Université de Montréal

Sécurité informationnelle des systèmes cyberphysiques et risques à la santé et sécurité : quelle responsabilité pour le fabricant ?

par
Hugo Fournier-Gendron

Faculté des études supérieures
Faculté de droit

Mémoire présenté à la Faculté de droit
en vue de l'obtention du grade de Maîtrise
en droit des technologies de l'information (LL.M.)

Décembre 2017

Résumé

Les systèmes cyberphysiques (S.C.P.) sont des objets informatisés disposant d'une connectivité aux réseaux numériques et dont la fonction première est d'agir sur le monde physique. Parmi les exemples de tels systèmes, on retrouve les voitures autonomes, les stimulateurs cardiaques intelligents et certains objets connectés de l'Internet des objets (I.d.O.). En raison de leur nature, ils ont la possibilité de causer un préjudice physique grave à la suite d'une faille de sécurité informationnelle. Le présent mémoire a pour but de dégager, des principes du droit québécois, un cadre de responsabilité civile extracontractuelle applicable au fabricant d'un système cyberphysique et capable d'appréhender les particularités d'une problématique à la frontière des mondes virtuels et physiques.

Mots-clés : Responsabilité civile, responsabilité extracontractuelle, responsabilité du fait des biens, responsabilité du fabricant, défaut de sécurité, risques de développement, sécurité informationnelle, cybersécurité, système cyberphysique, internet des objets, objets connectés, robots.

Abstract

Cyber-physical systems (CPS) are computerised objects with network capabilities that act on the physical world. Examples of such systems include autonomous vehicles, intelligent pacemakers and some devices in the Internet of Things (IoT). Due to their nature, they may cause important injury in the physical domain as a result of a cybersecurity breach. This master's thesis aims at uncovering, from the principles of liability law in Quebec, an extra-contractual liability framework applicable to the manufacturer of cyber-physical systems and capable of approaching the specificities of a problem set at the border between the virtual and physical realms.

Keywords: civil liability, extra-contractual liability, liability from the act of a thing, manufacturer liability, safety defect, cyber-security, cyber-physical system, internet of things, connected thing, robots.

Table des matières

Liste des tableaux

Liste des figures

Liste des sigles et abréviations

C.c.B.C.	Code civil du Bas-Canada
C.c.Q.	Code civil du Québec
C.Cr.	Code criminel
C.I.A.	Confidentialité, Intégrité, Accessibilité (disponibilité)
C.N.S.S.	*Committee on National Security Systems*
C.O.B.I.T.	*Control Objectives for Business and Related Technology*
C.P.S.	*Cyber-Physical System*
C.P.S.P.W.G.	*Cyber-Physical System Public Working Group* (N.I.S.T.)
C.V.E.	*Common Vulnerabilities and Exposures*
C.V.S.S.	*Common Vulnerability Scoring System*
D.A.R.P.A.	*Defense Advanced Research Projects Agency*
D.D.o.S.	*Distributed Denial of Service*
D.I.C.	Disponibilité, Intégrité, Confidentialité
D.I.C.A.I.	Disponibilité, Intégrité, Confidentialité, Authenticité, Irrévocabilité
D.N.S.	*Domain Name System*
D.o.S.	*Denial of Service*
E.C.U.	*Electronic Command Unit*
E.N.I.A.C.	*Electronic Numerical Integrator and Computer*
F.D.A.	*Food and Drug Administration*
F.T.C.	*Federal Trade Commission*
G.A.S.S.P.	*Generally Accepted System Security Principles*
I.d.O.	Internet des objets

I.E.E.E.	*Institute of Electrical and Electronics Engineers*
I.o.T.	*Internet of Things*
I.R.M.	*Information Risk Management*
I.S.O.	*International Organisation for Standardization*
L.C.C.J.T.I.	Loi concernant le cadre juridique des technologies de l'information
L.P.C.	Loi sur la protection du consommateur
L.P.R.P.D.E.	Loi sur la protection des renseignements personnels et des documents électroniques
L.P.R.P.S.P.	Loi sur la protection des renseignements personnels dans le secteur privé
M.C.E.	Module de commande électronique
N.I.S.T.	*National Institute of Standards and Technology*
N.R.C.	*National Research Council*
N.S.F.	*National Science Foundation*
N.V.D.	*National Vulnerability Database*
O.Q.L.F.	Office québécois de la Langue Française
O.R.C.C.	Office de révision du Code civil
P.C.	*Personal Computer*
R.F.I.D.	*Radio Frequency Identification*
S.C.P.	Système cyberphysique
S.F.P.B.Q.	Service de la formation permanente du Barreau du Québec

Remerciements

Je tiens à exprimer ma reconnaissance envers mon directeur de recherche, M. Nicolas W. Vermeys, pour sa disponibilité, sa compréhension et ses nombreux conseils tout au long de la rédaction de ce mémoire de maîtrise.

Merci à mes amis, qui m'ont permis de conserver un semblant de santé mentale, ainsi qu'à ma conjointe, pour ses encouragements durant le dernier droit de ce travail. Je tiens enfin à remercier mes parents pour leur amour et leur soutien indéfectibles depuis le début de mon parcours académique.

Introduction

Le 14 février 1946, l'Armée américaine dévoilait l'*Electronic Numerical Integrator and Computer*[1], le premier ordinateur électronique à usage général[2]. Développé dans le plus grand secret au courant de la Seconde Guerre mondiale par des chercheurs dirigés par J. W. Mauchly et J. Presper Eckert Jr., de la *Moore School of Electrical Engineering*, il devait permettre d'accélérer drastiquement le calcul des tables balistiques nécessaires à l'effort de guerre[3]. Malgré sa désuétude lorsqu'on le compare aux ordinateurs modernes, E.N.I.A.C. débuta sa carrière en faisant en seulement deux heures une série de calculs qui auraient demandé environ un siècle à une personne seule[4].

E.N.I.A.C. calcula des trajectoires balistiques jusqu'en 1955, mais servit également pour la recherche scientifique[5]. Bien qu'il fût vite surpassé par d'autres ordinateurs, il eut une influence majeure sur le développement des technologies de l'information. Il ouvrit la voie à de nouvelles possibilités, et on considère aujourd'hui que ce fut le prototype de la plupart des ordinateurs modernes[6].

Les formidables capacités de ces nouvelles machines firent évidemment rêver, et on voulut vite étendre leur domaine d'application. Aussi a-t-on conçu le désir d'employer des ordinateurs afin, par exemple, d'automatiser un procédé industriel[7]. Mais E.N.I.A.C. et ses contemporains ne s'intéressaient que de calcul. Que celui-ci requiert trente secondes ou une dizaine de minutes leur était indifférent, tant qu'ils arrivaient à la bonne réponse. Il fallait attendre 1973 pour que soient développés les premiers ordinateurs capables de planifier leurs

---

[1] Ci-après « **E.N.I.A.C.** ».
[2] WAR DEPARMENT, BUREAU OF PUBLIC RELATIONS, « Ordnance Department Develops All-Electronic Calculatic Machine », en ligne : <http://americanhistory.si.edu/comphist/pr1.pdf> (consulté le 12 décembre 2017) ; Steven LEVY, « The Brief History of the ENIAC Computer », *Smithsonian Magazine*, Novembre 2013, en ligne : https://www.smithsonianmag.com/history/the-brief-history-of-the-eniac-computer-3889120/ ; William T. MOYE, « ENIAC: The Army-Sponsored Revolution », Janvier 1996, en ligne : http://ftp.arl.mil/~mike/comphist/96summary/index.html (consulté le 12 décembre 2017).
[3] W. T. MOYE, préc., note 2.
[4] WAR DEPARMENT, préc., note 2.
[5] W. T. MOYE, préc., note 2.
[6] S. LEVY, préc., note 2 ; W. T. MOYE, préc., note 2.
[7] Kyoung-Dae KIM et P. R. KUMAR, « Cyber-Physical Systems: A Perspective at the Centennial », (2012) 100 *Proceedings of the IEEE*, p. 1288.

tâches pour arriver à un résultat dans un temps déterminé[8]. Cette innovation importante permit aux ordinateurs de s'infiltrer de plus en plus dans le contrôle des procédés industriels en temps réel[9]. Ce fut l'occasion d'un premier point de contact direct entre l'espace numérique et le monde physique.

Au fil des décennies qui suivirent, les technologies de l'information ne se cantonnèrent cependant pas aux procédés industriels. De moins en moins couteux et de plus en plus puissants, les ordinateurs entrèrent sur le marché des consommateurs, où leur croissance fut explosive : à la fin de 1976, plus de 40 000 ordinateurs personnels avaient été vendus au total, alors que pour la seule année de 1990, 16 000 000 d'ordinateurs du type « P.C. » d'I.B.M. entraient sur le marché[10].

À mesure qu'il devenait clair qu'on était en présence d'une véritable révolution technologique, l'ambition d'une rencontre entre les mondes physique et virtuel se sophistiquait également. En 1991, dans « *The Computer for the 21st Century* », Mark Weiser proposait une vision du futur dans laquelle les ordinateurs s'intégraient dans tous les objets de la vie courante :

> « *The most profound technologies are those that disappear. The weave themselves into the fabric of everyday life until they are indistinguishable from it.* »[11]

Selon cette conception, le monde virtuel n'est pas destiné à évoluer séparément du monde physique. Au contraire, les deux doivent s'entrecroiser pour créer un domaine cyberphysique – celui de « l'information omniprésente »[12] – où même les objets les plus insignifiants sont animés par algorithme. Un classeur pourrait alors présenter automatiquement le document voulu dès qu'on s'approche de lui. Une bibliothèque saurait indiquer à ses usagers l'emplacement exact d'un livre, quand bien même il aurait été égaré sur une table de travail. Une salle de conférence adapterait automatiquement son éclairage et sa configuration selon le

---

[8] K. KIM et P. R. KUMAR, préc., note 7, p. 1288 ; C. L. LIU et James W. LAYLAND, « Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment », (1973) 20-1 *Journal of the Association for Computing Machinery*, p. 46.
[9] C. L. LIU et J. W. LAYLAND, préc., note 8.
[10] Jeremy REIMER, « Total Share: 30 Years of Personal Computer Market Share Figures », (15 décembre 2005) *Ars Technica*, en ligne : <https://arstechnica.com/features/2005/12/total-share/> (consulté le 12 décembre 2017).
[11] Mark WEISER, « The Computer for the 21st Century », (septembre 1991) *Scientific American*, p. 100.
[12] En anglais, « *ubiquitous computing* ».

contexte et ses occupants[13]. Dans le paradigme que Mark Weiser proposait en 1991, les ordinateurs sont partout et leurs algorithmes enrichissent le monde physique.

Même s'il devait être tentant, à l'époque, de voir dans ces exemples une sorte de projet fantasque relevant de la science-fiction, la vision de Mark Weiser inspira beaucoup ses contemporains. À sa suite, certains auteurs prédisent aujourd'hui que le 21e siècle pourrait bien être celui de la construction à très grande échelle de ces systèmes à nature double[14], et d'autres parlent même d'un « monde cyberphysique » où l'informatique est si omniprésente qu'elle converge avec le monde physique[15]. Dans tous les cas, notamment avec le développement de l'« Internet des objets »[16], il semble que l'histoire donnera raison à Mark Weiser. Son article donna une impulsion vers l'intégration plus poussée des domaines physique et virtuel, et l'étude de systèmes dits « hybrides » (à la fois physiques et virtuels) est apparue vers cette époque[17].

Au courant des années suivantes, trois apports majeurs permirent d'approfondir cette intégration. En premier lieu, on trouve le développement de la réseautique et des diverses technologies de communication qui interviennent aujourd'hui quotidiennement dans nos vies. Entre autres choses, soulignons l'apparition de la technologie Ethernet en 1980 et du standard I.E.E.E. 802.11 en 1997 (lequel a répandu la technologie Wi-Fi), deux technologies qui permirent le déploiement à grande échelle d'un réseau capable de connecter l'ensemble des ordinateurs de la planète : Internet[18]. Le développement parallèle des réseaux de téléphonie mobile est également pertinent, en permettant à un ensemble d'appareils mobiles de se connecter eux aussi en ligne. Puis, en 1999, le centre *Auto-ID* du *Massachusetts Institute of Technology* débuta ses travaux sur l'identification d'objets à l'aide d'ondes radio, préfigurant ce qu'on appellera plus tard l'I.d.O.[19] Ils standardisèrent à cette fin une technologie appelée *Radio*

[13] Ces exemples proviennent de M. WEISER, préc., note 11.
[14] K. KIM et P. R. KUMAR, préc., note 7, p. 1289.
[15] Marco CONTI et al., « Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence », (2012) 8 *Pervasive and Mobile Computing*, p. 2.
[16] Ci-après « l'**I.d.O.** ». Nous parlerons plus en détail de l'I.d.O. dans le corps de ce mémoire.
[17] K. KIM et P. R. KUMAR, préc., note 7, p. 1288.
[18] *Id.*
[19] Dave EVANS, « The Internet of Things : How the Next Evolution of the Internet is Changing Everything », (avril 2011) *Cisco Internet Business Solutions Group White Paper*, p. 2, en ligne : <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> (consulté le 12 décembre 2017).

Frequency Identification[20] pour doter chaque objet d'un identifiant numérique répondant par ondes radio – une sorte de code-barres sophistiqué. Désireux d'exploiter les possibilités d'une telle identification, les chercheurs du centre *Auto-ID* proposèrent notamment un système de gestion de chaîne logistique capable de suivre le déplacement des stocks, dont chacune des unités était identifiée par puce R.F.I.D., le tout afin d'augmenter l'efficacité des procédés de l'industrie manufacturière[21]. Ils développèrent un protocole permettant aux identifications R.F.I.D. d'être reconnues sur le réseau Internet, afin de faire en sorte qu'un seul réseau puisse relier l'ensemble des objets du monde physique[22]. C'était le départ d'une tendance qui allait faire d'Internet le médium principal de communication de l'universalité des objets connectés[23].

En second lieu, la technologie des capteurs voit un développement accéléré depuis les années 1990[24]. Par exemple, en 1997, la *Defense Advanced Research Projects Agency*[25] subventionna le projet « *Smart Dust* » afin de construire des capteurs miniaturisés (de la taille d'un grain de riz), capables de communiquer par ondes électromagnétiques[26]. On suggérait de les disséminer sur un champ de bataille, afin qu'ils fournissent des informations cruciales aux soldats, telles que la position de troupes ennemies[27]. L'apparition de ces capteurs autonomes et leur sophistication subséquente a permis d'enrichir les systèmes d'information d'un accroissement exponentiel de données sur l'environnement pour leur permettre d'accomplir des tâches plus exigeantes[28].

---

[20] INTERNATIONAL TELECOMMUNICATION UNION, « The Internet of Things – Executive Summary », (2005) *ITU Internet Reports*, p. 8, en ligne : <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf> (consulté le 12 décembre 2017) ; Ci-après « **R.F.I.D.** ».

[21] Duncan McFARLANE et al., « Auto ID systems and intelligent manufacturing control », (2003) 16 *Engineering Applications of Artificial Intelligence*, p. 365.

[22] Sanjay SARMA, David L. BROCK et Kevin ASHTON, « The Networked Physical World », (2000) *Auto-ID Center White Paper*, p. 4.

[23] Abdullah Yasin NUR et Mehmet Engin TOZAL, « Defending Cyber-Physical Systems Against DoS Attacks », (2016) *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, p. 1.

[24] K. KIM et P. R. KUMAR, préc., note 7, p. 1288.

[25] Aussi connu sous son sigle : « D.A.R.P.A. ».

[26] Kristofer S. J. PISTER, « Smart Dust », *BAA 97-43*.

[27] *Id.*, p. 4.

[28] K. KIM et P. R. KUMAR, préc., note 7, p. 1288 ; John D. McGREGOR, David P. GLUCH et Peter H. FEILER, « Analysis and Design of Safety-critical, Cyber-Physical Systems », (2016) 36-2 *ACM SIGAda Ada Letters*.

En troisième lieu, on trouve l'accroissement des capacités des ordinateurs. Inspirée d'un article publié par le cofondateur d'Intel en 1965, la loi de Moore[29] a prédit correctement un rythme de croissance exponentiel de plusieurs caractéristiques des technologies de l'information, dont la performance en termes de rapidité de calcul, la miniaturisation et l'abordabilité des ordinateurs, lesquels ont diversifié les possibilités de leur application. Les composantes informatiques demandent également de moins en moins d'énergie, ce qui les rend plus mobiles. Notons au passage que ces améliorations ont également permis l'apparition des téléphones intelligents et autres appareils mobiles tout aussi capables que les ordinateurs. Bien entendu, les développeurs de logiciels n'ont pas tardé à tirer avantage de ces capacités croissantes : nous avons vu l'apparition de programmes informatiques sans cesse plus puissants, propulsés par les méthodes de plus en plus sophistiquées de l'intelligence artificielle[30].

Nourris de ces différentes innovations[31] ainsi que par un appétit social et économique croissant pour des systèmes plus efficaces, notamment dans les domaines du transport, de la gestion des ressources et de la santé[32], les systèmes physiques contrôlés par ordinateur et disposant d'une connectivité aux réseaux atteignent des capacités jusqu'alors inégalées. Au milieu des années 2000, l'expression « systèmes cyberphysiques »[33] apparaît afin de décrire ces objets[34], dont l'étude et la conception pourraient même devenir une nouvelle spécialisation de l'ingénierie[35].

La rencontre entre le monde physique et virtuel entraîne un changement de paradigme dans les technologies de l'information. Cet évènement sera certainement fécond en possibilités

---

[29] Gordon E. MOORE, « Cramming More Components onto Integrated Circuits », (1965) *Electronics*, p. 114-117, réimprimé dans (1998) 76-1 *Proceedings of the IEEE*, p. 83 et suiv. Cette prédiction est restée essentiellement confirmée depuis sa formulation en 1965 et jusqu'à tout récemment, où nous rencontrons un certain ralentissement.
[30] Celles, par exemple, qui relèvent de l'apprentissage automatique.
[31] Voir notamment : Ragunathan (Raj) RAJKUMAR et al., « Cyber-Physical Systems: The Next Computing Revolution », *Proceedings of the 47th Design Automation Conference*, (2010), p. 731 : « *The promise of CPS is* pushed *by several recent trends: the proliferation of low-cost and increased-capability sensors of increasingly smaller form factor; the availability of low-cost, low-power, high-capacity, small form-factor computing devices; the wireless communication revolution; abundant internet bandwidth; continuing improvements in energy capacity, alternative energy sources and energy harvesting.* »
[32] K. KIM et P. R. KUMAR, préc., note 7, p. 1289.
[33] Ci-après « **S.C.P.** ». En anglais, « *cyber-physical systems* » ou « *C.P.S.* ».
[34] K. KIM et P. R. KUMAR, préc., note 7, p. 1288.
[35] NATIONAL RESEARCH COUNCIL, *Interim Report on 21st Century Cyber-Physical Systems Education*, Washington (D.C.), The National Academies Press, 2015, p. 19 ; R. RAJKUMAR et al., préc., note 31, p. 734.

et en problématiques nouvelles. Parmi les défis posés par les S.C.P., on trouve notamment celui de la cybersécurité, une préoccupation partagée par la plupart des Canadiens[36]. Comme le système agit sur le monde physique, une faille de sécurité informationnelle peut avoir des incidences sur ce plan et causer un préjudice physique important. Les dégâts ne sont plus limités au vol d'identité ou à la seule destruction, altération ou diffusion non autorisée de données :

> « *[…] connected devices are "safe" as long as our identity is not stolen; however, the use of CPS can pose real physical threats to the health of humans simply due to product defects.* »[37]

Un exemple nous permettra d'appréhender ce danger nouveau. Depuis quelques années, les chercheurs s'intéressent à la sécurité informationnelle des systèmes à bord des véhicules[38], qui peuvent être qualifiés de S.C.P., tel que nous le verrons dans ce mémoire. Au courant des années 1970, les fabricants automobiles commencèrent à installer à bord de leurs voitures des « modules de commande électronique »[39], sortes d'ordinateurs de bord qui avaient pour rôle de contrôler électroniquement le mélange carburant / oxygène dans le moteur afin d'en réduire les émissions polluantes. Aujourd'hui, ils remplissent la plupart des fonctions à bord des automobiles[40], et ont souvent une incidence dans le monde physique. Fréquemment mis en commun par un réseau interne, ils visent par exemple à faire le lien entre le volant et la direction des roues, transmettre les commandes au moteur ou aux freins lorsque le conducteur appuie sur les pédales, afficher des renseignements sur le tableau de bord ou permettre le déverrouillage des portes. Ce sont également eux qui accomplissent des tâches plus exigeantes du point de vue computationnel, comme le contrôle des freins A.B.S., de la transmission, ainsi que les fonctions

---

[36] SÉCURITÉ PUBLIQUE CANADA, *Rapport : sondage auprès des utilisateurs d'Internet au sujet de la cybersécurité*, (2017), en ligne : <https://www.pensezcybersecurite.gc.ca/cnt/rsrcs/rsrch-fr.aspx> (consulté le 12 décembre 2017).

[37] J. D. McGREGOR, D. P. GLUCH et P. H. FEILER, préc., note 28, p. 1.

[38] Voir par exemple : Ulf E. LARSON et Dennis K. NILSSON, « Securing vehicules against cyber attacks », (2008) *CSIIRW'08: Proceedings of the 4th annual workshop on Cyber security and information intelligence research*, p. 1-3 ; P. R. THORN et C. A. MACCARLEY, « A spy under the hood : Controlling risks and automotive EDR », (2008) *Risk Management* ; M. WOLF, A. WEIMERSKIRCH et C. PAAR, « Security in automotive bus systems », (2004) *Proceedings of the Workshop on Embedded Security in Cars 2004* ; M. WOLF, A. WEIMERSKIRCH et T. WOLLINGER, « State of the art : Embedding security in vehicules », (2007) *EURASIP Journal on Embedded Systems* ; Y. ZHAO, « Telematics: safe and fun driving », (2002) 17-1 *Intelligent Systems*.

[39] Ci-après « **M.C.E.** ». En anglais, « *Engine Control Unit* », ou « *E.C.U.* ».

[40] Karl KOSCHER et al., « Experimental Security Analysis of a Modern Automobile » (2010) *2010 IEEE Symposium on Security and Privacy*, p. 448.

de pilotage ou de stationnement automatisé. En somme, les voitures contemporaines sont animées par un ensemble interconnecté de plusieurs dizaines de M.C.E., sur lesquels repose la bonne marche du véhicule et la sécurité de ses passagers.

En 2010, un groupe de chercheur, intéressé par la nature de plus en plus informationnelle du fonctionnement des véhicules, a voulu déterminer leur niveau de résilience face à une attaque informatique[41]. Leurs résultats portent à croire que ce niveau est, en somme, assez bas. Sans réelle difficulté, ils ont pu entrer dans le réseau interne du véhicule et y introduire des commandes destinées aux différents M.C.E., qui les exécutaient en n'effectuant presque aucune vérification à l'égard de leur authenticité. Les attaques ont été exécutées avec succès sur une automobile immobilisée et en mouvement sur un circuit fermé, en se connectant au réseau interne du véhicule par l'entremise d'un dispositif branché dans le port de service du véhicule. Ils ont même pu injecter leur propre code informatique à bord des M.C.E., afin notamment de cacher leurs traces en supprimant automatiquement les modifications qu'ils avaient effectuées. Ainsi ont-ils pu contrôler la radio du véhicule, de même que les données affichées par les instruments du tableau de bord. Ils ont pu verrouiller et déverrouiller les portes, ouvrir le coffre, activer le klaxon, ou coincer la clé dans le commutateur d'allumage.

Plus inquiétant encore, ils ont pu contrôler le moteur du véhicule, notamment en modifiant sa vitesse de rotation, en lui envoyant des commandes contradictoires pour troubler son fonctionnement interne et causer des contrecoups dommageables, ou, enfin, en le désactivant carrément en envoyant le signal factice que les coussins gonflables avaient été déployés. De même, les chercheurs ont facilement pu faire serrer les freins, les quatre à la fois ou individuellement, ou au contraire les desserrer sans qu'il soit possible de les réactiver, même lorsque le véhicule circulait sur la route[42]. Bon nombre de ces modifications ne pouvaient être corrigées par le conducteur.

Les chercheurs s'étonnaient de la facilité avec laquelle ils avaient pu manipuler directement des M.C.E. qui accomplissaient portant des fonctions essentielles à la sécurité des

[41] K. KOSCHER et al., préc., note 40, p. 448.
[42] *Id.*, p.455-457.

passagers[43]. Ils ont découvert que les standards existant pour assurer la sécurité des M.C.E. étaient à la fois déficients et souvent incorrectement mis en place par les fabricants. Ils s'inquiétaient en outre qu'un M.C.E. issu d'une entreprise tierce, par exemple une radio installée par l'acheteur du véhicule, puisse compromettre l'ensemble des systèmes de bord[44].

En 2015, deux chercheurs sont allés encore plus loin. Dans une affaire qui fit les manchettes, ils ont démontré qu'ils pouvaient prendre le contrôle total d'un véhicule à distance par l'entremise seulement d'un ordinateur portable[45]. Dans leur rapport, ils décrivent comment ils ont pu se connecter au module de radio d'un Jeep Cherokee 2014[46], qui acceptait les requêtes Internet de n'importe quelle source sans procéder à quelconque vérification de sécurité. Ils purent alors sans grande difficulté entrer sur le réseau interne du véhicule et d'envoyer des commandes de nature cyberphysique aux différents M.C.E. L'attaque ne requérait aucune action du conducteur, et pouvait être complétée sans jamais avoir un accès physique au véhicule[47]. En plus des manipulations qui avaient été démontrées en 2010, ils découvrirent de nouvelles attaques, rendues possibles par l'ajout de fonctions nouvellement disponibles. En exploitant le module de stationnement automatique, par exemple, ils ont pu contrôler la direction du véhicule. C'est ce qui leur fait dire : « *as new technology is added to vehicules, new attacks become possible* »[48]. Afin de dévoiler le résultat de leurs recherches au grand public, ils s'associèrent à un journaliste du magazine *Wired*, à qui ils firent une bonne frousse en désactivant la voiture par le biais d'Internet, alors qu'elle circulait sur l'autoroute[49].

---

[43] K. KOSCHER et al., préc., note 40, p. 459.
[44] *Id.*, p. 460.
[45] Charlie MILLER et Chris VALASEK, *Remote Exploitation of an Unaltered Passenger Vehicule*, 2015, p. 5, en ligne : <http://illmatics.com/Remote%20Car%20Hacking.pdf> (consulté le 12 décembre 2017).
[46] *Id.* Dans ce modèle automobile, le module radio accomplissait beaucoup de tâches computationnelles, par exemple gérer la connectivité cellulaire aux services télématiques (le service « UConnect » de Chrysler), Bluetooth, WiFi, GPS et autres, tout en étant sur le même réseau interne que les M.C.E. qui accomplissaient des fonctions essentielles à la sécurité.
[47] *Id*. p. 48. Ces caractéristiques rendent possible un type particulièrement inquiétant d'attaque : un virus (un « *worm* ») qui, une fois installé dans un véhicule, chercherait d'autres véhicules à exploiter pour les infecter automatiquement – par exemple ceux qu'ils croiseraient sur la route. Dans leur rapport, les auteurs implorent : « *Please don't do this. Please.* ».
[48] Id., p. 5.
[49] GREENBERG, Andy, « Hackers Remotely Kill a Jeep on the Highway – With Me In It », (21 juillet 2015) *Wired*, en ligne : <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> (consulté le 20 décembre 2017).

Évidemment, tout développement technologique aura des incidences sur le droit. L'apparition d'objets opérant dans le domaine cyberphysique ne fait pas exception. Auparavant, on pouvait considérer que les gestes commis dans la sphère virtuelle n'auraient que peu ou prou d'effets physiques directs, et donc qu'il était improbable que le droit de la responsabilité du fait des biens soit appelé à en traiter. Aujourd'hui, avec la venue des S.C.P., ce n'est manifestement plus le cas. Le juriste doit s'adapter à ce changement de paradigme. Dans ce mémoire, nous tentons de faire un pas dans cette direction.

Parmi les nouvelles questions juridiques qui émergent à la suite d'une rencontre entre les domaines physiques et virtuels, on trouve le cas de la responsabilité du fabricant d'un S.C.P. en cas de préjudice physique causé par une défaillance informatique.

De là se pose un ensemble d'autres problèmes. Quand peut-on considérer qu'un S.C.P., objet à nature à la fois virtuelle et physique, peut être visé par le cadre de responsabilité du fait des biens ? Doit-il au contraire être abordé du point de vue de l'obligation de sécurité informationnelle ? La responsabilité du développeur logiciel pourrait-elle être visée en raison d'un apport à la conception du bien assimilable à celui d'un fabricant, même s'il n'a aucune contribution « matérielle » au bien ? Et qu'est-ce qu'une faille de sécurité informationnelle dans un S.C.P. ?

Nous avons voulu, dans la mesure du possible, nous abstenir de nous adonner à un exercice de *création de législation*, mais en nous bornant à dégager le plus logiquement possible la solution permise par les règles préexistantes. Cette approche nous a ultimement poussés à nous demander si le droit québécois de la responsabilité extracontractuelle avait les outils pour traiter efficacement de la venue des objets cyberphysiques, ou si ses principes de bases ne suffisent pas et doivent être bonifiés. Nous croyons que le cadre de responsabilité pour le fabricant que nous présenterons au courant de ce mémoire nous permettra de montrer que le droit québécois, sans être absolument parfait, fournit déjà une réponse adéquate à la problématique cyberphysique, de même qu'on a considéré qu'il fournissait, en somme, une solution satisfaisante à l'avènement du cyberespace et d'Internet[50].

[50] Nicolas W. VERMEYS, *Droit codifié et nouvelles technologies : le Code civil*, Montréal, Éditions Yvon Blais, 2015, p. 124.

Nous espérons que le lecteur ne nous reprochera pas de nous concentrer aussi arbitrairement sur une fine tranche de la problématique entraînée par les S.C.P. Assurément, il n'est pas possible d'appréhender toute la richesse des questions juridiques soulevées par ces nouveaux objets dans un mémoire de maîtrise. C'est pourquoi nous avons voulu nous limiter à un cas d'étude qui nous semble intéressant : celui de la responsabilité extracontractuelle du fabricant en cas de préjudice physique causé par une faille de sécurité informationnelle dans un S.C.P. À cette fin, nous avons choisi de traiter des régimes de responsabilité du fabricant édicté aux articles 1468, 1469 et 1473 C.c.Q., et de l'obligation de sécurité informationnelle, à l'exclusion des nombreux autres qui peuvent s'appliquer dans des situations analogues. En outre, nous avons omis d'aborder directement les questions de partage de responsabilité qui, généralement complexifiées dans le domaine numérique[51], auraient obscurci nos raisonnements aux fins du présent travail.

Au courant de la préparation de ce mémoire, nous avons été confrontés à deux problèmes opposés. D'une part, une surabondance de sources techniques a parfois rendu difficile d'identifier l'information pertinente. D'autre part, nous avons constaté une certaine pauvreté des sources juridiques traitant de la problématique cyberphysique – qui est, il est vrai, somme toute assez nouvelle. Nous espérons avoir pu tirer notre épingle du jeu afin de proposer une réflexion utile et intéressante, en dépit de ces obstacles.

Le lecteur trouvera ce mémoire organisé selon un plan cartésien. Dans la première partie, nous présenterons les éléments pertinents de la problématique. Dans le chapitre A, nous traiterons du sujet de notre mémoire, les S.C.P., en rapportant d'abord la définition que la littérature technique a donnée pour ces objets. Puis, nous parlerons des domaines où ils sont appelés à trouver application. Nous prendrons soin, également, de distinguer les S.C.P. d'autres concepts analogues (objets connectés dans l'I.d.O. et robots). Enfin, nous dirons un mot sur la qualification juridique de ces objets nouveaux. Dans le chapitre B, nous exposerons dans l'abstrait les tenants et aboutissants des cadres juridiques que nous nous sommes proposé d'étudier : le cadre de la responsabilité du fabricant pour défaut de sécurité d'un bien meuble et celui de l'obligation de sécurité informationnelle.

[51] N. W. VERMEYS, préc., note 50, p. 142.

Dans la seconde partie, nous travaillerons à résoudre notre problématique en jonglant avec les différents concepts présentés jusque-là. Ainsi, dans le chapitre A, nous verrons quelles sont les incidences de la problématique cyberphysique sur les cadres de responsabilité présentés dans la première partie. Enfin, dans le chapitre B, nous aurons tous les éléments en main pour construire un cadre de responsabilité extracontractuelle applicable au fabricant d'un S.C.P. et capable d'appréhender les particularités d'une problématique cyberphysique.

PREMIÈRE PARTIE : LES SYSTÈMES CYBERPHYSIQUES ET LA SÉCURITÉ EN DROIT QUÉBÉCOIS

La problématique relative à la responsabilité du fabricant d'un produit causant un dommage physique à la suite d'une défaillance informatique est complexe. Elle met en jeu un certain nombre de notions tant techniques que juridiques qu'il convient de présenter adéquatement afin qu'il soit possible, par la suite, de voir émerger les critères qui nous permettront de construire un cadre juridique adéquat.

Dans le chapitre A suivant immédiatement cette introduction, nous parlerons de l'objet principal de notre étude : les S.C.P., notion peut-être méconnue, mais appelée sans doute à prendre de plus en plus d'importance. Nous en dresserons d'abord un portrait technique, pour ensuite discuter de leurs applications possibles et les distinguer des notions qui leur sont analogues – objets connectés dans l'I.d.O. et robotique. Ensuite, nous ferons quelques remarques sur leur qualification juridique, sous l'angle du droit des biens, puis sous celui du droit des technologies de l'information.

Ensuite, nous exposerons dans le chapitre B les deux cadres juridiques que nous avons choisis, tel que nous l'avons exposé dans notre introduction, pour appréhender la question de la responsabilité des fabricants d'un S.C.P. lorsque la défaillance informatique de celui-ci cause un dommage physique – en l'absence de lien contractuel liant les parties. Rappelons qu'il s'agit du régime de la responsabilité extracontractuelle du fabricant pour défaut de sécurité mis en place par l'article 1468 C.c.Q., ainsi que celui de la responsabilité relative à la sécurité informationnelle. Cette dernière exposée, nous aurons le vocabulaire pour dire un mot sur les enjeux en cybersécurité créés par les S.C.P.

A. Les systèmes cyberphysiques

Au courant de la préparation de ce mémoire, nous nous sommes demandé assez longuement comment qualifier les objets qui nous intéressent, à savoir les systèmes physiques contrôlés par algorithme, disposant de connectivité aux réseaux, et pouvant causer un dommage physique en raison d'une défaillance informatique. Il existe certes un certain nombre de

conceptions concurrentes, mais toutes ne servent pas nos fins aussi judicieusement. Au terme de notre démarche, nous nous sommes arrêtés sur la notion de « *système cyberphysique* », qui a le mérite d'apporter précisément le cadre théorique recherché pour traiter de la question que nous nous étions posée.

1. Qu'est-ce qu'un système cyberphysique ?

a) Définition et caractéristiques techniques

L'expression « système cyberphysique » est apparue relativement récemment dans la littérature[52]. Dit simplement, les S.C.P. sont des systèmes formés par la mise en synergie de trois éléments de base : (1) des composantes physiques (2) des composantes virtuelles, et (3) une connectivité aux réseaux numériques[53], tel qu'il appert de la figure 1 reproduite ci-après.

