Cyberassurance : instrument utile pour la cybersécurité des entreprises ? Analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (PME)

de Werra, Jacques; Benhamou, Yaniv

www.jusletter.ch

Jacques de Werra / Yaniv Benhamou

Cyberassurance : instrument utile pour la cybersécurité des entreprises ?

Analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (PME)

L'article est basé sur un rapport rédigé par les auteurs sur mandat de la République et Canton de Genève. Il analyse et discute les mesures concernant la cyberassurance qui sont susceptibles d'être prises par les autorités publiques afin d'améliorer la cybersécurité des entreprises et spécifiquement des petites et moyennes entreprises utilisatrices de technologies et ainsi exposées aux cyberrisques dans une perspective suisse en prenant en compte des sources internationales et étrangères.

Catégories d'articles : Articles scientifiques
Domaines juridiques : Informatique et droit ; Droit des assurances privées

Proposition de citation : Jacques de Werra / Yaniv Benhamou, Cyberassurance : instrument utile pour la cybersécurité des entreprises ?, in : Jusletter 24 août 2020

Table des matières

1. Introduction

1.1. Cyberrisque : le plus important risque des entreprises

[1] Dans notre environnement numérique et connecté, les cyberrisques constituent un risque majeur pour la société en général et pour les entreprises en particulier. Ceci est confirmé par le fait que, pour la première fois, le risque lié aux cyberincidents[1] a été classé au premier rang des

1 Tel que défini ci-dessous (cf. texte ad note 7).

risques d'entreprise dans le Allianz Risk Barometer 2020, alors qu'il figurait au 15ème rang avec seulement 6% des réponses il y a 7 ans.[2] Tel est également le cas dans le classement des risques en Suisse (selon la même source).[3] Il n'est dès lors pas surprenant que les autorités publiques y prêtent une attention soutenue. Pour ce qui concerne la Suisse, le Conseil fédéral vient ainsi d'adopter une ordonnance sur les cyberrisques (OPCy) (qui est entrée en vigueur le 1er juillet 2020 et définit en particulier les missions des organes de la Confédération en matière de cybersécurité, notamment celles du Délégué à la cybersécurité et du Centre national pour la cybersécurité) et de décider de créer 20 nouveaux postes en vue de la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2020 à 2022.[4]

[2] Il existe de multiples définitions des cyberrisques.[5] Une définition est notamment donnée dans l'Ordonnance sur les cyberrisques comme « le risque de survenance d'un cyberincident, son ampleur résultant du produit de la probabilité de survenance et de l'étendue des dommages ».[6] Le cyberincident y est pour sa part défini comme « tout événement nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé ».[7]

---

2 Allianz Risk Barometer, Global risks report, 2020 (« For the first time ever, Cyber incidents (39% of responses) ranks as the most important business risk globally in the ninth Allianz Risk Barometer 2020, relegating perennial top peril Business interruption (BI) (37% of responses) to second place. Awareness of the cyber threat has grown rapidly in recent years, driven by companies increasing reliance on data and IT systems and a number of high-profile incidents. Seven years ago it ranked only 15th with just 6% of responses. ») (https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html).

3 Allianz Risk Barometer, Results Appendix 2020, p.11, (https ://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020-Appendix.pdf), listant les « Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties) ».

4 Voir le Communiqué du Conseil fédéral du 28 mai 2020, Protection contre les cyberrisques : le Conseil fédéral adopte une ordonnance et une augmentation des effectifs, (https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79275.html) ; voir le texte (dans une version provisoire, seule la version qui sera publiée dans le Recueil officiel du droit fédéral faisant foi) de l'Ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (Ordonnance sur les cyberrisques, OPCy), (https://www.newsd.admin.ch/newsd/message/attachments/61510.pdf).

5 Voir p.ex. la définition donnée dans les lignes directrices pour la cyberassurance de l'International Organization for Standardization et de l'International Electrotechnical Commission (ISO/IEC) norme 27102 :2019 : « Gestion de la sécurité de l'information – Lignes directrices pour la cyber-assurance », publiée en août 2019, (https://www.iso.org/fr/standard/72436.html), qui est la suivante :

« 3.4 cyber-risk : risk caused by a cyber-threat (3.5) ; 3.5 cyber-threat : threat that exploits a cyberspace (3.6). 3.6 cyberspace : interconnected digital environment of networks, services, systems, and processes » ; pour des études récentes en matière de cyberassurance, voir p.ex. Dirk Wrede/Thorben Freers/Johann-Matthias Graf von der Schulenburg, Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken – Eine empirische Analyse, Vol. 4, 2018, p. 405 ss (https://link.springer.com/content/pdf/10.1007%2Fs12297-018-0425-2.pdf) et Christian Biener/Martin Eling/Jan Hendrik Wirfs, Cyber Risk im Risikomanagement-Prozess, Insurability of Cyber Risk : An empirical Analysis, in : Working Papers on Risk Management and Insurance, No. 151, St. Gallen, 2015, p.40, (https://www.alexandria.unisg.ch/238242/1/Insurability%20of%20Cyber%20Risk%20An%20Empirical%20Analysis.pdf).

6 Art. 3 let. c de l'Ordonnance sur les cyberrisques (note 4) ; voir aussi la définition donnée dans la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022, 2018, p. 31, (https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html) comme le « produit de la probabilité de survenance d'un cyberincident et de l'ampleur des dommages qui en résultent » ; ce document précise aussi qu'il s'agit des risques découlant de la dépendance accrue vis-à-vis du bon fonctionnement de l'informatique, conjuguée à l'intensification des cybermenaces, dont les principales peuvent être décrites selon deux catégories, soit « les menaces dues à des actes illicites délibérés (cyberattaques) et les dangers dus à des événements provoqués de façon non intentionnelle (erreurs humaines et pannes techniques) », p. 3 ; cf. aussi Financial Stability Board (FSB), Cyber Lexicon, 2018, p.9, https://www.fsb.org/2018/11/cyber-lexicon/, qui définit les cyberrisques comme « the combination of the probability of cyber incidents occuring and their impact ».

7 Art. 3 let. b de l'Ordonnance sur les cyberrisques (note 4) ; voir la définition donnée dans le SNPC (note 6), p.31 comme un « événement voulu ou non qui conduit à un processus nuisant à l'intégrité, la confidentialité ou la

[3] Le présent article examine en particulier le rôle potentiel que pourraient avoir les autorités publiques en matière de cyberassurance, définie comme l'assurance visant à couvrir contre les cyberincidents/cyberrisques[8] et des mesures que pourraient prendre ces autorités dans ce cadre.[9] Il convient de relever d'emblée que, vu leur globalité, la cybersécurité et la cyberassurance sont des domaines qui supposeraient la prise de mesures sur le plan national et même sur le plan international,[10] de sorte qu'une action qui ne serait que locale (p.ex. au niveau cantonal) devrait idéalement être accompagnée de mesures aux autres niveaux. La discussion des mesures et recommandations potentielles en matière de cyberassurance et la promotion de celles-ci devraient dès lors avoir lieu de manière coordonnée aux différents niveaux (international, national et local), en coopération avec les institutions publiques et privées concernées, la mise en place de solutions de cyberassurance supposant naturellement la participation des opérateurs du marché de l'assurance privée.

[4] Vu la complexité et la multidisciplinarité de la thématique de la cyberassurance, le présent article n'a pas pour ambition de faire un état des lieux complet de cette thématique, notamment sur le plan économique.[11]

1.2. Délimitations

[5] Le présent article se concentre sur la protection des entreprises et spécifiquement des Petites et Moyennes Entreprises (PME) contre les cyberrisques par le recours à la cyberassurance. Si les cyberrisques n'épargnent personne (ni l'Etat, ni les entreprises, ni les citoyens, qui sont tous vic-

disponibilité de données et d'informations et pouvant occasionner des défauts de fonctionnement » ; voir aussi FSB Cyber Lexicon (note 6), p. 8, qui définit les « Cyber Event » comme : « Any observable occurrence in an *information system*. *Cyber events* sometimes provide indication that a cyber incident is occurring. » et « Cyber Incident » comme un évènement qui : « (i) jeopardizes the *cyber security* of an *information system* or the information the system processes, stores or transmits ; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not ».

8 Pour une définition de la cyber assurance (« cyber insurance »), voir p.ex. https://www.merriam-webster.com/legal/cyber%20insurance (définie comme « insurance for businesses that covers liability arising from use of computers and computer networks (as from theft of private data, virus transmission, and trademark or copyright infringement ») ; voir aussi World Economic Forum (WEF), Future of Digital Economy and Society System Initiative, Cyber Resilience Playbook for Public-Private Collaboration (in collaboration with The Boston Consulting Group), janvier 2018, chapitre 4.14 Cyberinsurance, p.57 ss, (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf) ; accès direct : (http://reports.weforum.org/cyber-resilience/cyberinsurance/?doing_wp_cron=1587013517.1266589164733886718750) , p. 57, définissant la cyberassurance comme : « a rapidly growing form of insurance for organizations seeking to manage cyber-related risks, such as first-party costs incurred as a consequence of a cyberattack, breach, business interruption, restoration and third-party liability ; depending on the jurisdiction, regulatory fines/penalties may also be covered ».

9 Cf. le récent article de Josephine Wolff, Time for Regulators to take Cyber Insurance Seriously, 17 mars 2020, (https://www.lawfareblog.com/time-regulators-take-cyber-insurance-seriously).

10 Voir p.ex. les très récents travaux et rapports de l'OCDE sur la thématique (accessibles depuis cette page et cités ultérieurement dans le présent article) : (https://www.oecd.org/finance/insurance/building-a-sustainable-cyber-insurance-market.htm) ; voir aussi le rapport OCDE, Enhancing the Role of Insurance in Cyber Risk Management, Paris, 2017, (https://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en).

11 Pour des analyses approfondies, voir p.ex. le rapport de Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS), Cyberversicherungen als Beitrag zum IT-Risikomanagement – Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Grossbritannien, BIGS tandpunkt No. 8, Postdam, 2017, (https://www.bigs-potsdam.org/en/publikationen/cyberversicherungen-als-beitrag-zum-it-risikomanagement/) ; voir aussi toutes les publications identifiées dans le rapport de Biener et al. (note 5) ; voir Wrede et al. (note 5), pp. 405–434 ; voir aussi Sasha Romanosky/Lillian Ablon/Andreas Kuehn/Therese Jones, Content analysis of cyber insurance policies : how do carriers price cyber risk ?, *Journal of Cybersecurity*, Vol. 5, Issue 1, 2019, (https://doi.org/10.1093/cybsec/tyz002).

times de cyberincidents et cyberattaques), les PME y sont particulièrement exposées. Il est dès lors essentiel de les accompagner afin de leur permettre de faire face aux cyberrisques, puisqu'elles ne disposent pas nécessairement des outils adéquats en matière de cybersécurité et qu'elles constituent l'essentiel du tissu économique de la Suisse.[12] On note d'ailleurs que plusieurs offres de cyberassurance visent spécifiquement le marché des PME.[13]

[6] Le plan d'action Suisse numérique prévoit ainsi, à l'égard des PME, la création d'un kit de démarrage visant à « améliorer la cyberhygiène dans leur organisation ainsi qu'un plan de cybersécurité et une liste de contrôle pour faire face aux cybermenaces ».[14] La SNPC souligne également les défis posés par les cyberrisques pour les PME et la mission de la SNPC de créer « des conditions aussi sûres que possible pour les entreprises de Suisse » et de mettre à leur disposition « un soutien ciblé pour la gestion des cyberrisques, subsidiairement aux offres du marché ».[15] On relèvera que, dans les circonstances actuelles de travail à distance / télétravail forcé en raison du coronavirus, les cyberrisques sont d'autant plus élevés.[16]

[7] Le présent article se concentre sur les PME qui ne sont pas soumises à un régime réglementaire spécifique et qui ne relèvent donc pas d'une industrie régulée. Le présent article ne traite dès lors pas des entreprises régulées ni des exploitants d'infrastructures critiques :

- S'agissant des exploitants d'infrastructures critiques, l'Administration fédérale (soit les Départements concernés) a pris position de manière positive sur la recommandation 25 du rapport du groupe d'experts sur l'avenir du traitement et de la sécurité des données selon laquelle « [l]a Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques pouvant être auditées et obligent les exploitants d'infrastructures critiques à les observer ».[17] Sur cette base, le

12 Rapport du groupe d'experts concernant le traitement et la sécurité des données, 2018, chapitre 4.2.1.9, p.50, (https://www.newsd.admin.ch/newsd/message/attachments/55754.pdf) : « Les PME sont particulièrement pénalisées par le fait qu'elles ne disposent pas de service informatique dédié, et que leurs marges bénéficiaires ne leur permettent pas de s'offrir les services coûteux d'experts en cybersécurité. Cet aspect mérite la plus grande attention car elles constituent l'épine dorsale de l'économie suisse : plus de 99 % des entreprises sont des PME (de 1 à 250 collaborateurs), qui fournissent les deux tiers des emplois et qui génèrent une part non négligeable du PIB ». Les PME sont définies comme suit : « Les petites et moyennes entreprises (PME) sont des entreprises marchandes comptant moins de 250 emplois. », (https://www.bfs.admin.ch/bfs/fr/home/statistiques/industrie-services/entreprises-emplois/structure-economie-entreprises/pme.html).

13 Cf. p.ex. le produit de la Bâloise « La cyberassurance pour les PME », (https://www.baloise.ch/fr/clients-entreprises/responsabilite-civile-droit-biens-materiels/cyberassurance.html).

14 Office fédéral de la communication (OFCOM), Plan d'action Suisse numérique (état au 5 septembre 2018), p. 12, (https://www.bakom.admin.ch/dam/bakom/fr/dokumente/informationsgesellschaft/strategie2018/Aktionsplan%20Digitale%20Schweiz.pdf.download.pdf/plan-d-action-suisse-numerique_FR.pdf).

15 Voir SNPC (note 6), chap. 3.3., p.10 : « Les cyberrisques posent de grands défis non seulement aux infrastructures critiques, mais aussi à toutes les autres entreprises et en particulier aux PME. La SNPC crée des conditions aussi sûres que possible pour les entreprises de Suisse et met à leur disposition un soutien ciblé pour la gestion des cyberrisques, subsidiairement aux offres du marché ».

16 Algirde Pipikaite/Nicholas Davis, Why cybersecurity matters more than ever during the coronavirus pandemic, 17 mars 2020, (https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/) ; voir aussi Financial Industry Regulatory Authority (FINRA), Cybersecurity Alert : Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19), 26 mars 2020, (https://www.finra.org/rules-guidance/notices/information-notice-032620).

17 Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), Rapport sur les recommandations du groupe d'experts sur l'avenir du traitement et de la sécurité des données – Prise de connaissance et suite de la procédure (état au 15 octobre 2019), p.10, (https://www.newsd.admin.ch/newsd/message/attachments/58797.pdf) : « L'élaboration de normes de sécurité vérifiables en matière de TIC s'effectue dans le cadre des projets définis par le plan de mise en œuvre de la SNPC en étroite collaboration avec les offices spécialisés. Pour ces travaux, le standard minimum pour l'amélioration de la résilience des TIC de l'OFAE est pris

Conseil fédéral a pris position comme suit : « [v]u le progrès de la numérisation, la Suisse doit disposer d'un réseau d'électricité et de télécommunication intact. Par conséquent, il est important que ces infrastructures et d'autres infrastructures critiques soient protégées des défaillances et des cyberattaques. D'ici fin 2022, le nouveau Centre de compétence en matière de cybersécurité du DFF et l'Office fédéral pour l'approvisionnement économique du pays (DEFR) examineront des normes de sécurité contraignantes et identifieront les solutions possibles, en collaboration avec d'autres offices et les cantons ».[18] Par comparaison, dans l'Union européenne (UE), la Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS) requiert que les sociétés actives dans certains secteurs critiques (énergie, transport, eau, banque, infrastructures des marchés financiers, santé et infrastructures numériques) adoptent des pratiques en matière de gestion des risques et signalent les incidents majeurs les affectant à l'autorité nationale.[19]

- S'agissant des sociétés actives dans des secteurs régulés, celles-ci peuvent être soumises à des obligations et règles spécifiques qui dérogent à celles applicables aux PME. Les établissements bancaires et les sociétés d'assurance sont notamment soumises à des obligations spécifiques les obligeant à prendre les mesures requises en matière de protection contre les cyberrisques. Ils font ainsi l'objet d'une surveillance de la FINMA et sont soumis à des règles spécifiques en matière de gestion des risques, la FINMA venant d'ailleurs de publier une communication instituant une obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA.[20]

---

en compte. Le Centre de Compétence Cyber Sécurité coordonne les travaux. Toutefois, il reste à voir comment les exploitants d'infrastructures critiques seront obligés de se conformer à ces normes, et comment le suivi et la surveillance du respect de ces normes seront effectués. Il sera peut-être nécessaire d'adopter une nouvelle législation sectorielle » ; la thématique de la cyberassurance en matière d'infrastructures critiques est complexe et ne peut pas être traitée dans le présent article, cf. p.ex. Derek R. Young, A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies, International Journal of Critical Infrastructure Protection, 24 mars 2016, (https://scholar.afit.edu/cgi/viewcontent.cgi?article=1328&context=etd).

