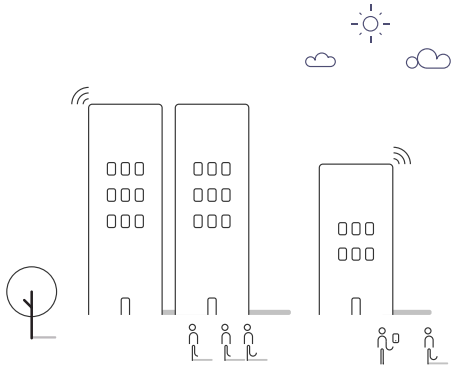
de « *rassembler sous une même bannière, l'ensemble des actions menées par l'État, les régions et leurs partenaires pour accompagner les TPE-PME vers le numérique* ».[23] Une partie est spécifiquement dédiée à « protéger son entreprise », et propose des contenus d'information et de formation à la cybersécurité pour les TPE-PME. En relayant notamment les moyens de sensibilisation mis en place par l'ANSSI, comme des cours en ligne gratuits « pour rendre la *cybersécurité accessible à tous* »[24] ou encore des kits de sensibilisation aux risques numériques[25], ainsi qu'en renvoyant sur la plateforme Cybermaveillance.gouv.fr, France Num s'attache ainsi, entre autres, à promouvoir l'amélioration de la sécurité numérique des TPE-PME.

Sans concerner l'enjeu direct de la cybersécurité, le dernier dispositif numérique en date à destination des TPE-PME, l'espace en ligne démarches-simplifiées.fr, illustre la difficulté à rassembler les TPE-PME sur des thématiques qui sont au cœur de leur activité. Ce dispositif a pour objectif d'assister les TPE-PME dans leur appréhension des plateformes de ventes, en leur permettant de témoigner des difficultés qu'elles rencontrent dans leurs relations avec ces acteurs et outils du numérique. Cependant, d'après les premiers résultats, il semblerait que celle-ci n'ait qu'un succès mitigé avec en tout et pour tout 56 TPE-PME qui auraient « témoigné » sur l'espace en ligne, ce qui représente un chiffre infime pour arriver à des constats généraux et aider les 3,8 millions de TPE-PME françaises – ou du moins une majorité d'entre elles – dans leur transition numérique.[26]

LA FRANCE, PRÉCURSEUR EN EUROPE

Bien qu'encore à ses prémices, le dispositif Cybermalveillance.gouv.fr fait aujourd'hui figure d'exception au niveau européen. Alors que le Luxembourg avait entrepris la mise en place d'un dispositif similaire à Cybermalveillance.gouv.fr à l'aube de la création de ce dernier, l'initiative luxembourgeoise, *Securitymadein.lu*, initiée par un groupement d'intérêt économique *Security made in Lëtzeburg* créé par le ministère de l'économie, ne fournit aujourd'hui que des actualités sur les cyberattaques, des informations pour la prévention et des contacts de prestataires de services de réparation informatique[27]. L'absence d'un rattachement aux services régaliens de l'État ainsi que d'une approche multipartite – au contraire de Cybermalveillance.gouv.fr – la contraint dans son rôle, et ne lui permet pas notamment de jouer un rôle d'observatoire. Ainsi, Cybermalveillance.gouv.fr s'inscrit comme modèle unique au sein des initiatives de promotion de la cybersécurité en Europe de par ses différents rôles d'information, de sensibilisation mais aussi d'observation.

La politique de l'Union européenne elle-même s'inspire directement du modèle français dans sa directive *Network and Information System* (NIS) qui vise, entre autres, à élargir la notion d'Opérateurs d'Importance Vitale en créant la notion d'Opérateur de Service Essentiel. Cette directive s'inscrit dans la nécessaire évolution vers une régulation européenne plus forte afin d'amener les entreprises à considérer la sécurité comme une préoccupation majeure. Le niveau de maturité en sécurité informatique et de conscience du cyber risque étant très diversifié au sein de l'Union européenne – la France, l'Allemagne et l'Estonie étant en pointe – la priorité, avant la mise en place de tout dispositif, est donc d'élever le niveau de la sécurité dans chaque pays européen, en encourageant le partage d'informations et d'expertise entre les États membres sur cet enjeu transfrontalier par nature. Cela appelle à de nouvelles logiques d'échanges entre États membres dans un domaine à forte dominance régalienne.