[52] Selon le site de Google « *Ngram Viewer* », qui permet d'illustrer sur un graphique la fréquence d'occurrence d'un terme dans la somme des livres numérisés par Google à travers le temps, l'expression « cyber physical », dans son sens actuel, est entrée en usage un peu avant l'an 2000. Voir, en ligne : https://books.google.com/ngrams/ (avec l'expression de recherche « cyber=>physical ») (consulté le 12 décembre 2017).

[53] Voir par exemple : Radhakistan BAHETI et Helen GILL, « Cyber-physical Systems », dans Tariq SAMAD et Anuradha ANASWAMY (dir.), *The Impact of Control Technology*, IEEE Control Systems Society, 2011, en ligne : <http://ieeecss.org/general/impact-control-technology> (consulté le 12 décembre 2017) ; Alvaro A. CARDENAS, Saurabh AMIN et Shankar SASTRY, « Secure Control: Towards Survivable Cyber-Physical Systems », (2008) *The 28th International Conference on Distributed Computing Systems Workshops* 495 ; CYBER PHYSICAL SYSTEMS PUBLIC WORKING GROUP (N.I.S.T.) (ci-après le « **C.P.S.P.W.G.** »), *Framework for Cyber-Physical Systems*, Release 1.0, 2016, en ligne : <https://pages.nist.gov/cpspwg/> (consulté le 12 décembre 2017) ; Siddhartha Kumar KHAITAN et James D. McCALLEY, « Design Techniques and Applications of Cyberphysical Systems: A Survey », (2015) 9-2 *IEEE Systems Journal* ; K. KIM et P. R. KUMAR, préc., note 7 ; Edward A. LEE, « Cyber-Physical Systems – Are Computing Foundations Adequate? », (2006) *Position Paper for NSF Workshop on Cyber-Physical Systems: Reserach Motivation, Techniques and Roadmap*, en ligne : <https://ptolemy.eecs.berkeley.edu/publications/papers/06/CPSPositionPaper/> (consulté le 12 décembre 2017) ; Edward A. LEE, « Cyber Physical Systems: Design Challenges », (2008) *11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC)* ; J. D. McGREGOR, D. P. GLUCH et P. H. FEILER, préc., note 28 ; A. R. NUR et M. E. TOZAL, préc., note 23 ; R. RAJKUMAR et al., préc., note 31 ; Jianhua SHI, Jiafu WAN et Hehua YAN, « A Survey of Cyber-Physical Systems », (2011) *Proceedings of the International Conference on Wireless Communications and Signal Processing, Nanjing, China, November 9-11*.

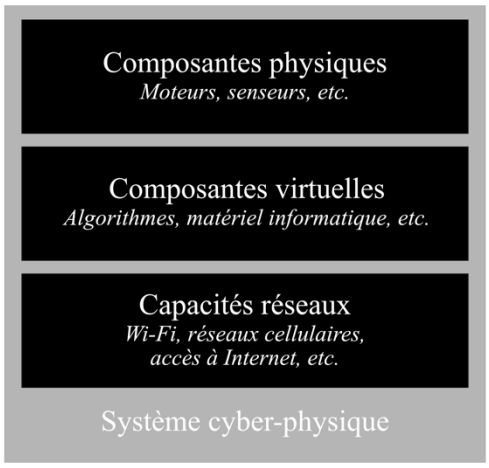

Figure 1 : schéma – composantes essentielles d'un S.C.P.

Les auteurs techniques ont évidemment formulé cette définition chacun à leur façon. Ainsi peut-on lire : « *Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components* »[54], ou « *Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components* »[55], ou encore : « *Cyber-physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world* »[56]. Un juriste a exprimé cette idée plus simplement encore : « *Cyberphysical systems [are] computers that act in and on the physical world* »[57].

La fonction première des S.C.P. est d'interagir avec le monde physique[58]. C'est leur particularité déterminante, surtout lorsqu'on les compare avec les systèmes informatiques qu'on pourrait qualifier de « traditionnels », et qui n'ont pour fonction que le seul traitement de données. Les S.C.P. ont une vocation plus large[59]. Ils peuvent viser à assurer le contrôle de flux énergétiques (réseau électrique), de la matière (oléoducs, fret), des signaux (contrôle aérien), la

[54] C.P.S.P.W.G., préc., note 53.
[55] NATIONAL SCIENCE FOUNDATION, *Cyber-Physical Systems (CPS) Program Solicitation NSF 17-529*, en ligne : <https://www.nsf.gov/pubs/2017/nsf17529/nsf17529.pdf> (consulté le 12 décembre 2017).
[56] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53, p. 495.
[57] Bryant WALKER SMITH, « Automated Driving and Product Liability », (2017) *Mich. St. L. Rev.* 1, p. 1.
[58] R. BAHETI et H. GILL, préc., note 53, p. 1.
[59] J. SHI, J. WAN et H. YAN, préc., note 53, p. 1.

transformation de matière (procédés industriels ou relatifs aux matières premières), ou encore animer plus « intelligemment » des objets (véhicules autonomes, robots)[60]. En intégrant des composantes des domaines virtuels et physiques, on peut dire que les S.C.P. évoluent à l'intersection de ces deux mondes, et les problèmes qu'ils posent – notamment ceux de la sécurité – deviennent de nature cyberphysique.

Il est vrai, cependant, que les systèmes physiques contrôlés par algorithme ne sont pas si inédits, et que certainement ils précèdent l'expression « système cyberphysique »[61]. Que justifie donc cette appellation nouvelle ? L'apport réellement nouveau est de prendre en compte la tendance à intégrer, désormais à bon marché, une connectivité avancée dans des objets qui auparavant fonctionnaient en circuit fermé. À cet égard, on peut dire qu'un système physique contrôlé informatiquement devient un S.C.P. dès lors qu'on y ajoute une fonctionnalité de connexion aux réseaux lui permettant d'interagir avec les utilisateurs ou avec d'autres systèmes, ce qui multiplie les possibilités associées à ces objets.

Mais il découle de la connectivité inhérente des S.C.P. une autre particularité qui justifie l'emploi du terme : c'est l'ampleur possible de leur déploiement. En effet, la technologie réseau permet des applications interactives qui ne sont plus cantonnées à un seul lieu. Il devient alors concevable de créer des « systèmes de systèmes », déployés à grande échelle, et qui comprennent une variété très hétérogène de dispositifs en constante communication afin de remplir des objectifs complexes – bien qu'un S.C.P. peut être composé d'un seul appareil[62].

Les S.C.P. sont favorisés en outre par les avancées dont bénéficient toutes les technologies de l'information : augmentation des capacités de calcul, miniaturisation, réduction des coûts et optimisations énergétiques se conjuguent aux nouveaux développements en intelligence artificielle afin de créer des systèmes dont le comportement est de moins en moins

[60] C.P.S.P.W.G., préc., note 53, p. 45.
[61] En effet, certaines technologies qui peuvent être qualifiés de S.C.P. sont au cœur de certains systèmes de contrôle industriel et d'infrastructure depuis plusieurs années déjà, voir des décennies. Voir : Alvaro A. CARDENAS et al., « Challenges for Securing Cyber Physical Systems », (2009) *Workshop on Future Directions in Cyber-physical Systems Security*, en ligne : <https://chess.eecs.berkeley.edu/pubs/601/cps-security-challenges.pdf> (consulté le 12 décembre 2017).
[62] K. KIM, et P.R. KUMAR, préc., note 7, p. 1296 ; C.P.S.P.W.G., préc., note 53, p. 46.

préprogrammé et de plus en plus autonome[63]. Par ailleurs, ils peuvent évidemment s'enrichir des possibilités apportées par les médias sociaux et des techniques tirant profit des mégadonnées[64], ou encore de l'informatique mobile et des téléphones intelligents, de même que de l'infonuagique[65].

Ceci dit, revenons à notre définition de base, à propos de laquelle il faut faire encore quelques précisions importantes. Nous avons dit qu'à la base, les S.C.P. sont composés de trois parties essentielles : les composantes physiques, virtuelles et les capacités réseau. Prenons soin de bien comprendre la portée de ces termes.

Un premier obstacle réside dans les expressions « composante physique » et « virtuelle ». À première vue, on pourrait penser qu'une composante physique est tout objet qui réside dans le monde réel, et que l'expression « composante virtuelle » fait référence à ce qui n'existerait que dans la sphère numérique, comme les logiciels et les données. Autrement dit, on pourrait penser que la désignation « physique » ou « virtuelle » se rattache à la *nature* de la composante. Mais il n'en est pas ainsi. Au contraire, la catégorisation d'une composante effectuée par la littérature technique préfère dépendre de la *fonction* de la composante.

En effet, l'expression « composante physique » ne fait pas référence à la *matérialité* de la composante elle-même. Elle n'est pas « physique » en raison du simple fait qu'elle existe dans le monde réel (par opposition aux logiciels, par exemple) – mais en raison de sa *vocation* à agir directement sur celui-ci. Une composante est donc « physique » lorsque sa fonction est,

---

[63] C.P.S.P.W.G., préc., note 53, p. 46 ; Radha POOVENDRAN, « Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds », (2010) 98-9 *Proceedings of the IEEE* 1363, p. 1363.

[64] C.P.S.P.W.G., préc., note 53, p. 46 ; OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (ci-après « **O.Q.L.F.** »), « Le grand dictionnaire terminologique », en ligne : <http://www.granddictionnaire.com/index.aspx> (consulté le 12 décembre 2017) – « mégadonnées » : « Ensemble des données produites en temps réel et en continu, structurées ou non, et dont la croissance est exponentielle. […] Les mégadonnées, à cause de leur démesure, deviennent impossibles à gérer avec des outils classiques de gestion de bases de données. Elles proviennent notamment des médias sociaux, des photos et des vidéos numériques transmises en ligne, des signaux des systèmes de localisation GPS, des téléphones intelligents, des relevés de transactions électroniques, des données publiques mises en ligne, etc. Elles servent à comprendre le présent et à faire des prédictions pour l'avenir. Le téraoctet, l'exaoctet et le pétaoctet sont les unités utilisées pour mesurer les mégadonnées. » On utilise le terme mégadonnées pour traduire l'expression anglaise « *big data* ».

[65] O.Q.L.F., préc., note 64, « infonuagique » : « Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. »

par exemple, de prélever des données sur le monde ou de poser sur lui une action directe. Parmi celles-ci, on retrouve tout actuateur[66] (un moteur) agissant sur le monde réel, ainsi que tout senseur ou capteur, lequel peuvent être appelés à mesurer tout type de propriété physique — température d'un corps ou d'un environnement, accélération, sons, poids, location précise d'un objet, présence d'une personne dans un espace, et son identité[67].

A contrario, un microprocesseur ne serait pas considéré comme une composante physique, en dépit de son évidente matérialité, parce que sa fonction première est le traitement de données. On devine donc que l'expression « composante virtuelle » fait référence à toute composante ayant pour *vocation* d'agir dans le monde algorithmique. Une composante virtuelle n'a donc pas besoin d'être dématérialisée (comme l'est un logiciel, par exemple) pour être qualifiée comme telle. Une composante virtuelle peut relever tant de *l'aspect numérique* (l'algorithme, qui sert notamment à interpréter les données recueillies par les composantes du S.C.P.[68], et les données elles-mêmes), que du *matériel informatique*[69] (par exemple le microprocesseur, le support de mémoire, ou toute autre composante qui remplit des fonctions de calcul). Ici, il faut éviter une autre confusion possible dans les termes : celle qui nous conduirait à assimiler ce matériel informatique à des « composantes physiques ». Bien que « matériel informatique », dans le langage courant, vise les processeurs, les cartes graphiques et autres dispositifs du genre, et même si, bien entendu, ces objets existent dans le monde physique, ils ont pour vocation première d'agir dans le monde virtuel et doivent par conséquent être considérés comme des composantes virtuelles.

Ces subtilités derrière nous, faisons une précision sur le troisième et dernier pilier de la définition des S.C.P. : la « connectivité aux réseaux numériques ». En raison notamment de la complexité des problèmes qu'ils sont appelés à résoudre, les S.C.P. sont fréquemment appelés à interagir avec les utilisateurs ou avec d'autres systèmes, que ce soit pour partager des données ou pour emprunter des capacités de calcul supérieures à des serveurs dédiés. Cette interaction se fait le plus souvent par le biais d'Internet, mais également par d'autres technologies de

[66] La littérature technique englobe tous les objets qui *agissent* directement sur le monde physique dans le terme anglais « *actuator* ».
[67] Jeffrey VOAS, « Networks of 'Things' », *NIST Special Publication 800-183*, 2016, p. 2, en ligne : <http://dx.doi.org/10.6028/NIST.SP.800-183> (consulté le 12 décembre 2017).
[68] *Id.*, p. 4.
[69] C'est-à-dire le « *hardware* », en anglais, par opposition au terme « *software* ».

communication comme Bluetooth ou les réseaux cellulaires. En outre, les S.C.P. sont souvent appelés à communiquer avec un serveur distant maintenu par le fabricant lui-même, afin de synchroniser des données générées par l'utilisateur, par exemple. Il est donc important de remarquer que le rôle du fabricant d'un S.C.P. peut ne pas se limiter à la seule fabrication du système : bien souvent, il agira également comme prestataire de services informatique tout au long de son cycle de vie[70].

C'est la synergie entre ces trois composantes de base qui offre aux S.C.P. un important avantage en termes d'efficacité, de flexibilité, d'autonomie, et de fiabilité sur les systèmes moins élaborés[71]. Ils deviennent alors une option intéressante pour une foule d'applications, dont certaines étaient jugées trop complexes pour la mise en place d'une gestion par ordinateur. Mais les S.C.P. ont également leur part de contraintes nouvelles.

En effet, il découle plusieurs conséquences intéressantes de la vocation des S.C.P. d'agir sur le monde physique, ainsi que de la coordination entre leurs composantes physiques et virtuelles. D'abord, il est essentiel que le fabricant d'un S.C.P. prenne en compte les parts physiques et virtuelles dès les premières étapes de la conception du système. Une parfaite synergie entre ces deux domaines est évidemment cruciale si on veut s'assurer d'un bon fonctionnement. Il n'est plus possible, comme il pouvait l'être auparavant, que les parts logicielles et physiques d'un système soient développées séparément : la littérature technique souligne à maintes reprises que les S.C.P. requièrent une stratégie de développement conjointe[72], notamment en raison des tâches beaucoup plus complexes (et plus dangereuses) qu'ils sont appelés à remplir. Ce besoin d'une nouvelle approche afin de mieux appréhender les S.C.P. a par ailleurs poussé certains acteurs à demander la mise en place d'un nouveau champ de recherche en ingénierie et dans les technologies de l'information[73].

Ensuite, puisque les S.C.P. agissent sur le physique, la dimension temporelle de leur fonctionnement prend une importance qui n'existait pas dans les systèmes informatiques

---

[70] Ce cycle de vie des données peut être divisé en quatre étapes : conservation, consultation, transmission et transmission. La *Loi concernant le cadre juridique des technologies de l'information* (articles 17 à 37), dont nous parlerons bientôt, reprend cette division.
[71] NATIONAL RESEARCH COUNCIL, préc., note 35, p. *ix*.
[72] *Id.*
[73] S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 350.

traditionnels. Une action prise trop tôt ou trop tard pourrait avoir des conséquences dramatiques sur le monde physique. C'est donc que les S.C.P. doivent avoir une perception de leur environnement soit adéquate et mise à jour en temps utile, et doivent pouvoir poser des gestes en temps opportun.

De même, puisqu'ils sont appelés à prendre des « décisions » dans la vie de tous les jours – laquelle compte bien sûr une part inhérente de chaos – les S.C.P. doivent pouvoir continuer d'assurer leur fonctionnement même lorsque surviennent des évènements impondérables qui n'avaient pas été anticipés par leurs concepteurs. Un S.C.P. doit donc disposer d'une certaine autonomie dans la gestion des erreurs qu'il rencontrera inévitablement, que ces erreurs soient internes ou externes, sans pour autant mettre en péril ses utilisateurs. Ainsi, ils doivent généralement requérir peu d'intervention humaine une fois qu'ils sont mis en marche.

Ceci nous amène à une dernière remarque : du fait de leur nature cyberphysique, toute défaillance informatique d'un S.C.P. peut causer des dommages physiques parfois irréparables aux biens et aux personnes. La section prochaine, qui explore certaines des applications des S.C.P., nous permettra d'apprécier plus concrètement l'ampleur de ce risque. C'est donc que lorsqu'on parle des S.C.P., tant la sécurité informationnelle que physique deviennent des considérations importantes. Nous détaillerons en quoi la cybersécurité S.C.P. est digne d'intérêt à la fin du chapitre B de la présente partie, après avoir présenté les principes généraux de la sécurité informationnelle.

b) Domaines d'application

Jusqu'à présent nous avons discuté des S.C.P. en termes surtout abstraits. Présentons-les maintenant plus concrètement dans leur mise en œuvre. Comme on peut sans doute le deviner, la gamme des domaines d'application couverts par les S.C.P. est très large. Il n'est évidemment pas possible d'en anticiper la totalité et nous n'avons pas l'ambition de présenter une liste exhaustive. Néanmoins, la présente sous-section permettra au lecteur à la fois de prendre conscience de la vaste gamme des applications auxquels sont destinés les S.C.P. et de mieux comprendre ces systèmes eux-mêmes dans la pratique.

La littérature technique s'est exprimée non sans un certain enthousiasme, à ce qu'il semble, à l'égard des applications présentes ou possibles pour les S.C.P.[74], et elle s'empresse de développer un cadre permettant de les adapter à ces différents emplois. Elle vise autant des systèmes de taille gigantesque, comme une infrastructure de service public, que d'autres, aussi miniatures qu'un stimulateur cardiaque intelligent[75]. À en croire les sources techniques, les S.C.P. sont appelés à s'intégrer dans tous les domaines.

À titre d'exemple, un document produit par le N.I.S.T. ne recense pas moins de vingt-quatre champs d'application possibles des S.C.P. :

Domains	
Advertising	*Entertainment/sports*
Aerospace	*Environmental monitoring*
Agriculture	*Financial services*
Buildings	*Healthcare*
Cities	*Infrastructure (communications, power, water)*
Communities	*Leisure*
Consumer	*Manufacturing*
Defense	*Science*
Disaster resilience	*Social networks*
Education	*Supply chain/retail*
Emergency response	*Transportation*
Energy	*Weather*
...perhaps others	

Tableau 1 : domaines d'application des S.C.P.[76]

Les auteurs techniques n'hésitent pas à fournir des listes assez généreuses des possibilités associées aux S.C.P., comme par exemple celle-ci :

> « *Examples of CPS include medical devices and systems, aerospace systems, transportation vehicles and intelligent highways, defense systems, robotic systems, process control, factory automation, building and environmental control and smart spaces.* »[77]

[74] Voir par exemple : R. RAJKUMAR et al., préc., note 31 ; K. KIM et P. R. KUMAR, préc., note 7, p. 1287-1288 ; S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 350.
[75] S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 350.
[76] C.P.S.P.W.G., préc, note 53, p. 26.
[77] R. RAJKUMAR et al., préc., note 31, p. 731.

Il est vrai que les S.C.P. jouissent d'une versatilité appréciable. Tel que nous l'avons dit précédemment, les systèmes les plus imposants peuvent se rattacher aux infrastructures, par exemple le réseau électrique, afin d'en faciliter la gestion pour l'entité qui en a la charge[78]. Les S.C.P. permettent alors de collecter des données sur les ressources disponibles, le niveau de production des parcs éoliens et solaires par exemple, et de maximiser l'utilisation de ces ressources en fonction de leur disponibilité[79]. Il en est de même pour les réseaux d'aqueduc et d'égouts, et d'autres applications relevant du concept de « ville intelligente ». En outre, ils peuvent s'intégrer dans l'industrie lourde, aux chaines de production ou de distribution afin d'en automatiser le fonctionnement[80], ou encore œuvrer à l'automatisation de l'agriculture[81] afin d'offrir des rendements améliorés[82]. Cependant, les plus petits systèmes intégrant des S.C.P. peuvent être des objets de la vie courante plutôt modestes, comme un système de serrure qu'on peut déverrouiller par l'entremise d'un téléphone intelligent, un système d'éclairage intelligent ou d'autres applications relevant de la domotique.

En raison des possibilités d'automatisation, de coordination et de collectes de données qu'ils offrent, les S.C.P. sont aussi appelés à se déployer dans le domaine de la santé[83]. Ceux-ci se retrouvent certes déjà dans les hôpitaux sous la forme d'instruments destinés à prodiguer des traitements ou d'appareils de surveillance des fonctions vitales des patients. On pense notamment aux appareils de radiographie, ventilateurs, pompes à infusion ou à certains instruments de laboratoire, dont les versions récentes peuvent bénéficier de capacité de connexion aux réseaux pour faciliter la tâche des praticiens et pour permettre une meilleure coordination entre les différents appareils au cours d'un traitement[84]. En outre, ces systèmes peuvent se connecter directement à des bases de données informatisées comme un dossier de

[78] J. SHI, J. WAN et H. Yan, préc., note 53.
[79] S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 350.
[80] Jay LEE, Behrad BAGHERI et Hung-An KAO, « A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems » (2015) 3 *Manufacturing Letters* 18.
[81] Voir par exemple Ciprian-Radu RAD et al., « Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture », (2015) 6 *Agriculture and Agricultural Science Procedia* 73.
[82] R. RAJKUMAR et al., préc., note 31, p. 732.
[83] S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 356 ; K. KIM et P. R. KUMAR, préc., note 7, p. 1288.
[84] Insup LEE, et Oleg SOKOLSKY, « Medical Cyber Physical Systems », (2010) *47th Design Automation Conference (DAC '10)* 743.

santé électronique, facilitant l'accès aux données générées (permettant notamment des applications d'infonuagique) ou ouvrant la porte à des techniques d'analyse relevant des techniques tirant profit des mégadonnées[85].

Mais les S.C.P. médicaux sont également appelés à sortir du cadre de l'établissement de santé. Certains prennent la forme de dispositifs intégrés directement dans le corps du patient afin de prélever et communiquer en temps réel des données médicales, les relayant au personnel traitant. D'autres encore jouent un rôle plus actif, comme un stimulateur cardiaque ou une pompe à insuline auxquels on peut se connecter par réseau sans fil[86]. La littérature technique explore d'autres possibilités d'application des S.C.P. dans le domaine de la santé. Entre autres choses, des auteurs ont proposé un système capable de traduire l'activité cognitive du patient en commandes pour animer directement une prothèse remplaçant un membre manquant[87], ou encore un S.C.P. capable de procéder automatiquement à une chirurgie à cœur ouvert[88].

Cependant, peut-être est-ce dans le domaine des transports que les S.C.P. seront appelés à jouer leur rôle le plus visible dans la vie courante. Il est déjà possible de considérer que tout aéronef ou automobile moderne est un S.C.P.[89] Tel que nous l'avons évoqué dans notre introduction, les ordinateurs ont intégré les automobiles pour la première fois dans les années 1970[90]. Incorporés dans ce qu'on appelle des M.C.E.[91], ils se sont multipliés et sophistiqués au courant des dernières décennies. Aujourd'hui, une voiture de luxe peut renfermer jusqu'à 70

[85] Yin ZHANG, et al., « Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data », (2015) *IEEE Systems Journal* ; Anthony J. CORONADO et Timothy L. WONG, « Healthcare Cybersecurity Risk Management: Keys to an Effective Plan », (2014) *Horizon*, p. 26.
[86] CONTI et al., préc, note 15.
[87] Gunar SHIRNER et al., « The Future of Human-in-the-Loop Cyber-Physical Systems », (Janvier 2013) *Computer* ; He HUANG et al., « Integrating neuromuscular and cyber systems for neural control of artificial legs », (2010) *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems* 129.
[88] Erol YENIARAS et al., « Towards A New Cyber-Physical System for MRI-Guided and Robot-Assisted Cardiac Procedures », (2010) *Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine*.
[89] R. RAJKUMAR et al., préc., note 31 ; K. KIM et P. R. KUMAR, préc., note 7, p. 1287 ; S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 355.
[90] Steve MERTL, « How cars have become rolling computers », (5 mars 2016) *The Globe and Mail*, en ligne : <http://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/> (consulté le 12 décembre 2017).
[91] *Supra*, note 40.

M.C.E. connectés par jusqu'à 50 kg de câblage[92], et ses algorithmes peuvent requérir jusqu'à 20 millions de lignes de code[93]. Ceux-ci jouent notamment un rôle dans la gestion du carburant, de la transmission, ainsi que dans les systèmes de sécurité tels que le système antiblocage des roues ou, plus récemment, dans les systèmes de détection de collision par sonar[94], ou encore pour surveiller l'éveil ou l'état de santé du conducteur[95]. Ils disposent en outre de capacités de connexion aux réseaux élaborés fonctionnant sous plusieurs protocoles : Bluetooth, Wi-Fi, réseaux cellulaires et autres[96]. Bien entendu, les S.C.P. à bord des véhicules continueront de gagner en complexité à mesure qu'entrent sur le marché les voitures autonomes. Le développement de cette technologie va bon train et certains fabricants automobiles offrent déjà des systèmes de pilotage presque complètement automatiques, là où la législation le permet.

Le développement des technologies entourant les S.C.P. dans le domaine des transports est intense. Des travaux sont en cours afin d'en standardiser le développement et la mise en place, tel le projet A.U.T.O.S.A.R. issu d'un partenariat d'acteurs de l'industrie automobile[97]. D'autres chercheurs travaillent à employer les possibilités des S.C.P. pour réduire la consommation de carburant[98], utilisent des méthodes d'apprentissage automatique[99] afin de perfectionner les algorithmes de conduite autonome du véhicule lorsqu'il côtoie des conducteurs humains[100], ou développent des technologies pour coordonner les interactions sur la route entre

[92] Fengzhong QU, Fei-Yue WANG et Liuqing YANG, « Intelligent Transportation Spaces : Vehicules, Traffic, Communications and Beyond », (novembre 2010) *IEEE Communications Magazine* 136, p. 136.
[93] Gaurav BHATIA, Kharthik LAKSHMANAN et Ragunathan (Raj) RAJKUMAR, « An End-to-End Integration Framework for Automotive Cyber-Physical Systems Using SysWeaver », (2010) *Proceedings of the AVICPS*.
[94] S. MERTL, préc., note 90.
[95] F. QU, F.-Y. WANG et L. YANG, préc., note 92, p. 136.
[96] *Id.*
[97] AUTOSAR, en ligne : <http://www.autosar.org> (consulté le 12 décembre 2017) ; G. BHATIA, K. LAKSHMANAN et R. RAJKUMAR, préc., note 93.
[98] Hossein AHMADI et al., « The Sparse Regression Cube: A Reliable Modeling Technique for Open Cyber-Physical Systems », (2011) *Proceedings of the IEEE/ACM Second International Conference on Cyber-Physical Systems* 87.
[99] O.Q.L.F., préc., note 64, « apprentissage automatique » : « Processus par lequel un ordinateur acquiert de nouvelles connaissances et améliore son mode de fonctionnement en tenant compte des résultats obtenus lors de traitements antérieurs. » Ce terme est utilisé pour traduire l'expression « *machine learning* ».
[100] Sumit Kumar JHA et Gita SUKTHANKAR, « Modeling and Verifying Intelligent Automotive Cyber-Physical Systems », (2011) *Proceedings of the NIST/NSF/USCAR Workshop on Developing Dependable and Secure Automotive Cyber-Physical Systems from Components*.

les véhicules à l'aide de réseaux sans fil[101]. Au-delà de la communication à l'intérieur même du véhicule ou d'un véhicule à l'autre, des auteurs proposent également d'intégrer des S.C.P. dans les infrastructures de transport elles-mêmes afin par exemple d'améliorer la fluidité du trafic et prévenir les accidents de la route[102], ou encore pour optimiser le stationnement des véhicules au sein d'un espace[103]. En mettant en commun les données générées par les automobiles, leurs conducteurs et les piétons (notamment par l'entremise de leurs téléphones intelligents), ainsi que par les infrastructures de la route, il serait possible de construire des S.C.P. de vaste ampleur, parfois appelés « systèmes de transport intelligents »[104].

c) Terminologie analogue

Tel que nous l'avons dit précédemment, certaines des applications mentionnées ci-dessus ont parfois été qualifiées différemment par d'autres auteurs. Cette possible confusion des termes découle de la fâcheuse impulsion, dans le domaine des technologies de l'information, à créer des néologismes visant parfois des concepts identiques ou très similaires[105]. Certaines de ces expressions, encore, relèvent de stratégies de marketing visant à distinguer artificiellement une technologie de celles proposées par les concurrents d'une entreprise. L'ensemble peut porter à confusion, même chez l'initié, et il est difficile de garder le rythme. Ce problème, qui est loin d'être nouveau, grève également les S.C.P. et il faut faire un travail de débroussaillage afin de bien les situer parmi un certain nombre de notions analogues. Dans cette sous-section, nous traiterons des notions les plus susceptibles d'être confondues avec les S.C.P. sous l'approche que nous avons choisie. Il s'agit des objets connectés dans l'Internet des objets, et des robots.

---

[101] He Hua YAN, Jia Fu WAN et Hui SUO, « Adaptive Resource Management for Cyber-Physical Systems », (2012) 157/158 *Applied Mechanics and Materials* 747.
[102] R. RAJKUMAR et al., préc., note 31 ; K. KIM et P. R. KUMAR, préc., note 7 ; J. SHI, J. WAN et H. Yan, préc., note 53.
[103] Jiafu WAN et al., « Context-Aware Vehicular Cyber-Physical Systems with Cloud Support : Architecture, Challenges, and Solutions », (août 2014) *IEEE Communications Magazine* 106.
[104] F. QU, F.-Y. WANG et L. YANG, préc., note 92, p. 136.
[105] Nicolas W. VERMEYS, Karim BENYEKHLEF et Vincent GAUTRAIS, « Réflexions juridiques autour de la terminologie associée aux places d'affaires électroniques », (2004) 38 *Revue juridique Thémis* 641.

i) Internet des objets et objets connectés

L'« Internet des objets » est depuis quelques années déjà un sujet d'intérêt dont l'existence n'aura certainement pas échappé au lecteur. Les objets connectés[106] qui constituent l'I.d.O. se rapprochent beaucoup des S.C.P., tant et si bien que certains auteurs utilisent indifféremment les deux expressions[107]. En effet, les S.C.P. s'inscrivent souvent dans la même dynamique que les objets connectés, de sorte qu'il peut être pertinent de prendre le temps de détailler un peu cette notion. La littérature technique donne en général une définition de l'I.d.O. qui se rapproche de celle-ci :

> « *[…] the term 'Internet-of-Things' (IoT) is broadly used to refer to both: (i) the resulting global network interconnecting smart objects by means of extended Internet technologies, (ii) the set of supporting technologies necessary to realize such a vision (including, e.g., RFIDs, sensor/actuators, machine-to-machine communication devices, etc.) and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities.* »[108]

On comprend donc que l'I.d.O. est moins une technologie à proprement parler que le vaste ensemble créé par la mise en réseau d'objets ne relevant traditionnellement pas de l'informatique, afin de tirer bénéfice de nouvelles capacités de collecte, de partage et de traitement de données. Le tout est appelé à se superposer à l'infrastructure préexistante d'Internet afin d'étendre ses capacités[109]. Ainsi a-t-on pu dire : « *Suddenly, everything from refrigerators to sprinker systems are wired and interconnected […] These devices are now collectively called the internet of things (IoT)* »[110]. La croissance de l'I.d.O. est explosive : selon la *Federal Trade Commission*[111], le nombre d'objets connectés à Internet s'estimait à 25

[106] En anglais, « smart object », « smart device » ou encore « connected device ».
[107] Hermann KOPETZ, *Real-Time Systems*, Springer, 2011, p. 308. Cette proximité est telle que ce mémoire traitait d'abord des objets connectés.
[108] Daniele MIORANDI et al., « Internet of things: Vision, applications and research challenges » (2012) 10 *Ad Hoc Networks* 1497, p. 1497-1498.
[109] *Id.*
[110] HP, *Security of the IoT*, 2015, p. 1, en ligne : <http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf> (consulté le 12 décembre 2017).
[111] Ci-après la « **F.T.C.** ».

milliards en 2015, et devrait doubler dès 2020[112]. Il est entendu que l'arrivée sur les réseaux d'une masse si considérable et si hétérogène d'objets engendrera bon nombre de défis sociaux, juridiques et techniques[113].

Mais que sont ces objets connectés qui composent l'I.d.O. ? La FTC observe laconiquement, dans son rapport, que c'est tout objet disposant de capacités de connexion à Internet et qui n'est pas un téléphone intelligent, une tablette ou un ordinateur dans le sens traditionnel du terme[114]. La littérature technique nous offre une définition plus poussée:

> « *We define smart objects (or things) as entities that:*
>
> - *Have a physical embodiment and a set of associated physical features (e.g., size, shape, etc.).*
> - *Have a minimal set of communication functionalities, such as the ability to be discovered and to accept incoming messages and reply to them.*
> - *Possess a unique identifier.*
> - *Are associated to at least one name and one address.*
> - *The name is a human-readable description of the object and can be used for reasoning purposes. The address is a machine-readable string that can be used to communicate to the object.*
> - *Possess some basic computing capabilities. This can range from the ability to match an incoming message to a given footprint (as in passive RFIDs) to the ability of performing rather complex computations, including service discovery and network management tasks.*
> - *May possess means to sense physical phenomena (e.g., temperature, light, electromagnetic radiation level) or to trigger actions having an effect on the physical reality (actuators)* ».[115]

Un objet connecté, ce peut donc être tant une pièce d'inventaire dotée d'une puce R.F.I.D. lui permettant d'être identifiée et suivie par réseau, qu'un podomètre se connectant au téléphone intelligent de l'utilisateur pour lui permettre d'assurer un suivi de ses résultats, ou une caméra vidéo accessible en ligne pour surveiller son enfant. Même une automobile, capable de

---

[112] F.T.C., *Internet of Things: Privacy & Security in a Connected World*, F.T.C. Staff Report, 2015, p. 1, en ligne : <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (consulté le 12 décembre 2017).
[113] H. KOPETZ, préc., note 107, p. 308.
[114] F.T.C., préc., note 112, p. 6.
[115] D. MIORANDI, préc., note 108, p. 1498.

se connecter soit à Internet, aux autres automobiles sur la route ou aux infrastructures routières peut être considérée comme un objet connecté. C'est dire que, tout comme les S.C.P., les objets connectés se retrouvent dans pratiquement tous les domaines[116].

En effet, les similitudes entre S.C.P. et objets connectés sont nombreuses. Pourquoi doit-on distinguer ces deux notions ? Ne serait-il pas plus opportun d'employer, dans notre mémoire, celle d'objet connecté, qui est bien mieux connue ? Il est vrai que les deux expressions relèvent fondamentalement de l'intégration de composantes informatiques dans des objets physiques, le tout afin de permettre notamment leur connexion aux réseaux. Tout comme pour les S.C.P., cette mise en réseau entraîne une grande préoccupation pour ce qui est de la sécurité informationnelle[117]. La presse technique relève d'ailleurs presque hebdomadairement des failles de sécurité informatique dans l'I.d.O.[118]. Il n'est pas rare que les fabricants d'objets connectés ne prennent pas en compte la sécurité informationnelle de leurs produits lors de leur conception, ce qui peut avoir des conséquences désastreuses[119].

---

[116] Pour des exemples d'applications de l'I.d.O., voir notamment Luigi ATZORI, Antonio IERA et Giacomo MORABITO, « The Internet of Things: A Survey », (2010) 54-15 *Computer Networks.* Ces auteurs les groupe en quatre domaines : « *Transportation and logistics […] Healthcare […] Smart environment (home, office, plant) […] Personal and social […]* ».