18 Conseil fédéral, Mise en œuvre de recommandations sur le traitement et la sécurité des données, 30 octobre 2019, (https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76854.html) ; on notera aussi que l'Ordonnance sur les cyberrisques (note 4) comporte une définition des infrastructures critiques qui y sont définies comme « les processus, systèmes et installations indispensables au fonctionnement de l'économie et au bien-être de la population » (art. 3 let. g) ; le régime spécial dont bénéficie les exploitants d'infrastructures se manifeste notamment par leur droit de bénéficier d'un « appui subsidiaire » du Centre national pour la cybersécurité (NCSC) qui est le centre de compétences de la Confédération en matière de cyberrisques et coordonne les travaux de la Confédération dans le domaine de la cybersécurité en vertu de l'art. 12 al. 1 let. b de l'Ordonnance sur les cyberrisques (note 4) qui prévoit ainsi que le NCSC a notamment pour tâche de « fournir, en collaboration avec les partenaires compétents au sein de l'administration fédérale, un appui subsidiaire aux exploitants d'infrastructures critiques et encourager entre eux l'échange d'informations concernant les cyberrisques ».

19 Art. 16 al. 5 de la Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après « Directive NIS »), (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148).

20 Communication FINMA sur la surveillance 05/2020 du 7 mai 2020, cette communication vise à rappeler aux établissements soumis à la surveillance de la FINMA l'exigence légale d'annoncer immédiatement tout événement important du point de vue de la surveillance (art. 29 al. 2 de la Loi sur l'Autorité fédérale de surveillance des marchés financiers, LFINMA, RS 956.1), ce qui vise les événements importants en lien avec des cyberattaques dont le degré d'importance est exposé dans la communication, cf. (https ://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf ?la=fr) ; voir aussi le site de la FINMA, Les cyberrisques font partie des principaux risques opérationnels des établissements financiers. La FINMA s'en occupe donc intensivement et elle a renforcé sa surveillance en conséquence, (https://www.finma.ch/fr/documentation/dossier/dossier-cyberrisiken/cyberrisiken-im-fokus-der-aufsicht/) ; voir aussi FINMA, Circulaire 2008/7, Outsourcing -- banques et FINMA, Circulaire 2008/21, Risques opérationnels -- banques ; voir également (en dehors de la Suisse), European Insurance and Occupational Pensions Authority (EIOPA), Cyber Risk for Insurers – Challenges and Opportunities, 2019, (https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_

- Il en va de même des sociétés offrant des infrastructures des marchés financiers qui sont soumises à des règles spécifiques quant à la sécurité de leurs systèmes informatiques et à une surveillance de la FINMA.[21]

[8] Le présent article se concentre ainsi sur les PME qui sont utilisatrices de solutions informatiques et technologiques fournies par des sociétés tierces (p.ex. externalisation/outsourcing de certaines prestations, services en nuage/cloud, etc.). Les PME visées sont des sociétés actives en matière industrielle ou commerciale (p.ex. producteurs de biens et services de consommation courante/actifs en matière industrielle, p.ex. entreprise de transport, boulangerie, menuiserie, industries du bâtiment, de la restauration, etc.) qui pourraient être *victimes* de cyberattaques ou subir des défaillances de solutions IT fournies par leurs fournisseurs de services technologiques. Le présent article ne traite dès lors pas de la gestion des cyberrisques auxquels les sociétés fournisseuses de solutions technologiques ou informatiques (p.ex. services cloud ou objets connectés, Internet of Things) et des cyberassurances que peuvent conclure de telles sociétés. De telles sociétés sont en effet particulièrement exposées aux cyberrisques et sont en outre susceptibles d'y exposer leurs propres clients de sorte qu'elles font l'objet de questions de cyberassurance spécifiques qui ne seront pas traitées ici.[22]

1.3. Structure de l'article

[9] Le présent article est structuré comme suit : il présentera tout d'abord les obligations et risques juridiques des PME en matière de cybersécurité (cf. 2. ci-dessous), avant de traiter de la cyberassurance en Suisse (cf. 3. ci-dessous). Il conclura par la formulation de recommandations (cf. 4. ci-dessous).

---

insurers_sept2019.pdf, p. 3) : « Cyber risk as an element of the insurer's own operational risk profile. Having clear, comprehensive and common requirements on governance of cybersecurity as part of operational resilience would help ensure the safe provision of insurance services. This includes a consistent set of definitions and terminology on cyber risks to enable a more structured and focused dialogue between the industry, supervisors and policymakers, which could further enhance the cyber resilience of the insurance sector. ».

21 Cf. art. 14 de la Loi fédérale sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (Loi sur l'infrastructure des marchés financiers, LIMF ; RS 958.1), en particulier l'art. 14 al. 2 qui dispose que l'infrastructure des marchés financiers « prévoit des mesures permettant de protéger l'intégrité et la confidentialité des informations concernant les participants et leurs transactions » et l'art. 15 de l'Ordonnance sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (Ordonnance sur l'infrastructure des marchés financiers, OIMF ; RS 958.11). Cf. Hugh Reeves/Jürg Schneider/Michael Isler, Cybersecurity in Switzerland, 24 février 2020, (https://www.lexology.com/library/detail.aspx?g=67fa41c8-03f1-44d7-a55f-d291c021a30a).

Les sociétés cotées sont également soumises à des règles spéciales, par exemple aux Etats-Unis. Cf. le très récent rapport de la United States of America Cyberspace Solarium Commission (CSC), Cyberspace Solarium Commission Report, 11 mars 2020, p.83, para. 4.4.4., (https://www.solarium.gov/home) aussi disponible à (https://www.insurancejournal.com/research/app/uploads/2020/03/Cyberspace-Solarium-Commission-Final-Report.pdf), comme indiqué sur le site internet de la CSC, « The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to ‹ develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences. › ».

22 Cf. p.ex. Human Development Index (HDI), IT liability insurance : insuring IT service providers and software producers against claims for compensation, 2020, (https://www.hdi.global/de/en/insurance-solutions/liability-insurance/it-liability-insurance).

2. Obligations et risques juridiques des PME en matière de cybersécurité

[10] Les PME peuvent être soumises à certaines obligations juridiques en matière de cybersécurité (cf. ci-dessous 2.1.) et la violation de leurs obligations peuvent avoir certaines conséquences juridiques et financières en cas de cyberincidents (cf. ci-dessous 2.2.). Compte tenu de l'importance de la protection des données personnelles comme source de cyberrisques pour les entreprises en général et particulièrement pour les PME, l'accent sera mis sur cette question à la lumière du droit suisse de la protection des données personnelles (tant sous l'angle de la loi actuelle sur la protection des données personnelles, LPD[23] que sous l'angle de sa révision et ainsi du projet de révision (P-LPD))[24] et du règlement européen sur la protection des données personnelles (RGPD)[25] vu son importance et son impact en Suisse.[26]

[11] Il convient de présenter ici les obligations générales en matière de cybersécurité (cf. 2.1. ci-dessous) et les conséquences juridiques et financières en cas de cyberincidents (cf. 2.2. ci-dessous).

2.1. Obligations générales en matière de cybersécurité

[12] En matière d'obligations de sécurité sous l'angle de la LPD, les entreprises ont une **obligation générale de prendre des mesures techniques et organisationnelles** pour protéger la sécurité des données. Cette obligation leur incombe, qu'elles agissent comme responsable de traitement (personne qui détermine les finalités de traitement) ou comme sous-traitant (personne qui traite les données pour le compte du responsable de traitement). Cette obligation est prévue dans la LPD (art. 7 LPD) et est complétée par l'OLPD[27] (art. 8–12 OLPD) et le Guide du PFPDT relatif aux mesures techniques et organisationnelles de la protection des données daté d'août 2015.[28] Selon les secteurs, cette obligation est également souvent précisée dans des recommandations de la branche concernée (p.ex. dans le domaine de la finance et de la santé). Certaines entreprises font par ailleurs référence aux normes standards, telles que l'ISO/IEC 27001 (Management de la sécurité de l'information) et l'ISO/IEC 27002 (Code de bonnes pratiques pour le management

23 Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1).

24 La LPD est en révision depuis le 9 décembre 2011 et a abouti à un projet de loi du 15 septembre 2017 (P-LPD). Le présent article se fonde sur la dernière version du projet, soit celle issue des décisions du Conseil national lors de la session d'automne 2019 et des décisions du Conseil des Etats lors de la session d'hiver 2019, étant précisé qu'au jour de la finalisation de cet article, la proposition du Conseil des Etats a été rejetée par le Conseil national et renvoyée au Conseil des Etats (https://www.parlament.ch/fr/services/news/Pages/2020/20200305122148690194158159041_bsf112.aspx).

25 Le Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) est entré en vigueur le 25 mai 2018 et s'applique aux entreprises suisses dont les activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées dans l'UE et au suivi du comportement de ces personnes (art. 3 al. 2 RGPD).

26 Cf. Préposé fédéral à la protection des données et à la transparence (ci-après « PFPDT »), Le RGPD et ses conséquences sur la Suisse, mars 2018, (https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2018/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf.download.pdf/Le%20RGPD%20et%20ses%20cons%C3%A9quences%20sur%20la%20Suisse_FR%20Jan%2018.pdf). Pour une discussion sur la mise en œuvre du RGPD en Suisse, voir Yaniv Benhamou/Emilie Jacot-Guillarmod, RGPD sur sol suisse : mise en œuvre, in : Digma Vol. 3, 2018, pp.142–149. Pour une discussion générale des questions juridiques en matière de sécurité des technologies de l'information, voir Rolf H. Weber/Annette Willi, IT-Sicherheit und Recht, IK – Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität, Zurich, Vol. 33, Zurich, 2006.

27 Ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11).

28 Téléchargeable en pdf sur le site du PFPDT : (https ://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html).

de la sécurité de l'information). Le RGPD comporte également une telle obligation en matière de sécurité, en prévoyant que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Ces mesures doivent être régulièrement réexaminées et actualisées si nécessaire (art. 24 al. 1 RGPD), ce qui est important en matière de cybersécurité puisque la plupart des vulnérabilités sont découvertes plus d'un an après leur survenance.[29]

[13] Selon le RGDP et la nLPD, les responsables de traitement ont une obligation d'annonce des violations de la sécurité des données respectivement de notification en cas de violation des données personnelles (art. 22 nLPD et art. 33 RGPD).[30] Il n'est pas nécessaire qu'un résultat ou un dommage se soit produit. On considère par exemple qu'il y a une faille dès que la sécurité des données n'est plus garantie et que les données ont été exposées, c'est-à-dire qu'il y a potentiellement eu un accès aux données ou un traitement non autorisé.[31] Il est en revanche nécessaire qu'il s'agisse de données personnelles.[32]

[14] Ni le RGPD ni le P-LPD ne prévoient un seuil quantitatif quant au nombre de personnes concernées par la faille de sécurité. Il suffit que les données d'une seule personne soient potentiellement affectées pour déclencher l'obligation d'annonce. En revanche, le RGPD et le P-LPD prévoient un seuil qualitatif puisqu'une telle obligation d'annonce s'applique lorsque la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques (art. 33 al. 1 RGPD) respectivement si la violation entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 al. 1 P-LPD).

[15] Outre ces obligations légales, les entreprises peuvent également assumer des obligations d'annonce sur une base contractuelle. Ainsi, des données, personnelles ou non, peuvent être soumises à des obligations spécifiques par un contrat, notamment dans le cadre d'accords de confidentialité, ce qui constitue une pratique courante s'agissant de données commerciales confidentielles ou stratégiques. Dans ce cas, le contrat peut prévoir des obligations qui seront le plus souvent une obligation d'informer le co-contractant en cas de fuite de données qui peut être couplée à une sanction contractuelle.[33]

---

29 Verizon 2015 Data Breach Investigations Report (https://higherlogicdownload.s3.amazonaws.com/GOVERNANCEPROFESSIONALS/a8892c7c-6297-4149-b9fc-378577d0b150/UploadedImages/Landing%20Page%20Documents/DBIR%20Executive%20Summary%20vv%204-10-15.pdf).

30 Aujourd'hui, la LPD ne prévoit pas expressément une telle obligation. Cette obligation pourrait toutefois découler d'une interprétation de la loi et est souvent prévue comme obligation contractuelle sur la sécurité et la confidentialité des données.

31 Sylvain Métille, Annoncer les failles de sécurité, n'est plus une option, in : Expert Focus 2017, Vol. 17, No. 8, pp. 863–867, p.864.

32 Par comparaison, la Directive NIS (note 19) impose aux opérateurs de services essentiels une obligation d'annonce à l'autorité compétente de tout incident ayant un impact sur la continuité des services essentiels qu'ils fournissent, qu'il s'agisse de données personnelles ou non (art. 14).

33 Par exemple une entreprise peut avoir une obligation d'informer ses clients au sujet de toute violation des données, basée sur une obligation contractuelle expresse ou une obligation générale de diligence.

2.2. Conséquences juridiques et financières en cas de cyberincidents

2.2.1. Responsabilité sur le plan civil (contractuelle et délictuelle)

[16] Les PME sont susceptibles d'être exposées à différentes conséquences juridiques et financières en cas de cyberincidents dont elles seraient victimes.

[17] Si ces cyberincidents sont dus à la responsabilité de tiers, la PME pourrait chercher à se retourner contre les tiers responsables. En cas de relations contractuelles (p.ex. avec un fournisseur de services technologiques de cloud, un employé), la PME pourra ainsi faire valoir des prétentions contractuelles en réparation du préjudice qu'elle aurait subi à l'encontre d'un fournisseur de services technologiques qui serait responsable du préjudice ainsi causé p.ex. en raison des déficiences de cybersécurité des services offerts ou à l'encontre de l'employé dont le comportement aurait conduit au cyberincident.[34] La PME fonderait alors sa prétention sur la base du contrat avec le tiers, sous réserve de clauses d'exclusion / réduction de la responsabilité que pourrait lui opposer ce dernier.[35]

[18] Les contrats entre un prestataire de services technologiques et une société cliente (PME) peuvent identifier certains postes susceptibles d'être considérés comme des dommages réparables en cas de cyberincidents :

- Coûts de restauration des données causés par la faille du prestataire ;
- Coûts de mise en place d'une solution de remplacement pour résoudre le problème ;
- Coûts de remplacement de la perte ou détérioration du matériel et/ou du logiciel ;
- Coûts et dépenses encourues par le client pour fournir ses services auprès de ses clients ;
- Dépenses additionnelles causées par la faille du prestataire (salaires et indemnités des employés, frais de voyages, heures supplémentaires, frais de télécommunication dus aux défaillances du prestataire de fournir les services) ;
- Sanctions et amendes imposées au client par une autorité compétente pour avoir manqué à ses obligations légales ;
- Dommages-intérêts, pertes, coûts et dépenses résultant directement de la faille de sécurité, utilisation abusive ou divulgation d'information confidentielle ou d'obligations de protection des données ;
- Frais de justice et d'avocat.

[19] En l'absence de relation contractuelle entre la PME et le tiers dont la responsabilité est recherchée, une responsabilité pourrait être engagée aux conditions de la responsabilité délictuelle, pour autant que les conditions de celles-ci soient remplies, En droit suisse,[36] cela supposera notamment la commission d'un acte illicite qui pourrait résulter de la commission d'une infraction

34 Une entreprise n'est pas nécessairement responsable des dommages résultant d'une fuite de données causée par l'un de ses employés, cf. l'affaire qui vient d'être jugée par la Cour suprême anglaise, cf. WM Morrisons Supermarkets plc v Various Claimants, [2020] UKSC 12, (https://www.supremecourt.uk/cases/uksc-2018-0213.html).