23 « Lancement de FranceNum : un outil au service de la transformation numérique », Ministère de l'Économie, des finances, de l'action et des comptes publics, communiqué de presse, octobre 2018.
24 « Formez-vous sur Internet gratuitement à la sécurité du numérique », France Num, décembre 2018.
25 « Assurer sa sécurité numérique : Télécharger le kit de sensibilisation aux risques numériques », France Num, décembre 2018.
26 « Difficultés des PME avec les "*Marketplaces*" : le site gouvernemental fait flop », *Next Inpact*, novembre 2018.
27 Plateforme Securitymadein.lu : https://securitymadein.lu

RGPD : QUEL RETOUR D'EXPÉRIENCE POUR LES TPE-PME SEPT MOIS APRÈS SON ENTRÉE EN VIGUEUR ?

Entré en application le 25 mai dernier, le Règlement général sur la protection des données (RGPD) amène de nouvelles obligations pour toutes les entreprises en termes de cybersécurité, précisément celle de garantir la sécurité des données personnelles qu'elles collectent. À ce titre, il s'agit du premier texte de loi à s'appliquer à l'ensemble des entreprises, quel que soit le type de structure et son rôle dans la chaîne de production : l'entreprise – même sous-traitante pour le compte d'une entreprise tiers – doit être en mesure, à tout moment, de démontrer que toutes les mesures techniques et organisationnelles exigées ont été mises en œuvre dans le traitement des données personnelles.

En matière de traitement des données personnelles, les entreprises françaises étaient jusque-là soumises à la loi Informatique et Libertés de 1978 et modifiée en 2004. La loi imposait une déclaration préalable de ces traitements auprès de la Commission nationale de l'informatique et des libertés (CNIL), voire une autorisation préalable pour les cas les plus sensibles. Avec le RGPD, ce fonctionnement disparaît. Plus de déclarations préalables : les entreprises sont censées être responsables. En cas de visite de la CNIL, elles doivent pouvoir démontrer qu'elles appliquent les bonnes politiques de gestion des données personnelles. Sept mois après son entrée en vigueur au sein de l'Union européenne, le retour d'expérience sur cette première phase et son « adoption » par les TPE-PME témoigne des défis que revêt la sensibilisation de ces entreprises et la mise à disposition de moyens suffisants par les pouvoirs publics pour garantir l'effectivité de ces cadres.

UN « ÉLECTROCHOC » À COURT TERME POUR LES DIRIGEANTS DES TPE-PME

L'innovation la plus frappante introduite par le nouveau règlement est le niveau inédit des amendes encourues pour les contrevenants. Jusqu'en 2016, la CNIL ne pouvait pas infliger d'amendes supérieures à 150 000 euros. Depuis la loi pour la République numérique, ce plafond a été relevé à 3 millions d'euros. Avec le RGPD, le pouvoir de sanction de la CNIL est très largement renforcé puisqu'il pourra s'élever jusqu'à 20 millions d'euros ou entre 2 % et 4 % du chiffre d'affaires selon la taille de l'entreprise.

Pour Joël Thiery, référent Intelligence économique et cybersécurité à la CCI Paris Ile-de-France, le RGPD a eu l'effet d'un « électrochoc », et a permis aux entrepreneurs de s'interroger sur leur organisation, la valeur de ce nouvel actif qu'est la donnée et leur responsabilité en la matière. En imposant de nouvelles régulations et la possibilité de sanctions financières lourdes pour les activités de l'entreprise, le RGPD est également apparu comme l'opportunité de faire monter la problématique de la sécurité numérique au cœur des réflexions et des priorités des entrepreneurs.

MAIS UNE APPROPRIATION ENCORE DIFFICILE

La CNIL souligne qu'elle a reçu 9 700 plaintes depuis le début de l'année 2018, dont 6 000 depuis le 25 mai dernier, soit 34 % de plus qu'en 2017.[28] Le RGPD semble ainsi avoir permis aux citoyens une utilisation renforcée des recours pour garantir la protection de leurs données, avec 3 767 plaintes émanant de particuliers contre 2 294 sur la même période en 2017, soit une augmentation de 64 %, mais également une appropriation progressive du côté des professionnels avec plus de 150 000 téléchargements du modèle de registre simplifié proposé par la CNIL.[29] Toutefois, les retours d'expériences montrent que l'impact concret que ce règlement peut avoir sur l'évolution de la pratique dans les TPE-PME reste flou et débattu.

28 « Données personnelles : + 34% de plaintes à la CNIL », *L'Express.fr*, novembre 2018. https://lexpansion.lexpress.fr/high-tech/donnees-personnelles-34-de-plaintes-a-la-cnil_2050100.html

29 « Infographie - RGPD : quel premier bilan 4 mois après son entrée en application ?», CNIL, septembre 2018.