[117] *Id.*, p. 15 : « *The IoT is extremely vulnerable to attacks for several reasons. First, often its components spend most of the time unattended; and thus, it is easy to physically attack them. Second, most of the communications are wireless, which makes eavesdropping extremely simple. Finally, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security.* ».

[118] Voir par exemple : Patrick NELSON, « Home IoT devices are wide open, security provider discovers », (7 avril 2016) *Network World*, en ligne : <https://www.networkworld.com/article/3051691/internet-of-things/home-iot-is-wide-open-security-provider-discovers.html> (consulté le 12 décembre 2017) ; Catalin CIMPANU, « Hacking of Another Four IoT Devices Reinforces Belief that IoT is Insecure », (30 mars 2016) *Softpedia News*, en ligne : <http://news.softpedia.com/news/hacking-of-another-four-iot-devices-reinforces-belief-that-iot-is-insecure-502350.shtml> (consulté le 12 décembre 2017) ; Mark STANISLAV et Tod BEARDSLEY, « Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities », (29 septembre 2015) *Rapid7 Report*, , en ligne : <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf> (consulté le 12 décembre 2017) ; Dan GOODIN, « Samsung Smart Home flaws let hackers make keys to front door », (2 mai 2016) *Ars Technica*, en ligne : <https://arstechnica.com/information-technology/2016/05/samsung-smart-home-flaws-lets-hackers-make-keys-to-front-door/> (consulté le 12 décembre 2016).

[119] Alexandra GHEORGE, « The Internet of Things: Risks in the Connected Home »*, Bit Defender Research Paper*, (2016), p. 13, en ligne : <http://download.bitdefender.com/resources/files/News/CaseStudies/study/87/Bitdefender-2016-IoT-A4-en-EN-web.pdf>, (consulté le 12 décembre 2017) : « *The IoT opens a completely new dimension to security – it is where the Internet meets the physical world. If projections of a hyper-connected world become reality and manufacturers don't bake security into their products, consequences can become life-threatening.* » ; voir aussi : Earlence FERNANDES, Jaeyeon JUNG et Atul PRAKASH, « Security Analysis of Emerging Smart Home Applications », (2016) *2016 IEEE Symposium on Security and Privacy (SP)*.

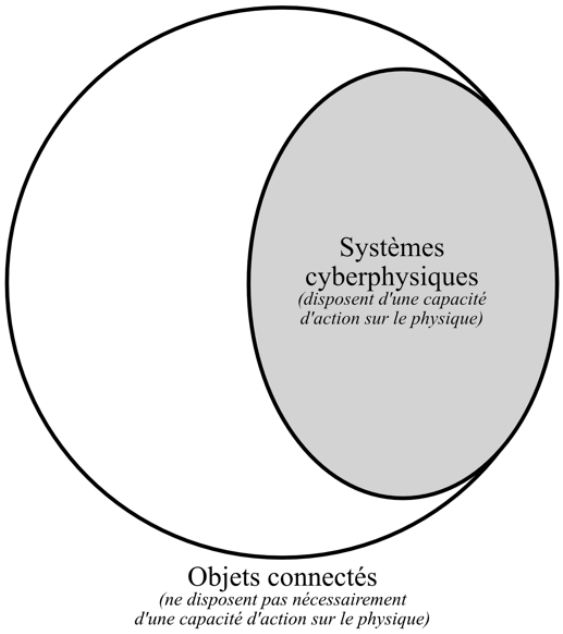

Figure 2 : diagramme – objets connectés et systèmes cyberphysiques

Mais il existe une différence fondamentale entre objets connectés et S.C.P., qui explique pourquoi nous avons rejeté ce terme aux fins de notre mémoire. Contrairement aux S.C.P., ce ne sont pas tous les objets connectés qui ont pour vocation d'agir directement sur le monde physique. C'est ainsi que, comme nous l'illustrons dans la figure 2 ci-dessus, si tous les S.C.P. sont des objets connectés, au contraire tous les objets connectés ne sont pas nécessairement des S.C.P. Par exemple, des objets connectés passifs comme une puce R.F.I.D., une caméra de surveillance connectée, ou plus généralement tout objet dont la vocation est d'assurer la collecte de donnée, ne peuvent que malaisément être considérés comme des S.C.P., car ils n'ont aucune action directe sur le monde physique. Par conséquent, il y a peu de risque qu'ils causent directement un dommage physique en raison d'une défaillance informatique, ce qui rend, selon nous, l'étiquette « objet connecté » moins précise et moins appropriée que celle de « système cyberphysique ».

ii) Robotique

La robotique est un autre domaine pouvant être considéré comme sous-jacent ou parallèle à celui des S.C.P.[120], et susceptible d'être invoqué lorsqu'on parle de systèmes physiques contrôlés informatiquement.

La définition du terme « robot » varie cependant beaucoup. L'emploi commun du mot semble référer davantage à des machines à l'apparence et au comportement vaguement humains, sans doute en raison du sens historique du terme[121]. La littérature technique donne évidemment une définition beaucoup plus large à cette expression, en prenant soin de ne pas se heurter aux écueils d'une conception anthropomorphique. Un consensus ne semble cependant pas avoir émergé de façon définitive, malgré qu'au fil du temps de nombreuses organisations techniques ont cherché à imposer une définition[122].

En raison de cette ambiguïté plutôt obstinée, les auteurs qui traitent des robots sont souvent portés à proposer leurs propres critères de définition, lesquels peuvent varier dépendamment de leur champ d'expertise. Un exemple d'une définition proposée dans le champ juridique observe qu'un robot, c'est toute machine matérielle alimentée en énergie, capable d'observer son environnement, de prendre des décisions et dotée d'une capacité d'apprentissage, le tout afin d'agir sur le réel[123]. Un autre juriste propose cette définition : « *A robot is a constructed system that displays both physical and mental agency but is not alive in the biological sense* »[124].

---

[120] Jan Oliver RINGERT, Bernhard RUMPE et Andreas WORTMANN, « A Requirements Modeling Language for Component Behavior of Cyber Physical Robotics Systems », dans Norbert SEYFF et Anne KOZIOLEK (dir.), *Modelling and Quality in Requirements Engineerings: Essays Dedicated to Martin Glinz on the Occasion of His 60th Birthday*, Monsenstein und Vannerdat, 2012.

[121] Voir par exemple la définition de « robot » donnée dans le Petit Robert : Paul ROBERT, Josette REY-DEBOVE et Alain REY, *Le Nouveau Petit Robert*, Paris, Dictionnaires Le Robert, 2010, p. 2260, « Robot » : « Machine, automate à l'aspect humain, capable de se mouvoir et d'agir » ; Nathalie NEVEJANS, « Les robots : tentative de définition », dans Alexandra BENSAMOUN (dir.), *Les Robots, objets scientifiques, objets de droits*, Paris, Éditions Mare & Martin, 2016, p. 86 et suiv.

[122] Voir par exemple les définitions proposées par le *Robot Institute of America*, la *Japan Robot Association*, ou celle de l'Association française de robotique industrielle. D'autres définitions ont également été proposées par les organismes de normalisation, comme l'I.S.O. avec la norme N.F. E.N. I.S.O. 8373 « Robots et composantes robotiques – Vocabulaire » et N.F. E.N. I.S.O. 13482 « Robots et composantes robotiques –Exigences de sécurité – Robots non médicaux pour les soins personnels ».

[123] N. NEVEJANS, préc., note 121, p. 101.

[124] Neil M. RICHARDS et William D. SMART, « How should the law think about robots? », (2013), en ligne : <https://ssrn.com/abstract=2263363> (consulté le 12 décembre 2017).

Malgré cette fluidité dans les définitions, il apparaît évidemment que de nombreux robots peuvent être qualifiés de S.C.P. ou d'objets connectés puisqu'en règle générale, il s'agit de systèmes contrôlés par procédés logiciels et appelés à agir de façon plus ou moins autonome sur le monde physique à l'aide de l'information prélevée sur son environnement.

Une différence majeure s'érige cependant du point de vue de la connectivité des robots aux réseaux numériques. En effet, il ne semble pas exister de tendance générale à considérer l'aspect de la connectivité comme une composante essentielle des robots, alors qu'elle est au cœur de la définition des S.C.P. et des objets connectés. Étant donné que c'est justement cette connectivité qui entraîne de nombreux risques de sécurité susceptibles d'avoir des incidences juridiques sur la responsabilité du fabricant (tel que nous le verrons tout à l'heure), il nous semble plutôt hardi d'omettre cet aspect dans notre étude.

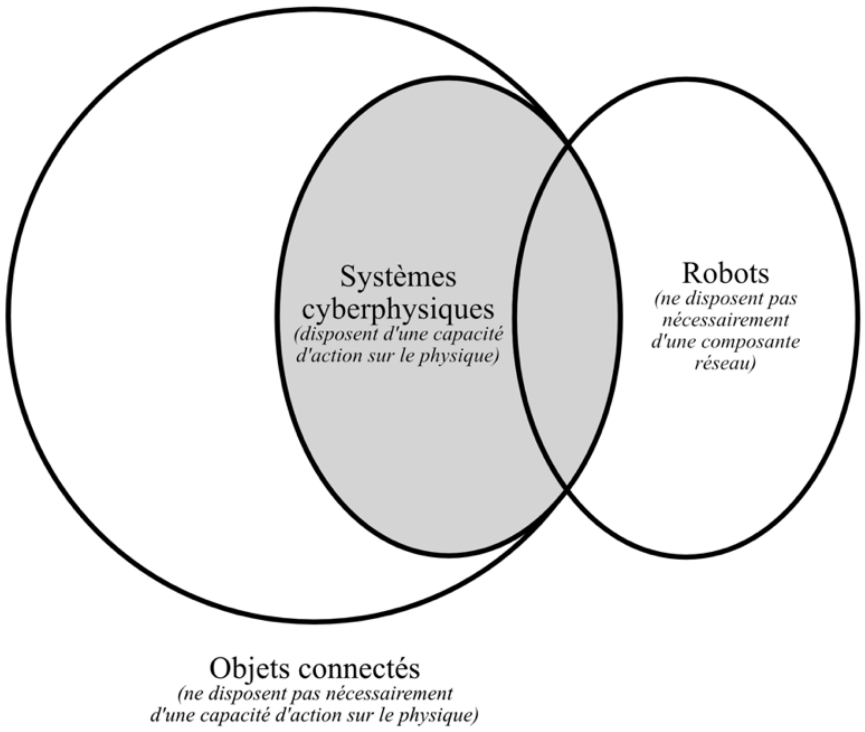

Figure 3 : diagramme – objets connectés, systèmes cyberphysiques et robots

C'est donc dire que les termes « robot » et « système cyberphysique » ne peuvent pas être employés comme des synonymes : si certains robots peuvent en effet être appelés des S.C.P., les robots qui n'ont pas de connectivité aux réseaux ne sont pas des S.C.P., tel que nous l'avons illustré dans la figure 3 à la page précédente. Nous invitons également le lecteur à se référer au tableau 2 ci-dessous :

Caractéristiques essentielles	Objets connectés	Systèmes cyberphysiques	Robots
Aspect algorithmique	X	X	X
Connectivité aux réseaux	X	X	
Action sur le monde physique		X	X

Tableau 2 : objets connectés, systèmes cyberphysiques et robots

Pour en revenir aux robots, c'est en raison du manque d'emphase sur la réseautique que nous avons choisi de nous abstenir d'utiliser cette expression dans le présent mémoire. Cette divergence entre les deux termes aurait seulement pu être comblée en apposant assez artificiellement un aspect de connectivité à notre propre définition du terme robot, ce en quoi nous aurions seulement participé à l'ambiguïté générale associée à ce terme.

Nous demandons cependant au lecteur de ne pas oublier que les notions juridiques qui seront présentées ci-après peuvent également s'appliquer aux systèmes qui seraient qualifiés de robots, de même que de nombreuses analyses juridiques sur les incidences découlant des robots sont appelées à se transposer aux S.C.P.

2. Qualification juridique des systèmes cyberphysiques

Le portrait technique ainsi éclairci, comment le juriste approchera-t-il les S.C.P. ? Dans le cas des systèmes les plus complexes, ceux qui sont composés de nombreux dispositifs hétérogènes formant un vaste ensemble (par exemple les infrastructures énergétiques ou routières), la question peut devenir rapidement ardue. En effet, la complexité technique des S.C.P. peut engendrer une complexité juridique proportionnelle, en créant un enchevêtrement

de droits personnels, réels et intellectuels qui impliquent une multitude de domaines du droit. En outre, ces grands systèmes peuvent mettre en cause toute une variété de sujets de droit, et ceux-ci peuvent relever du domaine tant public que privé : gouvernements fédéraux ou provinciaux, municipalités, sociétés privées (fabricants et prestataires de service informatiques en tout genre), ainsi que les utilisateurs eux-mêmes. Cependant, n'oublions pas l'objet de notre mémoire : appliquer les règles de la responsabilité civile à une situation nouvelle, celle du dommage physique causé par la défaillance informatique d'un S.C.P. Dans le cadre de cette démarche, nous gagnons à simplifier le portrait technique à son maximum. Ainsi, dans cette section, nous viserons à qualifier un S.C.P. composé d'un seul dispositif.

a) Un bien meuble au sens du Code civil du Québec

Notre premier angle d'approche se doit d'être sous celui du droit des biens. Il est entendu qu'un S.C.P. pourra être qualifié de bien corporel, étant donné qu'il s'agit d'une chose tangible et susceptible d'appropriation[125]. Il est alors nécessaire de déterminer s'il s'agit d'une bien meuble ou immeuble, selon la distinction traditionnelle du droit[126].

En règle générale, on considérera qu'un S.C.P. est un bien meuble. Il s'agit en effet le plus souvent d'une chose mobile, pouvant se transporter par elle-même ou à l'aide d'une force étrangère[127]. Du reste, le C.c.Q. a pour principe général de considérer meubles tous les biens non qualifiés d'immeubles[128]. On ne saurait ainsi considérer qu'un S.C.P. soit immeuble par nature, étant donné qu'ils ne figurent pas au C.c.Q. comme tel[129] et que, en outre, ils sont rarement immobiles à l'état normal[130]. Cependant, quand le S.C.P. est incorporé à un immeuble (par exemple au réseau électrique)[131], on peut envisager qu'il soit qualifié d'immeuble en raison

---

[125] *Covertite Ltd.* c. *Fonds d'indemnisation des victimes d'accidents d'automobiles*, [1965] C.S. 140 ; *Québec (Procureur général)* c. *Labrador Welding Ltd.*, [1972] C.S. 426 ; Denys-Claude LAMONTAGNE, *Biens et propriété*, 7e éd., Montréal, Éditions Yvon Blais, 2013, par. 5.
[126] C.c.Q., art. 899.
[127] *Id.*, art. 905.
[128] *Id.*, art. 907.
[129] *Id.*, art. 900.
[130] D.-C. LAMONTAGNE, préc., note 12, para. 58.
[131] *Montreal Light, Heat and Power Consolidated* v. *Westmount (City of)*, [1926] R.C.S. 515 ; *St-Laurent (Cité de)* c. *Commission hydroélectrique de Québec*, [1978] 2 R.C.S. 529 ; *Lower St. Lawrence Power Co*. c. *Immeuble Landry Ltée*, [1926] R.C.S. 655.

de cette incorporation[132]. De même, le S.C.P. pourrait être qualifié d'immeuble par attache ou par réunion dans certains cas[133]. Il reste que la qualification du S.C.P. en tant que bien – qu'il soit meuble ou qualifié d'immeuble – emporte la possibilité que soit engagée la responsabilité de son fabricant aux termes du C.c.Q.[134], tel que nous le verrons dans le chapitre A de la seconde partie de ce mémoire.

Qu'en est-il cependant de l'information générée et portée par le S.C.P. ? Lorsqu'on la considère sous l'angle du droit des biens, on entre dans un débat doctrinal complexe à saveur parfois philosophique. Si d'aucuns disent qu'il s'agit de « biens numériques »[135], le législateur québécois ne s'est pas exprimé définitivement sur leur qualification. Selon la doctrine, il est probable que l'information doive effectivement être considérée en tant que bien[136], mais des difficultés subsistent lorsqu'on cherche à déterminer s'il s'agit de biens mobiliers corporels ou incorporels[137]. Du reste, ces biens numériques se marient parfois malaisément avec certaines caractéristiques classiques des droits réels[138]. Or, pour notre part, il n'est pas nécessaire de prendre position sur cette question : le cadre de responsabilité découlant du fait des biens que nous avons choisi à titre de cas de figure (celui mis en place par l'article 1468 C.c.Q. que nous exposerons tout à l'heure) ne requiert que le caractère mobilier du bien causant un dommage pour devenir applicable, et nous avons démontré ci-dessus que les S.C.P. doivent être considérés comme des biens meubles.

b) Portant des documents technologiques au sens de la Loi concernant le cadre juridique des technologies de l'information

Étant donné la nature informatique des S.C.P., ceux-ci sont soumis aux dispositions relatives aux documents technologiques de la *Loi concernant le cadre juridique des*

---

[132] C.c.Q., art. 900-901.
[133] C.c.Q., art. 903. Voir par exemple *: Pomerleau* c. *East Broughton Station (Mun. du village d')*, [1965] C.S. 337 ; *Installations électriques R. Théberge inc.* c. *Rainville (Paré, Tanguay, notaires, s.e.n.c.)*, 2015 QCCQ 5590.
[134] C.c.Q., art. 1468 al 1.
[135] La doctrine a également utilisé les termes « actifs virtuels » et « biens virtuels ». Voir N. W. VERMEYS, préc., note 50, p. 71 à 102.
[136] *Id.*, p. 81.
[137] *Id*.
[138] *Id*.

technologies de l'information[139]. Celle-ci, entrée en vigueur en novembre 2001, vise notamment à assurer la sécurité juridique des communications ayant lieu par l'entremise de technologies de l'information, « qu'elles soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies »[140].

Au sens de la L.C.C.J.T.I., les données et les métadonnées[141] portées par les composantes virtuelles du S.C.P., de même que les logiciels s'y trouvant[142], seront qualifiées de « document technologique », c'est-à-dire « d'information portée par un support » faisant « appel aux technologiques de l'information »[143].

Selon nous, il n'est en rien fatal que les S.C.P. n'avaient pas été envisagés par le législateur lors de la rédaction de la L.C.C.J.T.I. : au contraire, celle-ci a été construite afin de permettre « une interprétation évolution de la Loi, évitant ainsi un amendement législatif pour chaque avancée technologique »[144]. Ainsi, les S.C.P. sont soumis aux dispositions relatives aux documents technologiques de cette loi, notamment aux articles 25 et 26 L.C.C.J.T.I., qui fondent, au moins en partie, l'obligation de sécurité informationnelle au Québec[145] sur laquelle nous nous pencherons bientôt.

Enfin, à titre de parenthèse, arrêtons-nous sur la qualification possible des S.C.P. en droit criminel. Nous estimons fort probable que ceux-ci soient assimilés à la notion d'« ordinateur » au sens du Code criminel, étant donné qu'ils se conforment à la définition qu'on trouve à l'article 342.1(2)[146]. Les infractions pertinentes trouveraient alors application, par exemple le fait

---

[139] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1 (ci-après la « **L.C.C.J.T.I.** »).

[140] L.C.C.J.T.I., art. 1 ; Jean-François DE RICO et Dominic JAAR, « Le cadre juridique des technologies de l'information », dans S.F.P.B.Q., vol. 298, *Développements récent en droit criminel (2008)*, Cowansville, Éditions Yvon Blais.

[141] Selon la doctrine, les métadonnées (les « données sur le document lui-même ») doivent être considérées comme un document technologique. Voir Pierre TRUDEL, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, Montréal, Éditions Yvon Blais, 2012, p. 36-37.

[142] Le terme « logiciel » étant explicitement assimilé à la notion de document par la loi : L.C.C.J.T.I., art. 71.

[143] L.C.C.J.T.I., art. 3. Pour une présentation plus détaillée de la notion de document et de document technologique, voir P. TRUDEL, préc., note 141, p. 29-43.

[144] J.-F. DE RICO, D. JAAR, préc., note 140.

[145] Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010, p. 101.

[146] C.Cr., art. 342.1 (2), « ordinateur » : « dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux : a) contient des programmes d'ordinateurs ou d'autres données; b)

d'utiliser le S.C.P. sans droit, d'intercepter toute fonction de celui-ci, ou encore de l'employer afin de détruire, détériorer ou de rendre inutilisables des données[147]. Évidemment, quiconque détourne un S.C.P. afin de causer volontairement une atteinte à des personnes ou des biens engagera sa responsabilité criminelle en plus de sa responsabilité civile.

B. Responsabilité : certains cadres juridiques applicables aux fabricants de systèmes cyberphysiques

Les S.C.P., que nous avons présentés dans le dernier chapitre, amènent à leur suite autant d'opportunités que de problématiques nouvelles. Ces nouveautés ont bien entendu des répercussions juridiques importantes, notamment du point de vue de la sécurité.

La vocation des S.C.P. d'utiliser des éléments algorithmiques afin d'agir sur le monde physique pose notamment la question de la responsabilité du fabricant en cas dommage physique causé par une défaillance informatique. Le juriste québécois qui cherche à établir en quels cas cette responsabilité est engagée, en l'absence de tout lien contractuel entre les parties, n'a malheureusement pas le secours d'un cadre juridique qui traite explicitement de ces systèmes, pas plus qu'il peut avoir recours aux enseignements d'une jurisprudence qui se serait penchée sur cette question précise. Cependant, sans doute peut-il tirer des régimes juridiques préexistants les règles qui lui permettront d'appréhender cette situation.

Dans ce chapitre, nous présenterons les principaux éléments juridiques qui nous permettront de mettre en place un cadre de responsabilité civile applicable au fabricant en cas de dommage physique. En reflétant la dualité cyberphysique des S.C.P., nous fonctionnerons en deux temps : chacun des cadres que nous présenterons traite d'un aspect de cette dualité. Nous en tirerons, à terme, une synthèse qui nous permette d'appréhender les particularités de ces systèmes. En premier lieu, nous parlerons de l'aspect physique de la sécurité des S.C.P. Rappelons que nous avons choisi de nous pencher sur la responsabilité extracontractuelle du fabricant pour tout dommage découlant du défaut de sécurité d'un bien meuble. En second lieu, nous répéterons le procédé pour la part informationnelle de notre problématique en traitant de

conformément à des programmes d'ordinateur : (i) soit exécutent des fonctions logiques et de commande, (ii) soit peuvent exécuter toute autre fonction. »

[147] *Id.*, art. 342.1 (1), 430.

l'obligation de sécurité informationnelle. Ceci fait, nous ferons une parenthèse sur la sécurité informationnelle des S.C.P.

1. Aspect physique de la sécurité

Le droit québécois reconnait depuis longtemps la pertinence d'un régime de responsabilité découlant du fait d'un bien[148]. Au fil du temps, ce droit s'est considérablement complexifié tant au niveau contractuel qu'extracontractuel, et s'est enrichi d'une perspective de protection du consommateur, notamment avec l'entrée en vigueur de la Loi sur la protection du consommateur[149].

Aujourd'hui, la victime d'un préjudice découlant du fait d'un bien a accès à un éventail de recours qui relèvent d'une approche protéiforme[150] (et qui n'est pas, d'ailleurs, sans présenter certaines incohérences)[151]. Lorsque le dommage résulte de l'inexécution d'une obligation spécifiée dans un contrat[152] – notamment dans le cadre d'un contrat de consommation – elle devra se prévaloir du régime de responsabilité contractuelle[153]. De même, lorsque le préjudice

---

[148] Les tribunaux québécois ont construit à partir du début du vingtième siècle un régime distinct de responsabilité du fait des choses, lequel se basait sur l'article 1054 du *Code civil du Bas-Canada.* Pour un historique de la responsabilité extracontractuelle découlant du fait des biens en droit québécois, voir Jean-Louis BAUDOUIN, Patrice DESLAURIERS et Benoît MOORE, *La responsabilité civile*, 8e éd., Montréal, Éditions Yvon Blais, 2014, par. 1-929 et suiv.

[149] *Loi sur la protection du consommateur*, L.R.Q., c. P-40.1. Ci-après la « **L.P.C.** ».

[150] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-372.

[151] Nathalie VÉZINA et Françoise MANIET, « La sécurité du consommateur au Québec… deux solitudes : mesures préventives et sanctions civiles des atteintes à la sécurité », (2008) 49-1 *Les cahiers de Droit*, sur les incohérences entre le régime extracontractuel du dommage causé par le défaut de sécurité et le régime contractuel établit par la L.P.C. Voir aussi Nathalie VÉZINA, « Obligation d'information relative à un bien dangereux et obligation de sécurité : régime général et droit de la consommation », dans JurisClasseur Québec, coll. « Droit des affaires », *Droit de la consommation et de la concurrence*, fasc. 4, Montréal, LexisNexis Canada, feuilles mobiles, par. 14 et suiv.

[152] Évidemment, ceci inclut non seulement ce qui se trouve expressément au contrat, mais également ce qui découle de sa nature, ainsi que des usages, de l'équité ou de la loi, en vertu du principe édicté à l'article 1434 C.c.Q. C'est ce principe qui rattache la sécurité du consommateur au droit de la responsabilité contractuelle tant pour ce qui est de ce qui découle du droit commun des contrats que du régime particulier de la sécurité des produits en vertu de la L.P.C., voir Nathalie VÉZINA, « La sécurité du consommateur au Québec… deux solitudes : mesures préventives et sanctions civiles des atteintes à la sécurité », (2008) 49-1 *Les cahiers de Droit*.

[153] C.c.Q., art. 1458. L'imposition d'avoir recours au régime contractuel dans un tel cas découle du principe de l'interdiction d'option, énoncé à l'article 1458 al 2 C.c.Q. Voir Nathalie VÉZINA, « Dualité de régimes et interdiction d'options », dans JurisClasseur Québec, coll. « Droit civil », *Obligations et responsabilité civile*, fasc. 16, Montréal, LexisNexis Canada, feuilles mobiles. Dans le cas d'un contrat de consommation, la L.P.C. offre un recours contre le fabricant dont nous discuterons brièvement dans les pages qui suivent. Autrement, nous nous abstiendront de discuter de la responsabilité contractuelle dans le cadre de dommage causé par le fait des biens.

découlant du fait d'un bien relève d'un domaine couvert par une loi particulière, on veillera à appliquer les règles prévues par cette loi[154]. Lorsqu'il n'existe aucun contrat entre les parties et qu'aucune loi ne vient proposer un régime particulier, la victime a alors accès aux recours découlant de la responsabilité extracontractuelle[155].

Parmi ces régimes traitants de responsabilité extracontractuelle, le C.c.Q. a codifié un cadre de responsabilité du fabricant pour tout dommage découlant du défaut de sécurité d'un bien meuble[156]. S'appliquant aux tiers lorsque la L.P.C. ne le peut pas, il présente un cas de figure intéressant pour l'objet de notre étude en ce qu'il peut trouver application dans un bon nombre de situations qui impliqueraient un S.C.P. Pensons par exemple au cas où la défaillance des systèmes informationnels d'un véhicule autonome cause un dommage aux piétons. Aussi présenterons-nous plus en détail les éléments pertinents de ce régime afin de pouvoir déterminer, par la suite, s'il peut s'appliquer – et comment – en cas de préjudice physique causé par une faille informatique d'un S.C.P.

a) La responsabilité du fabricant découlant du défaut de sécurité d'un bien meuble

i) Historique du régime

Avant d'être codifiés en 1994, les tenants d'une responsabilité extracontractuelle pour le fabricant étaient débattus dans la jurisprudence et la doctrine[157]. Il existait certes, sous le C.c.B.C., un recours contractuel contre le vendeur d'un bien,[158] mais aucun régime particulier en cas d'absence de lien contractuel. La victime n'avait par conséquent à sa disposition que le régime général de responsabilité extracontractuelle à faire valoir contre les personnes

---

[154] On peut penser notamment à la *Loi sur l'assurance automobile*, L.R.Q., c. A-25, la *Loi sur les accidents de travail*, L.R.Q., c. A-3, la *Loi sur l'indemnisation du dommage causé par les pesticides*, L.R.C. (1985), c. P-10, la *Loi sur la responsabilité nucléaire*, L.R.C. (1985), c. N-28, la *Loi sur la responsabilité en matière maritime*, L.C. 2001, c. 6, ou encore la *Loi sur le régime des eaux*, L.R.Q., c. R-13 ; Pascal FRÉCHETTE, « Fait des biens », dans JurisClasseur Québec, coll. « Droit civil », *Obligations et responsabilité civile*, fasc. 19, Montréal, LexisNexis Canada, feuilles mobiles, par. 4.

[155] C.c.Q., art. 1465-1469.

[156] C.c.Q., art. 1468, 1469, 1473.

[157] Voir par exemple : Peter HAANAPPEL, « La responsabilité civile du manufacturier en droit québécois », (1980) 25 *McGill Law Journal* 365 ; Alain BERNARDOT et Robert KHOURI, *La responsabilité du centre hospitalier et du fabricant résultant du fait d'appareils médicaux défectueux*, (1980) 26 *McGill Law Journal* 978.

[158] La victime pouvait poursuivre le fabricant en vertu du régime général de la responsabilité extracontractuelle en vertu de l'article de base, l'article 1053 C.c.B.C.

impliquées dans la fabrication et la distribution d'un bien défectueux. Elle se voyait alors confrontée à la difficulté (voir à l'impossibilité) de prouver, le plus souvent par expertise, que le fabricant avait eu une conduite qui sortait du cadre normal de la prudence et de la diligence par rapport aux règles de l'art[159]. Le législateur s'était penché sur ce problème avec la L.P.C., qui a créé un régime de responsabilité contre le fabricant, mais celui-ci ne pouvait pas être invoqué par les tiers qui n'étaient pas partis au contrat. La jurisprudence avait alors développé au fil des ans, notamment dans le célèbre arrêt *Kravitz*[160], une interprétation du régime de la responsabilité civile extracontractuelle basée sur l'article 1053 C.c.B.C. pour construire un régime de responsabilité du fabricant d'un bien défectueux[161].

Avec l'entrée en vigueur du C.c.Q. en 1994, le législateur québécois a visé à pallier à cette lacune par la mise en place, aux articles 1468, 1469 et 1473 C.c.Q., d'un régime de responsabilité visant à faciliter le recours des tiers contre le fabricant du bien grevé d'un défaut de sécurité[162]. Codification de la jurisprudence développée au cours des ans et inspiré du droit de l'Union européenne[163], de la L.P.C.[164] et des travaux de l'*Office de révision du Code civil*[165], le régime de responsabilité extracontractuelle du fabricant vise à « protéger le public contre les défauts de sécurité de certains produits manufacturés ou fabriqués »[166] et s'inscrit dans la tendance plus large de protection du consommateur. On a voulu donner au fabricant, tout comme

[159] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-344.
[160] *General Motors Products of Canada Ltd* v. *Kravitz*, [1979] 1 R.C.S. 790.
[161] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par 2-343 et suiv. Outre *Kravitz*, voir aussi les décisions : *Ross* v. *Dunstall*, (1921) 62 S.C.R. 393 ; *Monsanto Oakville Ltd* v. *Dominion Textile Co.*, 1985 B.R. 339 ; *London & Lancashire Guarantee & Accident Co.* v. *Cie F.X. Drolet*, 1944 S.C.R. 82 ; *Gauvin* v. *Canada Foundries & Forgings Ltd.*, 1964 C.S. 160 ; *Trudel* v. *Clairol Inc.*, 1975 2 R.C.S. 236 ; *Cohen* v. *Coca-Cola Ltd*., 1967 R.C.S. 469 ; *Gougeon* c. *Peugoet Canada ltée*, 1973 C.A. 824 ; *Wabasso Ltd.* c. *National Drying Machinery Co.*, 1981 1. R.C.S. 1554.
[162] P. FRÉCHETTE, préc., note 154, par. 64 ; Pierre-Claude LAFOND, *Droit de la protection du consommateur : Théorie et pratique*, Montréal, Éditions Yvon Blais, par. 458 et suiv.
[163] *Directive de la Communauté Économique Européenne du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux*, (85/374/CEE), Journal officiel n° L 210 du 07/08/1985 p. 0029 – 0033.
[164] L.P.C., art. 53.
[165] O.R.C.C., L.V., art. 102-103.
[166] MINISTÈRE DE LA JUSTICE, *Commentaires du ministre de la Justice, Le Code civil du Québec*, tome 1, Québec, Les Publications du Québec, 1993 ; Vincent KARIM, *Les Obligations*, 4e éd., Vol. 1, Montréal, Wilson & Lafleur, 2015, par. 3185.

au vendeur d'un bien, un fardeau juridique proportionnel au rôle qu'il est appelé à jouer dans la mise en marché de ses produits[167].

ii) Régime juridique de la responsabilité du fabricant pour défaut de sécurité d'un bien meuble

A. La responsabilité du fabricant

Comme nous venons de le dire, les articles 1468, 1469 et 1473 C.c.Q. forment le cœur de ce régime. Les articles 1468 et 1469 C.c.Q. contiennent les « règles générales touchant à la responsabilité du fabricant »[168], alors que l'article 1473 C.c.Q., quant à lui, traite des moyens d'exonération. Voyons comment s'articule, pour le fabricant, cette responsabilité :

> « **Art. 1468.** Le fabricant d'un bien meuble, même si ce bien est incorporé à un immeuble ou y est placé pour le service ou l'exploitation de celui-ci, est tenu de réparer le préjudice causé à un tiers par le défaut de sécurité du bien.
>
> Il en est de même pour la personne qui fait la distribution du bien sous son nom ou comme étant son bien et pour tout fournisseur du bien, qu'il soit grossiste ou détaillant, ou qu'il soit ou non l'importateur du bien. »[169]

La responsabilité du fabricant est donc impliquée à l'égard des tiers – et des tiers seulement[170] – dès lors qu'il est possible de prouver, non pas qu'il a commis une faute à proprement parler, mais que le bien meuble dans la fabrication ou la mise en marché duquel il était impliqué présente un danger découlant d'un défaut de sécurité[171] ayant causé un dommage à la victime[172]. Il doit alors réparer « tout préjudice corporel, matériel ou moral causé à autrui »[173] survenu en raison de ce défaut de sécurité.

---

[167] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-371.
[168] *Id.*, par. 2-374.
[169] C.c.Q., art. 1468.
[170] P.-C. LAFOND, préc., note 162, par. 459.
[171] C.c.Q., art. 1468 al 1 ; *Imbeault c. Bombardier inc.*, 2006 R.R.A. 462 (C.S.) ; 2009 QCCA 260 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc, par. 2-375, 2-367.
[172] *Desjardins Assurances générales* c. *Venmar ventilation inc.*, 2014 QCCS 3653 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-383 ; N. VÉZINA et F. MANIET, préc., note 152, par. 109. Sur la créancière de cette obligation, voir J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, para 2-380 : rien n'empêche une personne morale de se prévaloir de ce régime.
[173] V. KARIM, préc., note 166, par. 3183.

La jurisprudence a défini le terme « fabricant » très largement afin d'y inclure « toute personne dont les opérations de transformation permettent d'utiliser le bien selon l'usage auquel il est destiné »[174]. Le deuxième alinéa de cet article consacre en outre la responsabilité des autres intervenants dans la mise en marché du bien avec lesquels la victime n'aurait pas de lien direct : distributeurs, fournisseurs, grossistes, détaillants ou importateurs, même étrangers[175]. Ceux-ci se partagent solidairement la responsabilité du dommage causé par le défaut de sécurité du bien[176].