35 Pour une discussion sous l'angle du droit suisse, voir Jacques de Werra/Evelyne Studer, Regulating cybersecurity : what civil liability in case of cyber-attacks ?, in : Expert Focus 2017, Vol. 17, No. 8, pp. 511–517, p.513, (https://archive-ouverte.unige.ch/unige:96220) ; il sied de noter que la responsabilité pourra échapper au droit suisse dans le cas (fréquent) où le fournisseur sera localisé à l'étranger et que la relation contractuelle sera soumise à un droit étranger (dans le contrat concerné) ou lorsque la responsabilité délictuelle sera soumise au droit étranger en vertu des règles pertinentes de droit international privé.

36 Selon les règles générales de la responsabilité civile (art. 41ss du Code des obligations, CO).

pénale portant préjudice à la PME. Il sera toutefois souvent délicat d'identifier et de poursuivre les auteurs externes d'un cyberincident causant un dommage à une PME, l'environnement du cyberespace offrant aux auteurs de cybercrimes de nombreux moyens d'échapper à leur responsabilité.

[20] La PME pourra aussi engager *sa propre responsabilité* envers les personnes dont elle traiterait les données personnelles qui auraient été atteintes par un cyberincident. Ces personnes pourront fonder leur prétention à l'encontre de la PME sur une base délictuelle et/ou sur une base contractuelle (p.ex. comme client de la PME).

[21] En cas de violation de la LPD (et en l'absence de base contractuelle), la PME (qu'elle agisse comme responsable de traitement ou sous-traitant) peut être tenue pour responsable selon le régime de la responsabilité délictuelle pour faute aux conditions de l'art. 41 CO (faute, dommage, acte illicite, causalité). En cas de violation du RGPD, la PME peut être aussi tenue pour responsable pour le dommage causé par le traitement en violation du règlement (art. 82 al. 2 RGPD).[37] Le RGPD ne précise pas s'il s'agit d'une responsabilité avec ou sans faute mais le texte légal semble partir d'un régime strict de responsabilité sans faute du seul fait du manquement aux obligations légales, en particulier du seul fait de manquements constatés à l'obligation de sécurité (art. 82 al. 1 et 2 RGPD).[38] Le responsable de traitement ou le sous-traitant ne pourrait ainsi pas échapper à sa responsabilité simplement en prouvant l'absence de faute, étant précisé que le RGPD prévoit toutefois une clause d'exonération, en permettant au responsable du traitement ou un sous-traitant d'être exonéré de toute responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable (art. 82 al. 3 RGPD).

[22] Outre la responsabilité de la société (PME) comme telle, la responsabilité des organes de celle-ci pourrait également être engagée en cas de dommages causés par un cyberincident, ce en application des règles régissant la responsabilité des organes (art. 754 CO).[39] Ce risque de responsabilité des organes pour cybericident peut être assuré dans le cadre des polices générales d'assurance des organes dirigeants de sociétés (Director & Officer liability Insurance D&O).[40]

---

37 Le RGPD semble faire une distinction selon qu'il s'agit du responsable de traitement ou du sous-traitant en prévoyant : « Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci » (art. 82 al. 2 RGPD).

38 Pour un aperçu des obligations en matière de sécurité, cf. ci-dessus 2.1. Cf. la décision de la CNIL, n°SAN-2018-008 du 24 juillet 2018, prononçant une sanction de EUR 50'000 à l'encontre de Dailymotion du seul fait d'avoir manqué à son obligation de sécurité et de confidentialité des données, sans que la condition de faute ne soit examinée, (https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037273346&fastReqId=1889384723&fastPos=1).

39 Sur la question de la responsabilité des organes pour la sécurité informatique (conformément à l'art. 754 CO), voir Weber/Willi (note 26), p.197 ss ; voir aussi les documents suivants : Lucy Gordon/Martin Eckert, Wie können Cyber Risiken versichert werden ?, (https://www.mme.ch/de/magazin/wie_koennen_cyber_risiken_versichert_werden/) ; Martin Eckert/Eric Neuenschwander, Cyber Sicherheit – Gibt es rechtliche Vorgaben und Standards ?, (https://www.mme.ch/fileadmin/files/documents/MME_Compact/2018/181016_cyber_sicherheit_gibt_es_regulatorien_und_standards_final.pdf) ; Reeves/Schneider/Isler, Cybersecurity in Switzerland (note 21), (https://www.lexology.com/gtdt/tool/workareas/report/cybersecurity/chapter/switzerland) : « *personal liability of the responsible individuals may materialise if a company suffered loss because of a severe data breach that resulted from a lack of appropriate internal cybersecurity controls and procedures* ».

40 Sarah Turpin/Jeffrey J. Meagher, D&O Insurance for Cyber Liabilities : Increased Cyber Exposure Should Cause Directors & Officers to Take Another Look at Their D&O Policies, 4 avril 2018, (http ://www.klgates.com/do-insurance-for-cyber-liabilities-increased-cyber-exposure-should-cause-directors–officers-to-take-another-look-at-their-do-policies-04-04-2018/) ; voir en droit allemand, Natalie Daghles, Cybersecurity-Compliance : Pflichten und Haftungs-risiken für Geschäftsleiter in Zeiten fortschreitender Digitalisierung, Der Betrieb No. 38,

2.2.2. Responsabilité pénale et administrative (amendes pénales et administratives)

[23] Les sociétés peuvent être aussi sujettes à des amendes administratives ou pénales en cas de cyberincidents.

[24] En cas de violation de la LPD, les personnes privées auteures de certaines infractions (violation des obligations d'informer, de renseigner et de collaborer, des devoirs de diligence, du devoir de discrétion, insoumission à une décision) pourront être sanctionnées par une amende pénale de CHF 250'000 au plus (art. 54–57 nLPD). Au sein de l'entreprise, le chef d'entreprise et toute autre personne exerçant une fonction dirigeante pourront aussi être sanctionnées de telles amendes (art. 58 al. 1 nLPD) qui, lorsqu'elles ne dépassent pas CHF 50'000 et que toute enquête serait disproportionnée par rapport à la peine encourue, pourront être imposées à l'entreprise elle-même (art. 58 al. 2 nLPD). Sur cette base, une société (PME) pourrait se voir directement sanctionnée par une amende.

[25] En cas de violation du RGPD, les autorités de contrôle des Etats Membres peuvent également prononcer des amendes (jusqu'à EUR 20 mio ou 4% du chiffre d'affaires), ce qui pose la question de leur mise en œuvre en Suisse, en particulier lorsque la société n'a pas désigné de représentant (art. 27 RGPD) ou n'a aucun actif dans l'UE.[41] Ces amendes constituent a priori des décisions administratives au sens du droit suisse (soit des mesures propres à influencer la situation juridique du destinataire prises par une autorité dans un cas concret).[42] En l'absence de base légale pour la reconnaissance et l'exécution des décisions administratives étrangères, elles ne pourront pas être exécutées en Suisse au titre de l'entraide administrative. Cela étant, elles pourraient revêtir une nature pénale, en particulier au regard de leur gravité.[43] Dans une telle hypothèse, l'entraide en matière pénale pourrait être refusée en raison de l'impossibilité de faire appel au juge au sens de l'art. 1 al. 3 EIMP.[44] Même à supposer que l'entraide en matière pénale soit admise, les autorités suisses refuseront vraisemblablement leur exécution à défaut de double incrimination (le champ d'application des sanctions du RGPD excède largement celui des sanctions pénales de la LPD actuelle et, dans une moindre mesure, du P-LPD). Les autorités suisses n'exécuteront sans doute la sanction prononcée à l'étranger qu'à concurrence de la peine maximale prévue par le droit suisse pour la même infraction,[45] conformément au principe de la lex mitior.[46] Par conséquent, l'amende exécutée en Suisse ne saurait excéder CHF 10'000 selon le droit actuel[47] respectivement CHF 250'000 selon la nLPD.[48]

21.09.2018, p.2289 ss, p.2292, (https ://de.lw.com/thoughtLeadership/Cybersecurity-Compliance-Pflichten-und-Haftungsrisiken-fuer-Geschaeftsleiter).

41 A propos de l'exécution des amendes européennes en Suisse, cf. Benhamou/Jacot-Guillarmod (note 26), p.142.

42 Cf. art. 5 de la Loi fédérale sur la procédure administrative du 20 décembre 1968 (PA ; RS 172.021). Voir également J.B. Zufferey, La décision administrative – Un alibi au service de tous les intérêts, in : Mélanges Pierre Moor – Théorie du droit – Droit administratif – Organisation du territoire, Berne 2005, p.637 ss, p.639.

43 Cour Européenne des Droits de l'Homme (CEDH), Affaire Engel et autres c. Pays-Bas du 8 juin 1976, (http://hudoc.echr.coe.int/fre?i=001-62037).

44 Loi fédérale sur l'entraide internationale en matière pénale du 20 mars 1981 (Loi sur l'entraide pénale internationale, EIMP ; RS 351.1).

45 Art. 94 al. 2 EIMP.

46 Basler Kommentar Internationales Strafrecht – Youssef/Heimgartner, 2015, art. 94 EIMP N 22.

47 Art. 34 s LPD cum art. 106 CP.

48 Art. 54 ss P-LPD.

[26] Le montant des amendes européennes et l'insécurité juridique quant à leur exécution en Suisse pourrait ainsi avoir un impact sur l'existence et l'étendue de couverture de cyberassurance pour ce type de dommages.

3. La cyberassurance en Suisse

3.1. Introduction

[27] Il convient d'indiquer en préambule qu'il n'existe à l'heure actuelle aucune obligation de conclure une cyberassurance pour les entreprises actives en Suisse (en particulier pas pour les PME). Même les industries régulées ne prévoient aucune obligation spécifique de conclure une cyberassurance. Il sied de relever, au-delà de la cyberassurance, que dans certains domaines, une obligation de conclure une assurance peut être prévue par le droit fédéral (p.ex. en matière de circulation routière) ou par le droit cantonal (p.ex. en matière d'assurance incendie pour immeubles).[49]

[28] Une telle obligation d'assurance peut notamment exister en cas de risques de dommages à des tiers (responsabilité civile, ci-après RC). Une obligation de conclure une assurance RC est en effet prévue dans pas moins de quarante lois fédérales, auxquelles s'ajoutent nombre de dispositions cantonales.[50] Malgré une législation disparate, le régime de l'assurance RC obligatoire présente les trois caractéristiques générales suivantes : (i) il fixe en général des montants de garantie minimum ; (ii) il interdit le plus souvent à l'assureur RC d'opposer au lésé d'éventuelles exceptions tirées du contrat d'assurance ; (iii) il institue un droit de recours de l'assureur RC à l'encontre de son assuré dans les cas dans lesquels le premier verse à la victime plus que ce à quoi il était tenu selon le contrat d'assurance.[51] Au-delà de ces caractéristiques générales, l'introduction d'un régime d'assurance RC obligatoire doit pouvoir être motivé par un intérêt public d'une certaine importance, tel que la création d'un risque/état de fait dangereux, qui justifierait une intervention de l'Etat et une restriction à la liberté économique.[52]

[29] La création d'un risque/d'un état de fait dangereux (qui pourrait fonder une obligation d'assurance) pourrait être envisagée concernant certaines activités *technologiques* créant des risques particuliers susceptibles de causer des dommages à des tiers. Une telle hypothèse viserait primairement les entreprises qui proposeraient des produits et services technologiques créant des cyberrisques pour leurs clients/utilisateurs. Elle ne viserait donc pas les PME clientes de services

49 En matière de circulation routière, la Loi fédérale sur la circulation routière (LCR ; RS 741.01) prévoit une assurance RC obligatoire avant toute mise en circulation d'un véhicule (art. 63 al. 1 LCR : « Aucun véhicule automobile ne peut être mis en circulation sur la voie publique avant qu'ait été conclue une assurance-responsabilité civile (...) ») et l'Ordonnance sur l'assurance des véhicules du 20 novembre 1959 (OAV ; RS 741.31) en règle les modalités. En matière d'assurance incendie pour immeubles, 19 cantons prévoient une assurance obligatoire exploitee par des etablissements cantonaux avec statut de monopoles, tandis que les cantons de Geneve, du Tessin, d'Appenzell Rhodes-Interieures et du Valais (GUSTAVO) ne connaissent pas d'assurance obligatoire en la matiere.

50 Vincent Brulhart, Droit des assurances privées, Berne, 2017, p.52.

51 Ibid.

52 Vincent Brulhart, Regard critique sur quelques évolutions récentes en droit des assurances privées, in : SJ 2014 II, Vol. 136, p.73–107, p.73, à propos de l'ATF 138 I 378. Cet arrêt concerne la révision de la loi cantonale glaronnaise sur l'assurance de choses (SachVG), qui permet à l'établissement autonome de droit public cantonal au bénéfice d'un monopole sur l'assurance de choses d'intervenir, hors du domaine de son monopole, dans le champ des assurances privées en concurrence avec les assureurs privés. Le Tribunal fédéral a alors examiné la validité de cette loi à la lumière de la liberté économique et de l'intérêt public.

technologiques de sorte que la création d'une cyberassurance obligatoire pour ces PME paraît peu opportune (cf. Délimitations ci-dessus 1.2.). On doit de plus noter que les cyberassurances couvrent généralement tant les dommages propres que les dommages causés aux tiers (cf. ci-dessous 3.3.1.). Les cyberassurances ne sont ainsi pas seulement des assurances de responsabilité civile. L'imposition d'une cyberassurance obligatoire ne pourrait donc en tout état pas se justifier seulement sous l'angle de la responsabilité civile et de la création d'un état de fait dangereux. La question de l'imposition d'une obligation de conclure une cyberassurance est débattue. Certains experts plaident ainsi pour la création d'une cyberassurance obligatoire, en particulier dans certaines industries à risque, ce que 3/4 des entreprises et assureurs interrogés dans une enquête soutiennent, en particulier pour l'industrie de la finance et du transport.[53] Ils considèrent que les entreprises actives dans ces domaines seraient incitées à investir davantage dans les systèmes de cybersécurité et que cela conduirait à élargir les pools d'assureurs et à réduire les primes. D'autres experts craignent par opposition qu'une telle obligation engendre d'importants frais administratifs et des problèmes d'aléa moral (« moral hazard »), puisque l'assuré se reposerait alors sur l'assurance au lieu d'améliorer sa cybersécurité.[54]

[30] L'assurance obligatoire pourrait être basée sur un régime de responsabilité pour faute (de sorte que l'assureur paie pour le dommage subi par l'assuré selon son degré de faute, comparable à la responsabilité délictuelle) ou sur un régime strict de responsabilité sans faute (de sorte que l'assureur indemnise l'assuré, souvent jusqu'à une certaine somme, peu importe si ce dernier a commis une faute). Selon certains experts, une assurance obligatoire basée sur la faute permettrait à la victime d'être indemnisée dans la plupart des cas, sauf en cas de faute de l'entreprise, contrairement à un régime d'assurance sans faute qui conduirait certains assureurs à essayer de reporter la responsabilité sur l'entreprise prétendument fautive. Pour un exemple récent, on mentionnera le récent Automated and Electric Vehicles Act 2018 au Royaume-Uni selon lequel un assureur est responsable pour le dommage lié à un accident causé intégralement ou partiellement par un véhicule autonome (indépendamment de la responsabilité de personnes tierces, p.ex. conducteur, fabriquant).[55] Il s'agit donc bien d'une assurance sans faute.[56] Selon d'autres experts, une telle assurance sans faute aurait pour effet de dissuader les entreprises de renforcer leur cybersécurité. Il est par ailleurs difficile de déterminer les primes d'assurance et les assureurs tenteraient d'exclure certains types de dommage, p.ex. les dommages imprévisibles et indirects.[57] L'introduction d'une assurance obligatoire est au surplus très difficile à mettre en œuvre, car les assureurs ont besoin de données suffisantes pour apprécier la fréquence et la taille des prétentions, les types de risques à couvrir et suffisamment de capacité d'assurance/réassurance et une concurrence adéquate, ce qui n'est actuellement pas le cas (hormis certains domaines, dont le transport).[58] On constate en

53 Sigma/Swiss Re Institute, Cyber : getting to grips with a complex risk, No. 1, 2017, (https://media.swissre.com/documents/sigma1_2017_en.pdf).

54 Ibid. ; cf. aussi Debra Littlejohn Shinder, Cyber-Insurance : Is it necessary ? Should it be mandatory ?, 4 décembre 2014, (https://techtalk.gfi.com/cyber-insurance-is-it-necessary-should-it-be-mandatory).