La crainte de la « menace » financière semble en effet retomber chez les dirigeants de ces entreprises. D'une part, car la CNIL, qui a le rôle de contrôler le respect du RGPD pour les entreprises installées en France, a elle-même alerté sur son manque de moyens humains et financiers pour remplir ses nouvelles responsabilités d'Autorité de protection des données (ADP). Le RGPD entraînant un « *changement d'échelle dans son activité* », elle estime ne pas pouvoir assurer le respect des dispositions du règlement européen par chaque entreprise avec les moyens actuels qui lui sont alloués.[30] Cependant, les moyens de la CNIL devraient être renforcés grâce au projet de loi de finances 2019, dont le vote est en cours au Parlement, prévoyant une augmentation du budget annuel alloué à la CNIL de 6,59 %, passant de 17 658 988 euros à 18 823 353 euros.[31] Dans la lignée du premier point, en insistant sur le temps de transition pour ces acteurs – évidemment nécessaire –, le ressenti d'urgence s'en est trouvé affaibli. D'autant que le traitement médiatique après l'entrée en vigueur du texte, s'est avant tout intéressé aux « grands acteurs ».

Notons, en parallèle, que les offres de service – de qualité hétérogène – se sont multipliées depuis la mise en application du RGPD ; cela a d'ailleurs fait l'objet d'une alerte de la part de la CNIL. Or, les TPE-PME pâtissent d'un manque de compétences interne ne leur permettant pas d'évaluer et faire le « tri » dans la multitude des offres constatées sur le marché. Il reste à voir si les TPE-PME se saisiront des opportunités de formation offertes à l'instar de la formation en ligne ouverte à tous sur comment respecter les fondamentaux du RGPD, qui débutera au début de cette année et sera proposée par la CNIL.

30 « Données personnelles : rendre ces droits effectifs », Renaissance Numérique, mai 2018.
31 Avis n°53 (2018-2019) du sénateur Jean-Yves Leconte, au nom de la commission des lois, Sénat, le 22 novembre 2018.

PARTIE 2

EMBARQUER L'ENSEMBLE DE LA CHAÎNE DE PRODUCTION

Alors que les TPE-PME observent un retard en matière de cybersécurité, leur place au cœur de la chaîne de production leur confère une responsabilité particulière vis-à-vis des autres acteurs de la chaîne. Plus globalement, au regard de leur imbrication, c'est toute la chaîne qui doit évoluer sur cette problématique, y compris dans l'accompagnement des TPE-PME dans leur transformation.

LES TPE-PME AU CŒUR DE LA STRATÉGIE DES FILIÈRES

Les TPE-PME, qui possèdent un accès privilégié aux données des grandes entreprises, constituent aujourd'hui la porte d'entrée majoritaire des cyberattaques sur les grands groupes. Alors que l'espionnage économique est l'une des principales motivations du piratage[32], elles deviennent des cibles faciles pour attaquer l'ensemble de la chaîne de production. Les attaques envers les grandes entreprises sont en effet trop risquées et/ou trop coûteuses pour les pirates. Bien que les récentes attaques ont montré les difficultés et le retard pour certaines d'entre elles, elles sont en général mieux « armées » pour prévenir et se défendre en cas de cyberattaques que les TPE-PME, leurs moyens humains et financiers étant bien plus développés. En cela, les TPE-PME sont les premières touchées par les cyberattaques, bien que victimes collatérales.

Au-delà de ce rapport bilatéral, TPE-PME vs. grandes entreprises, il convient de considérer l'imbrication de l'ensemble des acteurs de la chaîne de production : clients, partenaires, fournisseurs, etc. Le risque cyber est un risque beaucoup plus diffus qui invite à revoir les process au sein des filières et entre les filières.

32 En 2013, 20% des cyberattaques recensées en Ile-de-France ont été causées pour des raisons d'espionnage économique. « Espionnage industriel, une menace à appréhender avec détermination », PwC France, mars 2014.