Il convient également de faire remarquer que le régime s'applique principalement aux biens meubles, mais peut aussi viser les biens devenus immeubles par incorporation (par exemple un détecteur de fumée)[177].

Mais quel est ce « défaut de sécurité » qui se trouve porté au cœur du régime, en lieu et place de la faute ? Le législateur offre de précisions sur ce qu'il entend par cette expression :

> « **Art. 1469.** Il y a défaut de sécurité du bien lorsque, compte tenu de toutes les circonstances, le bien n'offre pas la sécurité à laquelle on est normalement en droit de s'attendre, notamment en raison d'un vice de conception ou de fabrication du bien, d'une mauvaise conservation ou présentation du bien ou, encore, de l'absence d'indications suffisantes quant aux risques et dangers qu'il comporte ou quant aux moyens de s'en prémunir. »[178]
>
> (Nos soulignés).

On comprend à la lecture du libellé de cet article que le défaut de sécurité s'apprécie par rapport à une sorte de « standard d'attente raisonnable ou normale » relatif à la sécurité[179]. La doctrine a également utilisé l'expression « violation du standard de sécurité » afin de parler du fait générateur de responsabilité[180]. Le régime s'applique donc « lorsqu'on entend démontrer

---

[174] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, Vol. 2, note 208 ; V. KARIM, préc., note 166, par. 3188 : « toute personne qui transforme une matière première en vue d'en faire un bien meuble ».
[175] C.c.Q., art. 1468 al. 2 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-378 ; P.-C. LAFOND, préc., note 162, par. 461. Cette liste n'est pas limitative. D'autres personnes seront assimilées au fabricant par la jurisprudence, par exemple le locateur commercial (*Accessoires d'auto Vipa* c. *Therrien*, [2003] R.J.Q. 2390 (C.A.), par. 33-42 ; *Lebel* c. *2427-9457 Québec inc.*, 2007 QCCS 4644.)
[176] C.c.Q., art. 1526 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-378.
[177] Art 1468 al 1 ; N. VÉZINA et F. MANIET, préc., note 152, par. 108.
[178] C.c.Q., art. 1469.
[179] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-376.
[180] Pierre-Gabriel JOBIN, *La vente*, 3e éd., Cowansville, Éditions Yvon Blais, 2007, par. 209.

que le défaut de sécurité du bien fabriqué et mis en circulation est tel qu'il ne répond pas aux attentes raisonnables du public »[181]. Cette démonstration doit être contextualisée « par rapport à l'utilisation ordinaire du bien compte tenu de la connaissance, de l'habileté et des habitudes qu'on est en droit de s'attendre des utilisateurs »[182]. Le demandeur est ainsi épargné de devoir prouver la faute exacte du fabricant[183], ce qui constituait précédemment une difficulté du régime d'avant l'entrée en vigueur du C.c.Q.

Le législateur précise ensuite que le défaut de sécurité peut avoir trois origines, quoique cette liste n'est pas limitative[184]. Il peut prendre la forme d'un vice de conception ou de fabrication, d'une mauvaise conservation ou présentation, ou enfin, de façon intéressante, de l'absence d'indications suffisantes quant aux risques que le bien recèle ou quant aux moyens de se prémunir des dangers qui y sont associés[185]. Remarquons donc que le produit n'a pas besoin d'être défectueux pour que la responsabilité du fabricant soit engagée : celle-ci peut également l'être lorsque les instructions données n'exposent pas suffisamment bien les dangers inhérents à son utilisation, même si par ailleurs il fonctionne tel qu'on s'y attend[186].

Par conséquent, il est important de prendre note que le fabricant est assujetti à une obligation de renseignement à l'endroit des utilisateurs du produit[187] dont l'intensité variera en fonction du danger inhérent à l'utilisation du bien[188], de la qualité du défendeur (un fabricant ou un distributeur seront tenus à un plus haut niveau d'intensité d'obligation de renseignement), du public visé par le bien, ainsi que du degré général de connaissance des risques associés à l'utilisation du bien en question[189]. Cette obligation impose au fabricant qu'il divulgue à la fois les dangers inhérents au bien et les mesures à prendre lors de son utilisation afin d'éviter ce

[181] V. KARIM, préc., note 166, par. 3208.
[182] *Id.*, par. 3210.
[183] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-376.
[184] *Id.*, par. 2-377.
[185] V. KARIM, préc., note 166, par. 3212.
[186] N VÉZINA et F. MANIET, préc., note 152, par. 112.
[187] *Accessoires d'auto Vipa inc. c. Therrien*, préc., note 175 ; *Baldor Electric Company* c. *Delisle*, 2012 QCCA 1004 ; Jean-Louis BAUDOUIN et Yves RENAUD, *Code civil du Québec annoté*, 19e éd., Montréal, Wilson & Lafleur, 2016, par.1469/3.
[188] *Duteau* c. *Service agricole de l'Estrie*, 2013 QCCS 50 ; J.-L. BAUDOUIN, Y. RENAUD, préc., note 187 par. 1469/5 ; V. KARIM, préc., note 166, par. 3214.
[189] V. KARIM, préc., note 166, par. 3214.

danger[190]. De plus, il doit également s'assurer que les informations fournies soient comprises par les utilisateurs[191]. En pratique, cette obligation de renseignement peut se traduire en étiquettes prodiguant les avertissements appropriés, en manuel d'utilisation, ou en d'autres méthodes dépendamment du degré de dangerosité du bien[192].

Dès qu'un défaut de sécurité est prouvé, le fabricant est présumé en avoir eu connaissance[193]. Le fardeau de la preuve se renverse alors et il lui revient de démontrer qu'un moyen d'exonération s'applique[194]. Dans le cas contraire, il sera soumis aux sanctions habituelles lui imposant de réparer tout préjudice corporel, matériel ou moral[195] – lorsque, bien entendu, le recours est porté à l'intérieur du délai de prescription habituel de trois ans à partir de la naissance du droit d'action[196].

B. Moyens d'exonération

Disons en premier lieu qu'en raison de la nature objective de ce régime et à cause de la présomption qui court contre le fabricant, lorsque celui-ci souhaite être exonéré « il ne suffit pas de plaider l'absence de faute »[197], par exemple qu'il ignorait l'existence du défaut en question. Il pourra néanmoins se rabattre sur un ensemble de mécanismes d'exonération, dont certains sont spécifiques à ce régime.

Ainsi, à sa défense, le défendeur pourra invoquer le moyen d'exonération classique de la force majeure énoncé à l'article 1470 C.c.Q., c'est-à-dire un « évènement imprévisible et irrésistible »[198]. Évidemment, il faut que l'évènement de force majeure ait un caractère d'extranéité suffisant : c'est pour cette raison qu'il est impossible d'invoquer le défaut de

[190] V. KARIM, préc., note 166, par. 3216.
[191] *Duteau* c. *Service agricole de l'Estrie*, préc., note 188 ; J.-L. BAUDOUIN et Y. RENAUD, préc., note 187, para. 1469/9.
[192] Ces étiquettes doivent être complètes et rejoindre le consommateur du bien en question, voir : *Compagnie d'assurances Wellington* c. *Canadian Adhesives Ltd.*, [1997] R.R.A. 635.
[193] C.c.Q., art. 1469 ; *Lebel* c. *2427-9457 Québec inc.*, préc., note 175 ; J.-L. BAUDOUIN et Y. RENAUD, préc., note 187, par. 1468/5.
[194] N. VÉZINA et F. MANIET, préc., note 152, par. 109.
[195] À ce sujet, voir *Id.*, par. 118 et suiv.
[196] C.c.Q., art. 2880 al. 2, 2926.
[197] N. VÉZINA et F. MANIET, préc., note 152, par. 115.
[198] C.c.Q., art. 1470 al. 2.

sécurité du bien lui-même comme un évènement de force majeure, pas plus que les actes des autres personnes impliquées dans la mise en marché du produit[199].

Naturellement, le fabricant peut également s'exonérer s'il prouve que le préjudice découle d'une faute de la victime, de sa négligence ou encore du fait que la victime n'a pas pris les « mesures préventives pour empêcher la survenance du dommage », en vertu du principe général du partage de responsabilité[200].

De plus, le fabricant dispose des moyens particuliers pour échapper à sa responsabilité prévus à l'article 1473 C.c.Q. Il peut d'abord s'exonérer en démontrant que la faute de la victime avait connaissance du défaut de sécurité du bien ou qu'elle était en mesure de le connaître[201]. Ce sera notamment le cas lorsque le fabricant s'est acquitté de son obligation de renseignement, mais on prendra également en considération les connaissances qu'une personne raisonnable est censée avoir (aspect objectif de l'analyse), de même que les connaissances qu'elle devrait avoir en fonction de son expérience (aspect subjectif de l'analyse)[202].

De façon intéressante, il peut enfin s'exonérer en démontrant que le défaut de sécurité *ne pouvait pas* être connu lors de la conception, fabrication et distribution du bien, compte tenu de l'état des connaissances scientifiques et techniques : c'est la défense relative aux risques de développement[203]. Il s'agit d'un critère d'appréciation objectif : ce ne sont pas les connaissances de fabricant lui-même qu'on prendra en compte, mais celles du domaine dans son ensemble, dont on tentera de prouver l'ignorance générale et objective du défaut[204]. Par « état des

---

[199] N. VÉZINA et F. MANIET, préc., note 152, par. 116.
[200] C.c.Q., art. 1478 al. 2 ; V. KARIM, préc., note 166, par. 3200.
[201] C.c.Q., art. 1473 al. 1.
[202] P. FRÉCHETTE, préc., note 154, par. 73.
[203] C.c.Q., art. 1473 al. 2 ; V. KARIM, préc., note 166, par. 3200 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-384 ; P.-G. JOBIN, préc., note 180, par. 214 et suiv. ; Nathalie VÉZINA, « L'exonération fondée sur l'état des connaissances scientifiques et techniques, dites du 'risque de développement' : regard sur un élément perturbateur dans le droit québécois de la responsabilité du fait des produits », dans Pierre-Claude LAFOND (dir.), *Mélanges Claude Masse : En quête de justice et d'équité*, Cowansville, Éditions Yvon Blais, 2003, p. 433 et suiv. ; Marie-Ève ARBOUR, « Itinéraire du risque de développement à travers des codes et des constitutions », dans Benoît MOORE (dir.), *Mélanges Jean-Louis Baudouin*, Cowansville, Éditions Yvon Blais, 2012, p. 677 et suiv.
[204] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-384 ; P.-G. JOBIN, préc., note 180, par. 216 ; P. FRÉCHETTE, préc., note 154, par. 74.

connaissances », il faut entendre « l'ensemble des indications de dangers et de problèmes connus par les différents intervenants, scientifiques et techniques, sur le marché concerné »[205].

Ce dernier moyen d'exonération est controversé parce qu'il fait reposer sur les utilisateurs « le fardeau de l'évolution des connaissances scientifiques » et qu'il écarte l'application d'un principe de précaution afin d'imposer au fabricant celui, plus ancien, du danger prévisible en fonction des connaissances actuelles[206]. Mais, dès que le fabricant est mis au courant d'un défaut de sécurité grevant l'un de ses produits[207], il doit s'assurer d'exercer à nouveau son obligation de renseignement auprès des victimes potentielles[208]. S'il s'acquitte trop tardivement de cette obligation, il empêchera d'écarter sa responsabilité[209]. Terminons en faisant remarquer que cette obligation de renseignement continue est une : « […] obligation de moyens renforcée d'une présomption de faute, car le fardeau de la preuve repose sur le fabricant »[210].

b) Autres régimes applicables au fabricant en matière de sécurité du bien

Si nous avons décidé de porter notre attention sur le régime qui vient d'être présenté aux fins du présent mémoire, il convient cependant, par souci d'exhaustivité, de dire quelques mots sur les autres règles relatives à la sécurité des produits qui peuvent s'appliquer au fabricant.

---

[205] *Lebel* c. *2427-9457 Québec inc.*, préc., note 175, citant Jean PINEAU, « Théorie des obligations », dans *La réforme du Code civil, Obligations, contrats nommés*, tome II, textes réunis par le Barreau du Québec et la Chambre des notaires du Québec, Ste-Foy, P.U.L., 1993, 9-233, p. 304.

[206] P.-G. JOBIN, préc., note 180, par. 214 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, 2-384 ; On considère généralement que cette approche découle du souhait d'encourager l'innovation technologique, quoique les impacts supposés néfastes sur l'innovation de la suppression de ce moyen d'exonération sont parfois remis en question. À ce sujet, voir : Marie-Ève ARBOUR, « Portrait of Development Risk as a Young Defence », (2014) 59-4 *McGill Law Journal* « Technological Innovation and Civil Responsibility » 915. Pour un historique législatif québécois de ce moyen d'exonération et des objectifs divergents lors de la mise en place du régime, voir N. VÉZINA, préc., note 203, p. 442 et suiv.

[207] P. FRÉCHETTE, préc., note 154, par. 75 : étant donné que l'art. 1473 al. 2 C.c.Q. utilise l'expression « lorsqu'il a eu connaissance de l'existence du défaut », on peut faire remarquer que l'obligation de renseignement subséquente à la mise en marché du produit ne prend naissance qu'à moment de la connaissance, subjective, du fabricant.

[208] C.c.Q., art 1473 al. 2 *in fine* ; V. KARIM, préc., note 166, par. 3200 ; P.-G. JOBIN, préc., note 180, par. 217 : « même [les défauts de sécurité] qui ne sont pas visés par la théorie des risques de développement ».

[209] V. KARIM, préc., note 166, par. 3200.

[210] P.-G. JOBIN, préc., note 180, par. 217.

i) La responsabilité contractuelle dans le cadre du droit commun de la vente

Le régime de la responsabilité contractuelle découlant de la sécurité des biens a été développé antérieurement à celui que nous venons de décrire. Lorsque les parties sont liées par un contrat, les options de la victime d'un préjudice en raison d'un bien dangereux diffèrent sensiblement. D'une part, l'obligation de fournir un bien libre d'un défaut de sécurité découle du droit commun de la vente et plus précisément de la garantie de qualité prévue aux articles 1726 et suivants du C.c.Q. Ce sera le cas lorsque le défaut de sécurité découle d'une défectuosité qui n'était pas apparente au moment de la vente, par exemple. Notons qu'aux fins de cette garantie, le fabricant est assimilé au vendeur professionnel[211]. Aux termes du C.c.Q., le vendeur est tenu de garantir à l'acheteur que le bien vendu est exempt de vices cachés[212]. La notion de vice prévoit trois formes de défectuosités : « une défectuosité matérielle (le bien s'avère endommagé ou est affecté d'un défaut esthétique), une défectuosité fonctionnelle (impossibilité de s'en servir selon la destination normale) ou une défectuosité conventionnelle (impossibilité de s'en servir pour une fin spécifique) »[213]. Afin d'engager la responsabilité du vendeur, le demandeur doit démontrer l'existence d'un vice à la fois grave, caché, antérieur à la vente et inconnu de l'acheteur au moment de l'achat[214]. Ce régime, dont nous pourrions évidemment dire beaucoup, pourrait s'appliquer à l'encontre du fabricant d'un bien lorsque le défaut de sécurité découle d'un vice de conception ou de fabrication[215].

Cependant, la responsabilité du vendeur pourra être retenue même si le bien ne comporte pas de vice caché. Il suffit de penser à un bien fonctionnant correctement, mais présentant des risques à l'utilisation importants qui n'auraient pas été correctement divulgués par le vendeur[216]. Dans ce cas, on considérera que sa responsabilité contractuelle est engagée du fait de son manquement à l'obligation de divulguer les dangers inhérents du bien – laquelle découle du contenu implicite du contrat de vente[217]. On considère généralement que le régime

[211] C.c.Q., art. 1730 ; Jacques DESLAURIERS, *Vente, louage, contrat d'entreprise ou de service*, 2e éd., Montréal, Wilson & Lafleur, 2013, par. 442.
[212] C.c.Q., art. 1726 al. 1 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-388.
[213] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-289.
[214] *Id.*, par. 2-390.
[215] *Id.*, par. 2-392.
[216] J. DESLAURIERS, préc, note 211, par. 705.
[217] C.c.Q., art. 1434 ; J. DESLAURIERS, préc, note 211, par. 705.

extracontractuel de l'article 1468 C.c.Q. peut servir d'inspiration à cet égard[218]. Le C.c.Q. créé également un régime applicable au vendeur professionnel en lui opposant une présomption d'antériorité du vice qui fait que le demandeur n'a qu'à « prouver la détérioration objective prématurée du bien en le comparant à des biens de même espèce »[219].

ii) La responsabilité contractuelle dans le cadre du contrat de consommation

En ce qui concerne les contrats de consommation, le législateur québécois a créé un régime particulier concernant la sécurité des produits avec la L.P.C. À la suite de tout contrat passé entre un consommateur et un commerçant, la L.P.C. offre au consommateur un recours contre le fabricant dans le cas d'un dommage attribuable au défaut de sécurité d'un bien ou au manque d'informations nécessaires quant à son utilisation[220].

Notons immédiatement que la L.P.C. dispose d'un champ d'application différent de l'article 1468 C.c.Q. et ne s'adresse qu'aux consommateurs liés au fabricant par un contrat de consommation. Dans le cas d'un tiers qui se trouverait victime d'un dommage causé par la défaillance informatique d'un S.C.P., il ne pourrait invoquer ce régime. Le régime créé par la L.P.C. diffère également de celui créé par l'article 1468 C.c.Q. en ce qu'il écarte l'exonération relative aux risques de développement. En effet, la L.P.C. crée une présomption absolue de connaissance du vice contre le fabricant[221].

En raison du fait qu'elle ne s'applique pas en dehors de tout lien contractuel, nous ne nous pencherons pas davantage sur la L.P.C., quoique le recours qui y est prévu peut être intéressant pour qui peut s'en prévaloir étant donné qu'il impose une obligation de résultat au fabricant[222].

iii) Règles découlant de la législation fédérale

Outre les règles provinciales, les personnes impliquées dans la mise en marché d'un produit sont également soumises à quelques règles de juridiction fédérale visant à encadrer la

[218] J. DESLAURIERS, préc, note 211, par. 705.
[219] C.c.Q., art. 1729 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-397 et suiv.
[220] L.P.C., art. 53.
[221] L.P.C., art. 54 al. 3 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-401.
[222] V. KARIM, préc., note 166, par. 3185.

sécurité des produits de consommation. Celles-ci sont de nature surtout préventive et créent un cadre législatif moins large. Elles obligent notamment de faire figurer des indications sur l'étiquette d'un produit, notamment son identité, sa quantité nette et le nom et l'établissement principal du fournisseur[223]. De même, la législation fédérale interdit de mettre en marché un produit qui présente vraisemblablement un danger pour la santé ou la sécurité du public. Il faut remarquer cependant qu'en pratique, un produit dangereux sera interdit de commercialisation seulement après avoir été spécifiquement désigné comme tel par la Division de la Sécurité des produits de consommation en sein de Santé Canada[224]. Enfin, la loi fédérale n'impose aucune obligation directe au fabricant de notifier Santé Canada de l'existence d'un risque relatif à l'un de ses produits[225].

2. Aspect informationnel de la sécurité

Nous l'avons vu, en raison de la nature ni strictement physique, ni strictement virtuelle des S.C.P., il n'est pas possible d'étudier la question de leur sécurité sans aborder l'un et l'autre de ces aspects. C'est donc que le juriste, s'il veut déterminer la responsabilité du fabricant en cas de dommage causé par un S.C.P. en raison d'une défaillance informatique, devra également prendre conscience des particularités du volet numérique des S.C.P.

Heureusement, il existe un cadre juridique qui traite de cette question : celui de l'obligation générale de sécurité informationnelle. En effet, de même qu'il existe des règles visant à assurer la sécurité physique des personnes et des biens, de même a-t-on développé un régime afin d'assurer la protection des données informatiques. On peut difficilement s'en étonner, d'ailleurs, en considérant le rôle prédominant que l'information a acquis au courant des dernières décennies. Il n'y a guère d'État, de société ou même de particulier qui ne dépende pas aujourd'hui au moins indirectement du bon fonctionnement des systèmes informatiques. Il y a donc un impératif tant social qu'économique à assurer la sécurité informationnelle. Dans bien

[223] *Loi sur l'emballage et l'étiquetage des produits de consommation*, L.R.C. (1985), c. C-38 ; N. VÉZINA et F. MANIET, préc., note 152, par. 11.
[224] *Loi sur les produits dangereux*, L.R.C. (1985), c. H-3 ; N. VÉZINA et F. MANIET, préc., note 152, par. 15 et suiv.
[225] N. VÉZINA et F. MANIET, préc., note 152, par. 22.

des cas, une défaillance peut s'avérer extrêmement dommageable[226], même s'il n'est pas toujours facile de quantifier le phénomène de la cybercriminalité[227].

Évidemment, la sécurité informationnelle est un enjeu majeur dans la mise en place et l'opération des S.C.P. Une fois que nous aurons présenté la base théorique entourant cette obligation dans la section suivante, nous aurons le vocabulaire pour discuter de ce sujet en lien avec l'objet de notre étude, et nous terminerons ce chapitre avec quelques remarques sur la sécurité informationnelle des S.C.P.

a) L'obligation de sécurité informationnelle

i) Les bases législatives de l'obligation de sécurité informationnelle

Au Québec, l'obligation de sécurité informationnelle n'est pas mise en place par un instrument législatif monolithique. Elle est, au contraire, créée par le jeu de dispositions provenant de lois statuant sur des matières diverses : l'article 1457 C.c.Q., l'article 25 L.C.C.J.T.I., l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*[228] et, relativement aux données associées aux personnes canadiennes résidant hors du Québec[229], l'article 4.7 du *Code type sur la protection des renseignements personnels*[230]. En outre, il existe dans le domaine public d'autres lois qui s'expriment au sujet des mesures à

---

[226] De nombreux exemples récents l'attestent : Michael CIEPLY et Brooks BARNES, « Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm », (30 décembre 2014) *The New York Times*, en ligne : <https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html> (consulté le 12 décembre 2017) ; Tara S. BERNARD et al., « Equifax Says Cyberattack May Have Affected 143 Million in the U.S. », (7 septembre 2017) *The New York Times*, en ligne : <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html> (consulté le 12 décembre 2017) ; Rachel ABRAMS, « Target Puts Data breach Costs at $148 Million, and Forecasts Profit Drop », (5 août 2014) *The New York Times*, en ligne : <https://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html> (consulté le 12 décembre 2017).

[227] Anne-Marie CÔTÉ, Maxime BÉRUBÉ et Benoit DUPONT, « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », (2016) *Réseaux*, p. 203-224.

[228] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1 (la « **L.P.R.P.S.P.** »).

[229] N. W. VERMEYS, préc., note 145, p. 107.

[230] *Loi sur la protection des renseignements personnels et documents électroniques*, L.C. (2000), c. 5, (la « **L.P.R.P.D.E.** »), Annexe 1 : Principes énoncés dans la norme national du Canada intitulée Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96.

prendre par les organes du gouvernement pour assurer la sécurité des données qu'ils détiennent[231].

Les lois que nous venons d'aborder ont des objectifs divers : tantôt sanctionner la faute de celui qui gère les données pour autrui[232], tantôt assurer la sécurité juridique des communications[233], tantôt protéger la vie privée[234]. Les personnes qu'elles visent varient en fonction de l'objet de ces lois. Pour le C.c.Q., c'est « toute personne »[235], la L.C.C.J.T.I., notamment « la personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel »[236], tandis que la L.P.R.P.S.P. vise « toute personne qui exploite une entreprise » et qui gère des renseignements personnels[237].

Ces dispositions s'expriment assez vaguement sur les mesures exactes à prendre par le débiteur de l'obligation. L'article 1457 C.c.Q. est évidemment une disposition à vocation générale auprès de laquelle il serait hardi d'espérer trouver des enseignements précis au sujet de la sécurité informationnelle. Mais même les lois qui traitent plus spécifiquement du domaine ne nous offrent guère mieux que : « prendre les mesures de sécurité propres à […] assurer la confidentialité [des documents technologiques] »[238] ou « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels […] raisonnables […] »[239]. Que sont donc ces mesures de sécurité ? Quand sont-elles suffisantes ? Que visent-elles précisément à protéger, et contre quoi ?

---

[231] *Loi sur l'accès à l'information*, L.R.C. (1985), c. A-1 ; *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, L.R.Q., c. G-1.03.
[232] C.c.Q., art. 1457.
[233] L.C.C.J.T.I., art. 1 al. 1.
[234]L.P.R.P.S.P. ; L.P.R.P.D.E.
[235] C.c.Q., art. 1457.
[236] L.C.C.J.T.I., art. 25.
[237] L.P.R.P.S.P., art. 10.
[238] L.C.C.J.T.I., art. 25.
[239] L.P.R.P.S.P., art. 10.

ii) Ce qu'on cherche à sécuriser : l'information et ses attributs

En sécurité informationnelle, ce qu'on cherche à protéger, c'est évidemment l'information. Selon l'Office québécois de la langue française, la sécurité informationnelle, c'est la :

> « [P]rotection des ressources informationnelles d'une organisation, face à des risques identifiés, qui résulte d'un ensemble de mesures prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée. »[240]

Selon la position doctrinale dominante et tel qu'on peut le constater dans la définition qui vient d'être reproduite, lorsqu'on cherche à assurer la protection des ressources informatiques, c'est en réalité trois choses que l'on tente de protéger : la confidentialité, l'intégrité et la disponibilité des données[241]. Cette triade, parfois abrégée par l'expression « C.I.D. »[242], est composée des éléments les plus souvent considérés comme les principaux blocs constitutifs de la sécurité informationnelle[243], lesquels sont notamment repris par la loi québécoise[244].

Mais on considère parfois que deux éléments supplémentaires doivent être ajoutés à la triade C.I.D. : l'authenticité et l'irrévocabilité des données[245]. Ces deux dimensions sont souvent encastrées directement dans le concept d'intégrité, parce qu'on vérifie l'intégrité des données

---

[240] O.Q.L.F., préc., note 64, « sécurité informationnelle » ; N. W. VERMEYS, préc., note 145, p. 4.
[241] N. W. VERMEYS, préc., note 145, p. 23.
[242] En anglais, la triade « C.I.A. » pour les termes « *Confidentiality* », « *Integrity* » et « *Accessibility* ».
[243] Nicolas W. VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », *Document de travail du Labortoire de Cyberjustice* No. 11, 2014, p. 84. En effet, la triade C.I.D. revient continuellement afin de définir la sécurité informationnelle. Voir aussi : COMMITEE ON NATIONAL SECURITY SYSTEMS, « Information Security », en ligne : <https://www.hsdl.org/?view&did=7447> (consulté le 12 décembre 2017) : « *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability* ».
[244] L.C.C.J.T.I., art. 26 al. 2 : « […] assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance » ; N. W. VERMEYS, préc., note 145, p. 24.
[245] GOUVERNEMENT DU QUÉBEC, « Guide pour l'élaboration d'une politique de sécurité de l'information numérique et des échanges électroniques », S*tandards du gouvernement du Québec pour les ressources informationnelles (SGQRI 34)*, Version 1.0, Juillet 2003, p. 34.

notamment en validant leur authenticité et en s'assurant de leur irrévocabilité[246]. Néanmoins, nous dirons un mot à leur sujet, car elles peuvent nous aider à mettre l'emphase sur des notions qui prendront en importance dans la seconde partie de ce mémoire.

A. Disponibilité

Le mot « disponibilité » renvoie à la qualité d'une chose dont on peut « faire […] ce que l'on veut »[247], à laquelle on peut accéder[248]. En sécurité informatique, on dira que c'est « la propriété d'un document qui est accessible dans les délais convenables pour les personnes autorisées »[249]. D'autres sources définissent également la disponibilité comme étant l'exigence d'assurer que les systèmes fonctionnent en temps opportun et que le service ne soit pas inaccessible aux utilisateurs autorisés[250], ou encore, simplement : « *we want the computer to work <u>when</u> we expect it to » et « <u>as</u> we expect it to* »[251] (nos soulignés).

Logiquement, l'exigence de maintenir la disponibilité se manifestera de deux façons : d'abord préserver la disponibilité des données elles-mêmes et ensuite préserver la disponibilité de l'infrastructure informatique et logicielle permettant d'y accéder[252]. En effet, un document technologique est inutile si on ne peut pas le décoder, par exemple en raison du manque de logiciel compatible pour l'afficher.

La L.C.C.J.T.I. s'exprime sur l'exigence de disponibilité en reconnaissant le besoin d'assurer également la disponibilité des infrastructures[253]. L'article 19 de cette loi indique expressément qu'il faut voir à la « disponibilité du matériel qui permet de rendre [le document]

---

[246] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*, Guide for Conducting Risk Assessments*, SP 800-30 Revision 1, 2012, p. B-7, en ligne : <u>http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf</u> (consulté le 12 décembre 2017).
[247] Claude BLUM (dir.), *Le nouveau petit Littré*, Paris, Éditions Garnier, 2009, p. 610, « Disposer ».
[248] Afin de créer l'acronyme « C.I.A. », plus facile à retenir pour des raisons évidentes, on utilise parfois le terme « accessibilité », quoique moins propre à cette utilisation.
[249] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note 242, p. 85.
[250] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. B-2 ; Barbara GUTTMAN et Edward A. ROBACK (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), *An Introduction to Computer Security*: *The NIST Handbook*, Gaithersburg, NIST, 1995, p. 7.
[251] Bruce SCHNEIER, *Secrets and Lies. Digital Security in a Networked World*, 15th Anniversary Edition, Indianapolis, John Wiley & Sons, Inc., 2015, p. 122.
[252] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note 242, p. 85.
[253] L.C.C.J.T.I., art. 19, 23.

accessible […] »[254]. En droit public, les diverses lois sur l'accès à l'information prévoient aussi une obligation pour les organismes publics de préserver la disponibilité des documents visés par le droit d'accès[255].

Afin d'assurer cette disponibilité, il faudra généralement entretenir l'équipement informatique en effectuant les réparations et les mises à niveau nécessaires en temps opportun. La mise en place d'un système de sauvegarde des données (« *backup* ») est de mise afin de restaurer la disponibilité en cas de défaillance. Dans certains cas, des mesures de réponse aux désastres doivent être prévues afin de répondre aux éventuels incendies, tremblements de terre, et autres désastres.

Terminons en soulignant que l'impératif de disponibilité des informations est en contradiction avec l'idée d'une sécurité maximale : toute façon d'accéder aux données est en même temps une surface d'attaque qui en compromet la sécurité[256]. Un prudent calcul est donc de mise.

B. Intégrité

Est intègre ce « qui ne se laisse pas altérer, corrompre »[257], ce qui est « demeuré intact »[258]. C'est la « propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format pendant leur utilisation »[259]. Elle fait également référence aux propriétés de complétude et d'exactitude des données[260]. L'ensemble de ces qualités sont importantes lorsqu'on veut pouvoir faire confiance aux données et y fonder une quelconque décision[261].

---

[254] L.C.C.J.T.I., art. 19.
[255] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, art. 9 et 83 ; *Loi sur l'accès à l'information*, art. 4.
[256] N. W. VERMEYS, préc., note 145, p. 25.
[257] Le Nouveau Petit Littré, préc., note 247, p. 1074, « Intègre ».
[258] Le Nouveau Petit Robert, préc., note 121, p. 1349, « Intégrité ».
[259] O.Q.L.F., préc., note 64, « Intégrité » ; GOUVERNEMENT DU QUÉBEC, préc., note 245 ; C.N.S.S., *National Information Assurance Glossary*, 2010, p. 38 : « *integrity : The property whereby an entity has not been modified in an unauthorized manner* » ; B. SCHNEIER, préc., note 251, p. 73 : « *Integrity [is concerned] whether [data] has been modified since its creation* ».
[260] GOUVERNEMENT DU QUÉBEC, préc., note 245, p. 9 : « intégrité ».
[261] B. SCHNEIER, préc., note 251, p. 73.

La notion d'intégrité en sécurité informatique fait l'objet de conceptions parfois divergentes dans la littérature technique. Certaines sources distinguent deux types d'intégrité : l'intégrité des données et l'intégrité des systèmes. Selon cette première conception, l'intégrité des données réfère à l'exigence que les documents et les programmes informatiques d'un système soient seulement altérés de la façon voulue, alors que l'intégrité des systèmes, quant à elle, réfère à l'exigence que l'ordinateur puisse exécuter les fonctions voulues sans être entravées par une intervention délibérée ou involontaire[262].

On peut encore dire de la notion d'intégrité qu'elle fait référence à l'idée d'intelligibilité : la plupart du temps, un document corrompu ne sera plus lisible par l'ordinateur, qui n'arrivera plus à l'interpréter. En outre, il est possible de faire un rapprochement entre les idées d'intégrité et de fiabilité : un document dont on ne peut s'assurer de l'intégrité, et donc dont on ne peut pas s'assurer qu'il n'a pas été altéré ne saurait soutenir une prise de décision, notamment dans un contexte judiciaire[263].

Le législateur québécois a donné une définition de l'intégrité à l'article 6 L.C.C.J.T.I. : « [l]'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue »[264]. Cette loi s'intéresse à préserver l'intégrité des documents technologiques tout au long de leur cycle de vie (leur création, leur transfert, leur consultation, leur transmission et durant leur archivage ou leur conservation)[265]. Cette obligation ne se limite pas, comme on pourrait le penser, au seul cadre du droit de la preuve[266]. Elle s'applique à tous les documents technologiques, qu'il s'agisse des données, de bases de données, ou encore de logiciels, qu'ils soient fragmentés, compressés ou archivés[267].

D'ailleurs, il est intéressant de constater que la L.C.C.J.T.I. crée également l'obligation de mettre en place des mesures de sécurité permettant de s'assurer que l'intégrité des données a

[262] B. GUTTMAN et A. ROBACK, préc., note 250, p. 6.
[263] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note 242, p. 92.
[264] L.C.C.J.T.I., art. 6 al. 1.
[265] L.C.C.J.T.I., art. 3 al. 1, art. 6 ; P. TRUDEL, préc., note 141, p. 69.
[266] L.C.C.J.T.I., art. 19 ; N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note 242, p. 91.
[267] L.C.C.J.T.I., art. 30 al. 2.

été préservée[268]. À cette fin, l'usage de métadonnées est à recommander. Celles-ci sont liées au document principal et en spécifient certaines caractéristiques telles que sa date de création, de modification et l'identité des personnes les ayant effectués[269]. Il faudra évidemment s'assurer de préserver l'intégrité des métadonnées elles-mêmes[270]. De nombreuses méthodes cryptographiques existent pour effectuer ces vérifications[271] et celles-ci se rapportent notamment à l'authenticité et à l'irrévocabilité que nous verrons bientôt.

C. Confidentialité

Sans doute la confidentialité est-elle l'aspect auquel on accorde habituellement le plus d'attention en matière de sécurité de l'information. Ce qui est confidentiel, c'est ce « […] dont la diffusion se limite à un nombre restreint de personnes »[272]. Maintenir la confidentialité des données, c'est donc mettre en place des mesures qui restreignent l'accès aux données seulement aux personnes autorisées[273].

D'un point de vue juridique, quelles informations doivent être considérées confidentielles ? Bien que de nombreuses lois visant à encadrer la gestion de la confidentialité d'informations de tout type (secrets relevant de la sécurité nationale, secrets industriels ou de commerce ou encore les renseignements personnels) ont été édictées tant au niveau provincial que fédéral[274], nulle part parmi cette foule de textes législatifs retrouvons-nous une définition de l'expression « renseignement confidentiel »[275] (sauf dans le contexte des renseignements détenus par un organisme public). Généralement, il semble que la portée de ce terme variera en fonction du contexte. Il est cependant possible de faire certaines observations.