55 Automated and Electric Vehicles Act 2018, chapter 18, article 2(1).

56 Cette assurance est toutefois non obligatoire, l'article 2(2) de la loi prévoyant que, lorsqu'un accident est causé, intégralement ou partiellement par un *véhicule autonome qui n'est pas assuré* au moment de l'accident, le propriétaire est responsable pour le dommage causé.

57 Omri Rachum-Twaig, Whose Robot Is It Anyway ? : Liability for Artificial-Intelligence-Based Robots, University of Illinois Law Review, Vol. 2020, Forthcoming, p.29–32.

58 Insurance Europe, Insight briefing – Compulsory insurance : when it works and when it doesn't, (https://www.insuranceeurope.eu/compulsory-insurance-when-it-works-and-when-it-doesn-t) ; Lloyd's of London, Autonomous vehicles handing over control : Opportunities and risks for insurance, 31 décembre 2014, p.8.

tout état que ces assurances sont essentiellement des assurances responsabilité civile pour des risques technologiques causés par le preneur d'assurance, et pas pour des sociétés (PME) clientes de sociétés fournisseuses de solutions technologiques.

[31] Même s'il n'existe en l'état pas d'obligation de conclure une cyberassurance, il est utile de rappeler ici certains éléments de développements récents en matière de politique de cybersécurité en Suisse qui peuvent avoir un impact sur le traitement actuel et à venir de la cyberassurance en Suisse.

[32] Un groupe d'experts institué par la Confédération[59] a ainsi rédigé un rapport daté du 17 août 2018 concernant le traitement et la securite des donnees.[60] Ce rapport a évoqué la possibilité de recourir aux solutions d'assurance facultative ou obligatoire[61] dans le cadre de réflexions à poursuivre en matière de « nouveaux concepts de responsabilité »[62] en se référant à certaines propositions faites au sein de l'UE.

[33] A l'échelle européenne, l'introduction d'une cyberassurance obligatoire a en effet été évoquée dans le cadre des technologies émergentes (dont l'intelligence artificielle et les véhicules autonomes).

[34] La Commission européenne avait ainsi dans une communication du 10 janvier 2017 (« créer une économie européenne fondée sur les données »[63]) identifié le problème de l'application des règles de responsabilité sur le plan civil lié à « l'application, dans l'économie fondée sur les données, des règles actuellement en vigueur en matière de responsabilité pour ce qui est des produits et services fondés sur des technologies émergentes, telles que l'internet des objets, les usines du futur et les systèmes connectés autonomes »[64], la Commission estimant ainsi qu'il est « capital, pour favoriser l'avènement d'une économie fondée sur les données, de donner des certitudes aux utilisateurs et aux fabricants en ce qui concerne leur responsabilité potentielle ».[65]

[35] Dans ce cadre, la Commission européenne a discuté le besoin potentiel de réforme du régime de responsabilité du fait des produits (fondé sur la Directive sur la responsabilité du fait des produits défectueux (85/374/CEE)) qui établit le principe de la responsabilité objective en soulignant que l'application de cette directive « peut être difficile ou source de confusion dans le contexte de l'internet des objets et des systèmes connectés autonomes (par exemple en robo-

59 Le groupe d'experts avait été institué en réponse à la motion Rechsteiner déposée le 26 septembre 2013 (13.3841, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20133841) par le Département fédéral des finances en date du 27 août 2015).

60 Rapport du groupe d'experts concernant le traitement et la sécurité des données (note 12).

61 Rapport précité, chapitre 7.3.7.3, p.124 : « Solution d'assurance facultative ou obligatoire. Une autre option envisagée par l'UE consiste à introduire une solution d'assurance facultative ou obligatoire. Cette solution vise à dédommager la personne (en particulier le consommateur final d'un produit) qui a subi un (important) préjudice, sans qu'une indemnité ne soit versée par le responsable du préjudice, soit parce que ce dernier ne peut être désigné en raison de la complexité des relations économiques en jeu, soit parce que, compte tenu des circonstances, la personne lésée ne peut s'acquitter de la charge de la preuve. Il est actuellement difficile de savoir si cette solution trouvera un soutien suffisant dans le cadre de la consultation en cours. Quoi qu'il en soit, si cette approche était poursuivie, plusieurs questions devraient encore être examinées en détail, notamment aux niveaux technique et économique. ».

62 Titre du chapitre 7.3.7 du rapport précité (en allemand : « Neue Haftungskonzepte »).

63 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Créer une économique européenne fondée sur les données, ({SWD(2017) 2 final}) du 10 janvier 2017, (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017DC0009&from=EN).

64 Communication précitée, chapitre 4.

65 Ibid.

tique), pour les raisons suivantes : les caractéristiques de ces systèmes, par exemple une chaîne de valeur de produits ou services complexes, avec des interdépendances entre fournisseurs, fabricants et autres tiers ; des incertitudes concernant la nature juridique des dispositifs de l'internet des objets, à savoir s'il s'agit de produits, de services ou de produits accompagnant la vente d'un service ; et le caractère autonome de ces technologies ».[66] Sur cette base, la Commission a lancé une évaluation de l'application de cette directive afin d'« évaluer son fonctionnement global et à déterminer si ses règles, établies pour un environnement très différent, restent appropriées dans le contexte de technologies émergentes telles que l'internet des objets et les systèmes connectés autonomes ».[67]

[36] Dans ce contexte des nouveaux risques de responsabilité, la Commission avait alors évoqué la possibilité de créer un régime d'assurances volontaires ou obligatoires « qui dédommageraient les parties ayant subi le préjudice (c'est-à-dire les consommateurs). Ces régimes devraient garantir la protection juridique des investissements effectués par des entreprises tout en offrant aux victimes une compensation équitable ou une assurance appropriée en cas de préjudice ».[68] La Commission a ainsi initié une consultation des « parties prenantes en ce qui concerne le caractère adéquat des règles existantes de l'UE en matière de responsabilité dans le contexte de l'internet des objets et des systèmes connectés autonomes, et sur la façon de surmonter les difficultés qui se présentent actuellement pour l'imputation de cette responsabilité ».[69]

[37] La création potentielle de solutions d'assurance facultative ou obligatoire mentionnée par la Commission européenne visait toutefois la couverture des risques engendrés par des « produits et services fondés sur des technologies émergentes, telles que l'internet des objets, les usines du futur et les systèmes connectés autonomes »[70] afin de protéger les consommateurs (soit pour reprendre la formulation de la Communication « les parties ayant subi le préjudice (c'est-à-dire les consommateurs) »[71]). Ces solutions d'assurance ne visaient dès lors pas (ou pas principalement) les risques encourus par les sociétés victimes de cyberattaques et les solutions d'assurance dont celles-ci pourraient bénéficier sur lesquelles le présent article se concentre.[72]

[38] La Communication de la Commission européenne a en tout tat servi de source importante pour le groupe d'experts suisse, ce qui a conduit ce dernier à formuler la recommandation suivante (recommandation 24) : « La Confédération examine, en tenant compte des évolutions observées sur le plan international et en particulier dans l'UE, les mesures à prendre dans le domaine du droit de la responsabilité extracontractuelle (responsabilité du fait des produits, responsabilité de la sécurité des produits, responsabilité des prestataires et responsabilité de l'infrastructure numérique). Elle se penche également sur la possibilité d'introduire de nouveaux concepts de responsabilité ».[73]

66 Communication précitée, chapitre 4.1.

67 Ibid.

68 Communication précitée, chapitre 4.2.

69 Ibid.

70 Communication précitée, chapitre 4.

71 Communication précitée, chapitre 4.2.

72 Cf. ci-dessus le chapitre Délimitations (1.2) identifiant les PME ordinaires clientes de services IT de tiers et pas celles fournisseuses de services IT.

73 Rapport précité (note 12), p.124.

[39] Lors de sa séance du 5 septembre 2018, le Conseil fédéral a pris acte du rapport final du groupe d'experts « Avenir du traitement et de la sécurité des données » et le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) a été chargé d'examiner, en collaboration avec tous les départements concernés, les 51 recommandations formulées par le groupe d'experts et de présenter au Conseil fédéral les travaux de suivi correspondants.[74]

[40] Sur cette base, le DETEC a exposé dans son rapport au Conseil fédéral daté du 15 octobre 2019 la position de l'Administration fédérale et a identifié trois thématiques pour lesquelles la conduite de travaux supplémentaires et une analyse approfondie étaient recommandées, dont celle touchant les normes de cybersécurité, ce afin d' « [é]laborer des normes de sécurité informatiques vérifiables (par la Confédération, les cantons, les associations professionnelles des TIC) et instaurer pour les exploitants d'infrastructures critiques une obligation de les observer ».[75]

[41] Dans son rapport, l'Administration fédérale (soit le Département fédéral de Justice et Police) n'a pas considéré que la recommandation 24 concernant les questions de responsabilité devait être suivie en estimant notamment qu'il n'y avait « aucune nécessité d'intervenir »[76] (sans mentionner expressément la question des assurances). L'Administration fédérale (soit les Départements concernés) a toutefois pris position de manière positive sur la recommandation 25 selon laquelle « [l]a Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques pouvant être auditées et obligent les exploitants d'infrastructures critiques à les observer ».[77]

[42] Sur cette base, le Conseil fédéral a décidé que « [v]u le progrès de la numérisation, la Suisse doit disposer d'un réseau d'électricité et de télécommunication intact. Par conséquent, il est important que ces infrastructures et d'autres infrastructures critiques soient protégées des défaillances et des cyberattaques. D'ici fin 2022, le nouveau Centre de compétence en matière de cybersécurité du DFF et l'Office fédéral pour l'approvisionnement économique du pays (DEFR) examineront des normes de sécurité contraignantes et identifieront les solutions possibles, en collaboration avec d'autres offices et les cantons ».[78]

[43] La stratégie de la Suisse en matière de cybersécurité et de gestion des cyberrisques pour les entreprises se caractérise par une approche libérale qui repose ainsi sur la responsabilisation des entreprises elles-mêmes (« Eigenverantwortung »)[79], ces dernières devant ainsi largement prendre directement les mesures requises afin de viser à assurer leur propre cybersécurité.

74 Conseil fédéral, Le Conseil fédéral prend acte du rapport final du groupe d'experts « Avenir du traitement et de la sécurité des données », Berne, 10 septembre 2018, (https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-72083.html).

75 Rapport DETEC (note 17).

76 Rapport DETEC précité (note 17), p.23.

77 Rapport DETEC précité (note 17), p.10 : « *Entités compétentes : DFF, DDPS, DETEC : L'élaboration de normes de sécurité vérifiables en matière de TIC s'effectue dans le cadre des projets définis par le plan de mise en œuvre de la SNPC en étroite collaboration avec les offices spécialisés. Pour ces travaux, le standard minimum pour l'amélioration de la résilience des TIC de l'OFAE est pris en compte. Le Centre de Compétence Cyber Sécurité coordonne les travaux. Toutefois, il reste à voir comment les exploitants d'infrastructures critiques seront obligés de se conformer à ces normes, et comment le suivi et la surveillance du respect de ces normes seront effectués. Il sera peut-être nécessaire d'adopter une nouvelle législation sectorielle.* »

78 Conseil fédéral, Mise en œuvre de recommandations sur le traitement et la sécurité des données 30 octobre 2019, (https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-76854.html).

79 Rapport BIGS (note 11), p.43 et p.46.

Le marché de la cyberassurance est dès lors (encore) relativement peu développé en Suisse et il semble que les premières assurances pour cyberrisques ont été offertes en Suisse vers 2015.[80]

[44] Sur cette base, on constate que la cyberassurance ne fait pas l'objet à l'heure actuelle d'une réglementation spécifique en Suisse, étant précisé que les contrats de cyberassurance sont régis (comme les autres contrats d'assurance privée) par la loi fédérale sur le contrat d'assurance (LCA).[81]

3.2. Modalités de couverture des cyberrisques par les cyberassurances

[45] Les cyberassurances couvrant les cyberrisques qui sont offertes en Suisse (et dans d'autres pays dès lors que les pratiques sont comparables)[82] portent sur des risques très variés.[83] Le spectre des cyberattaques est toutefois si large qu'une assurance contre tous les risques n'est pas possible.[84]

[46] La couverture expresse des cyberrisques par des cyberassurances peut reposer sur des polices couvrant expressément de tels risques (« affirmative cyberinsurance ») qui peuvent être offertes soit sous la forme d'assurances spécifiques aux cyberrisques (« standalone »), soit comme assurance complémentaire à certaines polices existantes (« cyber endorsements »).[85]

[47] La question de la couverture éventuelle des cyberrisques se pose également pour des assurances qui ne couvrent pas expressément les cyberrisques et qui n'ont ainsi pas été conçues dans la perspective de tels risques (« silent cyber risk »). La couverture ou non des cyberrisques ou de certains d'entre eux sur la base de telles polices d'assurance est toutefois délicate.[86] Pour cette

---

80 Rapport BIGS (note 11), p.45 et p.58.

81 Loi fédérale sur le contrat d'assurance du 2 avril 1908 (Loi sur le contrat d'assurance, LCA ; RS 221.229.1).

82 Voir p.ex. Christopher French, Insuring Against Cyber Risk : The Evolution of an Industry, 122 Penn St. L. Rev. 607 (2018), 609, (http ://www.pennstatelawreview.org/wp-content/uploads/2018/07/Symposium-French.pdf) : « *The burgeoning market for cyber insurance has resulted in policy language and coverage that vary greatly from insurer to insurer, so an accurate ‹ apples to apples › comparison of the coverages for the premiums charged is difficult, if not impossible* » avec référence en note de bas de page 16 à l'article de Lyle Adriano, Cyber insurance is like « the Wild West », 1er novembre 2017, (https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-is-like-the-wild-west-83504.aspx) ; cet article de C. French introduit les autres contributions publiées suite à une conférence organisée le 13 avril 2018 par the Penn State Law Review à propos desquelles C. French écrit que : « *(611) [t]he articles also reveal that the kind of uniformity in the policy language that one finds in CGL policies sold by numerous insurers across the country currently does not exist in cyber insurance policies. To the contrary, insurers currently offer a wide array of coverages under cyber insurance policies that are sold ‹ à la carte › and without consistent policy language* » ; voir les autres contributions publiées (http://www.pennstatelawreview.org/wp-content/uploads/2018/07/) : David J. Baldwin/Jennifer Penberthy Buckley & D. Ryan Slaugh, Insuring against Privacy Claims Following A Data Breach, 122 Penn St. L. Rev. 683 (2018) ; Erik S. Knutsen & Jeffrey W. Stempel, The Techno-Neutrality Solution to Navigating Insurance Coverage for Cyber Losses, 122 Penn St. L. Rev. 645 (2018) ; Margaret A. Reetz, Lauren B. Prunty, Gregory S. Mantych & David J. Hommel, Cyber Risks : Evolving Threats, Emerging Coverages, and Ensuing Case Law, 122 Penn St. L. Rev. 727 (2018) et James E. Scheuermann, Cyber Risks, Systemic Risks, and Cyber Insurance, 122 Penn St. L. Rev. 613 (2018).

83 Reeves/Schneider/Isler, Cybersecurity in Switzerland (note 21) : « *The risks covered by this insurance vary significantly and include, for example, the loss or theft of data, unwanted publication of data, damage resulting from hacking and malware, or costs ensuing from investigations or crisis management as a result of cybercrime* ».

84 Gordon/Eckert (note 39) : « *Das Spektrum einer Cyberattacke ist so breit, dass eine Absicherung gegen alle Risiken schlicht unmöglich ist* ».

85 EIOPA (note 20), p.15.

86 Voir p.ex. le document Marsh, Silent Cyber – Frequently Asked Questions and Answers, (https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/silent-cyber-faqs.pdf) ; pour des illustrations des difficultés posées par ce type d'assurances, voir EIOPA (note 20), p.18 (note de bas de page 24 du rapport EIOPA : « *Silent or non-affirmative risks can be illustrated as a malware infecting a GPS, which might cause aviation, marine or car accidents ; or as cyber incident causing fire for example through a device connected to houses. Another example can be a malware event*

raison, les risques du « silent cyber risk » sont problématiques pour l'industrie de l'assurance et de la réassurance ainsi que pour les preneurs d'assurance.[87] Certains régulateurs, institutions de gouvernance, et opérateurs du marché de l'assurance / réassurance recommandent voire exigent ainsi que la clarté soit faite afin que les polices à conclure incluent ou excluent[88] expressément les cyberrisques.[89]

that embeds into a computer system that impacts multiple sites that a firm operates from where a manufacturing process is interrupted, causing business interruption and a fire causing physical damage to property – triggering multiple types of commercial insurance policies at the same time. »).