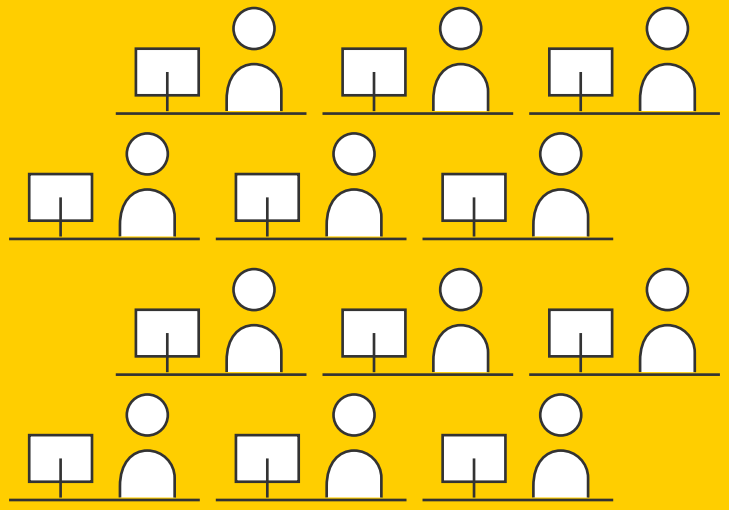
DE LA VULNÉRABILITÉ À LA RESPONSABILITÉ PARTAGÉE DES ACTEURS DE LA CHAÎNE

Le partage d'informations et la coopération entre acteurs au sein de la chaîne de production sont des incontournables de la prévention contre les cyber menaces. Les grandes entreprises doivent jouer un rôle majeur dans ce processus, en s'assurant que leurs sous-traitants et partenaires respectent les mesures de sécurité informatique. Il s'agit d'ailleurs d'une obligation légale en ce qui concerne les données, liée à la nouvelle relation établie entre le responsable de traitement et le sous-traitant dans le cadre du RGPD[33]. Désormais, grands groupes et sous-traitants, sont co-responsables de la sécurité des informations qu'ils partagent dans le cadre de leur partenariat économique. Si elles veulent être conformes à leurs obligations liées au RGPD, les grandes entreprises ne peuvent seulement renforcer la pression sur leurs sous-traitants. Elles doivent leur donner les moyens de participer au respect de leurs obligations. En ce sens, les grandes entreprises ont un devoir d'assistance au développement de la maturité numérique des TPE-PME.

Les fournisseurs de solutions technologiques doivent eux-mêmes jouer un rôle en la matière. Il est toujours plus compliqué de sécuriser une application qui n'a pas dès sa conception intégré ces critères de sécurité. Cet enjeu concerne également les prestataires informatiques de proximité (développeurs de sites web, etc.), encore peu sensibilisés aux enjeux de cybersécurité et notamment à la conservation des preuves numériques. Il conviendrait qu'à terme, ils puissent devenir des prestataires de la prévention et de l'assistance du risque numérique.

33 **«** CHAPITRE IV - Responsable du traitement et sous-traitant **»**, sur le site de la CNIL.

CONCLUSION



Face aux cyber risques, l'ensemble des maillons de la chaîne de production doit être embarqué dans le processus de sécurisation des systèmes d'information. Cependant, le monde des petites et moyennes entreprises semble encore peu focalisé sur le besoin de mûrir sur les enjeux liés au numérique. En ne considérant pas les effets de la transformation numérique sur leur activité comme majeure, les TPE-PME ont laissé une brèche s'ouvrir dans la sécurisation de leurs systèmes d'information. Or, non seulement cela les rend particulièrement vulnérables face aux cyber risques, mais cela fragilise également l'ensemble de la chaîne de production.

Les politiques publiques doivent aider à combler ce retard, la difficulté résultant en la très grande hétérogénéité de ces acteurs. Elles restent encore aujourd'hui trop lacunaires, notamment en termes des moyens humains et financiers qu'elles mettent à disposition des TPE-PME. Cette approche tend toutefois à évoluer. En témoignent les lancements récents des plateformes Cybermalveillance.gouv.fr et France Num. Les données récoltées par le biais de ces dispositifs, notamment par l'observatoire initié par Cybermalveillance.gouv.fr, devront servir à guider ces politiques. À terme, l'enjeu est que ces données permettent non seulement de mieux appréhender les cyber risques, mais également les usages des acteurs en matière de cybersécurité (les blocages, les difficultés d'anticipation et de résilience, etc.). À ce titre, le partage d'informations au niveau européen constitue également un enjeu majeur.

DIRECTION DE LA PUBLICATION

Henri Isaac, Président de Renaissance Numérique

Jennyfer Chrétien, Déléguée générale de Renaissance Numérique

RAPPORTEUR

Romane Malysza, Chargée de mission de Renaissance Numérique

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la promotion d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Janvier 2019
CC BY-SA 3.0