---

[268] L.C.C.J.T.I., art. 6.
[269] O.Q.L.F., préc., note 64, « métadonnées » : « Ensemble structuré de données accompagnant un ouvrage et servant notamment à en décrire le contenu et le format, à assurer son indexation dans les moteurs de recherche et les bases de données, et à faciliter la gestion des droits d'auteur qui y sont liés. ».
[270] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note 242, p. 94.
[271] B. GUTTMAN et A. ROBACK, préc., note 250, p. 227. La personne visée par l'obligation devra cependant s'assurer que ces mesures cryptographies (de même que toutes les autres mesures de sécurité, bien entendu) soient adéquates selon les circonstances et qu'elles ne soient pas tombées en désuétude, comme la méthode de hachage « M.D. 5 », dont l'usage n'est plus recommandé.
[272] Le Nouveau Petit Littré, préc., note 247, p. 397, « Confidentiel ».
[273] 44 U.S.C. § 3542 (b) (1) (B), repris par NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. B-3 ; GOUVERNEMENT DU QUÉBEC, préc., note 245, p. 34.
[274] Par exemple la L.C.C.J.T.I., art. 25.
[275] *R.* c. *Stewart*, [1988] 1 R.C.S., par. 33.

La jurisprudence a donné quelques pistes d'analyse afin de déterminer si un renseignement doit être considéré comme confidentiel. Il ne suffit évidemment pas qu'une personne déclare un renseignement est confidentiel pour qu'il en soit automatiquement ainsi[276]. La jurisprudence a dressé une liste de critères permettant d'identifier le caractère confidentiel d'une information[277].

Nous devons également dire que toute information confidentielle ne bénéficiera pas nécessairement du même degré de protection. Celui variera en fonction de l'ampleur du dommage qui serait causé si l'information était divulguée. En tous les cas, le juriste confronté au problème de la confidentialité des données devra se demander si, compte tenu des circonstances, le droit attribue un caractère confidentiel aux données visées et, par la suite, déterminer le degré de protection à assurer.

Notons enfin l'évidente tension qui apparaît entre deux exigences contradictoires de la triade C.I.D. En effet, les objectifs de la confidentialité et la disponibilité s'opposent par définition : l'une vise à restreindre l'accès aux données et l'autre à le permettre. La solution sera de permettre l'accès uniquement aux personnes autorisées, ce qui crée la nécessité de déterminer qui doit être autorisé et par quels moyens elles pourront accéder aux données.

D. Authenticité et irrévocabilité

Voyons finalement les deux dernières propriétés de l'information à protéger. D'abord, est authentique ce « dont la certitude, dont l'autorité ne peut être contestée »[278]. Selon le N.I.S.T., l'authenticité des données, c'est : « *the property of being genuine and being able to be verifiable and trusted; confidence in the validity of a transmission, a message, or message*

[276] Marie-France BICH, « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans S.F.P.B.Q., *Développements récents en droit de la propriété intellectuelle*, Cowansville, Éditions Yvon Blais, 2003, p. 305.
[277] *Pharand Ski Corp.* c. *Alberta*, 1991 CarswellAlta 85 (ABQB), par. 144, cité par N. W. VERMEYS, préc., note 145, p. 30-31. Cette liste non-exhaustive est composée des éléments suivants : (1) l'étendue de la diffusion de l'information à l'extérieur de l'entreprise ; (2) l'étendue de la diffusion de l'information au sein de l'entreprise ; (3) l'étendue des mesures de sécurité mise en place pour assurer la confidentialité de l'information ; (4) la valeur de l'information pour des tiers ; (5) l'argent ou l'effort investis afin de collecter ou développer l'information ; et (6) la facilité avec laquelle un tiers pourrait acquérir ou dupliquer l'information par lui-même.
[278] Le Nouveau Petit Littré, préc., note 247, p. 142, « Authentique ».

originator »[279]. Celle-ci s'assure par des procédés certifiant la validité d'un utilisateur, d'un processus ou d'un dispositif[280]. Contrairement à l'intégrité, l'authenticité ne s'intéresse pas directement de savoir si les données ont été modifiées après leur création. Elle vise seulement à permettre de s'assurer de leur origine[281].

Ensuite, est irrévocable ce qu'on ne peut « contester, mettre en doute »[282]. Également appelée la « non-répudiation », cette notion fait référence aux mesures mises en place pour empêcher un individu de nier avoir posé un geste sur des données – ce par quoi nous entendons par exemple l'action de créer un document, ou encore d'envoyer ou de recevoir un message[283].

En sécurité informationnelle, ces deux notions visent à permettre d'établir un lien entre une personne et une opération posée sur un document. L'authenticité vise à établir ce lien[284], alors que l'irrévocabilité, quant à elle, cherche à assurer que ce lien ne puisse être brisé. Ces deux caractéristiques s'obtiennent notamment par la mise en place de mesures cryptographiques, telles que l'usage de signatures numériques[285].

La L.C.C.J.T.I. réfère implicitement aux notions d'authenticité et d'irrévocabilité à son troisième chapitre intitulé « Établissement d'un lien avec un document technologique »[286]. En s'exprimant en termes techniques et plutôt abstraits, elle vise à permettre d'établir un lien entre une personne et un document, ou encore entre un objet et un document[287]. En pratique, ceci peut être accompli par un ensemble de technologies, dont la plus fréquente est celle de la

---

[279] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. B-2 ; C.N.S.S., préc., note 259, p. 5 ; B. SCHNEIER, préc., note 251, p. 73 : « *Authentification has to do with the origin of the data […]* ».

[280] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. B-2 ; GOUVERNEMENT DU QUÉBEC, préc., note 245, p. 34.

[281] B. SCHNEIER, préc., note 251, p. 73.

[282] Le Nouveau Petit Littré, préc., note 247, p. 1843, « révoquer ».

[283] C.N.S.S., préc., note 259, p. 50 : « *non-repudiation : Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. NIST 800-53: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message* ».

[284] B. SCHNEIER, préc., note 251, p. 68.

[285] *Id.*, p. 96-97, 225 : « *A digital signature is a mathematical operation on a bucket of bits [un fichier, par exemple] that only a certain key can do. […] The signing key is only known by Alice. Hence, the argument goes, only Alice could have performed the mathematical operation and therefore Alice 'signed' the bucket of bits* ».

[286] L.C.C.J.T.I., art. 38-62.

[287] À ce sujet, voir P. TRUDEL, préc., note 141, ch. 5, p. 113 à 166.

cryptographie asymétrique[288]. Évidemment, il y a encore fort à dire sur ce sujet assez complexe, mais ce n'est pas nécessaire dans le cadre de ce mémoire[289].

En somme, la sécurité de l'information est un lieu de tension entre des éléments interdépendants : disponibilité, intégrité, confidentialité, authenticité et irrévocabilité. Comment les acteurs chargés de sécuriser les données doivent-ils décider des mesures appropriées à prendre ? Pour répondre à cette question, il convient de développer davantage la notion de sécurité informationnelle afin de savoir à l'encontre de quoi on cherche à protéger l'information.

iii) Contre quoi on cherche à sécuriser l'information : le risque en sécurité informationnelle

Dans la définition de la sécurité informationnelle citée en début de la présente section, nous avons vu, en effet, que si on tente d'assurer « la confidentialité, l'intégrité et la disponibilité de l'information traitée », c'est face à des « risques identifiés »[290].

Comment définit-on le risque ? Selon l'Office québécois de la langue française, il s'agit d'un : « [é]vènement éventuel, incertain, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage »[291]. Autrement dit, c'est une « probabilité de subir […] un dommage »[292] découlant de la perte de confidentialité, d'intégrité ou de disponibilité d'information ou de systèmes informatiques[293]. Le législateur américain offre une description plus précise de ces dommages : il s'agit de tout accès, usage, divulgation, interruption, modification ou destruction non autorisée de données ou de systèmes informationnels[294].

Ici quelques remarques s'imposent. Selon le N.I.S.T. : « *Threats to information systems can include purposeful attacks, environmental diruptions, human/machine errors, and*

[288] P. TRUDEL, préc., note 141.
[289] Voir P. TRUDEL, préc., note 141, pour des explications détaillées à ce sujet.
[290] O.Q.L.F., préc, note 64, « sécurité informationnelle ».
[291] *Id.*, « risque » ; N. W. VERMEYS, préc., note 145, p. 17.
[292] N. W. VERMEYS, préc., note 145.
[293] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. 6.
[294] 44 U.S.C. § 3542 (b) « Information Security » : « *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability* ».

structural failures […] »[295]. La sécurité informationnelle ne se limite donc pas à la sécurisation des systèmes informatiques eux-mêmes, mais vise également l'environnement physique qui les entoure et les pratiques des employés qui y ont accès[296]. De même est-il possible d'affirmer que la sécurité informationnelle vise tant le support que le contenu[297], ou qu'elle ne vise pas uniquement à protéger les systèmes des attaques malicieuses de pirates ou de bidouilleurs[298]. Au contraire, elle est aussi appelée à répondre à des atteintes non intentionnelles à la sécurité, telles la survenance de bris de matériel informatique ou d'erreurs humaines imputables aux employés d'une organisation.

Afin de mieux appréhender le risque dans son étourdissante variété, nous utilisons des modèles du risque. Ceux-ci proposent différents concepts clés qui aident à décortiquer celui-ci, par exemple la menace, la vulnérabilité, le dommage possible en cas de survenance du risque, sa probabilité les conditions prédisposant à sa celle-ci[299]. Ces différentes propositions de taxinomie du risque visent à faciliter l'approche d'une personne chargée de sécuriser les ressources informationnelles d'une organisation.

iv) Comment on sécurise l'information : les mesures de sécurité

À cette étape de notre réflexion, il est temps de dévoiler la triste réalité de la sécurité informationnelle : la mise en place d'une sécurité parfaite est impossible[300]. Comme on ne peut pas prédire l'avenir, il est en effet vain d'espérer prévoir toutes les manifestations du risque. Par ailleurs, à mesure que l'organisation qu'on cherche à sécuriser augmente en taille et en complexité, il sera de plus en plus difficile de colmater toutes ses vulnérabilités.

Le mieux qu'on peut espérer pour remplir ses obligations en sécurité informationnelle, c'est de procéder à une gestion du risque adéquate en fonction des circonstances. En effet, si

[295] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. 1.
[296] C'est ainsi que l'expression « sécurité informatique » n'est pas équivalente à l'expression « sécurité informationnelle » que nous utilisons depuis le début de cette étude. La « sécurité informatique » est en réalité une sous-catégorie de la « sécurité informationnelle », laquelle est plus large. Voir N. W. VERMEYS, préc., note 145, p. 20.
[297] N. W. VERMEYS, préc., note 145, p. 21.
[298] Le terme recommandé pour l'anglais « *hacker* ».
[299] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. 8.
[300] N. W. VERMEYS, préc., note 145, p. 14.

l'on ne peut pas éliminer le risque entièrement, on peut cependant chercher à le maintenir dans des proportions normales. À cette fin, le N.I.S.T. propose une démarche en quatre étapes : (1) l'identification des risques ; (2) l'analyse des risques ; (3) la réponse aux risques (la mise en place de mesures de sécurité) ; et (4) la surveillance des risques[301]. Dans certaines juridictions, la loi exige explicitement de procéder à une analyse de risques[302]. Au Québec, cette obligation est sous-entendue au libellé de l'article 25 de la L.C.C.J.T.I.[303]

Concrètement, on peut soit éviter le risque, soit le transférer ou le mitiger, ou, à défaut, l'accepter – s'il est d'un niveau raisonnable[304]. Mais quand le risque ne saurait être accepté, nous mettons en place des mesures de sécurité informationnelles, c'est-à-dire des : « moyen[s] concret[s] assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent »[305]. Celles-ci se manifestent notamment dans l'élaboration et l'adoption d'une politique de sécurité de l'information.

Mais malgré toute démarche entreprise, en sécurité informationnelle, il n'existe pas de solution permanente. Les étapes de la gestion de risque, par exemple celles qui sont proposées par le N.I.S.T., doivent être répétées aussi souvent que nécessaire afin de s'assurer que l'approche reste pertinente au vu des circonstances[306].

Sans doute est-il clair à présent que la sécurité informationnelle relève plus d'un processus que d'un état ou d'un produit qu'on offrirait à ses clients[307] : ce qu'on considérera comme pouvant engager la responsabilité, c'est moins les contre-mesures particulières mises en place par une organisation que son processus de gestion de risque en général. C'est donc dire

[301] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. 4.
[302] N. W. VERMEYS, préc., note 145, p. 72.
[303] L.C.C.J.T.I., art 25 ; N. W. VERMEYS, préc., note 145, p. 73.
[304] N. W. VERMEYS, préc., note 145, p. 17, 34. Cette analyse est appelée « *information risk management* » (« I.R.M. ») par les experts.
[305] O.Q.L.F., préc., note 64, « mesure de sécurité de l'information ». Cette définition est reprise dans GOUVERNEMENT DU QUÉBEC, préc., note 246, p. 9 ; Voir également B. SCHNEIER, préc., note 251, p. 278 : « *Countermeasures are methods to reduce vulnerabilities.* ».
[306] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246, p. 5.
[307] B. SCHNEIER, préc., note 251, p. 84.

qu'une organisation doit pouvoir démontrer que celui-ci était adéquat dans les circonstances. Voyons plus précisément en quoi cela se manifeste.

v) Le niveau de sécurité à mettre en place par le débiteur de l'obligation

On dira qu'une organisation a commis une faute lorsqu'elle a procédé à « une mauvaise appréciation des risques, ou plutôt à l'acceptation d'un niveau de risque ''socialement anormal'' »[308]. Ceci nous amène à conclure qu'une organisation pourra éviter d'engager sa responsabilité en adoptant une conduite raisonnablement prudente et diligente, en mettant en place « toutes les mesures de sécurité jugées socialement normales [et en éliminant] tous les risques socialement inacceptables »[309]. Au Québec, bien que l'obligation de protéger la confidentialité, l'intégrité ou la disponibilité revient à plusieurs endroits[310], le cadre juridique reste cependant plutôt laconique sur le niveau de sécurité exact à atteindre et plus encore sur les mesures précises à mettre en place[311].

Comment déterminerons-nous en pratique ce qu'est un niveau de sécurité adéquat ? Pour répondre à cette question, on peut se tourner vers quelques barèmes – desquels il est évidemment possible de dire beaucoup, quoique nous nous en tiendrons à quelques lignes seulement.

Les normes de l'industrie[312], c'est-à-dire les usages en cours au sein de celle-ci, seront sans doute nos premiers guides. Elles peuvent être d'une aide incontestable. Cependant, il serait erroné de croire qu'elles nous permettront d'assurer une sécurité parfaite ou même nous empêcher d'être trouvés responsables – un usage largement répandu n'étant pas de ce seul fait automatiquement raisonnable[313].

Les normes développées par les organismes de normalisations publics ou privés peuvent être un autre outil[314]. Certaines normes, comme la norme I.S.O. 27002, la norme C.O.B.I.T. ou encore les G.A.S.S.P. visent en effet la sécurité informationnelle[315]. Il faut cependant s'abstenir

[308] N. W. VERMEYS, préc., note 145, p. 93.
[309] *Id.*, p. 94.
[310] L.P.R.P.S.P., art. 10 ; L.C.C.J.T.I., art. 25 ; C.c.Q., art. 1457 ; *Code-type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, annexe A à L.P.R.P.D.E., art. 4.7.
[311] N. W. VERMEYS, préc., note 145, p. 71
[312] Pour reprendre une expression plus ancienne, les « règle de l'art » : *Id.*, p. 119.
[313] *Id.*, p. 121.
[314] *Id.*, p. 128-138.
[315] *Id.*, p. 131.

de considérer que le respect de ces normes nous protégera des poursuites, car elles ne sont pas de nature juridique.

Sans doute peut-on également s'inspirer des recommandations émises par les organismes gouvernementaux. Par exemple, le N.I.S.T. publie des guides destinés aux différentes agences du gouvernement fédéral américain sur la mise en place de meilleures pratiques dans le domaine de la sécurité informationnelle[316]. Bien que les acteurs privés ou étrangers ne soient évidemment pas tenus de suivre ces guides, ils peuvent y trouver des renseignements pertinents.

On peut aussi se tourner vers les repères jurisprudentiels. Si les cours de justice ne peuvent nous venir en aide que d'une façon limitée en raison de la rareté des décisions sur ce sujet[317], les tribunaux administratifs responsables de la protection de la vie privée se sont prononcés plus souvent sur ce sujet[318]. Ainsi, on pourra s'informer dans une certaine mesure en lisant les recommandations de la *Commission d'accès à l'information du Québec*[319] et les conclusions du *Commissariat à la protection de la vie privée du Canada*[320].

Concrètement, le tout se manifestera par la mise en place d'un processus d'évaluation des actifs informationnels d'une organisation, par une analyse des risques les visant, suivi de l'élaboration d'une politique de sécurité et de la formation des employés à ce sujet, le tout devant être périodiquement révisé et mis à jour.

---

[316] Il s'agit de la série de publications spéciale 800 du N.I.S.T., dont certaines sont assez techniques. Voir par exemple : NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, préc., note 246 ; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, 2013, en ligne : <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (consulté le 12 décembre 2017) ; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Managing Information Security Risk*, Special Publication 800-39, 2011, en ligne : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> (consulté le 12 décembre 2017) ; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Guide to General Server Security*, Special Publication 800-123, 2008, en ligne : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf> (consulté le 12 décembre 2017) ; J. VOAS, préc., note 67.

[317] N. W. VERMEYS, préc., note 145, p. 174.

[318] *Id.*, p. 177.

[319] *Id.*

[320] *Id.*, p. 180.

b) Enjeux en sécurité informationnelle des systèmes cyberphysiques

S'il était peut-être intrépide de discuter de ce sujet sans avoir au moins préalablement posé les bases terminologiques nécessaires, il est désormais possible d'aborder les enjeux de la sécurité informationnelle des S.C.P.

Notre récit de l'exploitation des systèmes informatiques à bord des véhicules automobiles, dans l'introduction de ce mémoire, a sans doute déjà sensibilisé le lecteur quant aux conséquences physiques potentiellement catastrophiques d'un bris de sécurité informationnel au sein d'un S.C.P. Il existe malheureusement d'autres cas de faille de sécurité informationnelle ayant eu des conséquences dans le monde physique. Par exemple, dès l'année 2000, un employé mécontent avait exploité le système informatique de contrôle des égouts du comté de Maroochy Shire, en Australie, afin de provoquer un important déversement d'eaux usées dans des parcs, rivières et sur certaines propriétés privées des environs, causant ainsi des dommages considérables[321].

Les S.C.P. sont effectivement loin d'être à l'abri de telles failles, et la littérature technique souligne fréquemment la nécessité d'assurer leur sécurité[322]. Dans cette section, nous souhaitons explorer plus en détail les raisons derrière l'importance accrue de la sécurité informationnelle des S.C.P., et conséquemment de la pertinence de notre étude. Pourquoi dit-on qu'il est si important d'assurer la sécurité informationnelle des S.C.P. ?

i) Gravité des dommages amplifiée

En premier lieu, les conséquences d'une défaillance des systèmes informatiques d'un S.C.P. sont potentiellement beaucoup plus importantes que pour les systèmes informatiques traditionnels[323]. Leur vocation à agir sur le monde physique amplifie effectivement de beaucoup

[321] A. A. CARNENAS et al., préc., note 61 ; Tony SMITH, « Hacker jailed for revenge sewage attacks », (31 octobre 2001) *The Register*, en ligne : <https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/> (consulté le 12 décembre 2017).
[322] Voir par exemple : R. BAHETI et H. GILL, préc., note 53 ; A. A. CARENAS, S. AMIN et S. SASTRY, préc., note 53 ; M. CONTI et al., préc., note 15, p. 15 et suiv. ; C.P.S.P.W.G., préc., note 53, p. 13 ; S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 353 et suiv. ; K. KIM et P.R. KUMAR, préc., note 7, p. 1300 ; NATIONAL SCIENCE FOUNDATION, préc., note 55 ; R. RAJKUMAR et al., préc., note 31, p. 731 ; J. SHI, J. WAN et H. YAN, préc., note 53.
[323] C.P.S.P.W.G., préc., note 53, p. 13.

la gravité potentielle des dommages qu'une faille de sécurité informatique peut causer. Alors qu'auparavant un bris de sécurité pouvait mener au vol ou à la perte de données, désormais, dans le pire des cas, une défectuosité dans le domaine virtuel d'un S.C.P. peut causer la mort de son utilisateur ou d'une tierce partie, ou encore de graves dommages physiques.

Nous avons évoqué dans notre introduction les dangers associés à l'exploitation des systèmes informatiques à bord des automobiles[324]. Ceux-ci, cependant, ne sont qu'un type de S.C.P. pouvant faire l'objet d'une attaque informatique et de causer un sérieux préjudice. Peut-être plus inquiétantes encore sont les attaques contre les S.C.P. médicaux : stimulateurs cardiaques, défibrillateurs implantables, stimulateurs de neurones ou systèmes de pompe à médicament implantables, par exemple[325]. Ceux-ci offrent certes des avantages importants aux patients et à leurs médecins, mais ils peuvent être exploités et mettre leurs usagers en danger[326]. Des chercheurs ont démontré, en effet, qu'il était possible de reprogrammer un dispositif médical en s'y connectant à distance pour changer son fonctionnement ou carrément opérer une attaque par déni de service sur l'appareil, privant le patient de soins et, dans le pire des cas,

---

[324] D'autres exemples existent aussi dans le domaine des transports. Voir par exemple B. SCHNEIER, préc., note 251, p. 202 : « *In June 1996, the European Space Agency's Ariane 5 rocket exploded after launch because of a software error: the program tried to stick a 64-bit number into a 16-bit space, causing an overflow. Its lessons are particularly relevant to computer security* ».

[325] Kim ZETTER, « It's Insanely Easy to Hack Hospital Equipment », (25 avril 2014) *Wired*, en ligne : <https://www.wired.com/2014/04/hospital-equipment-vulnerable/> (consulté le 12 décembre 2017) : « *[…] Some of the most disturbing problems they found involved infusion pumps, ICDs (implantable cardiovascular defibrillators that deliver shocks to a patient who shows signs of going into cardiac arrest) and CT scans. They found a number of infusion pumps that have a web administration interface for nurses to change drug dosage levels from their workstations. Some of the systems are not password-protected, while others have hardcoded passwords that are weak and universal to all customers. […]* »

[326] Voir aussi, par exemple : U.S. FOOD AND DRUG ADMINISTRATION (« F.D.A. »), *Firmware Update to Adress Cybersecurity Vulnerabilities Identified in Abbott's (formely St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication* (29 août 2017), en ligne : <www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm> (consulté le 12 décembre 2017). Dans cette affaire, la F.D.A. a émis une notice à l'égard de défibrillateurs cardiaques qui disposaient de capacité de connectivité et qui étaient vulnérables à certaines attaques informatiques : « *As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates. The FDA […] has confirmed that these vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment. This access could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing* ». La F.D.A. recommande ensuite l'installation d'une mise à jour du logiciel interne du produit en question, laquelle doit être effectuée en visitant un médecin.

mettant carrément sa vie en danger[327]. Il n'est du reste pas nécessaire de s'en tenir aux spéculations : on a déjà recensé des cas d'infection par logiciel malicieux d'appareils de radiographie en hôpital, par exemple[328]. Aux États-Unis, entre 2006 et 2011, pas moins d'environ 1200 rappels d'instruments médicaux effectués seraient attribuables à une faille informatique quelconque, dont 94% posaient supposément des risques modérés ou graves pour la santé[329].

Remarquons enfin que certains S.C.P. peuvent recueillir des données personnelles particulièrement sensibles dont la divulgation aurait des conséquences préjudiciables. Bien que nous ayons choisi d'omettre de discuter des questions découlant de la protection de la vie privée dans ce mémoire, il est entendu que les S.C.P. – et les objets connectés – posent d'importantes questions juridiques à cet égard également.

ii) Nouvelles vulnérabilités

En second lieu, les caractéristiques inhérentes des S.C.P. entrainent à leur suite des vulnérabilités nouvelles[330]. L'ajout de composantes virtuelles et d'une connectivité aux réseaux numériques rend la sécurité physique tributaire de la bonne marche des technologies de l'information[331]. Toute défaillance de calcul ou de communication peut avoir des répercussions sur le domaine physique.

Mais avant même d'aborder les vulnérabilités spécifiques aux S.C.P., il faut dire un mot sur celles déjà connues qui peuvent également grever ces systèmes. En effet, étant donné qu'ils utilisent parfois les mêmes technologies que celles employées dans les ordinateurs, certaines

[327] Daniel HALPERIN et al., « Pacemakers and Implantable Cardiac Defibrillators : Software Radio Attacks and Zero-Power Defenses », (2008) *2008 IEEE Symposium on Security and Privacy*.
[328] Kevin FU et James BLUM, « Controlling for Cybersecurity Risks of Medical Device Software », (2013) 56-10 *Communications of the ACM*, p. 21.
[329] *Id.* ; ALEMZADEH et al., « Analysis of Safety-Critical Computer Failers in Medical Devices », (Juillet-Août 2013) *IEEE Security and Privacy* 14.
[330] C.P.S.P.W.G. préc., note 53, p. 13 ; A. A. CARDENAS et al., préc., note 61, p. 1.
[331] Au sujet de l'impact sécuritaire de l'ajout de capacités réseaux à un système informatique, voir B. SCHNEIER, préc., note 251, p. 176 : « *[…] it is much more difficult to build a computer that is secure when attached to a network. And networked computers are even more pregnable; instead of an attacker needing to be in front of the computer he is attacking, he can be halfway across the planet and attack the computer using the network. A networked world may be more convenient, but it is also much more insecure* ».

vulnérabilités préexistantes peuvent se transposer dans le domaine cyberphysique[332]. Ce sera par exemple le cas d'un S.C.P. fonctionnant avec un système d'exploitation dont l'usage est généralisé[333] et portant des vulnérabilités informatiques connues desquelles il faudra se protéger.

Cependant, les méthodes employées pour sécuriser les vulnérabilités informatiques des systèmes dits traditionnels ne sont pas nécessairement adéquates pour les S.C.P. D'une part, elles visent surtout à protéger l'information, et n'ont pas été conçues pour anticiper directement les effets d'une faille de sécurité sur le monde physique[334]. D'autre part, l'emploi général des mises à jour logicielles (lesquelles sont généralement utilisées pour colmater les vulnérabilités informatiques) peut être plus difficile à mettre en œuvre sur un S.C.P. : dans certains cas, le S.C.P. ne peut pas être facilement mis hors service afin de compléter la mise à jour parce qu'il offre un service essentiel ; dans d'autres, ils n'ont pas nécessairement d'écran ou de dispositif d'entrée de donnée (comme un clavier), et il peut être plus difficile de procéder à la mise à jour de leur logiciel interne – ou même d'obtenir facilement de l'information sur leur état[335].

Mais les caractéristiques uniques des S.C.P. posent aussi un certain nombre de problèmes nouveaux et fondamentalement différents de ceux rencontrés dans le champ de la sécurité purement informationnelle[336]. Bien qu'il soit impossible de les présenter exhaustivement, voyons-en au moins quelques-uns.

Par exemple, en raison de leur vocation à agir sur le réel, les S.C.P. doivent avoir des données à jour et exactes sur leur environnement. La sécurité du système serait compromise s'il était introduit – en raison de la défaillance d'une composante ou d'une attaque malicieuse – un délai dans la captation ou le traitement des données. Ce délai aurait des répercussions sur l'action prise par le système : le S.C.P. agirait alors trop tôt ou trop tard, et causerait potentiellement un dommage. C'est donc que la dimension temporelle du fonctionnement du S.C.P. créé une nouvelle surface d'attaque qui n'existait pas avec la même acuité dans les systèmes informatiques traditionnels.

[332] K. KIM et P. R. KUMAR, préc., note 7.
[333] Par exemple Windows, dérivés de Linux ou d'Unix et autres.
[334] A. A. CARDENAS, et al., préc., note 61, p. 2.
[335] S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 353.
[336] A. A. CARDENAS, et al., préc., note 61, p. 1.

De même, le bon fonctionnement du S.C.P. serait compromis si ses capteurs étaient défectueux ou que l'information qu'il a sur le monde est inexacte ou altérée malicieusement. De même, certaines circonstances rendent les informations plus difficiles à acquérir. On peut prendre en exemple les voitures autonomes, qui peuvent avoir des problèmes pour s'orienter notamment lorsque les lignes sur la route sont obscurcies par des précipitations ou en raison de zones d'ombre sur la voie qui pourraient être des nids-de-poule à éviter, ou des flaques d'eau qui ne posent pas de danger[337].

L'accès aux réseaux, et plus particulièrement à Internet, est également susceptible d'affecter d'une nouvelle façon les systèmes qui intègrent cette fonctionnalité. D'une part, cette connectivité peut exposer le système à une attaque malicieuse en permettant à l'attaquant de se connecter et d'effectuer à distance des modifications dans le logiciel du système. Si le S.C.P. n'est pas sécurisé adéquatement, une attaque peut être assez facile à exécuter. Par défaut de conception ou de configuration, certains S.C.P., dont quelques-uns accomplissent pourtant des tâches critiques, sont entièrement accessibles sur Internet et acceptent les connexions entrantes[338]. Il est entendu qu'il faudra veiller à sécuriser adéquatement les S.C.P. qui disposent de cette connectivité.

Il se peut aussi que le S.C.P. dépende de données entreposées sur un serveur distant. Par conséquent, le S.C.P. dépend également de la bonne marche générale des réseaux, ce sur quoi ses concepteurs ont bien peu d'emprise. En cas de problème, le fonctionnement pourrait alors

[337] Neal E. BOUDETTE, « 5 Things That Give Self-Driving Cars Headaches », (4 juin 2016) *The New York Times*, en ligne : <https://www.nytimes.com/interactive/2016/06/06/automobiles/autonomous-cars-problems.html?_r=0> (consulté le 12 décembre 2017).

[338] Pour s'en convaincre, le lecteur n'a qu'à visiter le site Shodan, en ligne : <https://www.shodan.io> (consulté le 12 décembre 2017). Ce moteur de recherche permet d'identifier toutes sortes d'objets connectés et de S.C.P., et même, invraisemblablement, des systèmes de contrôle industriel (par exemple, une usine de filtration des eaux). Voir : Robert O. HARROW JR., « Cyber search engine Shodan exposes industrial control systems to new risks », (3 juin 2012) *The Washington Post*, 3 juin 2012, en ligne : <https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html> (consulté le 12 décembre 2017).

se trouver retardé ou même paralysé. On parlerait alors d'un « déni de service » du S.C.P.[339], et la littérature technique souligne la vulnérabilité des S.C.P. à cet égard[340].

Il découle enfin de la connectivité des S.C.P. une autre vulnérabilité : lorsque le S.C.P. doit se connecter aux serveurs du fabricant, le service doit être continuellement assuré par ce dernier. S'il n'est plus en mesure, soit en raison d'une défaillance temporaire de ses serveurs, soit de façon plus permanente en raison d'une faillite de l'entreprise par exemple, ses produits peuvent devenir inutilisables. En effet, le S.C.P. est, dans un tel cas, dépendant de la personne contrôlant les serveurs auxquels se connecte le S.C.P. Il y a même lieu, dans certains cas, de souhaiter de la bonne foi de cette personne : si, par exemple, le fabricant décidait de bloquer les connexions sur son serveur afin de se venger d'une critique défavorable de son produit laissé en ligne par un consommateur, le dispositif pourrait devenir non fonctionnel[341].

D'autres caractéristiques des S.C.P. ont également des incidences en matière de sécurité. Par exemple, de la complexité inhérente aux S.C.P. elle-même émerge une nouvelle surface de vulnérabilité. Étant donné qu'ils peuvent être la somme de plusieurs systèmes, il se peut que

---

[339] En anglais « *denial of service* » (« D.o.S. »). Les opérateurs de sites web connaissent bien le danger du déni de service. Il existe un type d'attaque auquel ont fréquemment recours les acteurs malicieux, dit « *distributed denial of service* » (« D.D.o.S. »), et qui permet d'engorger le serveur du site visé avec un flot de requêtes frauduleuses. Le serveur attaqué n'a alors plus les ressources nécessaires pour répondre aux requêtes valides et n'est plus accessible sur Internet : il y a un déni de service, ou pour prendre une expression du droit de la sécurité informationnelle, la *disponibilité* des données est affectée. En théorie, tout serveur peut être visé par ce type d'attaque, même les serveurs qui ne sont pas hôtes d'un site web comme ceux qui seraient nécessaires au bon fonctionnement d'un S.C.P. Certaines attaques de type D.D.o.S. peuvent même faire des victimes collatérales : par exemple, en octobre 2016, une importante attaque D.D.o.S. a visé Dyn, une société qui fournit un service de direction des paquets sur le réseau Internet (le « *Domain Name System* », ou « D.N.S. »). Bien que ce soit uniquement Dyn qui avait été visé, l'attaque a résulté indirectement en un déni de service pour une proportion non négligeable des sites sur Internet, auxquels les utilisateurs ne pouvaient plus se connecter faute d'intermédiaire pour diriger leur trafic. Voir : DYN, « Dyn Statement on 10/21/2016 DDoS Attack », en ligne : <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/> (consulté le 12 décembre 2017).

[340] A. Y. NUR et M. E. TOZAL, préc., note 23.

[341] Incroyablement, cela s'est vu : Garadget, une entreprise fabricant un dispositif visant à permettre l'ouverture d'une porte de garage par l'entremise d'Internet, à l'aide d'une application pour téléphone intelligent, s'est vengée d'un consommateur qui lui avait laissé un commentaire défavorable sur Amazon en bloquant l'accès de son dispositif aux serveurs de l'entreprise. Étant donné que la commande d'ouverture de la porte transitait nécessairement par ces serveurs avant de se rendre à la porte de garage, le consommateur n'était plus en mesure d'utiliser le produit qu'il avait acheté. Voir : Kaveh WADDEL, « Avenging a One-Star Review With Digital Sabotage », (5 avril 2017) *The Atlantic*, en ligne : <https://www.theatlantic.com/technology/archive/2017/04/garadget-sabotage/521937/> (consulté le 12 décembre 2017).

l'ensemble dépende du bon fonctionnement de chacune des parties. En effet, plus l'ensemble est grand, plus il est difficile d'en assurer la sécurité.

iii) Attrait pour les acteurs malicieux

Enfin, un troisième facteur augmentant le risque associé aux S.C.P. est l'attrait puissant que ceux-ci peuvent exercer sur les acteurs malicieux. En effet, ces objets peuvent devenir la cible de cybercriminels, d'employés mécontents cherchant à se venger de leur employeur, de terroristes, d'activistes ou de groupes criminels organisés en tout genre, et même d'acteurs étatiques[342]. C'est que : « *Cyber-attacks are a natural progression to physical attacks: they are cheaper, less risky for the attacker, are not constrained by distance, and are easier to replicate and to coordinate* »[343]. Cela n'est pas que pure conjecture : le virus « Stuxnet » est un exemple relativement récent d'attaque contre un S.C.P. par ce qu'on peut présumer être un acteur étatique[344].