87 EIOPA (note 20), p.20 : « *[. . .] while common initiatives in the market to address non-affirmative cyber risks are under way, further effort is needed to properly address the risks associated with silent cyber exposures. The lack of quantitative assessment of non-affirmative risks combined with a generalized absence of cyber exclusion practices and action plans suggest insurers are currently not fully aware of the potential exposures to cyber risk. Hence, it is essential to consider further actions to prevent non-affirmative risks and ultimately, cyber accumulation risk.* ».

88 Référence est parfois faite à la « Institute Cyber Attack Exclusion Clause (CL. 380) 10/11/2003 » qui a été adoptée sur la base des « Guidelines of the International Maritime Organization Institute ». Le premier paragraphe de Cl 380 prévoit ainsi : « *(. . .) in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.* » ; cf. EIOPA (note 20), p.19.

89 Voir le Supervisory Statement 4/17 – Cyber insurance underwriting risk, émis par le Prudential Regulation Authority (PRA) de la Banque d'Angleterre (Bank of England), (https://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss) : « *This supervisory statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations of firms regarding cyber insurance underwriting risk. For the purposes of this SS cyber insurance underwriting risk is defined as the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (e.g. cyber attack, infection of an IT system with malicious code) and non-malicious acts (e.g. loss of data, accidental acts or omissions) involving both tangible and intangible assets.* » ; la question de la cyber-assurance continue à faire l'objet d'une attention soutenue par le PRA, cf. Cyber underwriting risk : follow-up survey results, Letter to Chief Executives of specialist general insurance firms regulated by the PRA from Anna Sweeney, Director, Insurance Supervision, 30 janvier 2019, (https://www.bankofengland.co.uk/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results) et (https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results.pdf) ; le Supervisory Statement 4/17 attend des sociétés d'assurance destinataires de ces instructions une gestion adéquate des cyberrisques silencieux (aussi désignés comme les « *non-affirmative cyber risk, ie insurance policies that do not explicitly include or exclude coverage for cyber risk* », cf. para. 1.6) en identifiant certains moyens (de manière non exhaustive) comme l'ajustement de la prime d'assurance pour refléter le cyber-risque additionnel accompagné d'une offre explicite de couverture, l'introduction de clauses claires d'exclusion des cyberrisques ou l'introduction de limites spécifiques à la couverture d'assurance des cyberrisques (para. 2.1) ; voir aussi OCDE, Encouraging Clarity in Cyber Insurance Coverage : The Role of Public Policy and Regulation, 2020, (www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf), p.13 : « *2.3. Supporting clarity in cyber insurance coverage : recommendations As some companies have not begun to address non-affirmative (silent) cyber risk across their lines of business, insurance regulators and supervisors should explicitly require insurance companies to clearly state whether cyber risks are covered or not in all relevant policies (i.e. across relevant lines of business). The transition to affirmative coverage for cyber risk should be closely monitored to ensure that significant gaps in coverage do not emerge based on the application of broad exclusions of cyber risk.* » ; Marsh, Silent Cyber : What It is and How You Can Cover Cyber Perils, (https://www.marsh.com/uk/insights/research/silent-cyber-how-you-can-cover-perils.html) : « *Lloyd's, are requiring insurers to either expressly exclude or include cyber risk in their traditional lines policy wordings, as of January 2020.* ».

3.3. Aperçu de certaines polices de cyberassurance offertes aux entreprises (PME)

3.3.1. Dommages propres, dommages de tiers et autres prestations

[48] Les conditions générales de cyberassurance offertes en Suisse et destinées aux entreprises[90] qui ont pu être consultées dans le cadre de ce mandat[91] offrent des couvertures variées.[92] Elles combinent généralement (tout en les distinguant clairement dans leur structure) l'assurance pour dommages propres subis par le preneur d'assurance (« Cyber Propres Dommages »)[93] et celle pour dommages causés par le preneur d'assurance à des tiers (« Cyber Dommages de tiers » ou

90 Des produits de cyberassurance sont également offerts aux particuliers ; ceux-ci étant en dehors du champ du présent article, ils ne seront pas analysés ici, cf. p.ex. (https://www.swissre.com/dam/jcr:7afc5541-3adc-4e25-9a74-35bc55e057ac/cyber-assurance-individuelle.pdf) ; (https://www.allianz-assistance.ch/fr/cyber-assurance/) ; (https://www.generali.ch/fr/privatkunden/wohnen-bauen/hausratversicherung/cyberversicherung).

91 Les polices d'assurance consultées dans le présent article sont (il est fait référence aux clauses de ces polices en les identifiant par le nom de la compagnie d'assurance concernée et la numérotation de la clause concernée dans la police) :

- AXA Assurance Cyber entreprises édition 01.2018 – Conditions générales d'assurance (CGA), (https://www.axa.ch/fr/clients-entreprises/offres/responsabilite-civile-choses/cyberassurance.html) ;

- Bâloise cyberassurance PME – L'assurance des risques cyber (« Bâloise »), Informations sur le produit et conditions contractuelles – édition 2019, (https://www.baloise.ch/dam/baloise-ch/unternehmenskunden/documents/fr/vertragsbedingungen/140_1021_f.pdf) ;

- Chubb Cyber Enterprise Risk Management (Cyber ERM), Terms and Conditions, Cyber Enterprise Risk, Management Insurance, (https://www.chubb.com/cz-cz/_assets/documents/chubb_pp-cyber-enterprise-risk-management-en.pdf) ;

- Helvetia : offre modèle de cyber-assurance ;

- Zurich Cyberassurance Information client selon la LCA et Conditions générales d'assurance (CGA) – édition 08/2018 (« Zurich ») ;

- Conditions générales modèles (non contraignantes) pour les cyberassurances développées par l'association de l'industrie de l'assurance allemande (« Gesamtverband der Deutschen Versicherungswirtschaft e.V. », (www.gdv.de)) sous la forme de « Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber) Musterbedingungen des GDV » (citées : « GDV »), accessibles depuis : (https://www.gdv.de/de/ueber-uns/unsere-services/musterbedingungen-23924#) ; lien direct : (https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung--avb-cyber--data.pdf) : voir aussi l'article en ligne « Das leistet eine Cyberversicherung », (https://www.gdv.de/de/themen/news/das-leistet-eine-cyberversicherung-31152).

92 Michaela Zellnig/Gaby Stäheli (Gryps), Versicherungsschutz im digitalen Arbeitsalltag, Swiss IT Magazine No. 04, avril 2017, p.37. Vu la grande diversité des cyberassurances, des conditions générales modèles (non contraignantes) pour les cyberassurances ont été développées par l'association de l'industrie de l'assurance allemande (« Gesamtverband der Deutschen Versicherungswirtschaft e.V. »), soit les « Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB Cyber) Musterbedingungen des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) », (https://www.gdv.de/de/ueber-uns/unsere-services/musterbedingungen-23924#) ; pour une analyse juridique de la cyberassurance en droit allemand, voir Matthias Achenbach, Die Cyber-Versicherung – Überblick und Analyse, VersR 2017, 1493 ; voir aussi Christian Wirth, Versicherungsrecht chapitre 12, in : Rechtshandbuch Cyber-Security : IT-Sicherheit, Datenschutz, Gesellschaftsrecht, Compliance, M&A, Versicherungen, Aufsichtsrecht, Arbeitsrecht, Litigation (Detlev Gabel, Tobias Heinrich, Alexander Kiefner éds.), 2019, p.315 ss.

93 Bâloise, titre B ; cf. Axa, B1 « Cyberévènement causant un dommage propre » ; dans les contrats d'assurances entre la PME et l'assureur, il est fréquent de retrouver les postes suivants :

Pertes financières et réputationnelles (p.ex. interruptions d'activités) ;

- Détérioration des infrastructures (hardware) et biens numériques (digital assets) ;

- Frais de minimisation du dommage (Eigenschaden).

« Cyber-responsabilité civile »).[94] Les conditions générales ajoutent parfois d'autres prestations spécifiques (« Cyber assistance ») (p.ex. frais de communication et de gestion de crise et de manipulation des solutions d'online banking, protection juridique, frais forensiques d'enquêtes et investigations).[95] On notera aussi que les réassureurs soutiennent également le développement de solutions de cyberassurance en faveur des PME.[96]

[49] Sans présenter ici toutes les clauses de ces polices d'assurance (dont nombre d'entre elles sont des clauses standards de polices d'assurance), il nous paraît utile de présenter ici certaines clauses spécifiques qui sont propres aux cyberrisques et qui paraissent particulièrement importantes pour déterminer l'attrait ou non d'une police de cyberassurance. Ces clauses sont les suivantes :

3.3.2. Clauses concernant la protection des données personnelles

[50] Certaines polices permettent une indemnisation pour le dommage causé suite à la violation de la protection des données ou de l'obligation de la préservation du secret (violation de la confidentialité des données). L'indemnisation peut être intégrale et sans réserve ou *plafonnée* à un certain montant et/ou *limitée à une certaine période* donnée. Ainsi, la police de la Bâloise prévoit qu'est « assurée la responsabilité civile pour les dommages résultant de la divulgation illicite ou du vol de données à caractère personnel » (B1.5) et, sous cyber assistance – prestations en cas de sinistre (D.2.2 let. e), une « indemnisation à hauteur des honoraires, frais, taxes et autres dépenses nécessaires et adaptés qui sont engendrés chez le preneur d'assurance dans les 12 mois suivant la prise de connaissance de la violation de la protection des données ou de la confidentialité pour [...] les amendes, les pénalités et les autres sanctions financières infligées en raison de dispositions en matière de protection des données ou qui résultent de procédures administratives ou judiciaires, pour autant que la couverture d'assurance soit autorisée ».[97]

3.3.3. Clauses concernant les prétentions liées à des amendes, peines pécuniaires, conventionnelles ou indemnités à caractère punitif

[51] Certaines clauses prévoient une couverture spécifique pour les amendes en matière de protection des données personnelles (cf. ci-dessus 3.3.1.) qui peut être toutefois soumise à certaines procédures spécifiques.[98] D'autres clauses excluent au contraire les prétentions résultant d'amendes

94 Zurich, B ; AXA, B2 « Cyberévènement engageant la responsabilité civile » ; Bâloise, titre C ; cf. aussi la distinction faite dans les GDV, A3 (« Drittschaden ») et A4 (« Eigenschaden ») respectivement.

95 Ces prestations spécifiques sont généralement traitées de manière séparée dans certaines conditions générales. Ces catégories étant faites dans la police AXA, sous titres B3 et B4 respectivement. Cf. Bâloise, D5 ; Zurich D (Cyber-protection juridique) ; Bâloise, D1 ; Bâloise, D3 ; GDV, A2-2.2 Krisenkommunikation und PR-Massnahmen.

96 Swiss Re, Cyber Products Suite for SME, (https://www.swissre.com/reinsurance/property-and-casualty/solutions/cyber-solutions/cyber-product-suite-sme.html) : « We support clients in the development of cyber insurance products for small and medium sized companies (SME) that require end-to-end cyber solutions to protect their business. ».

97 Cf. Bâloise, B1.5 Dommage causé suite à la violation de la protection des données ou de l'obligation de la préservation du secret (violation de la confidentialité des données) et D2.2 let. e Prestation en cas de sinistre.

98 Cf. Bâloise, B4.3 : « Les prétentions relatives à des indemnités à caractère pénal (par ex. les amendes), même si elles ressortent de par leur nature au droit privé (par ex. les punitive damages) ». Certains cas spéciaux sont toutefois réservés : cf. Bâloise B1.6 al.2, « En dérogation partielle à B4.4, sont co-assurées les demandes de paiement de pénalités contractuelles élevées contre le preneur d'assurance pour violation d'une norme de sécurité des données Payment Card Industry (PCI). ».

rendues sous l'angle du RGPD[99] ou plus généralement les « prestations à caractère pénal » (p.ex. amendes), même si elles ressortent de par leur nature au droit privé (par ex. les punitive damages), en laissant toutefois apparaître la possibilité d'assurer une couverture.[100]

3.3.4. Clauses concernant les prétentions découlant de dommages en rapport avec des chantages (ransomware)

[52] Certaines polices prévoient une indemnisation complète ou partielle en cas de chantage (ransomware) (p.ex. frais de conseils et paiement de la rançon effectué par l'assuré),[101] tandis que d'autres polices excluent toute couverture.[102]

3.3.5. Clauses concernant les actes de guerre / cyberguerre

[53] Certaines polices prévoient une exclusion des dommages causés en cas d'actes de guerre, ce qui peut poser des questions délicates d'interprétation et de délimitation (entre acte de guerre et autres cyberattaques), comme le litige Mondelez Zurich Assurance le prouve.[103]

D5.1, « En complément à la partie E, ne sont pas assurées les obligations présentant un caractère pénal ou similaire (par ex. les sanctions financières ou les amendes). Demeure réservé D2.2 litt. e (procédures en relation avec la violation de la protection des données) ».

99 Zurich, Art. 5 (Exclusions) : « Sont exclues de l'assurance les sinistres en lien avec [...] les prétentions pour des indemnités à caractère pénal ou analogue, tels que les amendes, les ‹ punitive or exemplary damages ›, les peines conventionnelles ainsi que les couvertures forfaitaires des coûts. Cette exclusion ne s'applique pas aux peines et amendes du RGPD et du PCI selon l'article 303 (NB PCI = Payment Card Industry Data Security Standard (PCI DSS). ».

100 Cf. AXA, C1.4 ; GDV A1-17.11 : « Behördliche Maßnahmen, Strafen/Bußgelder – Versicherungsfälle oder Schäden aus behördlichen Vollstreckungen oder Anordnungen, Strafen, Bußgelder, Punitive und Exemplary Damages gegen den Versicherungsnehmer, sofern keine abweichenden Regelungen getroffen sind). ».

101 Pour un exemple de couverture complète, cf. La Bâloise D4.2 – Cyberchantage (pour autant que la couverture soit convenue) : indemnisation pour « a) les frais des fournisseurs de prestations de sécurité informatique pour l'évaluation de la situation de menace ainsi que, pour autant qu'il y ait lieu d'estimer la menace comme concrète, les frais de conseils pour éviter que les menaces du maître chanteur ne se concrétisent ; b) les paiements de rançons effectués sur accord écrit préalable de la Bâloise ainsi que les dépenses adaptées et nécessaires qui y sont liées, qui sont en relation avec le cyberchantage et visent à s'en défendre ou à y mettre fin. ». Pour un exemple de couverture partielle, cf. Zurich, art. 104 : « Suite à un événement assuré conformément à l'art. 103, et après accord préalable de Zurich, les prestations supplémentaires suivantes sont fournies jusqu'à 25% au maximum de la somme d'assurance pour des dommages propres, dans la mesure où cela est raisonnable et nécessaire en de telles circonstances (liste exhaustive) : [...] le remboursement de paiements de rançons (en particulier en cas de ransomware). ».

102 Pour un exemple d'exclusion de couverture, cf. AXA, C1.12 excluant « les demandes d'argent dans le cadre d'un chantage », étant toutefois noté que sont « assurés les frais de reconstitution consécutifs à un chantage au moyen d'un ransomware ou rançongiciel » (B1.1.2).

103 Cf. AXA, C1.1 ; Bâloise, E2, a) qui fait expressément référence à la « cyberguerre et cyber-événements catastrophiques dans et pour l'espace virtuel avec des moyens principalement infomatiques » ; GDV, A1-17.2 ; Zurich, art. 5 excluant de l'assurance « les actes de guerre et de terrorisme, les troubles en tout genre, hormis le cyberterrorisme ». Sur le litige Mondelez Zurich Assurance, cf. Justine Ferland, Cyber insurance – What coverage in case of an alleged act of War ? Questions raised by the Mondelez v. Zurich case, Computer Law & Security Review Vol. 25, Issue 4, août 2019, pp. 369–376, (https://doi.org/10.1016/j.clsr.2019.06.003) (article rédigé dans le contexte du projet de recherche conduit avec les auteurs du présent article avec l'Université Hébraïque de Jérusalem, cf. (www.cybersecurity-liability.ch).