En effet, les jours où les logiciels malveillants visaient uniquement les ordinateurs sont désormais bien révolus. Ceux-ci s'attaquent bien volontiers aux cibles non traditionnelles qui prolifèrent depuis quelques années, tels que les téléphones intelligents et autres appareils mobiles, ainsi que les objets connectés et aux autres systèmes intégrés, S.C.P. y compris. Il serait bien audacieux de considérer que ces systèmes sont protégés en raison du seul fait qu'ils n'entrent pas dans la conception classique de serveurs ou d'ordinateurs de bureau[345].

L'appât du gain financier est l'une des motivations du piratage informatique[346]. Les attaquants ont développé depuis quelques années des méthodes qui leur permettent de tirer un avantage pécuniaire beaucoup plus direct des attaques préparent. Les logiciels de type

[342] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53.
[343] *Id.*
[344] Thomas M. CHEN et Saeed ABU-NIMEH, « Lessons from Stuxnet », (2011) 44-4 *Computer*, p. 91.
[345] M. CONTI et al., CPS Convergence, p. 16.
[346] Benoît DUPONT, « L'évolution du piratage informatique : De la curiosité technique au crime par sous-traitance », dans ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION (dir.), *Le respons@able 2.0 : Acteur clé en AIPRP*, Cowansville, Québec, Éditions Yvon Blais, p. 4, en ligne : <http://benoitdupont.openum.ca/files/sites/31/2015/07/Dupont-2010-Les-pirates-informatiques_0.pdf> (consulté le 12 décembre 2017).

rançongiciel[347] cryptent les données de leurs victimes, et parfois même le système d'exploitation lui-même, qu'on ne peut alors plus accéder sans la clé de décryptage détenue par l'attaquant. La victime doit payer une rançon, le plus souvent en bitcoins afin de préserver l'anonymat de l'acteur malicieux, afin d'accéder à cette clé et déverrouiller leurs données. Certaines de ces attaques ont même visé des hôpitaux, dont les opérations ont été gravement compromises[348]. Au vu des fonctions cruciales que certains S.C.P. accomplissent, leurs opérateurs pourraient être enclins à payer la rançon demandée rapidement afin d'éviter que se prolonge un déni de service, ce qui rend ces cibles encore plus attrayantes pour les criminels.

Finalement, l'important volume de S.C.P. et d'objets connectés – ainsi que dans certains cas la faiblesse de leur niveau de sécurité (notamment en raison d'une configuration par défaut peu sécuritaire) – peut les rendre une cible intéressante pour être intégrées dans un « *botnet* », c'est-à-dire un ensemble de systèmes informatiques, secrètement infectés et répondant aux commandes de l'attaquant, duquel il est possible de lancer des attaques informatiques de type D.D.o.S.[349] Étant donné qu'ils peuvent être installés et oubliés (un appareil ménager, par exemple) ou encore employés par des utilisateurs qui n'ont pas de connaissances techniques particulières, il peut être long avant que l'infection soit détectée, si elle l'est un jour. Aujourd'hui, les « *botnets* » ont une composition très hétérogène qui leur permet d'atteindre des proportions énormes et leurs attaques sont plus dévastatrices[350]. C'est ainsi que le niveau de

---

[347] O.Q.L.F., préc., note 64, « rançongiciel » : « Logiciel malveillant qui permet de verrouiller un ordinateur ou de chiffrer ses données dans le but d'extorquer de l'argent à son utilisateur avant de lui en rendre l'accès. » Il s'agit du terme français recommandé pour l'anglais « *ransomware* ». « Wannacry » est un exemple récent de ce type d'attaque. Voir à cet égard : Savita MOHURLE et Manisha PATIL, « A Brief Study of Wannacry Threat : Ransomware Attack 2017 », (2017) 8-5 *International Journal of Advanced Research in Computer Science*.

[348] Kim ZETTER, « Why Hospitals Are The Perfect Targets For Ransomware », (30 mars 2016) *Wired*, en ligne : <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/> (consulté le 12 décembre 2017).

[349] Brian KREBS, « The Lingering Mess from Default Insecurity », (12 novembre 2015), en ligne : <https://krebsonsecurity.com/2015/11/the-lingering-mess-from-default-insecurity/> (consulté le 12 décembre 2017).

[350] Le réseau « *Mirai* » est un exemple d'attaque utilisant des dispositifs hétérogènes relevant d'objets connectés dans l'I.d.O. Voir à cet effet : Ben HERZBERG, Dima BEKERMAN et Igal ZEIFMAN, « Breaking Down Mirai: An IoT DDoS Botnet Analysis », (26 octobre 2016), en ligne : <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html> (consulté le 12 décembre 2017). Pour un exemple à plus petite échelle, mais utilisant aussi des objets connectés qu'on ne soupçonnerait pas de participer à des attaques informatiques : Lee MATHEWS, « Infected Vending Machines and Light Bulbs DDoS A University », (13 février 2017) *Forbes*, en ligne : <https://www.forbes.com/sites/leemathews/2017/02/13/infected-vending-machines-and-light-bulbs-ddos-a-university/#4527d87b178f> (consulté le 12 décembre 2017).

sécurité parfois défaillant des S.C.P. (et surtout des objets connectés) est au cœur d'inquiétudes quant à la santé générale du réseau Internet.

On constate donc à la fois une augmentation de la gravité des dommages possibles en raison d'une défaillance des S.C.P., l'ajout de vulnérabilités informationnelles préexistantes et nouvelles pouvant les viser, ainsi qu'un attrait considérable pour les personnes désirant exploiter ces vulnérabilités. Ceci justifie amplement, selon nous, qu'il soit raisonnable de s'inquiéter des incidences sécuritaires de l'entrée sur le marché d'une quantité sans cesse croissante des S.C.P., et des questions juridiques qui découlent de ce phénomène.

DEUXIÈME PARTIE : LA RESPONSABILITÉ DU FABRICANT À L'ÈRE CYBERPHYSIQUE

A. Certains effets de la problématique cyberphysique sur le droit

Avant de discuter d'un cadre de responsabilité applicable au fabricant, nous devons explorer, dans ce chapitre, les effets que peuvent avoir les S.C.P. sur les cadres de responsabilité que nous venons de présenter dans l'abstrait au courant de la dernière partie. À cette fin, nous verrons en premier lieu comment les particularités des S.C.P. affectent le régime de la responsabilité du fabricant mis en place par l'article 1468 C.c.Q., en nous penchant notamment sur les débiteurs de l'obligation, la question des bogues informatiques telle que comprise sous ce régime, de même que celle de l'exonération du risque de développement en matière de cybersécurité. En second lieu, nous ferons le même exercice pour ce qui est de l'obligation de sécurité informationnelle, en nous demandant notamment si elle peut sanctionner le préjudice physique découlant d'une faille de sécurité informationnelle. Ceci fait, nous serons en mesure d'approcher, dans le chapitre B de cette partie, un cadre de responsabilité approprié pour le fabricant d'un S.C.P. qui aurait causé un dommage physique en raison d'un défaut de sécurité informationnel.

1. Le régime de responsabilité du fabricant en cas de défaut de sécurité informationnel d'un système cyberphysique

a) Débiteurs et créanciers

Débutons nos remarques en nous penchant sur le cas du débiteur de l'obligation de réparer le préjudice causé par le défaut de sécurité du bien. Lorsqu'un S.C.P. est entièrement conçu et fabriqué par un seul sujet de droit, l'article 1468 C.c.Q. ne laisse aucun doute : celui-ci doit être visé par le régime à titre de « fabricant »[351]. Disons aussi que peut être visé au même titre que le fabricant tout distributeur, fournisseur (agissant en tant que grossiste ou détaillant) ou importateur du S.C.P.[352] Ici encore, nul besoin de procéder à un long exercice d'interprétation du texte de loi.

Mais les S.C.P. posent un bon nombre de questions intéressantes à l'égard des débiteurs possibles dans le régime de 1468 C.c.Q. En effet, certaines personnes qui n'auraient traditionnellement pas été visées par un régime visant à sanctionner le préjudice physique peuvent désormais le devenir, avec l'apport de la dimension cyberphysique des S.C.P.

Prenons par exemple le cas du sous-traitant ayant participé à la conception du S.C.P., ou encore celui du fournisseur de composantes virtuelles intégrées dans le produit final[353]. Ceux-ci seront-ils assimilés au fabricant au sens de la loi ? Tel que nous l'avons vu, la définition législative de « fabricant » n'est pas limitative : toute personne ayant apporté une contribution à la production de l'objet en question peut être visée par l'article 1468 C.c.Q.[354] – même le sous-traitant qui en aurait fabriqué seulement une partie[355]. C'est donc que les personnes ayant fourni une composante intégrée dans un S.C.P. devront s'assurer que cette partie du système n'est pas affectée d'un défaut de sécurité. De même, les personnes chargées par le fabricant de concevoir une partie ou l'entièreté du S.C.P. devront s'assurer que celui-ci est bien conçu et ne présente

[351] C.c.Q., art 1468 al. 1.
[352] *Id.*, art 1468 al. 2.
[353] *Supra*, p. 13 et suiv. Rappelons qu'une composante virtuelle est l'une des trois parties constituantes des S.C.P., avec les composantes physiques et la connectivité aux réseaux. Il s'agit de tout objet ayant pour vocation d'agir dans le monde algorithmique, que ce soit des composantes informatiques matérielles (processeurs, cartes graphiques, etc.), ou logicielles.
[354] *Véranda Industries inc.* c. *Beaver Lumber Co.*, [1992] R.J.Q. 1763 (C.A.) ; *Gagnon* c. *Ratté*, [1996] R.R.A. 766 (C.S.) ; P.-G. JOBIN, préc., note 180, p. 287.
[355] *Cigna du Canada* c. *A.C.F. Grew Inc.*, [1993] R.R.A. 295 ; MINISTÈRE DE LA JUSTICE, préc., note 166, art. 1468 al. 1.

aucun défaut de sécurité, leur statut de sous-traitant ne les protégeant pas de l'application du régime de 1468 C.c.Q.

Qu'en est-il du sous-traitant ayant développé une composante virtuelle de nature purement logicielle et intégrée au sein d'un S.C.P. ? Si ce programme informatique présente un défaut de sécurité à l'origine d'un préjudice physique, le développeur logiciel pourrait-il être tenu responsable en vertu de l'article 1468 C.c.Q. ?

Peut-être est-on tenté de s'arrêter au fait que le développeur logiciel n'apporte aucune contribution matérielle à la fabrication du produit[356]. Il est vrai, par ailleurs, que la doctrine observe qu'afin de pouvoir considérer qu'une personne est un fabricant au sens de la loi : « […] encore faut-il qu'il y ait fabrication »[357], et que le terme « fabrication » – dans son sens courant, à tout le moins – fait référence aux transformations de matière première par l'usage de procédés mécaniques[358], et non pas au développement d'un produit de l'esprit comme un programme informatique.

Nous croyons cependant que ni la doctrine ni la définition courante du terme « fabrication » ne doivent être interprétées afin de nous pousser à exclure un développeur logiciel du régime de 1468 C.c.Q. Selon nous, la doctrine, en soulignant la nécessité d'une opération de fabrication sur le bien en question, ne cherchait pas à dire qu'il fallait exclure du régime toute personne non impliquée dans la fabrication matérielle dans son sens le plus strict, mais seulement à rapporter le désir du législateur d'écarter le producteur d'une matière première du régime de responsabilité du fabricant[359]. De même, le sens courant d'un mot ne doit pas

[356] Évidemment, le développeur dont le logiciel n'est pas intégré dans un S.C.P., et dont le code n'a pour vocation que le traitement de données et non pas l'action directe sur le monde physique, ne saurait être visé par 1468 C.c.Q., puisqu'il ne participe pas à la conception d'un bien meuble. Ici, nous explorons plutôt le cas, moins commun, du développeur dont le logiciel est susceptible d'avoir une incidence sur le monde physique par l'entremise de l'action d'un bien meuble.
[357] P.G. JOBIN, préc., note 180, p. 287-288.
[358] Le Nouveau Petit Robert, préc., note 121, p. 995, « fabrication » ; Le Nouveau Petit Littré, préc., note 247, p. 792, « fabrication ».
[359] MINISTÈRE DE LA JUSTICE, préc., note 166, art. 1469. La doctrine considère que le législateur québécois a effectivement écarté de ce régime le producteur de matière première : agriculteur, producteur d'électricité, éleveur d'animaux, etc. P.-C. LAFOND, préc., note 162, par. 461.

nécessairement nous empêcher d'en faire une interprétation divergente dans le cadre d'un texte de loi[360].

De toute façon, puisque le défaut de sécurité peut prendre la forme d'un vice de conception, on doit comprendre que le concepteur du produit serait assimilé au fabricant, même si celui-ci n'a pas d'implication directe dans la construction du produit au sens premier du terme[361]. Le facteur déterminant, semble-t-il, doit être celui de la contribution importante à la réalisation du bien[362]. C'est certainement le cas du développeur logiciel ayant participé à la conception d'un S.C.P. Étant donné sa nature cyberphysique, le S.C.P. ne saurait tout simplement pas fonctionner sans l'apport du développeur logiciel : c'est lui qui est responsable du comportement du S.C.P. ; c'est lui qui peut prévoir les failles informatiques susceptibles de survenir ; enfin, sans doute est-ce lui qui dispose de la meilleure emprise sur le domaine de la sécurité informationnelle.

Ainsi, en conséquence de l'importance de sa contribution, nous croyons que le développeur logiciel doive être assimilé au fabricant au sens de la loi, même s'il n'aurait produit qu'une partie de la plateforme logicielle du S.C.P. Par ailleurs, une telle interprétation nous semble cohérente avec l'objectif du législateur lors de la mise en place du régime. En utilisant le terme « fabricant », il cherchait à viser « *tout participant* au processus de fabrication du bien »[363] et « […] atteindre *toute personne impliquée dans la production* et la distribution du produit […] »[364] (nos italiques) – le tout dans un but de protection du public. Dans cette optique, il serait inconséquent de refuser de viser le développeur logiciel ayant apporté une contribution appréciable au S.C.P.

Or, des questions subsistent à l'égard des développeurs tiers volontaires qui mettent gratuitement des logithèques[365] à la disposition de tous, lesquelles seraient par la suite

---

[360] Pierre-André CÔTÉ, *Interprétation des lois*, 4e éd., Montréal, Les Éditions Thémis, 2009, p. 302 et suiv.
[361] C.c.Q., art 1469.
[362] Et non pas seulement le fait d'avoir procédé à une transformation d'une matière première, selon nous.
[363] MINISTÈRE DE LA JUSTICE, préc., note 166, art. 1468.
[364] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-378.
[365] O.Q.L.F., préc., note 64. Il s'agit du terme recommandé pour l'anglais « *software library* ». Le site Technopedia fournit des explications relatives aux logithèques : « *A software library generally consists of pre-written code, classes, procedures, scripts, configuration data and more. Typically, a developer might manually add a software library to a program to achieve more functionality or to automate a process without writing code for it.*

employées par les concepteurs de S.C.P. Un exemple d'une telle logithèque fort utilisée en pratique est celle développée par le projet OpenSSL[366]. Parfois, des failles de sécurité importantes sont trouvées dans ces logithèques : en 2014, on a découvert une vulnérabilité majeure dans le code d'OpenSSL (qui pris le nom d'« *Heartbleed* »), et qui pouvait permettre d'accéder au contenu crypté, comme les renseignements personnels les plus sensibles des utilisateurs[367]. Comme le logiciel affecté avait été intégré dans de très nombreux systèmes (incluant dans ceux de Facebook, Netflix et d'Amazon[368], et même ceux de l'Agence du revenu du Canada[369]), beaucoup se trouvèrent tout d'un coup vulnérables. Qu'en serait-il si un S.C.P. causait un dommage physique en raison d'un défaut de sécurité provenant d'une telle logithèque ? Le développeur logiciel tiers pourrait-il être visé à titre de fabricant sous le régime de 1468 C.c.Q. ? Il est vrai que toute clause, dans son contrat de licence, qui limiterait ou exclurait sa responsabilité pour préjudice corporel ou moral causé à autrui serait trouvée nulle par les tribunaux québécois[370]. Mais son cas est particulier et pousse, selon nous, le régime de 1468 C.c.Q. à la limite de l'intention du législateur. Ce dernier visait, rappelons-le, à donner au fabricant un fardeau juridique proportionnel au rôle qu'il a joué dans la mise en marché du produit[371]. Or, au contraire du simple développeur logiciel qui aurait fourni un apport avec l'intention que celui-ci soit intégré au S.C.P., le développeur logiciel tiers n'a aucun contrôle

---

For example, when developing a mathematical program or application, a developer may add a mathematics software library to the program to eliminate the need for writing complex functions. All of the available functions within a software library can just be called/used within the program body without defining them explicitly. Similarly, a compiler might automatically add a related software library to a program on run time. » TECHNOPEDIA, « Software Library », en ligne : <https://www.techopedia.com/definition/3828/software-library> (consulté le 12 décembre 2017).

[366] OPENSSL, en ligne : <https://www.openssl.org> (consulté le 12 décembre 2017). Ce projet vise à fournir des outils de cryptographie sous les protocoles *Secure Socket Layer (S.S.L.)* et *Transport Layer Security (T.L.S.)*. Comme il s'agit d'outils mathématiques complexes, les développeurs logiciels préfèrent y avoir recours plutôt que de développer des applications en partant du début.

[367] Voir par exemple : Craig TIMBERG, « Heartbleed bug puts the chaotic nature of the Internet under the magnifying glass », (9 avril 2014) *The Washington* Post, en ligne : <https://www.washingtonpost.com/business/technology/heartbleed-bug-puts-the-chaotic-nature-of-the-internet-under-the-magnifying-glass/2014/04/09/00f7064c-c00b-11e3-bcec-b71ee10e9bc3_story.html> (consulté le 12 décembre 2017) ; Nicole PERLROTH, « Heartbleed Highlights a Contradiction in the Web », (18 avril 2014) *The New York Times*, en ligne <https://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html> (consulté le 12 décembre 2017).

[368] N. PERLROTH, préc., note 367.

[369] Hugo DE GRANDPRÉ, « Agence du revenu du Canada : 900 NAS volés », (14 avril 2014) *La Presse*, en ligne : <http://www.lapresse.ca/actualites/201404/14/01-4757316-agence-du-revenu-du-canada-900-nas-voles.php> (consulté le 12 décembre 2017).

[370] C.c.Q., art. 1474 al. 2.

[371] *Supra*, p. 38-39.

sur la façon dont est utilisé sa logithèque, qui peut avoir été conçue sans qu'on prenne en considération qu'elle serait intégrée dans un S.C.P. Participe-t-il vraiment au développement du produit ? Et doit-il être sanctionné en raison d'une contribution qu'il rend disponible après l'avoir développé bénévolement ? Le viser n'aurait-il pas, par ailleurs, un effet préjudiciable le domaine des technologies de l'information, en ralentissant l'innovation et en détruisant les projets de logithèques libres qui empêchent les développeurs d'avoir à réinventer des solutions cryptographiques (moins prouvées et donc moins sécuritaires) ? Pour dire vrai, il nous répugne que soient visés les développeurs tiers à titre de fabricant selon l'article 1468 C.c.Q., bien que nous voyions en quoi omettre de les considérer pourrait manquerait de cohérence dans l'application de la règle de droit. Ici sans doute nous bénéficierions d'un éclaircissement législatif, car il est fort à parier qu'un tel type de contribution au bien n'avait jamais été envisagé par le législateur lors de la création du régime.

Concernant le créancier de l'obligation, enfin, il s'agira bien sûr de toute personne ayant un subi un préjudice en raison du défaut de sécurité du S.C.P., pourvu qu'il n'existe aucun lien contractuel entre les parties[372]. Observons au passage que rien n'empêche une personne morale de se prévaloir de ce régime[373].

b) Les systèmes cyberphysiques dans le régime de la responsabilité du fabricant

Les S.C.P. peuvent-ils être faire l'objet du régime de la responsabilité du fabricant ? Sans doute. Observons d'abord que nous ne voyons rien qui empêcherait de viser par ce mécanisme des objets dont le fonctionnement est partiellement numérique s'ils sont susceptibles de causer un préjudice en raison d'un défaut de sécurité. Du reste, nous avons démontré dans la première partie de ce mémoire que les S.C.P. étaient des biens meubles (ou immeubles, par exemple lorsqu'ils sont intégrés à des installations d'une infrastructure énergétique)[374]. Il en découle naturellement qu'un défaut de sécurité en leur sein causant préjudice à un tiers peut être

[372] C.c.Q., art. 1468 al. 1.
[373] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-380.
[374] Auquel cas ils seraient tout de même visé par le régime de responsabilité du fabricant en raison de l'art. 1468 al. 1 C.c.Q. ; voir aussi : P.-G. JOBIN, préc., note 180, p. 288.

générateur de responsabilité pour le fabricant[375]. Il s'agit donc de savoir comment se manifeste le défaut de sécurité informationnel dans un S.C.P. au sens de ce régime.

c) La conception classique du défaut de sécurité appliquée aux systèmes cyberphysiques

Dans cette sous-section, verrons comment la conception classique, telle qu'on la retrouve dans le texte de loi, la jurisprudence et la doctrine, appréhende assez malaisément le défaut de sécurité informationnel. Nous rencontrons en effet un certain flou conceptuel lorsqu'il s'agit de traiter d'un défaut de sécurité informationnel causant directement un préjudice physique. Afin de s'en convaincre, examinons les diverses catégories de défaut proposées par le législateur à travers le prisme d'une problématique cyberphysique. Remarquons néanmoins tout de suite que cette apparente incompatibilité n'est en rien fatale puisque, comme nous le savons, les catégories de défaut retrouvées à l'article 1469 C.c.Q. ne sont pas limitatives[376].

i) Vice de conception ou de fabrication

La première catégorie d'origine du défaut de sécurité fournie par le législateur à l'article 1469 C.c.Q. est celle du « vice de conception ou de fabrication »[377]. Le vice de fabrication, pour aborder celui-ci en premier lieu, est peut-être moins pertinent dans la sphère informationnelle. En effet, la jurisprudence semble avoir attribué à cette catégorie de défaut un caractère surtout physique : pensons par exemple au traitement inadéquat de matériaux, ou encore à une construction ou un assemblage défectueux[378]. Il serait plutôt difficile de traduire ce type de défaut directement en termes logiciels, ceux-ci étant des produits de l'esprit moins fabriqués que *conçus*, pour ainsi dire.

C'est pourquoi le deuxième type de vice proposé dans cette catégorie, celui du vice de conception, nous semble beaucoup plus pertinent. Dans la jurisprudence, ce type de défaut s'est

---

[375] C.c.Q., art. 1468.
[376] C.c.Q., art. 1469 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-383.
[377] C.c.Q., art. 1469.
[378] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-353 ; *Danson* c. *Château Motors Ltd.*, 1976 C.P. ; *Allstate du Canada, compagnie d'assurances* c. *Assurance royale du Canada*, [1994] R.J.Q. 2045 (C.S.) ; *General Steel Wares Ltd.* c. *Raymond*, 1978 C.A. 288. ; *Bédard* c. *Location Val-d'Or inc.*, J.E. 85-1029 (C.S.).

par exemple traduit en « espace insuffisant entre les pneus et le plancher d'une roulotte mobile », en « mèche d'un lampion » susceptible de se déplacer, ou encore en « mauvaise isolation d'une photocopieuse », causant des chocs électriques[379]. Il s'agit donc en général d'erreurs survenues lors de l'étape du développement du produit : les concepteurs n'avaient pas anticipé toutes les conséquences potentiellement néfastes de leurs décisions, de telle sorte qu'un défaut de sécurité en découle.

À notre avis, un vice de conception peut certainement se manifester dans la sphère numérique. Un algorithme conçu incorrectement, par exemple, peut faire en sorte que le S.C.P. qui l'emploie soit susceptible de présenter un danger sur la sécurité physique. Ce serait le cas, notamment, d'un logiciel omettant de faire usage des méthodes de cryptage reconnues pour sécuriser les flux de données, ou ne procédant pas à l'authentification des utilisateurs ou des autres systèmes avec qui il communique. Un vice de conception pourrait également se présenter lorsque les concepteurs du S.C.P. n'ont pas employé des composantes informatiques assez puissantes, par exemple en employant un processeur trop peu puissant, pour que le système puisse exécuter en temps utile les opérations de cryptage requises, lesquelles peuvent être exigeantes du point de vue computationnel[380].

ii) Mauvaise conservation ou présentation

Le défaut de sécurité découlant d'une mauvaise conservation ou présentation fait généralement référence à un emballage inadéquat[381]. Rappelant la *Convention des Nations Unies relative aux contrats de vente internationale de marchandises*[382] et le droit européen[383], il vise par exemple les défauts qui découleraient de dégradation causée au produit lors de son

[379] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-352.
[380] L. ATZORI, A. IERA et G. MORABITO, préc., note 116, p. 15.
[381] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-377.
[382] *Convention des Nations Unies relative aux contrats de vente internationale de marchandises*, Vienne, 11 avril 1980, art. 35 (2) : « les marchandises ne sont conformes au contrat que si : […] d) elles sont emballées ou conditionnées selon le mode habituel pour les marchandises du même type ou, à défaut de mode habituel, d'une manière propre à les conserver et à les protéger ».
[383] *Directive du Conseil des Communautés européennes du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux*, (85/374/CEE), Journal officiel n° L 210 du 07/08/1985 p. 0029 - 0033, art. 6.

transport ou entreposage, ou les dommages qui découleraient directement de l'emballage lui-même, comme dans le cas de l'explosion d'un contenant de boisson gazeuse[384].

Toutefois, étant donné la nature intangible du monde informationnel, nous estimons peu probable qu'un S.C.P. soit grevé d'un défaut de sécurité informationnel résultant de la mauvaise conservation ou présentation du produit. En effet, nous voyons mal en quoi la partie algorithmique d'un S.C.P. puisse se dégrader en raison d'une mauvaise conservation. Du reste, pour que le défaut de sécurité informationnel puisse se manifester, il faut que le S.C.P. soit mis en fonction et qu'il y ait traitement de données, et donc qu'il soit sorti de son emballage. Néanmoins, il n'est évidemment pas exclu qu'un S.C.P. puisse être grevé d'un défaut de ce type pour ce qui est de sa part physique, et qu'une mauvaise conservation du S.C.P. puisse avoir des conséquences dans la sphère virtuelle – par exemple lorsque l'emballage a pris l'eau, endommageant ses circuits électroniques.

iii) Absence d'indications suffisantes quant aux risques et danger qu'il comporte

Le troisième type de défaut de sécurité donné en exemple par le législateur découle de l'absence d'avertissements à propos du danger inhérent à l'utilisation du produit, ainsi qu'aux précautions d'utilisation à prendre afin de s'en préserver[385]. En effet, comme on le sait, tout en fonctionnant tel que prévu, un produit peut être néanmoins dangereux en soi : il faut alors que ces dangers soient dénoncés adéquatement à l'utilisateur par le fabricant[386].

Étant donné que les S.C.P. sont susceptibles d'être employés par des personnes qui ne possèdent pas d'expertise particulière en informatique, nous croyons que ce type de défaut de sécurité est particulièrement pertinent. D'abord, la part informationnelle d'un S.C.P. peut poser un danger pour la sécurité physique : nous l'avons amplement démontré dans la première partie de ce mémoire. Le fabricant devra donc dénoncer clairement ces dangers aux utilisateurs, et ce en prenant soin de vulgariser tant les risques associés à l'informatique que les impacts physiques qui peuvent en découler, incluant ceux qui peuvent résulter de mauvaises pratiques de

[384] *Cohen* c. *Coca Cola Ltd.*, [1967] R.C.S. 469 ; *Ladouceur* c. *Brasserie Labatt ltée*, B.E. 99BE-779 (Q.C.p.c.) ; *Connolly* c. *Seven-up Canada Inc.*, J.E. 85-909 (C.S.) ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-377.
[385] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-377.
[386] N. VÉZINA et F. MANIET, préc., note 152, par. 112.

l'utilisateur lui-même (configuration inadéquate, omission de procéder aux mises à jour logicielles disponibles, et autres). En effet, comme chacun sait, l'usage des technologies de l'information requiert généralement l'apprentissage de connaissances propres à ce domaine, lesquelles ne sont pas nécessairement accessibles pour tous. Le fabricant devra donc veiller à ce que les informations essentielles soient bien comprises par l'utilisateur, tel que l'exige par ailleurs l'obligation de renseignement.

De même, en plus des risques, il devra informer l'utilisateur des précautions qui s'imposent afin de préserver sa sécurité. Encore une fois, le fabricant devra porter attention à ce que ces instructions soient facilement compréhensibles, compte tenu du niveau d'expertise propre à son public. Il devra informer les utilisateurs des mesures à prendre pour s'assurer d'un fonctionnement sécuritaire du S.C.P., par exemple en procédant à une configuration adéquate du système, de même qu'en ayant recours aux pratiques recommandées en sécurité informationnelle (emploi de mots de passe forts et uniques), ou en mettant à jour du logiciel dès que possible.

d) Moyens d'exonération

Rappelons qu'au cours d'une action en responsabilité civile en vertu de ce régime, une fois que le demandeur aura rempli son fardeau de preuve en démontrant l'existence d'un défaut de sécurité lui ayant occasionné un préjudice, il revient au fabricant de repousser la présomption de responsabilité courant contre lui[387]. Évidemment, lorsqu'il parvient simplement à démontrer qu'il n'y a pas de défaut de sécurité informationnel (et donc qu'il n'y a pas de violation du standard de sécurité), le fabricant ne sera pas tenu responsable. En cela, il vient simplement répondre à la preuve faite par la victime de l'existence d'un défaut de sécurité.

Mais, tel que nous l'avons vu, le C.c.Q. prévoit d'autres moyens d'exonération, dont certains sont spécifiques à ce régime. Il convient de les explorer plus en détail au regard des spécificités cyberphysiques des objets qui nous intéressent.

[387] N. VÉZINA et F. MANIET, préc., note 152, par. 114.

i) Force majeure

Abordons d'abord le moyen d'exonération classique, commun à toutes les formes de responsabilité civile : la force majeure[388]. Il convient cependant de traiter celle-ci avec une certaine circonspection dans les cas de responsabilité découlant d'un défaut de sécurité[389].

C'est ici l'occasion de traiter de la problématique des bogues informatiques, lesquels grèvent presque tous les logiciels[390]. Si le préjudice reproché découle de la survenance d'un bogue informatique dans le logiciel du S.C.P., pourra-t-on considérer qu'il s'agit d'un cas de force majeure, et non d'un défaut de sécurité ? La question n'est pas bête, surtout si on prend en compte que, dans certains scénarios se déroulant dans un environnement numérique, il semble effectivement possible de considérer qu'il s'agira d'un cas de force majeure[391]. Il est vrai, en outre, qu'un bogue informatique présente souvent, du moins en apparence, un caractère imprévisible et irrésistible du point de vue de l'utilisateur.

Cependant, nous ne croyons pas que le bogue informatique ayant une incidence sur la sécurité physique d'un S.C.P. doive nécessairement être considéré comme un cas de force majeure. D'abord, en règle générale, le bogue attribué à une application « mal programmée ou qui n'est pas mise à jour ne saurait être qualifié de force majeure »[392]. De même en est-il lorsque la faute découle du non-respect d'une obligation prévue par le législateur, comme celle afférente à la sécurité informationnelle formulée par l'article 25 de la L.C.C.J.T.I.[393] Du reste, un tel bogue informatique n'aurait probablement pas un caractère d'extranéité suffisant. S'il se manifeste souvent de manière inattendue et certes inopportune pour l'utilisateur qui en souffre, nous croyons qu'il ne saurait en être de même pour le fabricant d'un S.C.P. C'est lui, vraisemblablement, qui a accès au code source du logiciel, et c'est lui qui est chargé de s'assurer de son bon fonctionnement. Du reste, puisque l'aspect logiciel est une partie intégrante du S.C.P., il serait inconséquent de considérer qu'une erreur dans sa conception puisse être un

[388] C.c.Q., art. 1470.
[389] P.-G. JOBIN, préc., note 180, par. 209.
[390] Stefan FREI et al., « Large-Scale Vulnerability Analysis », (2006) *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, p. 131-138.
[391] N. W. VERMEYS, préc., note 50, p. 138-139.
[392] *Id.*, p. 139.
[393] *Id.*, p. 139-140.

évènement suffisamment étranger à la sécurité du produit pour qu'il entre dans la catégorie de la force majeure. N'oublions pas qu'il est proscrit de considérer le défaut de sécurité lui-même comme un évènement de force majeure, car ce défaut de sécurité est intrinsèque au bien[394].

ii) Faute de la victime

Lorsque le fabricant est en mesure de démontrer que la victime « connaissait ou était en mesure de connaître le défaut de sécurité du bien, ou qu'elle pouvait prévoir le préjudice », celui-ci ne sera pas tenu de réparer ce préjudice[395].

Dans cette hypothèse, le fabricant aura donc rempli son obligation de renseignement à l'égard du défaut de sécurité[396]. Ses avertissements étaient appropriés en fonction de la nature du bien et du niveau de danger inhérent au bien[397]. Le fabricant devra néanmoins faire attention que ses renseignements soient bien compris des utilisateurs. De même, un utilisateur qui n'a pas procédé à la mise à jour logicielle rendue disponible par le fabricant pour régler un défaut de sécurité, en dépit des instructions de ce dernier, ne devrait pas avoir gain de cause[398].

Le défi sera sans doute de vulgariser adéquatement les enjeux de sécurité informationnelle associés aux S.C.P., car le domaine informationnel peut devenir rapidement complexe. Il existe un danger que, malgré les meilleures précautions du fabricant, ses instructions n'étaient pas suffisamment limpides pour que la victime puisse les comprendre, compte tenu du caractère souvent assez technique des technologies de l'information.

iii) Risques de développement

Rappelons que le régime de responsabilité découlant du défaut de sécurité d'un produit, au contraire de celui mis en place par la L.P.C.[399], refuse de tenir le fabricant responsable d'un

---

[394] N. VÉZINA et F. MANIET, préc., note 152, par. 116.
[395] C.c.Q., art. 1473 al. 1 ; P.-G. JOBIN, préc., note 180, par. 212 ; N. VÉZINA et F. MANIET, préc., note 152, par. 116 ; P. FRÉCHETTE, préc., note 154, par. 73.
[396] P.-G. JOBIN, préc., note 180, par. 213.
[397] P.-G. JOBIN, préc., note 180, par. 211.
[398] Généralement, on pourra considérer qu'il s'agit d'une négligence. Voir à cet égard, N. W. VERMEYS, préc., note 145, p. 127 : « […] les tribunaux américains semblent d'avis que le fait d'installer les dernières rustines avec célérité constitue un comportement raisonnable et diligent », ce qui n'est pas sans laisser des ambiguïtés quant à ce que constitue la « célérité » dans ce contexte.
[399] L.P.C., art. 53.

défaut qui serait « indécelable » en raison de l'état objectif des connaissances scientifiques et techniques[400]. Il peut être approprié de reproduire le libellé de l'article mettant en place ce moyen d'exonération :

> « **Art. 1473.** […] [Le fabricant] n'est pas tenu, non plus, de réparer le préjudice s'il prouve que le défaut ne pouvait pas être connu, compte tenu de l'état des connaissances, au moment où il a fabriqué, distribué ou fourni le bien et qu'il n'a pas été négligent dans son devoir d'information lorsqu'il a eu connaissance de l'existence de ce défaut. »[401]

Selon nous, ce moyen est certainement pertinent dans le cas de la sécurité informationnelle, domaine sans cesse en mouvement et certainement tributaire de l'innovation technologique dont cet article est censé traiter[402].

À cet égard, il y a lieu de se demander si une faille de sécurité logicielle inconnue lors de la fabrication du S.C.P. pourrait donner lieu à l'application de l'exonération pour risque de développement. Plus précisément, un fabricant pourrait-il être exonéré d'un dommage découlant de l'exploitation d'une vulnérabilité dite « *zero day* » dans le logiciel de son S.C.P. ?

Celles-ci peuvent être décrites ainsi :

> « *A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning.* »[403]

Étant donné le caractère inconnu de la vulnérabilité exploitée au moment d'une attaque, et donc de l'impossibilité d'y répondre, on pourrait croire qu'il s'agit nécessairement d'un défaut

---

[400] C.c.Q., art. 1473 al. 2 ; N. VÉZINA, préc., note 203.
[401] C.c.Q., art .1473 al. 2.
[402] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-384.
[403] Leyla BILGE et Tudor DUMITRAS, « Before We Knew It. An Empirical Study of Zero-Day Attacks in the Real World », (2012) *Proceedings of the 2012 ACM conference on Computer and communications security*, p. 833. Voir aussi SYMANTEC, « Zero Day Vulnerability », en ligne : <http://www.pctools.com/security-news/zero-day-vulnerability/> (consulté le 12 décembre 2017) : « *A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack* » ; Stefan FREI et al., préc., note 390 : « *Zero-day exploits are exploits available at the date of the disclosure* » ; T. M. CHEN et S. ABU-NIMEH, préc, note 344 : « *Unpatched vulnerabilities* ».

indécelable compte tenu de l'état des connaissances conformément à l'article 1473 al. 2 C.c.Q. Nous croyons cependant qu'une approche plus nuancée s'impose. C'est que le critère choisi par le législateur pour l'application du moyen d'exonération de risque de développement, celui de « l'état des connaissances »[404], se veut de nature objective[405] : dans le cadre de l'analyse prescrite, on ne doit considérer ni les connaissances subjectives du fabricant, ni sa capacité à en prendre connaissance, mais seulement l'état des connaissances en général, indépendamment de celles du défendeur[406]. Or, bien qu'il soit juste de prétendre qu'une vulnérabilité « *zero day* » est effectivement inconnue de tous, ça ne saurait être une justification pour ce moyen d'exonération. C'est que, sauf dans le cas de logiciel en code source libre[407], il est vraisemblable que la communauté n'ait pas accès au code source du S.C.P. dans lequel est découvert la vulnérabilité. Il lui était donc impossible d'y identifier les failles. Comment, alors, pourrait-on parler de connaissances générales à l'égard du logiciel exploité ?

On serait alors forcé de procéder à une évaluation des connaissances du seul concepteur du logiciel, et donc à faire une analyse subjective là où le législateur voulait mettre en place une analyse objective. Du reste, le fabricant aurait tout avantage à ne prétendre simplement n'avoir jamais eu connaissance d'aucune des vulnérabilités exploitées, ce qui dénaturerait encore davantage le moyen d'exonération de risque de développement.

On ne peut donc pas systématiquement recourir à l'exonération du risque de développement dès qu'on est confronté à l'exploitation d'une vulnérabilité « *zero day* ». Après tout, c'est le fabricant qui a la responsabilité de produire le code source logiciel dans lequel la vulnérabilité est identifiée et, vraisemblablement, c'est lui seul qui y aura accès. Il n'est pas plus pertinent de pardonner une erreur dans la conception logicielle, qu'elle se manifeste par une vulnérabilité « *zero day* » ou autrement, que tout autre défaut de conception du fabricant. Lorsque le préjudice résulte d'une erreur grossière dans le domaine algorithmique, par exemple l'omission du fabricant de procéder à une révision soignée du code source, d'utiliser les meilleures pratiques connues en date de la conception (par exemple en utilisant des algorithmes

[404] C.c.Q., art. 1473 al. 2.
[405] P. FRÉCHETTE, préc., note 154, par. 74.
[406] J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-384 ; N. VÉZINA, préc., note 203, p. 464.
[407] O.Q.L.F., préc., note 64, « code source libre » : « Code source que l'on rend disponible gratuitement pour qu'il puisse être modifié et redistribué, dans un contexte de développement communautaire. »

de cryptage considérés sécuritaires par la communauté) ou de répondre aux rapports de bogue que lui seraient soumis, il serait inconséquent qu'il puisse trouver défense dans sa propre ignorance ou sa propre négligence.

Mais, à l'opposé, il ne serait pas approprié d'exclure complètement toute exploitation d'une vulnérabilité « *zero day* » de ce moyen d'exonération. Sans doute est-il vraisemblable qu'un bidouilleur puisse découvrir et exploiter une toute nouvelle vulnérabilité logicielle qu'aucun expert n'aurait pu anticiper, et qui viendrait causer un préjudice que les meilleures pratiques n'auraient jamais pu prévenir. Dans un tel cas, le droit prescrit que le fabricant doit être exonéré, car le défaut était bel et bien indécelable compte tenu de l'état des connaissances, ce qui jette sur les épaules du consommateur le poids, il est vrai assez lourd, des risques associés aux nombreux développements en cybersécurité[408].

Pour résumer, c'est donc que, pour procéder à une analyse plus nuancée, il vaudrait mieux dire que la défense de risque de développement doit seulement trouver à s'appliquer lorsqu'un dommage résulte de l'exploitation d'une faille de sécurité informationnelle en dépit de l'emploi par le fabricant des pratiques les plus conformes à l'état des connaissances en cybersécurité. Ce faisant, on procède à une analyse selon un critère objectif, conformément à la prescription du législateur. Il reste que cela impose tout de même à la victime de faire une preuve extrêmement technique, probablement impossible à faire sans l'aide d'un témoin expert.

Ceci dit, une autre particularité découlant de la nature informationnelle des S.C.P. nous impose un questionnement. Rappelons que le C.c.Q. donne au fabricant un devoir d'information envers les utilisateurs lorsqu'il découvre un défaut de sécurité après la mise en marché du produit[409]. Mais peut-on considérer que le régime va au-delà de cette obligation de renseignement et impose au fabricant l'obligation de mettre à la disposition de ses utilisateurs une mise à jour logicielle afin de colmater ce défaut de sécurité informationnel dans le logiciel du S.C.P. ? L'article 1473 al. 2 C.c.Q. est silencieux à cet égard et nous sommes probablement autorisés de prétendre que la possibilité qu'un défaut de sécurité physique puisse être réparé, à

[408] La doctrine avait déjà identifié le risque d'imposer un tel fardeau sur les utilisateurs dans les cas de produits de haute technologie : N. VÉZINA, préc., note 203, p. 433 ; J.-L. BAUDOUIN, P. DESLAURIERS, B. MOORE, préc., note 148, par. 2-384 ; P.-G. JOBIN, préc., note 180, par. 214.
[409] C.c.Q., art. 1473 al. 2. Le fabricant doit remplir son devoir d'information en temps opportun, dès que le fabricant acquiert la connaissance du défaut : V. KARIM, préc., note 166, par. 3200.

distance et par une mise à jour logicielle, n'avait pas été envisagée par le législateur lors de la codification de ce régime.

Mais, nonobstant le silence de 1473 C.c.Q., n'oublions pas que l'article 1468 al. 1 C.c.Q. rend le fabricant responsable du préjudice causé par un défaut de sécurité, sans égard au moment où est apparu ce défaut. S'il veut écarter sa responsabilité et qu'il a la possibilité de régler le défaut de sécurité, sans doute sera-t-il plus prudent de procéder à la mise à jour. En effet, nous croyons que le seul fait de remplir son obligation de renseignement eu égard aux nouveaux dangers sera peut-être considéré insuffisant par les tribunaux s'il est établi que le fabricant avait la possibilité d'offrir une mise à jour de ses logiciels et qu'il a omis de le faire, surtout compte tenu de la relative facilité et du peu de coûts qu'implique une telle mesure.

Enfin, concernant l'obligation de renseignement elle-même, sans doute peut-on considérer que l'avertissement qu'une mise à jour logicielle est disponible, accompagnée d'un énoncé détaillant les failles corrigées, suffiront remplir cette obligation à l'égard des l'utilisateur, pour autant que les instructions soient claires et compréhensibles, et que les mises à jour elles-mêmes soient accessibles et pas trop difficiles à installer – compte tenu, bien sûr, des connaissances que sont censés avoir les utilisateurs du S.C.P.

2. L'obligation de sécurité informationnelle en cas de faille de sécurité d'un système cyberphysique

Répétons à présent l'exercice que nous venons d'accomplir, en traitant désormais de l'obligation de sécurité informationnelle. Ce faisant, nous changerons de paradigme : là où notre approche était d'abord axée sur la sécurité physique des produits, le régime de l'obligation de sécurité informationnelle nous impose un renversement pour traiter d'abord et surtout de la sécurité sous l'angle de données générées par les S.C.P.

a) Débiteurs et créanciers

Comme nous l'avons vu dans la première partie de ce mémoire, le législateur québécois a favorisé une approche composite pour traiter de la question de la sécurité informationnelle. C'est pourquoi il faut prendre un soin supplémentaire pour identifier créanciers et débiteurs dans cette obligation, en nous référant aux lois pertinentes.

Commençons par nous demander si le fabricant d'un S.C.P. pourra être considéré comme débiteur de l'obligation de préserver la sécurité des données traitées par ses produits. Aux termes de la L.C.C.J.T.I., doivent être considérées débitrices de diverses obligations relatives à la cybersécurité « toute personne […] tenue de conserver un document »[410], « la personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel »[411], ou encore le « prestataire de services »[412]. Ces dispositions deviennent pertinentes pour le fabricant d'un S.C.P. notamment lorsque, dans le cadre des communications réseau entre un S.C.P. et un serveur distant, les fabricants sont appelés à agir comme intermédiaires et prestataires de services au sens de cette loi.

Mais, comme nous l'avons montré dans la première partie de ce mémoire, l'obligation de sécurité informationnelle peut également découler du principe général de la responsabilité extracontractuelle codifié à l'article 1457 C.c.Q. Celui-ci rend « toute personne »[413] débiteur de l'obligation de ne pas causer préjudice à autrui, et, peut-on déduire, d'assurer la sécurité informationnelle des données, pour peu que cette personne soit effectivement impliquée dans la gestion de celles-ci pour autrui. Sans doute cela est-il suffisant pour faire du fabricant d'un S.C.P. dont les serveurs entreposent les données de ses clients le débiteur de cette obligation à l'égard des tiers, quoiqu'il soit moins clair que les autres personnes visées dans le régime de la responsabilité du fabricant (distributeurs, fournisseurs et importateurs[414]) puissent être visées de la même façon.

Disons que le régime de l'article 1457 C.c.Q. nous semble aussi assez général pour sanctionner le préjudice physique découlant de mauvaises pratiques en sécurité informationnelle par le fabricant d'un S.C.P., tel que peut le faire celui de l'article 1468 C.c.Q. Rien ne nous empêche donc de considérer que le fabricant d'un S.C.P. puisse être débiteur de l'obligation d'assurer la sécurité informationnelle de son produit dans le but d'éviter la survenance d'un

[410] L.C.C.J.T.I., art. 19, concernant l'obligation de préserver la disponibilité et l'intégrité du document technologique.
[411] *Id.*, art. 25, concernant l'obligation de maintenir la confidentialité du document technologique.
[412] *Id.*, art. 26, concernant l'obligation du prestataire de service de maintenir l'intégrité, la confidentialité et la disponibilité des documents technologiques qui lui sont confiés.
[413] C.c.Q., art. 1457 al. 1.
[414] *Id.,* art. 1468 al. 2.

préjudice physique sous ce régime. Il faut dire cependant que le régime que nous avons étudié dans la section précédente est plus spécifique.

S'agissant du créancier de cette obligation, nous proposons de faire un exercice similaire. Aux termes de la L.C.C.J.T.I., le créancier sera tour à tour la personne pour qui on conserve un document technologique[415], la personne à qui appartient le document technologique portant un renseignement confidentiel[416], ou encore « quiconque confie un document technologique à un prestataire de service »[417]. Il semble donc qu'il existera toujours une sorte d'arrangement entre les parties concernant la gestion de données, ce qui laisse entendre qu'il doit exister un lien contractuel les liant. Dans ce cas, la L.C.C.J.T.I. ne viendra pas s'appliquer aux fabricants d'un S.C.P. à l'égard des tiers qui se trouveraient victimes d'un préjudice physique découlant d'une faille de sécurité informationnelle, notamment puisque ceux-ci n'auraient pas de lien contractuel avec le défendeur à l'égard de la gestion de données.

Mais on peut aussi s'asseoir sur une assise plus large, celle de 1457 C.c.Q., qui fait bénéficier sa protection à « autrui »[418], c'est-à-dire à tous ceux qui ne sont pas liés contractuellement avec l'auteur du préjudice. De cette façon, les tiers auraient accès à un recours contre le fabricant du S.C.P. Cela ne veut pas dire pour autant que ce sera l'avenue la plus appropriée, par contre. Répétons que l'obligation de sécurité informationnelle n'a pas été développée pour assurer la sécurité physique découlant de l'action dans la sphère numérique. Du reste, il existe d'autres recours plus appropriés pour traiter du défaut de sécurité causant un préjudice physique. Celui codifié par l'article 1468 C.c.Q. en est un exemple.

b) Les systèmes cyberphysiques dans l'obligation de sécurité informationnelle

Peut-on être obligé d'assurer la sécurité informationnelle d'un S.C.P. ? Pour ce qui est de la L.C.C.J.T.I., nous avons vu dans la première partie de ce mémoire que celle-ci s'intéresse notamment à encadrer les documents technologiques, et que les S.C.P. doivent être considérés comme portant des documents de ce type[419]. De plus, n'oublions pas que l'obligation de sécurité

[415] L.C.C.J.T.I., art. 19.
[416] *Id.*, art. 25.
[417] *Id.*, art. 26 al. 1.
[418] C.c.Q., art. 1457 al. 1.
[419] *Supra*, p. 33-35 ; L.C.C.J.T.I., art. 3, 4 et 71. Rappelons également qu'un logiciel sera considéré un document technologique au sens de cette loi.

informationnelle peut se fonder sur l'article 1457 C.c.Q., qui est très général. Il ne fait donc pas de doute que cette obligation vise les S.C.P., pour ce qui est de la sécurité de l'information elle-même.

Mais peut-on être obligé, en vertu de l'obligation de sécurité informationnelle, de veiller à ce que la sécurité physique des personnes et des biens soit préservée ? Voilà qui est peut-être moins encourageant. S'il traite de matière numérique, comme celle dont est partiellement composée les S.C.P., ce cadre juridique a tout de même été développé pour viser des systèmes informatiques dont le seul but est le traitement de données. Ainsi, on considérera qu'une personne est responsable lorsqu'elle n'a pas « mis en œuvre les mesures de sécurité adéquates […] pour protéger son *système d'information* contre des atteintes intérieures ou extérieures […] »[420] (nos italiques). Nulle part trouve-t-on de référence à la sécurité physique à titre de préoccupation principale, ce qui nous incite à croire que les enjeux juridiques découlant de l'action directe du numérique sur le physique n'ont pas été pris en compte de façon significative dans la construction de ce cadre. C'est dire qu'il ne peut servir directement à sanctionner un dommage physique causé par un défaut émanant du numérique.

Doit-on pour autant considérer qu'il n'est pas pertinent pour notre étude ? Sûrement pas, croyons-nous. L'obligation de sécurité informationnelle a quand même vocation de traiter du domaine virtuel, et les technologies de l'information qu'elle aborde ne diffèrent pas fondamentalement de celles employées par les S.C.P. En bout de compte, ce sera bien souvent les mêmes protocoles réseau, les mêmes systèmes d'exploitation, et les mêmes architectures computationnelles qu'on retrouvera tant dans les S.C.P. que dans les systèmes informatiques dits classiques. La plupart du temps, ceux-ci seront même compatibles et appelés à communiquer entre eux. Sans doute les enseignements découlant de l'obligation de sécurité informationnelle nous seront-ils utiles pour aborder le problème du défaut de sécurité informationnelle dans le cadre de 1468 C.c.Q.

[420] N. W. VERMEYS, préc., note 145, p. 118, citant Nicolas SAMARCQ et Luc MASSON, « Les agissements en ligne des salariés : un risque majeur pour les entreprises », (2006) *Juriscom*, en ligne : <http://www.juriscom.net/documents/resp20060605.pdf> (lien non accessible).

Il serait donc malavisé de l'écarter complètement, du moins à titre de réservoir d'où puiser les concepts pertinents. Afin qu'elle nous soit utile, nous devons voir comment l'obligation de sécurité informationnelle s'adapte à la problématique cyberphysique.

i) Disponibilité

Il n'est pas trop difficile d'imaginer des conditions qui pourraient faire en sorte qu'un S.C.P. ne soit plus en mesure de fournir ses services en devant inopérant, c'est-à-dire qu'est compromise sa disponibilité. Réfléchissons par exemple à l'incidence possible de conditions environnementales défavorables (vents violents, précipitations de neige affectant la bonne marche de capteurs en les obstruant), de l'action d'un acteur malicieux, ou encore d'une panne du réseau électrique ou des réseaux de communication.

Or, puisqu'un S.C.P. peut avoir à remplir des fonctions cruciales et que des dommages physiques importants peuvent résulter d'une interruption inopportune de ses services, celui-ci doit continuer d'opérer même en des conditions défavorables[421]. Le défi est évidemment de taille, car il est difficile de prévoir toutes les éventualités pouvant survenir dans les environnements variés dans lesquels les S.C.P. sont appelés à opérer. En effet, assurer la disponibilité est peut-être le plus grand défi lorsqu'il s'agit d'assurer la sécurité informationnelle de ce type de système[422].

Il n'est donc pas surprenant que la conception classique de la disponibilité – selon laquelle les données (et les infrastructures permettant d'accéder à celles-ci) doivent rester accessibles aux personnes autorisées – soit jugée trop restreinte. Dans le monde cyberphysique, cet aspect de la sécurité s'étend au-delà de son cadre naturel.

Un premier constat s'impose lorsqu'on lit la littérature technique afférente aux S.C.P. : celle-ci comprend la notion de disponibilité moins comme protection de l'accessibilité des *données*, et plus comme celle s'intéressant aux *systèmes* eux-mêmes[423], bien que ces deux objectifs soient évidemment reliés. En raison de la vocation des S.C.P. d'agir dans le monde

[421] Christian BERGER et Bernhard RUMPE, « Autonomous Driving—5 Years after the Urban Challenge: The Anticipatory Behicule as a Cyber-Physical System » (2014) *Proceedings of the INFORMATIK 2012*.
[422] C.P.S.P.W.G., préc., note 53, p. 69 ; A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53, p. 495-496.
[423] C.P.S.P.W.G., préc., note 53, p. 31.

physique, le critère de la disponibilité serait plutôt celui selon lequel on cherche à assurer : « *[…] timely and reliable access and use of a system* »[424]. Autrement dit, un système sécuritaire reste opérationnel, prêt à entrer en service en tout temps.

Par ailleurs, pour les S.C.P. qui remplissent des fonctions critiques et dont la défaillance pourrait avoir des conséquences dommageables dans le monde physique, l'impératif du maintien de la disponibilité est augmenté sensiblement. Alors que dans la conception classique, les données doivent être accessibles par les personnes autorisées « dès qu'elles le désirent »[425], dans le cas de ces S.C.P., au contraire, la disponibilité du système doit être maintenue en tout temps, à défaut de quoi des dommages physiques pourraient survenir. C'est ainsi, croyons-nous, que la disponibilité prend une place plus grande au sein des différents aspects de la sécurité informationnelle.

Mais, fait intéressant, à la notion de disponibilité[426] la littérature rattache aussi la notion de *résilience* du S.C.P. Celle-ci vise la capacité d'un système à résister à des conditions pouvant affecter sa disponibilité. Un S.C.P. doit continuer d'assurer son fonctionnement même dans des conditions difficiles et imprévues ou, à défaut, la recouvrer en temps opportun. À cet égard, un auteur s'est exprimé de cette façon : « *Resilience comes from a combination of elements: fault-tolerance, redundancy, adaptability, mitigation, and survivability* »[427]. Ces différents éléments sont en prendre en considération par le fabricant d'un S.C.P.

En pratique, cela se traduira évidemment en s'assurant que les données soient bel et bien accessibles, même dans des conditions imprévues et même en cas de défaillance d'une des composantes du S.C.P.[428]. En outre, un S.C.P. sera résilient si, à l'aide de procédés de détection d'erreurs par exemple, il était capable de prendre lui-même certaines des mesures nécessaires pour continuer d'assurer sa disponibilité, en temps réel et sans intervention humaine directe[429]. Il faudra également prendre garde à ce qu'un déni de service affectant un serveur distant dont

[424] C.P.S.P.W.G., préc., note 53, p. 31.
[425] N. W. VERMEYS, préc., note 145, p. 25.
[426] On parle aussi de *fiabilité*, C.P.S.P.W.G., préc., note 53, p. 69 : c'est-à-dire le fait pour un S.C.P. de maintenir ses opérations dans des conditions prédéterminées et connues par les concepteurs.
[427] B. SCHNEIER, préc., note 251, p. *x*.
[428] C.P.S.P.W.G., préc., note 53, p. 34, 71-72.
[429] Par exemple en procédant à un nettoyage de ses caméras lui permettant de s'orienter, ou encore en changeant de protocole de communication si celles-ci deviennent plus difficiles, etc.

dépendrait le S.C.P. n'affecte pas indûment la disponibilité du système[430]. Compte tenu des circonstances, des solutions doivent donc être prévues pour mitiger les dégâts en cas de panne électrique ou des réseaux de communications. Finalement, des procédés de détection d'erreur humaine peuvent également être à prescrire afin qu'une commande clairement fautive entrée dans le S.C.P. par un utilisateur n'ait pas de conséquences catastrophiques[431]. On entrevoit donc sans peine en quoi assurer la disponibilité d'un S.C.P. peut s'avérer une tâche complexe.

ii) Intégrité

La question de l'intégrité s'enrichit également d'une dimension supplémentaire lorsqu'on lui rajoute un aspect de sécurité physique. Rappelons l'existence parallèle de deux conceptions complémentaires de l'intégrité : celles de l'intégrité des données et de l'intégrité des systèmes.

Souvenons-nous que dans l'approche classique de la sécurité informationnelle, l'emphase est d'abord mise sur la protection de l'intégrité des *données*. Celle-ci est préservée quand, lors de son traitement ou de sa transmission, l'information ne subit aucune modification ou destruction, que celles-ci soient volontaires ou accidentelles[432]. On peut également faire un lien entre intégrité et intelligibilité des données, laquelle est préservée en s'assurant du maintien de leur formatage, ou entre intégrité et fiabilité : en s'assurant que l'information n'a pas été modifiée, on peut l'utiliser avec confiance. C'est, comme nous l'avons vu, ce type d'intégrité qui doit être préservée dans les documents technologiques au sens de la L.C.C.J.T.I.[433]

Or, lorsqu'on rajoute une dimension physique à la sécurité informationnelle, il n'est pas étonnant qu'on soit plutôt porté à mettre l'emphase sur l'intégrité du *système* lui-même. Comment doit-on définir une telle conception de l'intégrité ? La littérature technique propose cette définition : « *[the] ability to execute the correct instructions using the correct data at the correct time* »[434]. Le but de l'intégrité devient donc de s'assurer que le système ne pose que les gestes voulus dans le domaine physique : l'intégrité des données devient l'intégrité du

[430] C.P.S.P.W.G., préc., note 53, p. 34.
[431] *Id.*, p. 72.
[432] O.Q.L.F., préc., note 64, « Intégrité ».
[433] L.C.C.J.T.I., art. 6.
[434] C.P.S.P.W.G., préc., note 53, p. 88.

fonctionnement du système. Un S.C.P. dont l'intégrité du fonctionnement est préservée est moins susceptible de causer un préjudice physique.

Ceci est accompli en prévenant, en détectant ou en mitigeant la corruption ou la destruction de l'information reçue ou envoyée des capteurs du S.C.P., de ses composantes computationnelles et de ses actuateurs[435]. On doit également mettre en place des méthodes préventives afin que le S.C.P. puisse s'adapter en temps utile à des conditions d'opération qui déformeraient, corrompraient ou affecteraient de toute autre façon les données générées ou traitées par ses composantes physiques, virtuelles ou réseautiques[436]. Compte tenu de l'imprévisibilité inhérente du monde physique, la tâche est ardue, tel que le reconnait la littérature qui souligne le besoin de davantage de recherche dans ce domaine[437].

iii) Confidentialité

Appliquée au S.C.P., la confidentialité conserve évidemment son objectif premier, qui est de prévenir la divulgation des données à des personnes non autorisées[438]. Tel que nous l'avons vu, certains S.C.P. peuvent être appelés à recueillir et traiter des informations confidentielles ou des renseignements personnels, dont certains peuvent être particulièrement sensibles (pensons notamment aux données générées par les S.C.P. médicaux)[439].

À ce sujet, une attention particulière doit être portée aux données qui sembleraient inoffensives du premier abord, mais qui pourraient en réalité poser un risque du point de vue de la confidentialité. Un auteur donne l'exemple d'un S.C.P. qui prélèverait des données sur l'humidité d'un environnement : à première vue, celles-ci ne semblent confidentielles, mais en réalité elles pourraient acquérir un tel caractère, car elles peuvent permettre de savoir quand un

[435] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53 ; C.P.S.P.W.G., préc., note 53, p. 34.
[436] C.P.S.P.W.G., préc., note 53, p. 71.
[437] *Id.*, p. 68.
[438] O.Q.L.F., préc., note 64, « Confidentialité ».
[439] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53.

espace est occupé par une ou plusieurs personnes, en raison d'une augmentation mesurable de l'humidité dégagée par les corps[440].

La prudence est également de mise concernant certaines données qui n'auraient pas de caractère confidentiel à elles seules, mais qui pourraient révéler des renseignements sur l'utilisateur du S.C.P. une fois croisées à d'autres données[441]. C'est donc dire que la confidentialité des informations générées et traitées par les S.C.P. doit être préservée à l'aide des mesures appropriées, tout comme dans les systèmes informatiques qui n'ont pas de composante physique. La masse importante de données personnelles générées par les S.C.P. peut, par ailleurs, compliquer cette tâche[442].

Mais la confidentialité, appliquée aux S.C.P., acquiert un autre caractère lorsqu'on doit prendre en compte le besoin d'assurer la sécurité physique des utilisateurs. En effet, l'impératif de contrôle d'accès aux données s'étend au-delà du renseignement personnel ou des données traditionnellement considérées confidentielles dans le domaine cyberphysique. Alors que, dans la conception classique de la confidentialité, on s'applique à contrôler les données dont la divulgation est susceptible de causer un préjudice surtout économique ou moral (sur la réputation d'une personne, par exemple), c'est au contraire toute donnée susceptible de modifier le comportement physique du S.C.P. qu'on doit protéger contre la divulgation à des personnes ou des programmes informatiques non autorisés. On comprend aussi que la confidentialité perd sa prééminence au sein des attributs protégés de l'information, pour se soumettre à l'objectif d'intégrité. Un bris de confidentialité des données d'un S.C.P. permet à un attaquant d'agir sur l'intégrité du fonctionnement du système :

> « *Individuals may suffer physical harm as a result of privacy violations in CPS. These may include, for example, through the generation of inaccurate medical device sensor readings, the automated delivery of incorrect medication dosages via a compromised insulin pump, or the*

[440] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53 ; Han, A. JAIN, M. LUK, and A. PERRIG, « Don't sweat your privacy: Using humidity to detect human presence », (2007) *Proceedings of 5th International Workshop on Privacy in UbiComp (UbiPriv'07)*.
[441] C.P.S.P.W.G., préc., note 53, p. 74-75.
[442] *Id.*

malfunctioning of critical smart car controls, such as braking and acceleration. »[443]

La confidentialité, ainsi comprise, vise à interdire la divulgation à des personnes non autorisées d'une gamme assez étendue, et même presque complète, des données traitées par le S.C.P. Celles-ci peuvent inclure le micrologiciel[444], mais aussi les flux de données transitant entre les différentes composantes du système[445]. Pensons aux données circulant entre les composantes physiques (qui comprennent les capteurs qui prélèvent des informations sur l'environnement, de même que les actuateurs – moteurs, etc. – qui interagissent avec celui-ci), et les composantes virtuelles (qui interprètent et envoient des commandes aux composantes physiques en fonction des données sur l'environnement). Un acteur malicieux qui intercepterait ces échanges au sein du S.C.P. serait en mesure de modifier le comportement physique du système[446]. Évidemment, la même chose peut être dite des échanges entre plusieurs S.C.P. qui formeraient un système de systèmes, ou entre un S.C.P. et un serveur distant. Une prudence est donc également de mise à cet égard.

iv) Authenticité et irrévocabilité

Traitons en dernier lieu de l'authenticité et de l'irrévocabilité, lesquelles visent à établir un lien entre l'origine d'une action et un document, et à éviter que ce lien puisse être brisé ou falsifié. Dans le domaine cyberphysique, comme dans celui de la sécurité informationnelle classique, ces deux notions viennent soutenir l'impératif d'intégrité. Cependant, elles prennent en importance lorsqu'on parle non pas d'intégrité des données, mais d'intégrité du fonctionnement dans le monde physique. Il convient alors, lors de la conception logicielle d'un S.C.P., de mettre une emphase les procédés cryptographiques visant à assurer l'authenticité et l'irrévocabilité.

En pratique, on voudra qu'elles s'appliquent aux données et aux commandes qui transitent dans un S.C.P. et entre ce dernier et un serveur distant. En utilisant les méthodes de cryptographie appropriées, on doit par exemple pouvoir s'assurer qu'une commande provienne

[443] C.P.S.P.W.G., préc., note 53, p. 75.
[444] C'est-à-dire le « *firmware* », le système d'exploitation logiciel monté à bord du S.C.P.
[445] A. A. CARDENAS, S. AMIN et S. SASTRY, préc., note 53 ; C.P.S.P.W.G., préc., note 53, p. 88.
[446] C'est d'ailleurs de cette façon qu'avaient procédé les chercheurs qui avaient exploité les S.C.P. montés à bord du véhicule Jeep, dont nous avons parlé précédemment dans notre introduction.

bien d'une composante d'un S.C.P., que les données sur l'environnement proviennent bien des capteurs, ou encore qu'un signal modifié par une personne ne puisse être confondu avec un signal authentique ou légitime. En effet, nous avons vu que la sécurité physique d'un S.C.P. pouvait être compromise notamment lorsque l'information provenant de ses capteurs ou les commandes informatiques circulant au sein d'un S.C.P. étaient altérées, tel que l'exemple de l'exploitation des véhicules vu dans l'introduction de ce mémoire l'a illustré[447]. De même, quand un utilisateur fourni une commande au S.C.P. lui imposant de changer son comportement, une attention accrue devra être donnée à ce qu'il soit correctement authentifié, compte tenu de l'amplification des conséquences d'un dommage possible.

B. Quelle responsabilité pour le fabricant d'un système cyberphysique en cas de préjudice causé par un défaut de sécurité informationnel ?

Alors que nous débutons le dernier quart de ce mémoire, il y a lieu de rappeler notre objectif général: explorer les incidences de la survenance d'un préjudice physique causé par un défaut de sécurité informationnel sur le droit de la responsabilité civile. Jusqu'à présent, nous avons présenté un portrait technique des S.C.P., et expliqué en quoi ils posent un problème nouveau du point de vue de la sécurité : celui du préjudice physique causé par un défaut de sécurité informationnel au sein du système. Nous avons ensuite présenté, dans l'abstrait et tel qu'ils se sont développés pour répondre à leurs impératifs, certains des cadres juridiques pertinents qui peuvent nous éclairer quant à la responsabilité du fabricant d'un tel produit. Enfin, dans le chapitre que nous venons de conclure, nous avons vu certains des effets que peuvent avoir les S.C.P. sur ces régimes.

Le gros du travail ainsi fait, nous sommes en mesure de montrer comment ces pièces de casse-tête peuvent s'assembler afin de construire un régime de responsabilité cohérent applicable au fabricant d'un S.C.P. En effet, tel que nous allons le voir tout de suite, les outils

[447] Rappelons que les S.C.P. montés à bord des voitures en question ne procédaient à presque aucune authentification des données qui auraient permis de détecter et d'ignorer les commandes injectées frauduleusement en son sein par les chercheurs.

préexistants du droit québécois nous permettent d'appréhender une problématique cyberphysique de façon assez satisfaisante, bien qu'elle ne soit pas parfaite.

1. Un cadre de responsabilité pour appréhender les particularités des systèmes cyberphysiques

a) Une assise juridique pour appréhender le défaut de sécurité informationnel d'un système cyberphysique : le régime de 1468 C.c.Q.

En traitant de la responsabilité du fabricant d'un S.C.P., nous nous trouvons confrontés à un problème se déployant tant dans les sphères physiques que virtuelles : le préjudice se manifeste dans le monde réel, mais il prend naissance dans l'espace informationnel. Par ailleurs, bien que nous ayons choisi d'étudier le régime mis en place par l'article 1468 C.c.Q., à l'exclusion des autres traitant des questions analogues, sans doute est-il tout de même prudent de s'assurer de l'opportunité d'y faire reposer un recours ayant pris naissance dans la sphère informationnelle. En effet, peut-on appréhender un tel problème en se fondant sur un régime développé avant l'apparition d'une problématique numérique ? L'obligation de sécurité informationnelle ne serait-elle pas une assise plus propice ?

Nous croyons que non. Il nous semble préférable de sanctionner le préjudice physique né dans le monde virtuel par le truchement du régime de l'article 1468 C.c.Q., afin de réserver les enseignements de l'obligation de sécurité informationnelle à titre d'appui dans la qualification du « défaut de sécurité » au sens de l'article 1469 C.c.Q. Dans cette sous-section, nous expliquerons pourquoi.

C'est que l'obligation de sécurité informationnelle, pour débuter nos remarques en parlant d'elle, est grevée de problème d'applicabilité dans le cas d'un préjudice physique découlant d'un défaut de sécurité informationnel. Si, comme nous l'avons vu, elle peut viser la sécurité des données traitées par le S.C.P., il est moins clair qu'elle pourra s'appliquer à l'égard des dommages physiques découlant de la mauvaise gestion de l'information, surtout en l'absence d'un lien contractuel entre les parties. En effet, les lois qui mettent en place l'obligation d'assurer la sécurité des données sont silencieuses à l'égard d'un préjudice physique

qui découlerait d'une mauvaise gestion de données[448]. Cela nous porte à penser qu'il n'était pas dans l'intention du législateur de traiter de cette question lors de la création du régime. Afin de pouvoir viser le cas du préjudice physique par le truchement de l'obligation de sécurité informationnelle, nous serions obligés de procéder à un exercice assez spéculatif de création de droit, ce qui nous répugne. Cette omission de traiter des possibles incidences physiques du numérique n'est, du reste, pas particulièrement étonnante : le champ de la sécurité informationnelle a traditionnellement eu pour objectif de préserver la sécurité des données seulement[449], et l'émergence d'une problématique de sécurité cyberphysique est tout de même assez récente.

Mais même si nous étions en mesure, non sans avoir exécuté quelques contorsions inconfortables, de faire reposer sur l'obligation de sécurité informationnelle un recours en responsabilité à la suite d'un préjudice physique, nous serions confrontés à des difficultés qui nous seraient épargnées en choisissant le régime de 1468 C.c.Q. Nous nous refuserions la béquille offerte par la notion de « défaut de sécurité », qui facilite la preuve en épargnant au demandeur d'identifier la faute précise à l'origine du préjudice, puis d'en faire la preuve[450]. Il serait également plus difficile de poursuivre les autres personnes impliquées dans la mise en marché du S.C.P. : distributeurs, fournisseurs ou importateurs, qui sont par ailleurs explicitement visés par le deuxième alinéa de 1468 C.c.Q. Compte tenu de la mondialisation du commerce, surtout en ce qui a trait aux technologies de l'information, la victime perdrait une protection importante.