3.3.6. Clauses concernant les actes de terrorisme

[54] La majorité des polices excluent la couverture de dommages causés par le terrorisme,[104] à l'exception de la couverture offerte par Zurich (art. 5 excluant de l'assurance « les actes de guerre et de terrorisme, les troubles en tout genre, hormis le cyberterrorisme » – le terme de « cyberterrorisme » n'étant au demeurant pas défini dans les conditions générales).

3.3.7. Clauses concernant les monnaies virtuelles

[55] Les polices excluent parfois d'autres cyberrisques, tels que les dommages liés aux monnaies virtuelles comme le Bitcoin.[105]

3.4. Incertitudes juridiques concernant la couverture des cyberrisques par la cyberassurance

[56] L'efficacité de solutions de cyberassurance dépend de nombreux facteurs qui ne sont pas limités aux facteurs juridiques. Parmi ces derniers, on peut identifier les facteurs suivants qui sont susceptibles de constituer des limites à la couverture efficace des cyberrisques par la cyberassurance :

3.4.1. Diversité de polices de cyberassurance rendant difficile toute comparaison

[57] Il résulte de l'analyse de certaines polices d'assurances offertes en Suisse que celles-ci sont très variables et ne permettent vraisemblablement pas une comparaison facile des polices par les clients prospectifs, spécifiquement par les PME. On doit naturellement signaler que des intermédiaires (brokers)[106] peuvent contribuer à faciliter la comparaison comme cela est déjà fait pour d'autres produits d'assurance, mais on peut douter que ceci satisfasse le besoin d'information et de sensibilisation des PME en matière de cyberassurance.

3.4.2. Incertitude sur la couverture de dommages résultant de cyberrisques

[58] Plusieurs facteurs causent une certaine incertitude quant à la couverture de dommages résultant de certains cyberrisques. Cela découle d'abord de l'absence de conclusion de cyberassurance spécifique et donc de couverture expresse des risques découlant de cyberincidents (« silent cyber risk »).[107] De plus, même en cas de conclusion d'une cyberassurance spécifique, il peut subsister une certaine incertitude sur la portée de la couverture offerte dans certaines circonstances particulières. Sur le plan juridique, la question se pose aussi de la validité de couverture d'assurance pour certains risques. Ainsi, la question de la possibilité de couvrir par une assurance le risque de

104 Cf. AXA, C1.2) ; Bâloise, E2 d) ; GDV, A1-17.4.

105 AXA, C1.9 ; Zurich, art. 5 excluant de l'assurance les sinistres en lien avec « les opérations et pertes commerciales en bourse ou sur titres ainsi que les monnaies numériques ».

106 Cf. p.ex. Kessler, Rapport du sondage sur les cyberrisques 2019 – Les cyberrisques du point de vue de la Suisse, 2019, (https://www.kessler.ch/fr/gestion-des-risques/cyberrisques/).

107 Cf. ci-dessus texte à 3.2.

devoir payer une amende est débattue.[108] De plus, même si les polices offrent fréquemment une couverture pour les cas de « cyberextorsion »,[109] la question de l'assurabilité des montants payés comme rançons par les preneurs d'assurance (« Erpressung »/rançons) reste controversée,[110] certains considérant que les cyberassurances ne devraient pas pouvoir être utilisées pour financer le crime et ne devraient pas non plus déresponsabiliser les preneurs d'assurance et leur permettre de garder des standards de cybersécurité défaillants.[111]

[59] La couverture de dommages causés par des cyberincidents liés à des actes de terrorisme ou de cyberguerre peut également être incertaine comme le démontre le litige (toujours en cours) entre Mondelez et l'assureur Zurich,[112] ceci dépendant – au-delà de la question de l'incertitude sur la formulation contractuelle – également de la preuve de l'existence d'une cyberguerre et de la preuve de l'imputation d'une cyberattaque à un ou plusieurs Etats concernés.

3.4.3. Incertitude concernant l'étendue du devoir de diligence attendu du preneur d'assurance en matière de cybersécurité

[60] La couverture d'un cyberrisque par une cyberassurance suppose que le preneur puisse établir avoir pris les mesures nécessaires en matière de cybersécurité (ce qu'il peut être tenu de faire

108 Une amende est de nature strictement personnelle et toute convention visant à la faire supporter par un tiers est nulle (art. 20 al. 2 CO) (ATF 86 II 71, cons. 4). La jurisprudence suisse (arrêt du Tribunal fédéral 4A_21/2017 du 29 juin 2017 résumé à la SJ 2017 I 455) a ainsi tranché que les amendes fiscales revêtent un caractère strictement personnel et qu'elles ne sauraient être des dommages réparables selon le droit civil (sauf circonstances exceptionnelles). Voir Arnaud Nussbaumer/Jean-René Oettli, Le recouvrement de l'amende pénale en droit civil, RSJ 2017, 173 ss. Voir aussi le rapport de Aon/DLA Piper, The price of data security, A guide to the insurability of GDPR fines across Europe (2nd ed.), juillet 2019, (https://www.dlapiper.com/de/austria/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe/) (p.20 pour la Suisse indiquant que « [r]egulatory fines are generally not insurable in Switzerland » et que « GDPR fines are generally expected not to be insurable in Switzerland ») ; voir aussi Nicholas Bracher, Rechtliche Stolpersteine bei der Versicherung von Cyberrisiken, 2017, p.185 ss, (https://blog.hslu.ch/investments/files/2017/07/Rechtliche-Stolpersteine-bei-der-Versicherung-von-Cyberrisiken.pdf), p.191 : « Zu nennen ist hier zunächst die Versicherbarkeit von Bussen und entsprechenden Verfahrenskosten bei regulatorischen Verfahren, namentlich im Zusammenhang mit Datenschutzverletzungen. Die Deckung entsprechender Kosten wird teilweise als Baustein spezifischer Cyberpolicen angeboten. Als Einkäufer muss man sich bewusst sein, dass namentlich die Abwälzung von Bussen, teilweise aber sogar diejenige von Rechtskosten im Zusammenhang mit entsprechenden Verfahren, auf eine Versicherung in zahlreichen Ländern unzulässig ist. Der vertragliche Anspruch auf entsprechende Versicherungsleistung ist dann rechtlich nicht durchsetzbar. In der Schweiz ist die diesbezügliche Rechtslage nicht restlos geklärt. Bussen mit Strafcharakter gelten nach dem Bundesgericht nicht als ersatzfähiger Schaden und sind dementsprechend grundsätzlich nicht versicherbar. Diese Rechtsprechung gilt allerdings nicht ausnahmslos, und gerade bei administrativen Bussen im Unternehmensstrafrecht besteht Raum für Ausnahmen. ».

109 EIOPA (note 20), p.15 et 16.

110 Bracher (note 108), p.191 : « Juristisch diskutabel ist auch die Zulässigkeit der Versicherung von Lösegeldzahlungen bei Cyber-erpressung, einem weiteren typischen Baustein von Cyberpolicen. Die Versicherung dieses Risikos könnte nämlich als sittenwidrig angesehen werden, zumal Lösegeldzahlungen weitere kriminelle und terroristische Aktivitäten provozieren und auch finanzieren können. Es besteht deshalb ein gewisses rechtliches Risiko, dass entsprechende Policen zivilrechtlich nichtig sind ».

111 Wolff (note 9) : « Finally, regulators should prohibit insurers from paying online extortion demands, including ransoms to recover files and infected systems. They should further limit how much insurance money can be put toward paying legal settlements and government fines for companies that experience cybersecurity breaches and are found to be negligent in their security practices by courts or regulators. This will prevent businesses from using cyber-insurance policies to insulate themselves from the direct costs of ransomware and other forms of online extortion and reduce the profits reaped by the criminals perpetrating these schemes. It will also force firms to more directly face the financial consequences of their security decisions and allow for lawsuits and regulatory investigations to serve as more effective deterrents of poor security practices ».

112 Voir Ferland (note 103) ; voir aussi Brian Corcoran, What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict, 8 mars 2019, (https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict).

en vertu des règles applicables, en particulier celles en matière de protection des données personnelles, cf. 2.1.). Certaines polices précisent dans ce contexte le degré de la diligence attendue pour bénéficier de la couverture, par exemple le fait que le preneur doive prendre des mesures de cybersécurité suffisantes.[113] L'étendue du devoir de diligence du preneur en matière de cybersécurité peut toutefois être difficile à cerner, particulièrement dans les industries non régulées et pour les PME.

4. Recommandations de mesures étatiques susceptibles d'améliorer la cybersécurité des entreprises et spécifiquement des PME

[61] Sur la base des éléments figurant ci-dessus[114], il est possible de formuler certaines recommandations à destination des autorités publiques, étant rappelé que la mise en œuvre efficace de ces recommandations supposera généralement une action des autorités publiques à plusieurs niveaux (international, national, et régional, i.e. cantonal pour la Suisse). Il conviendra aussi de déterminer par quel(s) moyen(s) les autorités publiques peuvent contribuer à assurer la mise en œuvre des recommandations concernées de manière autonome ou en concertation avec d'autres institutions publiques ou privées.[115]

[62] Dans ce contexte, les autorités publiques pourraient envisager d'agir sur la base de législations expérimentales qui permettent de dégager les éléments nécessaires à l'adoption d'une réglementation ultérieure définitive.[116] A Genève, ceci pourrait se fonder sur la Loi expérimentale (LLExp)[117] dont l'article unique prévoit que : « Une loi peut être établie à titre expérimental à condition : a) qu'elle soit limitée au temps strictement nécessaire à l'expérimentation ; b) qu'elle fixe le but de l'expérimentation et les hypothèses qu'elle cherche à vérifier ; c) que ses effets soient

113 Cf. AXA A9 ; Bâloise, F2 : « Les entreprises assurées doivent prendre des mesures de sécurité techniques et organisationnelles afin de garantir la confidentialité, l'intégrité et la disponibilité des données et des systèmes. Cette protection doit être adaptée à l'importance et la sensibilité des données et des processus et être conforme aux usages de la profession applicables en la matière [...] » ; cf. Zurich, art. 6 , « Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der ITSicherheit » : « Les assurés s'engagent à respecter les dispositions applicables relatives à la protection des données. Les entreprises assurées doivent notamment prendre les mesures techniques et organisationnelles de protection du réseau informatique et des données pendant toute la durée du contrat et garantir leur respect [...] ».

114 Selon l'étude du WEF (note 8), trois approches et stratégies étatiques peuvent entrer en ligne de compte afin de promouvoir la cyberassurance, p.57 : « Broadly speaking, a state may intervene at three levels in the insurance market, with increasing likelihood of private-sector adoption but increasing costs, as well : voluntary (no incentives) ; incentivized (e.g. tax deduction) ; and mandated insurance. If no incentives for insurance exist, the upfront costs are likely to be low but, in the long run, depending on how liability is defined, at some point cyber costs will be borne in an outsized fashion by some entity either in the private or public sector. These costs are likely to be greater in the absence of the security control adoption promoted by insurance. On the other end of the spectrum, an insurance mandate will lead to greater upfront costs for the private sector but to smaller costs in the long run as companies adopt security controls to minimize insurance costs » ; cette étude relève également que l'intervention étatique paraît la moins justifiée pour les PME selon le graphique figurant en p.58 du rapport.

115 Référence peut être faite ici au rapport du DETEC du 15 octobre 2019 (cf. note 17) concernant les recommandations du groupe d'expert qui indique à propos de la recommandation 25 sur les exploitants d'infrastructures critiques « [l]a Confédération et les cantons élaborent, en étroite collaboration avec les associations professionnelles, des normes de sécurité informatiques » et à la prise de position du Conseil fédéral qui indique que d'ici fin 2020 « le nouveau Centre de compétence en matière de cybersécurité examinera des normes de sécurité contraignantes et identifieront les solutions possibles, en collaboration avec d'autres offices et les cantons ».

116 Voir le Guide de législation, Guide pour l'élaboration de la législation fédérale, 4ème éd. 2019, Office fédéral de la Justice, (https://www.bj.admin.ch/dam/data/bj/staat/legistik/hauptinstrumente/gleitf-f.pdf), p. 269, exposant les principes devant être respectés lors de la création et de l'application d'actes législatifs à caractère expérimental.

117 Loi genevoise concernant la législation expérimentale du 14 décembre 1995 (A 2 35).

évalués dans un rapport remis sur le bureau du Grand Conseil au plus tard 3 mois avant la date prévue pour son expiration ». La loi expérimentale doit par ailleurs « déterminer le type de données à récolter, la démarche méthodologique, les critères d'appréciation de l'expérimentation et les organes responsables pour l'effectuer ».

[63] Les recommandations sont les suivantes :

4.1. Sensibiliser les PME aux cyberassurances

[64] Le présent article a démontré la complexité des exigences juridiques auxquelles doivent faire face les PME en matière de cybersécurité et les risques juridiques et financiers auxquels elles sont confrontées. Il a également démontré la grande diversité des offres de cyberassurance qui ne couvrent pas toutes les mêmes risques. Il en résulte ainsi un besoin de sensibiliser les PME aux cyberassurances et de leur fournir des moyens de mieux comprendre l'apport potentiel de celles-ci,[118] cette sensibilisation des PME aux cyberassurances pouvant être faite dans le contexte de la nécessité (toujours existante) de sensibiliser les PME en matière de cybersécurité et de gestion des cyberrisques.

[65] Les cyberassurances ne sont en effet que peu ou pas mentionnées dans les informations données aux PME en matière de cybersécurité[119], ce qui peut se concevoir vu l'absence actuelle de maturité du marché de la cyberassurance et de comparabilité des polices de cyberassurance.

[66] Les autorités publiques pourraient ainsi soutenir des initiatives visant à sensibiliser les PME aux cyberrassurances. A titre de comparaison, le gouvernement anglais a ainsi soutenu l'élaboration d'un guide pratique à l'attention des PME « Making Sense of Cyber Insurance : a Guide for SMEs » paru sous l'égide de l'Association of British Insurers (ABI).[120] Il pourrait ainsi être

118 Sur l'importance de sensibiliser les PME en matière de cyberassurance, voir aussi le Rapport Chubb, SME Cyber Claims are on the increase – Understand your business exposure, 2019, (https://www.chubb.com/uk/en/business/by-category/by-category-cyber-risks/assets/uk7439-md-0219-chubb_claims_sme_cyber_tl_1g.pdf) ; voir aussi le Rapport de l'ENISA (European Union Agency for Cybersecurity), Commonality of risk assessment language in cyber insurance, novembre 2017, p.46, (https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance) : « 5.4.3 Demand Side Evolution : The demand side for cyber insurance offerings in the EU is expected to grow significantly within the next few years and its evolution may be a key driver for carriers to adopt a more harmonized approach in their offerings. A key factor in this demand side evolution will be SMEs ; contrary to large organisations with internal Risk Management resources and complex environments, SMEs will likely pose different requirements, opting for standardized, understandable, easily comparable and transferable cyber insurance products. In order for carriers to tap this market segment, they will need to better communicate their offerings and to exhibit consistency in terminology, coverage types, policy triggers and pricing among others in order to build the buyers' trust ».

119 Ainsi, sur le plan national, à titre d'exemple, il pourrait être opportun de mentionner la question des cyberassurances dans le contexte des informations fournies aux PME en matière de cybersécurité, p.ex. dans le cadre des informations et documents mis à disposition par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI et en particulier le document « Sécurité de l'information : aide-mémoire pour les PME » (v. 2.0), 5 juillet 2018, p.2, (https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html). On notera aussi que, sur le plan international, le Guide de la Chambre de Commerce Internationale (CCI) ne fait pas non plus mention de la question des assurances pour cyberrisques, cf. Chambre de Commerce Internationale (ICC), Guide ICC de la cybersécurité à l'intention des entreprise, 2015, (https://iccwbo.org/content/uploads/sites/3/2016/11/ICC-Cyber-Security-Guidelines-for-Business-French-version.pdf).

120 Association of British Insurers (ABI), Making Sense of Cyber Insurance : A Guide for SMEs, 2016, https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/cyber-insurance/making-sense-of-cyber-insurance-a-guide-for-smes.pdf ; voir plus généralement le site : https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/. Cf. aussi l'association de l'industrie de l'assurance allemande (« Gesamtverband der Deutschen Versicherungswirtschaft e.V. ») qui a rédigé des conditions générales modèles (note 92).

opportun de développer des outils d'information et de sensibilisation sur la cyberassurance en faveur des PME (en coopération avec les acteurs du marché).

4.2. Assurer une standardisation des offres de cyberassurance

[67] Comme relevé précédemment (cf. 3.4.1.), la diversité des polices de cyberassurance rend difficile la comparaison entre celles-ci, particulièrement par les PME qui n'ont pas nécessairement les ressources et l'expertise pour procéder à une comparaison détaillée des offres disponibles.

[68] Même si certains acteurs du marché peuvent contribuer à faciliter la comparaison des offres de cyberassurance (notamment les courtiers d'assurance), il ne paraît pas superflu de recommander (comme cela a été fait à l'étranger)[121] que l'Etat soutienne une certaine standardisation des polices de cyberassurance afin de faire en sorte que celles-ci couvrent au moins certains risques minimaux. La question se pose en particulier pour les dommages résultant de violations du droit de la protection des données personnelles, notamment pour ce qui concerne l'assurabilité des amendes, mais aussi pour d'autres thématiques, p.ex. l'assurabilité des rançons payées, ce qui pourrait faire l'objet d'une clarification étatique.[122] En plus de ces questions concernant la portée de la couverture des polices d'assurance, l'attention devrait aussi être portée aux modes de résolution des litiges pouvant survenir entre preneurs d'assurance et cyberassureurs qui ne sont pas nécesssairement standardisés. On notera en effet l'intérêt qui a été exprimé (à l'étranger) de soumettre les litiges de cyberassurance à l'arbitrage plutôt qu'aux tribunaux étatiques (notam-

121 Cf. ENISA (note 118), p.50 : « 6.2 Recommendations towards Policy makers. The following recommendations are addressed to EU and Member State Policy Makers : (i) Create minimum coverage requirements per type of coverage on top of which insurers can build extra coverage. These requirements should define what should at least be included for each type of coverage to provide a common, comparable point of reference. For instance, providing a minimum definition of what should be covered under a data breach cover policy would increase consumer trust in products offering this coverage via clarity and transparency and it will not be limiting to carriers developing offerings on top of that ; (iii) Regulatory authorities could define these minimum coverage requirements as common definitions organically emerge from the insurance industry ; (iv) Minimum coverage requirements should be aimed at providing modules/building blocks and not at imposing insurance obligations to buyers ».

Cf. Rapport BIGS (note 11), p.60 : « Abbau von Informationsasymmetrien durch Versicherungsstandards und Datenbanken » ; voir aussi (https://www.gdv.de/de/themen/news/das-leistet-eine-cyberversicherung-31152 ; tableau accessible à : https://www.gdv.de/resource/blob/11198/aff433d8af06fdbd33f5d790826f3c4f/grafik-die-cyberversicherung-deckt---data.pdf).

122 OCDE (note 89), p. 25 : « Box 3.4. Supporting consistency in cyber insurance coverage : recommendations

- Insurance regulators and supervisors should encourage the harmonisation of coverage definitions and exclusions applied to cyber risks and monitor the level of claims disputes that arise due to ambiguous policy language – while taking into account the risk that any forced standardisation could stifle innovations in coverage. If sufficient convergence is not achieved in the near-term, governments should encourage industry associations to develop standardized language for voluntary use.

- Governments should provide a clear statement on the insurability of fines, penalties and ransoms in their jurisdiction. Any decision limiting insurability should consider the possibility of exceptions for : (i) situations where the insured was not directly negligent (in the case of fines) ; and/or (ii) in the case of ransom payments, where the payment of a ransom is necessary to avoid significant harm to life or property. A consistent approach to these issues across jurisdictions would reduce the risk of insurers providing coverage for uninsurable losses on a cross-border basis and support a level-playing field for insurance providers and policyholders.

- Where ransoms payments are insurable, governments should clarify (or confirm) the responsibility of insurance companies for ensuring compliance with relevant sanctions. Insurance companies' implementation of international sanctions in the context of cyber-extortion claims may require increased attention in supervisory reviews ».

ment pour des raisons de confidentialité)[123], ce qui pourrait faire l'objet d'une harmonisation des polices.

[69] Au-delà des conditions contractuelles de cyberassurance, il paraît également opportun de procéder à une standardisation de l'appréciation des risques par les cyberassureurs en vue de la conclusion de cyberassurances, soit la standardisation des processus permettant la conclusion de contrats d'assurance visant à donner aux assureurs l'occasion d'apprécier plus précisément les cyberrisques des preneurs.[124]

[70] Afin de créer des standards minimaux et homogènes relatifs à une couverture d'assurance minimale pour les cyberrisques (au-dessus de laquelle les assureurs peuvent proposer des couvertures supplémentaires), les autorités publiques pourraient ainsi :

- émettre des lignes directrices en matière de cyberassurance, qui détermineront notamment ce qui doit être inclus dans une couverture minimale afin d'avoir une référence commune et comparable. Par exemple, il pourrait donner une définition de ce que la couverture d'assurance inclut en cas de violation de la protection des données afin d'augmenter la confiance des clients quant aux offres proposées grâce à la transparence et la clarté (les assureurs pouvant offrir une couverture plus large sur la base d'offres complémentaires). Ces lignes directrices pourraient être émises en lien avec la très récente norme ISO/IEC 27102 :2019 (lignes directrices pour la cyber-assurance) qui donne des recommandations en matière de cyberassurances ;[125]
- établir des modèles de contrats (non obligatoires) vu la diversité des offres existantes et la difficulté de les comparer.[126] Ceci pourrait être fait en prenant le modèle de ce qui a été fait

123 Voir Andrew Nadolna/Adrienne Publicover/Daniel Garrie, Why Arbitration Clauses May Make Sense in Cyber Insurance Policies, Cardozo Journal of Conflict Resolution, Vol. 19, 2017, p. 43 (https ://cardozojcr.com/wp-content/uploads/2018/01/Why-Arbitration-Clauses-May-Make-Sense-in-Cyber-Insurance-Policies.pdf).

124 Cf. GDV Die Deutschen Versicherer, Unverbindlicher Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen, décembre 2019, (https://www.gdv.de/resource/blob/6102/aa4b9afe6fa3e23c51c598bd23194ba1/02-risikofragebogen-cyber-data.pdf) ; cf. ENISA (note 118).

125 ISO/IEC 27102 :2019 : Gestion de la sécurité de l'information – Lignes directrices pour la cyber-assurance, date de publication : août 2019 (https://www.iso.org/fr/standard/72436.html) dont l'objet y est présenté comme suit : « This document provides guidelines when considering purchasing cyber-insurance as a risk treatment option to manage the impact of a cyber-incident within the organization's information security risk management framework.

This document gives guidelines for :

a) considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks ;

b) leveraging cyber-insurance to assist manage the impact of a cyber-incident ;

c) sharing of data and information between the insured and an insurer to support underwriting, monitoring and claims activities associated with a cyber-insurance policy ;

d) leveraging an information security management system when sharing relevant data and information with an insurer.

This document is applicable to organizations of all types, sizes and nature to assist in the planning and purchase of cyber-insurance by the organization ».

126 Voir aussi (pour le marché américain) Wolff (note 9) : « State regulators should help provide insurers with standardized templates and wording developed in partnership with the Insurance Services Office for designating which risks are and are not covered under their policies. This will further help clarify for customers what risks they are purchasing protection for and enable clearer comparison across insurance policies for brokers and insurance holders ».

au Royaume-Uni avec un guide (Leitfaden) et aussi avec la base de données de la British Insurance Brokers' Association (BIBA) ;[127]

- établir des bonnes pratiques avec des terminologies et concepts homogènes pouvant être utilisés par les assureurs pour améliorer leurs questionnaires ainsi que des *standards de cybersécurité*. Ces bonnes pratiques et standards pourraient être établis à la lumière de normes existantes, dont les normes ISO/IEC 27001 et 27002 (cf. ci-dessus 2.1.) et en consultation avec les acteurs du marché pour inventorier d'éventuelles exigences spécifiques.

4.3. Contribuer au partage des données sur les cyberincidents entre les cyberassureurs

[71] Afin de pouvoir développer et affiner leurs solutions de cyberassurance sur le plan commercial (calcul du risque et des primes), les cyberassureurs auraient intérêt à pouvoir accéder aux données concernant les cyberincidents qui se sont produits. Des projets ont ainsi été initiés afin d'encourager l'industrie de l'assurance à partager ces données,[128] ce qui fait l'objet de travaux en cours notamment au sein de la « Geneva Association ».[129] Les autorités étatiques pourraient et devraient ainsi soutenir ce partage de données[130], ce dans le contexte des obligations légales de notification en cas de cyberincidents.[131]

---

127 HM Government & Marsh, UK Cyber Security – The Role of Insurance in Managing and Mitigating Risk, mars 2015, (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf).

128 The Geneva Association, The Geneva Association highlights the role of collaboration between cyber insurers, mars 2020, (https ://www.insurancebusinessmag.com/uk/news/cyber/the-geneva-association-highlights-the-role-of-collaboration-between-cyber-insurers-216954.aspx).

129 Cf. le projet de la Geneva Association, Exploring the opportunity for a Cyber Incident Data Exchange and Repository (CIDER), (https ://www.genevaassociation.org/news/articles-interest/exploring-opportunity-cyber-incident-data-exchange-and-repository-cider) : « In 2018, The Geneva Association initiated a study to explore the opportunity of building an international cyber claims and cyber incident database, the Cyber Incident Data Exchange and Repository (CIDER). By giving insurers access to a pool of anonymised data, such a tool would aim to assist them in better understanding threat vectors and impacts and in improving their ability to protect people and businesses from cyber incidents. CIDER is now moving from the conceptual to operational stage. The GA has developed a full proposal for CIDER's operating model : its legal and governance structures, IT requirements and taxonomy and a business plan. [. . .] CIDER is the first project of its kind to be collectively owned and driven by the insurance industry. In 2020–21, The Geneva Association Secretariat will focus its cyber work on the economic and societal importance of cyber resilience and the conditions for cyber insurability ».

130 Rapport BIGS (note 11), par. 2.1 p.59 : « Abbau von Informationsdefiziten durch Meldepflichten » ; voir aussi EIOPA (note 20), p.4 : « It is essential for the industry to further improve its assessments and data collection, so that cyber risks can be adequately measured, monitored and managed. Ultimately, having common and harmonized standards for both cyber risk measurement and reporting purposes could greatly facilitate the understanding of cyber risk underwriting. To this end, creating a European-wide cyber incident reporting database, based on a common taxonomy, could be considered as well » ; voir aussi Wolff (note 9) : « States should also consider requiring insurers to report aggregate claims data to state regulatory authorities on the correlations between different cybersecurity products, frameworks, and guidelines and claims data. This will help businesses, governments and researchers learn from the collected experience of insurers in trying to assess the effectiveness of different cybersecurity techniques, tools and services. It will also allow insurers to aggregate more data across their customer bases and develop stronger data sets to determine the cybersecurity best practices that yield better outcomes » ; voir aussi le tout récent rapport de l'OCDE (février 2020), Enhancing the Availability of Data for Cyber Insurance Underwriting : The Role of Public Policy and Regulation, (https://www.oecd.org/daf/fin/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf).

131 ENISA (note 118), p.50 : « Leverage the upcoming mandatory incident reporting schemes via the NIS Directive and the GDPR to produce meaningful data that could be used, among others, by the cyber insurance industry to expand its evidence base. Specific actions may include : (i) consulting the Cyber Insurance industry stakeholders to map specific industry requirements as to useful information ; (ii) Defining anonymization criteria that could

[72] A ce propos, on relèvera que les annonces de failles de sécurité, prévues dans la nLPD, dans le projet de loi sur la sécurité de l'information[132] et dans le RGPD (et dans la Directive NIS pour les opérateurs de services essentiels) permettraient aux autorités de collecter des données fiables, qui pourraient être agrégées pour déterminer l'impact des cyberincidents.

[73] Cas échéant et sous une forme à déterminer (p.ex. données agrégées anonymisées), certaines informations et conclusions tirées de ces données pourraient être partagées avec l'industrie de la cyberassurance afin d'affiner et d'améliorer leur offre de produits de cyberassurance. L'Etat pourrait ainsi contribuer à créer un dépôt central de cyberincidents pour avoir des données agrégées de sources multiples, permettre une collecte d'information par secteur et déterminer l'impact des incidents par secteur. Ce dépôt pourrait permettre de mettre à disposition des entreprises des données permettant aux compagnies d'assurance de mieux calculer leurs primes, ce qui peut être rendu difficile en raison d'un déficit d'information.[133] Il s'agira aussi de définir les critères d'anonymisation qui permettraient le partage des données avec l'industrie.

4.4. Créer des moyens d'incitation visant à la conclusion de cyberassurances par les PME

[74] Les autorités publiques pourraient envisager de prendre des mesures incitatives (notamment fiscales) afin de motiver la conclusion de cyberassurances par les PME, dans la mesure où la cybersécurité n'est pas seulement l'affaire individuelle des entreprises mais qu'elle touche toute la société.[134] Un facteur pourrait être de faire en sorte que les PME obtiennent des conditions d'assurance plus favorables dans le cas où elles respecteraient certains standards de sécurité (ce qui pourrait être confirmé par une certification, cf. 4.5. ci-dessous). En effet, des mesures peuvent être prises afin de créer des incitations pour que les entreprises respectent certains standards de cybersécurité dans le but de bénéficier de conditions d'assurance plus avantageuses (p.ex. primes réduites).[135] Ceci suppose que le gain résultant de cette opération (soit la réduction des primes)

---

make the data appropriate for sharing with the industry ; (iii) Incident reporting will lead to a static snapshot at the time the notification takes place so data needs to be updated over time and versioning control should be used ; (iv) create a central EU wide repository of incidents to provide aggregate data from multiple sources. Identify ways for sectorial ISACs to contribute to the data collection and to determine cross-sectorial impact of incidents ».

132 On notera que, à propos du projet de loi fédérale sur la sécurité de l'information, le Conseil fédéral a adopté le message y relatif le 23 février 2017 et le Conseil des Etats le Conseil national ont décidé d'entrer en matière le 26 septembre et 9 octobre 2018 mais de demander des améliorations au DPPS.

133 Voir EIOPA (note 20), p.4 : « It is essential for the industry to further improve its assessments and data collection, so that cyber risks can be adequately measured, monitored and managed. Ultimately, having common and harmonized standards for both cyber risk measurement and reporting purposes could greatly facilitate the understanding of cyber risk underwriting. To this end, creating a European-wide cyber incident reporting database, based on a common taxonomy, could be considered as well » ; voir aussi Wolff (note 9), « States should also consider requiring insurers to report aggregate claims data to state regulatory authorities on the correlations between different cybersecurity products, frameworks, and guidelines and claims data. This will help businesses, governments and researchers learn from the collected experience of insurers in trying to assess the effectiveness of different cybersecurity techniques, tools and services. It will also allow insurers to aggregate more data across their customer bases and develop stronger data sets to determine the cybersecurity best practices that yield better outcomes ».

134 Rapport BIGS (note 11), p.60 : « Die Erhöhung der IT-Sicherheit in einzelnen Unternehmen ist nicht nur vorteilhaft für das betreffende Unternehmen, sondern erhöht auch die Sicherheit in der vernetzten Gesellschaft insgesamt. Diese positiven Externalitäten können eine staatliche Subvention für Sicherheitszertifizierungen oder für Cyberversicherungen, welche die Sicherheitszertifizierung zur Bedingung haben, rechtfertigen ».

135 Voir US Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity insurance, 22 juin 2015 (https://www.cisa.gov/cybersecurity-insurance) : « Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity

soit supérieur au coût pour les entreprises concernées.[136] Ainsi, la cyberassurance pourrait contribuer non seulement au transfert du risque (du preneur à l'assureur, ce qui est le but premier de l'assurance) mais aussi à la réduction du risque. Dans cet esprit, la cyberassurance et les cyberassureurs (grâce aux mesures incitatives étatiques) pourraient jouer un rôle moteur dans la création d'un cadre de cybersécurité adéquat.[137]

4.5. Contribuer à créer un standard de certification des cyberassurances

[75] Les autorités publiques pourraient favoriser l'émergence de mécanismes de label ou de certification des produits de cyberassurance qui proviennent d'initiatives privées ou publiques.[138] On pense aux mécanismes suivants :

- labels conventionnels (i.e. normes privées édictées par des organismes privés, pouvant être enregistrées comme marques collectives ou de garantie), qui ne font l'objet d'aucune réglementation spécifique et sont généralement régulés par les lois du marché.[139]
- certifications (i.e. normes édictées par des organismes privés puis certifiées par un organisme de certification indépendant accrédité), prévues par les lois de protection des données, dont la LPD et la nLPD (ce qui permet d'alléger les responsables de traitement et sous-traitants de certaines obligations, art. 11 LPD, 12 P-LPD) et le RGPD (qui permet en outre à l'entreprise certifiée de démontrer sa conformité au RGPD, art. 42 RGPD).
- labels obligatoires (i.e. normes étatiques que tout prestataire doit respecter), tels que le marquage CE mis en œuvre dans l'UE pour garantir la conformité européenne et dont la mention est obligatoire. Précisons toutefois qu'un label obligatoire semble peu probable, en tous les cas dans le domaine de la protection des données personnelles. Le Conseil fédéral a en effet refusé d'inclure dans P-LPD la proposition de rendre obligatoire la certification des systèmes de traitement à risque élevé.

insurance market could help reduce the number of successful cyber attacks by : (1) promoting the adoption of preventative measures in return for more coverage ; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack. In recent years, the Cybersecurity and Infrastructure Security Agency (CISA) has engaged key stakeholders to address this emerging cyber risk area ».

136 Au Royaume-Uni, l'expérience visant à offrir des conditions de cyberassurances plus avantageuses en cas de respect des standards « Cyber essentials » ne s'est pas montrée pleinement concluante, dès lors que le coût de compliance était supérieur au gain résultant de la réduction des primes d'assurances, cf. Rapport BIGS (note 11), p.60.

137 Mark Camillo, Cyber risk and the changing role of insurance, in : Journal of Cyber Policy, Vol. 2, Issue 1, 2017, 2 :1, pp.53–63, (https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878) : « [...] the insurance industry will become a de facto regulator, setting the bar for the standards necessary to qualify for cyber coverage. Insureds will need to demonstrate that they have met certain cyber hygiene and pre-loss standards in order to obtain indemnification and, increasingly, these requirements will extend to the supply chain as part of the procurement process. This is not a new role for the insurance industry. In the same way that insurers drove greater safety standards in the property insurance market, setting up the first fire departments in the seventeenth century following the Great Fire of London in 1666 and later encouraging the installation of sprinkler systems and other fire-fighting technology, the insurance industry will help to drive best practice around cybersecurity as the twenty-first century progresses ».

138 Pour un aperçu des différents mécanismes d'auto-régulation, cf. Alexandre Flückiger, (Re)faire la loi : traité de légistique à l'ère du droit souple, 2019, p.325 ss, (https://archive-ouverte.unige.ch/unige:116477).

139 Dans le domaine des services, on peut se référer aux labels en matière de sécurité de l'information (p.ex. norme ISO/IEC 27001, Tier I-IV, (https://www.iso.org/fr/isoiec-27001-information-security.html)).

[76] Les autorités publiques pourraient ainsi soutenir des initiatives de labels privés et certifications en matière de cybersécurité et/ou identifier et lister les labels privés considérés comme fiables et conformes à certaines normes de sécurité qu'elles communiqueraient aux entreprises désireuses d'adhérer à des standards de sécurité. De telles initiatives ont été lancées, à l'image du label Cybersafe émis par l'Association suisse pour le label de cybersécurité, et pourraient continuer d'être soutenues. Plus spécifiquement en matière de cyberassurance, les autorités publiques pourraient développer, ou contribuer à développer avec les acteurs concernés, des normes minimales qu'une couverture d'assurance devrait respecter (p.ex. terminologie commune, risques couverts, cf. ci-dessus 4.2.), qui pourraient ensuite faire l'objet d'une certification. Par comparaison, aux Etats-Unis, la Cyberspace Solarium Commission (CSC)[140] a récemment proposé une certification en matière de cyberassurance visant à instaurer des normes minimales que les polices d'assurance doivent respecter, notamment être équitables et raisonnables et ne contenir aucune lacune mal comprise par l'assuré quant aux risques couverts.[141]

4.6. Envisager l'imposition d'une cyberassurance obligatoire dans certaines circonstances (p.ex. marchés publics)

[77] Comme exposé précédemment, il n'existe à l'heure actuelle aucune obligation de conclure une cyberassurance en Suisse et, si une telle obligation devait être envisagée, elle ne concernerait vraisemblablement pas les PME qui sont utilisatrices de produits et services technologiques fournis par d'autres entreprises mais éventuellement ces dernières entreprises qui créent des cyberrisques particuliers (cf. ci-dessus 3.1.).

[78] Vu la difficulté à introduire une cyberassurance obligatoire générale, les autorités publiques pourraient limiter la question d'une cyberassurance obligatoire à certains cas, potentiellement aux parties contractantes dans le cadre de marchés publics, comme cela est projeté en Californie pour certains contrats conclus avec l'Etat présentant des risques pour les données personnelles.[142] Les conditions et modalités d'une telle assurance devraient aussi être spécifiées, notamment l'existence potentielle d'un droit d'action direct du lésé envers l'assurance et l'opposabilité des exceptions.[143] Les autorités publiques pourraient ainsi conditionner la soumission ou l'adjudication de marchés publics à la conclusion préalable d'une cyberassurance, ce qui garantirait ainsi que les entreprises concernées soient couvertes par une assurance contre les cyberincidents,[144]

---

140 Cette Commission a été établie pour développer une approche stratégique pour défendre les Etats-Unis contre les cyber-incidents (« develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences »). Voir note 21.

141 Cf. US Cyberspace Solarium Commission 2020 (note 21), p.80 : « *Cyber Insurance Product Certification :* State insurance regulators can and often do set minimum standards that insurance products must meet in order to be offered in their state », thereby « ensuring that insurance policy provisions comply with state law, are reasonable and fair, and do not contain major gaps in coverage that might be misunderstood by consumers and leave them unprotected [...]. The FFRDC should develop cybersecurity product certifications based on a common lexicon and security standards ».

142 Anne Hobson/Ian Adams, California dreams about cyber insurance, and federal lawmakers should pay attention, 3 mars 2020, (https ://thehill.com/opinion/cybersecurity/486427-california-dreams-about-cyber-insurance-federal-lawmakers).

143 Par exemple comme cela est prévu à l'art. 65 al. 1 LCR s'agissant du droit d'action directe qui prévoit que « [d]ans la limite des montants prévus par le contrat d'assurance, le lésé peut intenter une action directe contre l'assureur » et à l'art. 65 al. 2 LCR s'agissant des exceptions disposant que « [l]es exceptions découlant du contrat d'assurance ou de la loi fédérale du 2 avril 1908 sur le contrat d'assurance ne peuvent être opposées au lésé ».

144 Cf. Assembly Bill No. 2320, February 14, 2020, section 1, chapter 2.3, 10601,

et contribuer à la gestion de certains cyberrisques systémiques. Une telle condition pourrait être toutefois considérée comme une modification du Règlement sur la passation des marchés publics (RMP), en particulier les conditions pour être admis à soumissionner (art. 31 ss RMP) ou pour l'adjudication (art. 43 ss RMP).[145]

4.7. Contribuer à la gestion de certains cyberrisques systémiques

[79] Les autorités publiques pourraient enfin contribuer à assurer la prise en charge et à l'absorption de certains cyberrisques de nature systémique (p.ex. terrorisme, cyberguerre), soit de risques qui ne se limitent pas à affecter des entreprises individuelles mais qui portent au contraire atteinte à toute la société et vise ainsi la cybersécurité de l'Etat comme tel.[146] Des recommandations ont ainsi été formulées sur le plan international[147] et à l'étranger, notamment afin de faire en sorte que l'Etat participe à la prise en charge de l'assurance / réassurance de certains cyberrisques systémiques, particulièrement en matière de cyberterrorisme ou de cyberguerre.[148] De telles initiatives doivent naturellement être organisées en coopération avec les parties prenantes.[149]

[80] Une telle approche pourrait conduire à inclure les risques de cyberguerres[150]/cyberterrorismes dans les polices de cyberassurance (à certaines conditions cas échéant). C'est ce qui a été fait au Royaume-Uni par le gouvernement et le réassureur Pool Re qui couvre les risques du terrorisme et qui devrait couvrir les risques du cyberterrorisme depuis 2018.[151] C'est également ce qui pourrait se faire aux Etats-Unis en lien avec le Further Consolidated Appropriations Act 2020 selon la Cyberspace Solarium Commission évoquée précédemment.[152]

(http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB2320) : « If the contract contemplates that, in the course of doing business with an agency, a contractor will receive or have access to records containing personal information protected under the Information Practices Act of 1977 (Title 1.8 (commencing with Section 1798) of Part 4 of Division 3 of the Civil Code), the contract shall require the contractor to carry cyber insurance sufficient to cover all losses resulting from potential unlawful access to or disclosure of personal information, in an amount determined by the contracting agency ».

145 Règlement sur la passation des marchés publics du 17 décembre 2007 (RMP ; L 6 05.01).

146 La distinction entre cyberrisques systémiques et non-systémiques peut être complexe ; pour une analyse, voir James E. Scheuermann, Cyber Risks, Systemic Risks, and Cyber Insurance, 122 Penn St. L. Rev. 613 (2018).

147 Cf. OCDE (note 89), p.13 : « Governments should clarify the availability and scope of (re)insurance coverage through terrorism (re)insurance programmes for cyber-terrorism and other politically-motivated (and destructive) cyber-attacks – and address any gaps that may emerge due to the application of exclusions by the insurance sector. » ; voir aussi cet autre rapport de l'OCDE, Insurance Coverage for Cyber Terrorism in Australia, février 2020, (www.oecd.org/finance/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.htm), accès direct : (http://www.oecd.org/daf/fin/insurance/Insurance-Coverage-for-Cyber-Terrorism-in-Australia.pdf).

148 Rapport BIGS (note 11), p.60 : « Der Staat als Rückversicherer bei Angriffen, deren eigentliches Ziel der Staat ist (Terrorismus) ».

149 Voir le projet en cours de la Geneva Association en matière de cyberterrorisme (note 129) : « The Geneva Association's Cyber programme, under Carter's leadership, is now working on another initiative regarding cyber terrorism and cyber warfare : a collaboration with various organisations that cover terrorism and/or cyber terrorism, and which is operating under the auspices of the International Forum of Terrorism Risk (Re)Insurance (IFTRIP) ».

150 Pour une discussion de la notion de cyberguerre dans les polices d'assurance, voir Daniel W. Woods/Jessica Weinkle, Market Definitions of Cyber War, in : Conference on Cyber Norms : Dealing with Uncertainty, 2019, (https://ssrn.com/abstract=3464218).

151 Rapport BIGS (note 11), p.60.

152 US Cyberspace Solarium Commission 2020 (note 21), p.82.

5. Conclusion

[81] Sur la base de l'analyse conduite et pour répondre à la question constituant le titre de la présente contribution, on peut considérer que la cyberassurance constitue un instrument utile pour assurer la cybersécurité des entreprises.

[82] Toutefois, en dépit de son utilité parmi les différents moyens visant à assurer la cybersécurité de la société en général et des PME en particulier, la cyberassurance ne constitue pas la solution ultime qui permettrait de résoudre tous les défis posés par la cybersécurité,[153] cela d'autant moins que le marché de la cyberassurance est en pleine évolution[154] et qu'il mérite assurément des analyses additionnelles dans une perspective interdisciplinaire.[155]

[83] Quoi qu'il en soit, on doit considérer que les cyberassureurs pourraient avoir un rôle important à jouer au-delà de leur fonction de couverture du risque économique de leurs clients assurés, comme moteur de prévention et de protection contre les cyberrisques, de par la contribution qu'ils peuvent faire à l'établissement d'un écosystème offrant un degré adéquat de cybersécurité.[156] Les cyberassureurs sont en effet susceptibles de contribuer significativement à la cyberhygiène des entreprises qui sont leurs clientes en leur fournissant des services de soutien (visant la prévention et la gestion des cyberincidents), non seulement après la survenance d'un cyberincident, (de manière réactive et réparatrice), mais aussi en amont de manière préventive sous forme de services d'assistance (forensiques, gestion de crise, gestion de la communication) mais également sur le plan technologique.

[84] Bien que la question de la cyberassurance relève à l'heure actuelle essentiellement de l'autonomie privée et de la libre décision de chaque entreprise, elle appelle néanmoins une attention accrue des autorités publiques, comme le montre l'activité très importante sur ces questions en particulier aux Etats-Unis, le plus grand marché actuel de la cyberassurance.[157] Les cyberrisques sont en effet susceptibles d'affecter toute entreprise de tout secteur. Les cyberrisques peuvent en outre souvent être viraux et s'attaquer ainsi à tout un écosystème, de par le fait que nombre d'entreprises (particulièrement les PME) sont fortement dépendantes en matière de technologie de l'information et recourent ainsi largement à des sociétés tierces pour leur fournir les services dont elles ont besoin, ce qui contribue à créer des cyberrisques.[158]

---

153 Cf. US Cyberspace Solarium Commission 2020 (note 21), p.81 : « Cyberinsurance is not the silver bullet to solve the nation's cybersecurity challenges. Indeed, a robust and market for cybersecurity insurance is not an end in and of itself, but a means to improve the cybersecurity of the U.S. private sector and the security of the nation as a whole in cyberspace ».

154 De même que celui de la cyber-réassurance, cf. p.ex. la très récente annonce de lancement d'un nouveau produit de cyber-réassurance par Swiss Re et Capsicum Re, Swiss Re and Capsicum Re deliver « Decrypt » – a holistic cyber reinsurance solution, 2 septembre 2019, (https://www.swissre.com/media/news-releases/nr-20190902-new-holistic-cyber-solution-decrypt.html).

155 Falco Gregory/Eling Martin/Danielle Jablanski/Mathias Weber/Virginia Miller/Lawrence A. Gordon/Shaun Shuxun Want/Joan Schmit/Russell Thomas/Mauro Elvedi/Thomas Maillart/Emy Donavan/Simon Dejung/Eric Durant/Franklin Nutter/Uzi Scheffer/Gil Arazi/Gilbert Ohana/Herbert Lin, Cyber risk research impeded by disciplinary barriers, in : Science, Vol. 366, Issue 6469, novembre 2019, pp.1068–1069 : « Cyber risk management today mainly focuses on prevention, whereas risk-transfer instruments such as insurance are in their infancy ».

156 Rapport BIGS (note 11), p.63.

157 Andrew G. Simpson, U.S. Cybersecurity Report Calls for Major Government Role in Cyber Insurance, 20 mars 2020, (https://www.insurancejournal.com/news/national/2020/03/11/560918.htm).

158 Il est ainsi nécessaire d'intégrer le risque des sous-traitants IT dans la gestion des risques par les entreprises clients / PME (comme le font certaines polices de cyberassurance), cf. Kessler (note 106), p.22 : « On oublie trop souvent les cyberrisques émanant des sous-traitants IT. Force est de constater que les entreprises subissent de plus

[85] Les autorités publiques peuvent ainsi juger opportun de prendre certaines mesures visant à favoriser voire à imposer la conclusion de cyberassurances telles que celles qui font l'objet des recommandations formulées dans le présent article, ce afin de faire en sorte que les PME puissent se protéger contre les cyberrisques qui sans doute ne feront qu'augmenter à l'avenir. Dans cette perspective, les cyberassurances peuvent constituer un instrument utile visant à protéger les entreprises contre les cyberrisques.

Jacques de Werra, professeur à la Faculté de droit de l'Université de Genève et directeur du Centre de Droit du Numérique (www.digitallawcenter.ch).

Yaniv Benhamou, docteur en droit, chargé de cours à la Faculté de droit de l'Université de Genève, Centre de Droit du Numérique, et avocat-conseil (*Of Counsel*) en droit de la propriété intellectuelle, des données et des nouvelles technologies.

Les auteurs remercient vivement Mme Ana Andrijevic, assistante et doctorante au Centre de Droit du Numérique, pour ses recherches et son aide précieuse, ainsi que M. Siroos Tanner, auxiliaire de recherche et d'enseignement au Centre de Droit du Numérique, pour son aide à la finalisation de l'article.

Tous les sites web ont été consultés pour la dernière fois le 14 août 2020.

en plus fréquemment des attaques par le biais de leurs sous-traitants IT. Plus la dépendance vis-à-vis de partenaires d'externalisation externes est grande, plus la défaillance de ces derniers devrait être intégrée dans la gestion des cyberrisques de l'entreprise. Dans l'idéal, l'accent devrait être mis sur l'ensemble de la chaîne de création de valeur. A l'heure actuelle, les entreprises ne peuvent plus être considérées isolément ».