Sans surprise, le régime mis en place par 1468 C.c.Q. nous semble bien plus approprié : il n'est grevé d'aucun problème d'applicabilité relativement au préjudice physique causé à un tiers par le défaut de sécurité. Il fournit en outre des mesures de protection pour la victime, lesquelles sont contrebalancées par certains moyens d'exonération offerts au fabricant. Là où cependant le régime de la responsabilité du fabricant se prête moins bien au jeu, c'est à l'égard de la qualification du défaut de sécurité informationnel. Mais cela ne nous semble pas fatal –

---

[448] Voir par exemple L.C.C.J.T.I., art. 1. La L.C.C.J.T.I. s'intéresse notamment d'assurer « la sécurité juridique des *communications* effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports » (nos italiques), mais ne fournit aucune prescription quant aux mesures à prendre dans la sphère informationnelle afin de préserver la sécurité physique de ces personnes.
[449] Chris SUNDT, « Information Security and the Law », (2006) 2 *Information Security Technical Report*, p. 1.
[450] C.c.Q., art. 1468 al. 1 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-376.

nous ne voyons pas d'obstacle juridique, dans le régime de 1468 C.c.Q., à ce qu'un défaut de sécurité naisse dans la sphère informationnelle. Rappelons que l'article 1469 C.c.Q., qui définit le défaut de sécurité, avait été rédigé afin de permettre aux tribunaux d'appréhender tout développement nouveau, même ceux qu'il n'était pas possible d'anticiper lors de la création du régime, afin que celui-ci puisse s'adapter aux circonstances propres à chaque époque[451]. La notion de « défaut de sécurité » nous semble donc suffisamment flexible pour englober les cas qui relèveraient d'une problématique cyberphysique.

Il est vrai, néanmoins, que le juriste dispose de peu en matière de guide pour déterminer ce qu'est un défaut de sécurité informationnel dans le cadre de ce régime. Une lecture du C.c.Q. révèle que le législateur québécois – sans y avoir fermé la porte – n'avait peut-être pas envisagé le défaut de sécurité informationnel. Les catégories de défauts qu'il propose semblent en effet avoir été pensées pour le défaut de sécurité prenant naissance dans le domaine physique, et nous avons vu en quoi certaines de ces catégories ne s'appliquent que malaisément au défaut de sécurité informationnel[452].

Quant au corpus jurisprudentiel développé afin de déterminer dans quelles conditions nous sommes en présence d'un défaut de sécurité, force est d'admettre qu'il nous est d'un secours relativement limité pour ce qui est d'un défaut prenant naissance dans la sphère informationnelle. À notre connaissance, les tribunaux québécois se sont exclusivement penchés sur des cas de défaut de sécurité qui qui n'avaient aucun caractère numérique.

C'est donc que le régime mis en place par 1468 C.c.Q. nous permet de tenir le défaut de sécurité informationnel comme générateur de responsabilité pour le fabricant, tout en gardant malheureusement le silence sur la nature exacte de ce défaut. Il nous faut donc trouver une dernière pièce au casse-tête afin de parvenir à un cadre conceptuel capable d'appréhender le défaut de sécurité informationnel aux fins du régime que nous avons choisi. Pour ce faire, nous proposons de puiser dans le réservoir conceptuel de l'obligation de sécurité informationnelle.

[451] P.-G. JOBIN, préc., note 180, par. 210-211.
[452] *Supra*, p. 76-79.

b) Le défaut de sécurité informationnel d'un système cyberphysique dans le régime de la responsabilité du fabricant

Nous avons identifié dans la sous-section précédente la pièce manquante au régime de la responsabilité du fabricant pour traiter d'un problème cyberphysique : un appareillage conceptuel approprié pour traiter du défaut de sécurité informationnel. En effet, nous ne sommes pas à l'aise de laisser subsister un flou concernant la notion de « défaut de sécurité » dans la sphère numérique.

Devant ce silence concernant la perspective numérique du fait générateur de responsabilité dans 1468 C.c.Q., nous sommes de nouveau confrontés à un choix : doit-on remplir le vide conceptuel en érigeant de toutes pièces un échafaudage pour traiter du virtuel, ou bien peut-on emprunter des outils qui nous permettront de nous orienter par rapport à cette situation nouvelle ?

Face à ce problème, nous songeons, tel que nous l'avons annoncé plus haut, à importer certaines notions de l'obligation de sécurité informationnelle dans le régime de 1468 C.c.Q., afin de faciliter la qualification du défaut de sécurité informationnel. Cette solution est séduisante en ce qu'elle nous évite l'effort de suggérer de nouvelles normes. Mais une telle opération est-elle permise ? Existe-t-il une incompatibilité entre ces deux régimes qui empêcherait d'introduire les notions de l'obligation de sécurité informationnelle dans le cadre de la responsabilité du fabricant ? Nous croyons que non. D'une part, il existe une similitude entre les faits générateurs de responsabilité des deux régimes qui suggère une comptabilité nous permettant l'emprunt que nous envisageons. En effet, selon l'article 1469 C.c.Q., la responsabilité du fabricant est engagée lorsque le bien « n'offre pas la sécurité à laquelle on est normalement en droit de s'attendre »[453], alors que dans l'obligation de sécurité informationnelle, la responsabilité du gestionnaire des données est mise en jeu lorsqu'il « n'a pas mis en œuvre les mesures de sécurité adéquates […] pour protéger son système d'information […] »[454], le caractère adéquat de ces mesures s'évaluant en fonction de ce qui est « socialement acceptable »[455]. On remarque donc que dans les deux cas, on fait emploi d'un critère d'analyse

[453] C.c.Q., art. 1469.
[454] N. W. VERMEYS, préc., note 145, p. 118.
[455] *Id*.

évaluant l'acceptabilité sociale du niveau de sécurité mis en place afin de déterminer quand la responsabilité du débiteur doit être engagée – en présence, évidemment, d'un préjudice. De même, dans les deux cas, le législateur s'exprime en termes assez larges pour appréhender toutes sortes de situations[456].

D'autre part, d'un point de vue plus pratique, les professionnels appelés à sécuriser les S.C.P. auront recours à des notions tirées du domaine de la cybersécurité, après avoir effectué les adaptations requises par la nature cyberphysique des S.C.P. dont nous avons parlé plus haut. Puisque les S.C.P. se reposent bien souvent sur les infrastructures informationnelles préexistantes, on devra vraisemblablement avoir recours aux mêmes techniques de base pour assurer leur sécurité. En important des notions de l'obligation de sécurité informationnelle dans le cadre de la responsabilité du fabricant, le droit ne ferait que refléter cet usage.

Ceci étant dit, nous arrivons enfin au cœur du problème : qu'est-ce donc qu'un défaut de sécurité *informationnel* dans 1468 C.c.Q. ? N'oublions pas que nous devons nous assurer de rester conformes à l'esprit de l'article 1469 C.c.Q., où le législateur définit le « défaut de sécurité ». Si nous voulons ne pas dire de bêtises, nous ne pouvons nous en écarter.

C'est donc qu'à notre sens, il y a un défaut de sécurité informationnel d'un S.C.P. lorsque le fabricant n'aura pas mis en place les *mesures de sécurité informationnelle* auxquelles on est normalement en droit de s'attendre. Ces mesures doivent viser à assurer la sécurité des attributs de l'information traitée par le système : la disponibilité, l'intégrité, la confidentialité, l'authenticité et l'irrévocabilité (D.I.C.A.I.). Ces attributs, évidemment, doivent être compris selon la perspective cyberphysique de la sécurité informationnelle que nous avons évoquée plus haut. Notons également que l'information à protéger peut n'être pas confinée au S.C.P. lui-même, par exemple pour se trouver sur des serveurs distants, où elle devra également faire l'objet de mesures.

En assurant ainsi la sécurité informationnelle des S.C.P., on obtient corrélativement une plus grande sécurité physique du système. Ceci est du reste logique compte tenu de leur nature à la fois virtuelle et physique. Plus précisément, on se trouvera à assurer l'intégrité et la

[456] N. W. VERMEYS, préc., note 145, p. 71 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-376.

disponibilité du système, qui sera alors capable de continuer d'offrir ses services tel que prévu. Reprenons ici l'exemple de notre introduction pour illustrer notre propos. Dans les études citées, les véhicules piratés exécutaient les commandes injectées par les chercheurs sans authentifier leur origine. On pouvait alors les faire freiner contre la volonté de leur conducteur, par exemple. Si, au contraire, leur fabricant avait mis en place des mesures visant à assurer l'intégrité, l'authenticité et l'irrévocabilité de l'information circulant au sein des différents M.C.E. à bord de leurs véhicules, il est vraisemblable que cette attaque n'aurait pas été possible, et un tribunal serait probablement moins susceptible de considérer qu'il y a un défaut de sécurité à cet égard.

Malgré tout, il restera peut-être difficile pour le fabricant de déterminer quelles sont les mesures à mettre en œuvre afin d'éviter d'engager sa responsabilité en raison d'un préjudice physique causé par une faille informatique. Aussi proposons-nous de discuter brièvement, dans la section suivante, de certaines des incidences pratiques possibles du cadre de responsabilité que nous venons de présenter.

2. Incidences du cadre de responsabilité proposé sur les personnes impliquées dans la mise en marché d'un système cyberphysique

Quelles sont les conséquences de ce que nous achevons de voir dans ce mémoire ? Nous croyons que nous arrivons à un régime de responsabilité cohérent et pour l'essentiel capable d'appréhender la plupart des particularités d'une problématique cyberphysique, même s'il subsiste certaines questions. Afin de nous en convaincre, voyons, dans une perspective plus pratique, les incidences d'un tel cadre.

En premier lieu, toute personne impliquée dans la production d'un produit devra déterminer si le bien doit être qualifié de S.C.P. L'appellation spécifique importe en vérité assez peu – S.C.P., objet connecté robot ou autre – et il n'est évidemment pas nécessaire d'en arriver à la même désignation que nous. L'essentiel est de déterminer si l'objet contrôlé par algorithme est en mesure *d'agir dans et sur le monde réel*[457], et par conséquent de causer un préjudice physique. En se référant aux critères élaborés par la littérature technique, on peut par exemple affirmer qu'une voiture disposant de connectivité devra être qualifiée de S.C.P., car sa part

[457] Ici, afin de qualifier les S.C.P, nous reprenons l'essence de l'énoncé utilisé dans B. WALKER SMITH, préc., note 57, p. 1.

informationnelle a pour vocation d'agir dans le monde physique. Au contraire, une puce R.F.I.D. passive ou une caméra de surveillance connectée par Internet ne peuvent pas agir dans le monde physique (de façon à causer un préjudice sur ce plan, du moins). Dès lors qu'on aura déterminé que l'objet en question est un S.C.P., il faudra redoubler de précautions à son égard. Il peut en effet devenir un risque juridique à l'égard de notre responsabilité civile en raison d'un préjudice physique, par exemple en donnant lieu à l'application d'un régime comme celui de 1468 C.c.Q. Il s'agit, en fin de compte, d'identifier les objets informatisés qui sont susceptibles d'engager notre responsabilité par l'entremise de régimes sanctionnant le préjudice physique.

En second lieu, toute personne impliquée dans la mise en marché d'un S.C.P. devra se demander si elle peut être visée à titre de « fabricant » au sens de 1468 C.c.Q. Lorsqu'un S.C.P. est conçu par une seule société, la question n'est pas bien compliquée. Mais, tel que nous l'avons vu dans le chapitre précédent, il est désormais possible qu'un développeur logiciel chargé de développer une composante virtuelle du S.C.P. – et donc qui n'aurait apporté aucune contribution *tangible* à l'objet – soit inclus dans la définition de « fabricant ». C'est donc que toute personne devra se demander si elle apporte une contribution importante à la réalisation du bien, sans égard, par ailleurs, à la nature virtuelle ou matérielle de cet apport. En conséquence, beaucoup de personnes qui, auparavant, auraient été exclues de l'application d'un régime de responsabilité comme celui de l'article 1468 C.c.Q. doivent désormais faire preuve d'une vigilance accrue. Mais en réalité, il n'est pas toujours facile de déterminer qui devra être visé, tel que l'exemple du développeur tiers d'une logithèque utilisée par le fabricant dans un S.C.P. nous l'a montré. Celui-ci aura tout de même avantage à se demander si sa responsabilité pourra être engagée à la suite d'un défaut de sécurité dans un S.C.P., et, le cas échéant, chercher peut-être que ses logithèques n'y soient pas incluses.

Dès lors qu'aura déterminé que, d'une part, on travaille à la production ou la mise en marché d'un S.C.P. et que, d'autre part, notre participation est telle qu'on peut être visé par le régime de 1468 C.c.Q., il faut évidemment chercher à éviter la présence d'un défaut de sécurité susceptible d'engager notre responsabilité.

À cette fin, et avant même de discuter de la sécurité informationnelle à mettre en place, il faudra dès les premières étapes de la conception du S.C.P. procéder avec soin, en prenant en compte la nature cyberphysique de notre problème. Par exemple, le développement des moitiés

informationnelle et physique du S.C.P. devra idéalement se faire conjointement, ou à tout le moins en prenant en compte l'importance de la synergie entre celles-ci[458], en utilisant une méthode de conception appropriée[459]. De même, la sécurité du système devra être une préoccupation du fabricant dès les premières étapes du développement du produit :

> « *The entire product must be designed and maintained with an eye toward security. This means partnering with reputable device and chip manufacturers that consider security from the outset and offer appropriate warranties for their products.* »[460]

Il est en effet beaucoup plus difficile de rajouter, par mise à jour logicielle, des mesures de sécurité efficaces dans un système complété. Enfin, le fabricant devra procéder à des tests physiques des prototypes du produit en s'assurant de reproduire, autant que possible, les imprévus que pourrait rencontrer le S.C.P. une fois mis en marché. Nous estimons donc préférable d'effectuer des tests étendus hors du laboratoire, avec des sujets humains qui devront effectuer les tâches requises par les utilisateurs, afin que le fabricant puisse s'assurer de la bonne marche du système et de sa facilité d'utilisation en pratique.

En plus de chercher à écarter la survenance d'un défaut de sécurité plus « traditionnel », on devra voir à traiter également du défaut de sécurité prenant place dans la sphère strictement informationnelle. À cette fin, on peut se référer à la définition de ce défaut que nous avons proposé dans la section précédente.

En termes plus concrets, il est entendu que la mise en place d'une sécurité informationnelle d'un S.C.P. passera par la protection de la disponibilité, de l'intégrité, de la confidentialité, de l'authenticité et de l'irrévocabilité de l'information (D.I.C.A.I.), attributs adaptés en fonction de la problématique cyberphysique (que cette information se trouve à bord du système ou sur les serveurs distants dont il dépend). Cette conception cyberphysique de la sécurité de l'information, rappelons-le, met une emphase sur la disponibilité et l'intégrité des systèmes, et non pas seulement des données.

---

[458] NATIONAL RESEARCH COUNCIL, préc., note 35.
[459] Voir par exemple S. K. KHAITAN et J. D. McCALLEY, préc., note 53, p. 350.
[460] Mauricio PAEZ et Mike LA MARCA, « The Internet of Things: Emerging Legal Issues for Business », (2016) 43 *Northern Kentucky Law Review* 29, p. 53.

Afin d'assurer cette protection, on s'inspirera des notions en sécurité informationnelle « traditionnelle ». Le fabricant devra donc adopter un processus de gestion adéquate du risque cyberphysique, en s'inspirant par exemple de celle proposée par le N.I.S.T. : identification des risques, analyse des risques, réponse aux risques (mise en place de mesures de sécurité), et surveillance des risques[461].

Nous souhaitons dire quelques mots relativement aux mesures de sécurité concrètes qu'il sera appelé à mettre en place, dans le cadre de sa procédure de gestion de risque, bien que nous n'ayons évidemment pas l'ambition (ni la possibilité) de fournir une liste exhaustive. Il est en outre entendu que celles-ci varieront en fonction des circonstances propres à chaque produit. Néanmoins, sans doute devra-t-on retrouver dans tous les cas au moins la mise en place de procédures, de normes, de directives ou de politiques de sécurité visant à assurer la sécurité informationnelle des S.C.P. Le fabricant devra veiller à former ses employés à l'égard de ces documents, ainsi que de procéder à un certain contrôle au moment de l'embauche du personnel susceptible d'entrer en contact avec l'information gérée par les produits – celui-ci ayant la possibilité d'en modifier le comportement.

Il est également entendu qu'il devra prendre soin d'utiliser de bonnes pratiques en programmation dans l'élaboration des composantes virtuelles du S.C.P., ce par quoi nous pouvons entendre :

> « *A responsible programmer will use a good programming language, carefully design programs, continually inspect source code, and reason about it (or even prove many parts of it correct), chose trusted language processors, and extensively test the resulting executables.* »[462]

Une vérification attentive du code logiciel employé par le S.C.P. est donc de mise. Lorsqu'il emprunte du matériel logiciel d'un développeur tiers, par exemple lorsqu'il puisera dans le vaste éventail de logithèques offertes gratuitement, il devra agir diligemment pour s'assurer qu'un défaut de sécurité ne s'y trouve pas.

---

[461] *Supra*, p. 59.

[462] Hans MEIJER, Jaap-Henk HOEPMAN, Bart JACOBS et Erik POLL, « Computer Security Through Correctness and Transparency », dans Karl de LEEUW et Jan BERGSTRA (dir.), *The History of Information Security: A Comprehensive Handbook*, Elsevier B.V., 2007, p. 647.

Il est entendu que la configuration initiale des paramètres du S.C.P. devra être sécuritaire. Étonnement, les vulnérabilités causées par une configuration par défaut insuffisamment sécuritaire d'objets connectés sur Internet sont, en pratique, un problème récurrent :

> « *Almost daily now we are hearing about virtual shakedowns wherein attackers demand payment in Bitcoin virtual currency from a bank, e-retailer or online service. […] These attacks are fueled in part by an explosion in the number of Internet-connected things that are either misconfigured or shipped in a default insecure state.* »[463]

Du point de vue spécifique de la disponibilité et la résilience du système, le fabricant devra mettre en place des procédures afin de la préserver, dans la mesure du possible, en dépit des imprévus de la vie courante. Il faudra, par exemple, qu'il prévoie des procédures en cas de panne électrique, peut-être en incluant une batterie d'urgence afin d'éviter une interruption de service trop soudaine. De même, il pourrait anticiper une panne dans les réseaux de communication. Pensons à la serrure intelligente d'une porte d'entrée qui, ne pouvant plus communiquer avec le téléphone intelligent qui y est lié, pourrait tout de même être débarrée à l'aide d'une clé physique.

Pour ce qui est de l'intégrité du système, il est entendu que le fabricant devra mettre en place des mesures spécifiques à cet égard. Celles-ci reposeront notamment sur l'authenticité et l'irrévocabilité de l'information traitée, tel que nous l'avons annoncé plus haut. En pratique, il mettra en œuvre des méthodes de cryptage reconnues (notamment de vérification par signature numérique) pour arriver à ses fins, en s'assurant naturellement d'employer les protocoles les plus respectés et à jour. Ces démarches devront soutenir l'identification de l'utilisateur, afin qu'on puisse s'assurer que les commandes proviennent bien de la personne autorisée, mais aussi elle de l'information provenant de serveurs distants et même de celle circulant au sein même d'un S.C.P. (entre ses différentes composantes). À cet égard, rappelons à nouveau l'exemple de notre introduction, où les chercheurs avaient réussi à exploiter des vulnérabilités des véhicules notamment parce que leurs différents M.C.E. ne procédaient pas à de vérification quant à l'origine des commandes qu'ils recevaient. Notons que certaines de mesures cryptographiques

[463] B. KREBS, préc., note 349.

pourraient être assez exigeantes du point de vue computationnel, de sorte que le fabricant devra concevoir le S.C.P. en lui offrant assez de puissance pour qu'il puisse effectuer ces opérations.

De façon plus générale, le fabricant gagnera toujours à préserver autant que possible la confidentialité des communications (encore une fois par cryptographie) entre utilisateurs et S.C.P., entre S.C.P. et S.C.P., ainsi qu'entre S.C.P. et serveurs distants. Rappelons que, sous la conception cyberphysique de la confidentialité, celle-ci couvre bien plus que le renseignement personnel, pour s'étendre à une gamme très étendue (et peut-être même complète) de l'information. En effet, la confidentialité sert surtout à préserver l'intégrité et la disponibilité du système, et toute atteinte à l'information (surtout à celle du système d'exploitation du S.C.P.) est susceptible de modifier son comportement. Il faudra en outre sécuriser les lieux où les serveurs distants avec lesquels le S.C.P. communiquent sont entreposés afin d'en interdire l'accès aux personnes non autorisées.

Une fois ces mesures mises en place, le fabricant devra fréquemment répéter l'exercice d'évaluation des risques afin de s'assurer que sa démarche est toujours adéquate. Nous avons vu que la sécurité informationnelle découle d'un processus[464], et non pas d'un état figé dans le temps, précepte auquel la sécurité cyberphysique adhère également. C'est en grande partie ce processus qui sera évalué lorsqu'il s'agira de savoir si le bien est grevé d'un défaut de sécurité informationnel.

À notre avis, afin de procéder au maintien d'un niveau sécurité adéquat au fil de la vie d'un produit, le fabricant a tout à gagner à mettre en place un programme de divulgation des bogues et des failles de sécurité, possiblement en échange de récompenses monétaires. Développée dans l'industrie des technologies de l'information dans les années 1990[465], elle a

[464] B. SCHNEIER, préc., note 251, p. 84.
[465] Andreas KUEHN et Milton MUELLER, « Analysing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities », (2014) *2014 TPRC Conference Paper*, en ligne : <https://ssrn.com/abstract=2418812> (consulté le 12 décembre 2017).

notamment été reprise par certains fabricants automobiles[466] et dans le domaine médical[467]. Il s'agit en effet d'une pratique en croissance[468]. Cette démarche l'aiderait, dans tous les cas, à démontrer que son processus de gestion des risques informationnels relève d'une approche diligente et met en place un niveau de sécurité suffisamment élevé pour écarter le défaut de sécurité au sens de l'article 1469 C.c.Q.

Enfin, afin de pouvoir déterminer quelles failles informationnelles méritent une action de sa part, peut-être pourrait-il aussi faire usage d'un système de classement par sévérité des vulnérabilités[469], comme celui proposé par le *Common Vulnerability Scoring System*[470], en fonction des adaptations rendues nécessaires par la problématique cyberphysique[471]. Les répertoires de vulnérabilités informationnelles peuvent également être utiles[472].

---

[466] Par exemple : Andy GREENBERG, « Chrysler Launches Detroit's First 'Bug Bounty' For Hackers », (13 juillet 2016) *Wired*, en ligne : <https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/> (consulté le 12 décembre 2017) ; Andy GREENBERG, « GM Asks Friendly Hackers to Report Its Cars' Security Flaws », (8 janvier 2016) *Wired*, en ligne : <https://www.wired.com/2016/01/gm-asks-friendly-hackers-to-report-its-cars-security-flaws/> (consulté le 12 décembre 2017). En date de rédaction de ce mémoire, Fiat Chrysler Automobiles utilisait la plateforme Bugcrowd pour la divulgation des bogues, en ligne : <https://bugcrowd.com/fca> (consulté le 12 décembre 2017).

[467] Par exemple : PHILIPS, en ligne : <https://www.philips.com/a-w/security/responsible-disclosure-statement.html> et DRÄGER, en ligne : <http://static.draeger.com/security/> (consultés le 12 décembre 2017). La *Food and Drug Administration* américaine encourage ce type de mesures : J. M. PORUP, « FDA presses medical device makers to OK good faith hacking », (10 février 2016) *The Christian Science Monitor*, en ligne : <https://www.csmonitor.com/World/Passcode/2016/0210/FDA-presses-medical-device-makers-to-OK-good-faith-hacking> (consulté le 12 décembre 2017).

[468] BIT DEFENDER, « Bug bounty programs triple in 2017; $742 payout per vulnerability », 30 juin 2017, en ligne : <https://www.bitdefender.com/box/blog/iot-news/bug-bounty-programs-triple-2017-742-payout-per-vulnerability/> (consulté le 12 décembre 2017) ; HACKERONE, « The Hacker-Powered Security Report 2017 », p. 8, en ligne : <https://www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf> (consulté le 12 décembre 2017).

[469] Voir, à l'égard des différents systèmes de classification disponibles : Marcus PENDLETON et al., « A Survey on Systems Security Metrics », (2017) 49-4 *ACM Computing Surveys*.

[470] Le « C.V.S.S. ». Pour une description rapide, voir : Paul E. BLACK, Karen A. SCARFONE et Murugiah P. SOUPPAYA, « Cyber Security Metrics and Measures », dans *Wiley Handbook of Science and Technology for Homeland Security*, (2009), John Wiley & Sons Inc., Hoboken (N.J.), p. 6., en ligne : <https://www.nist.gov/publications/cyber-security-metrics-and-measures> (consulté le 12 décembre 2017).

[471] La littérature technique semble commencer à s'intéresser à créer une façon de classer ou d'appréhender les vulnérabilités par gravité dans le domaine cyberphysique. Voir par exemple : Xiaming YE, Junhua ZHAO, Yan ZHANG et Fushuan WEN, « Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems », (2015) 8 *Energies* 5266 ; Zach DeSMIT, et al., « Cyber-Physical Vulnerability Assessment in Manufacturing Systems », (2016) 5 *44th Proceedings of the North American Manufacturing Research Institution of SME* 1060.

[472] Par exemple le répertoire offert par le N.I.S.T., NATIONAL VULNERABILITY DATABASE (« N.V.D. »), en ligne : <https://nvd.nist.gov/home> (consulté le 12 décembre 2017). N.V.D. dépend d'un système mis en place

Évidemment, les mesures de sécurité cyberphysique qui devront être employées varieront beaucoup en fonction des circonstances. Vers quels guides se tourner pour avoir une meilleure idée du niveau de sécurité à assurer pour éviter l'apparition d'un défaut de sécurité informationnel ?

Le fabricant pourra bien sûr se tourner d'abord vers le libellé du C.c.Q., qui prescrit qu'on doive mettre en place un niveau de sécurité auquel « on est *normalement en droit de s'attendre* »[473] (nos italiques). Évidemment, cela n'impose pas de mettre en place une sécurité absolue, ce qui est du reste impossible comme nous l'avons vu[474]. Il doit toutefois répondre aux attentes raisonnables du public[475]. À cet égard, sans doute est-il probable que l'on considérera ces attentes généralement élevées. On peut dire qu'éviter tout préjudice physique est une priorité partagée par tous. Ce sera particulièrement vrai à l'égard des S.C.P. qui sont vendus avec la promesse d'offrir une sécurité supérieure, comme les voitures autonomes censées pouvoir prendre des décisions beaucoup plus rapidement que les conducteurs humains[476]. Compte tenu de la gravité amplifiée des dommages associés à une faille informatique, il est vraisemblable que la sécurité informationnelle des S.C.P. sera considérée très importante, et que que le fabricant devra déployer plus de ressources à assurer la sécurité de son produit qu'il en aurait alloué pour la sécurité des seules données.

Il est également entendu que le niveau de sécurité à mettre en place variera en fonction de l'utilisation ordinaire du bien, et de la connaissance, de l'habileté et des habitudes des consommateurs[477]. Le niveau de sécurité à mettre en place différera probablement que le S.C.P. soit destiné à un simple consommateur ou un utilisateur professionnel.

Il existe en outre des documents auxquels le fabricant pourra se référer pour se guider. Par exemple, il pourra s'inspirer de normes provenant d'organismes de normalisation, comme

---

par MITRE et soutenu par le département de la Sécurité intérieure américain, le COMMON VULNTERABILITIES AND EXPOSURES (« C.V.E. »), en ligne : <http://www.cve.mitre.org> (consulté le 12 décembre 2017).

[473] C.c.Q., art. 1469.

[474] N. W. VERMEYS, préc., note 145, p. 14.

[475] V. KARIM, préc., note 166, par. 3208.

[476] B. WALKER SMITH, préc., note 57, p. 15.

[477] V. KARIM, préc., note 166, par. 3210.

la norme I.S.O. 27002[478], C.O.B.I.T.[479] ou G.A.S.S.P.[480] Néanmoins, il devra faire preuve de prudence parce que celles-ci n'ont pas force de loi : le fait de les respecter même intégralement n'empêchera pas nécessairement la survenance d'un défaut de sécurité engageant notre responsabilité. Il faut prendre en compte qu'elles ont été développées afin d'assurer la sécurité informationnelle, sans prendre en considération une problématique cyberphysique.

Le fabricant pourra évidemment se référer aux normes de l'industrie. Au sujet des S.C.P., il existe des cadres à portée générale visant à développer une méthodologie pour mieux comprendre ces objets, comme celui proposé par le N.I.S.T. que nous avons beaucoup utilisé dans le cadre de ce mémoire[481]. Enfin, certains outils construits pour approcher d'autres types de produits peuvent être tout de même pertinents pour le fabricant d'un S.C.P. : nous pensons notamment aux multiples travaux effectués sur les objets connectés dans l'I.d.O.[482].

Dans tous les cas, le fabricant aura avantage de faire emploi des meilleures méthodes connues en sécurité informationnelle (c'est-à-dire d'user des pratiques les plus conformes à l'état des connaissances en sécurité). Juridiquement, il lui bénéficiera d'aller au-delà de ce qui semble strictement nécessaire, car de cette façon il conservera son accès au moyen d'exonération du risque de développement. Cet effet incitatif est une conséquence intéressante de ce régime.

La problématique cyberphysique aura également des incidences à l'égard de l'obligation de renseignement à laquelle est soumis le fabricant. Rappelons que le manque d'information relatif aux dangers associés au bien donne naissance à un défaut de sécurité en soi[483]. En premier lieu, le fabricant devra donc dénoncer clairement les dangers inhérents au S.C.P., en fournissant

---

[478] Cette norme peut être consultée en ligne moyennant le paiement d'une somme relativement importante. Voir, I.S.O., en ligne : <https://www.iso.org/fr/standard/54533.html> (consulté le 12 décembre 2017).
[479] *Control Objectives for Information and related Technology*.
[480] *Generally Accepted System Security Principles*.
[481] C.P.S.P.W.G., préc., note 53.
[482] Voir : Michael O'BRIAN, « The Internet of Things: The Inevitable collision with Product Liability », (2015) *The Licensing Journal*, p. 6 et suiv. L'auteur relève des projets de standardisation pour l'I.d.O., dont celui de l'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (« I.E.E.E. »), « P2413 », en ligne : <https://standards.ieee.org/develop/project/2413.html> (consulté le 12 décembre 2017) et celui de l'UNION INTERNATIONALE DES COMMUNICATIONS (« U.I.C. » ou « *I.T.U.* » en anglais), « Y2060 », en ligne : <https://www.itu.int/rec/T-REC-Y.2060-201206-I/fr> (consulté le 12 décembre 2017). Voir aussi L. ATZORI, A. IERA et G. MORABITO, préc., note 116.
[483] *Imbeault* c. *Bombardier inc.*, préc., note 171, par. 136-137.

un « portrait complet »[484] adapté aux connaissances usuelles de son public. En second lieu, le fabricant devra fournir des renseignements concernant les mesures à prendre pour se prémunir des dangers découlant de la nature cyberphysique du bien. Il faudra fournir des instructions pour minimiser ou éviter le risque[485]. Il est entendu qu'il devra parler des incidences du cyberphysique, notamment des impacts possibles d'une faille de sécurité informationnelle, par exemple en cas de panne des réseaux de communication, ou encore lorsque les capteurs sont affectés par des conditions météorologiques défavorables. Il sera sans doute opportun de divulguer les dangers d'une configuration logicielle inadéquate du S.C.P., ou de l'omission d'employer des pratiques sûres en sécurité informationnelle (notamment l'emploi d'un mot de passe sécuritaire).

En pratique, comment le fabricant remplira-t-il cette obligation de renseignement ? Rappelons que les mesures à mettre en place varient en fonction du public ciblé, des circonstances, du niveau de dangerosité du bien (par exemple des conséquences possibles d'une faille de sécurité informationnelle). Naturellement, les méthodes habituelles restent de mise, lorsque les circonstances le permettent. On pourra alors faire emploi d'étiquettes d'avertissement sur l'emballage ou sur le S.C.P. lui-même. Un manuel d'utilisation joint au produit peut également être à recommander. En proportion avec le niveau de danger associé au bien, un manuel papier ou une carte de mise en garde seront nécessaires : un simple lien vers un manuel en ligne pourrait ne pas suffire s'il faut prodiguer des avertissements particulièrement importants. Évidemment, le S.C.P. lui-même pourrait servir à partager des renseignements, soit par l'entremise d'un écran, s'il en dispose d'un (les avertissements prodigués sur les consoles des automobiles modernes à leur démarrage en sont un exemple), ou encore par l'entremise d'une application sur un téléphone intelligent, si le S.C.P. y est lié. Enfin, dans certains cas le S.C.P. devra communiquer efficacement à l'utilisateur les dangers qui peuvent survenir au courant de son utilisation : pensons au cas où un véhicule autonome avertirait le conducteur qu'il doit prendre le volant afin de prendre contrôle du véhicule lorsque ses capteurs ne parviennent plus à percevoir adéquatement l'environnement.

[484] *Létourneau* c. *JTI-Macdonald Corp*, 2015 QCCS 2382, par. 227.
[485] *Id.*

Finalement, n'oublions pas que le fabricant devra divulguer les vulnérabilités nouvellement découvertes qui créent un défaut de sécurité, dès qu'il en prend connaissance, pour préserver le recours à l'exonération du risque de développement, et que la connaissance du fabricant que son produit a causé un dommage corporel dans un autre cas met en jeu le principe de précaution qui emporte qu'il doit avertir de cette possibilité[486]. À cette fin, il gagnera sans doute à utiliser les possibilités des nouvelles technologies pour faciliter l'exécution de cette obligation. Par exemple, il pourrait avoir recours aux informations associées aux comptes d'utilisateur (le cas échéant) pour contacter les personnes pertinentes par courriel, ou directement par l'entremise du S.C.P., et les informations de nouveaux dangers, en tant évidemment compte des règles du droit de la protection de la vie privée. Lorsqu'il procède à la mise à jour du logiciel interne du S.C.P., un avis clair que la mise à jour en question est essentielle afin de régler une faille de sécurité est peut-être suffisante, quoique cela doit être évalué en fonction des circonstances propres à chaque situation.

Enfin, afin de se protéger, le fabricant aura avantage à faire usage de journalisation logicielle[487] de tous les évènements pertinents au sein du S.C.P., afin de faciliter la réfutation du défaut de sécurité au sein de son produit. Plus on a de données sur le fonctionnement du système, c'est-à-dire sur le processus « décisionnel » ayant mené à l'évènement litigieux, plus on a d'outils pour prouver que le dommage ne découlait pas d'un défaut de sécurité, mais que le système a fonctionné comme prévu et que le préjudice est survenu en raison, par exemple, d'une mauvaise utilisation de l'utilisateur. Cependant, il faudra conserver en tête que les données enregistrées ne sont pas toujours considérées fiables par les tribunaux[488].

Avec ces quelques remarques, nous espérons avoir démontré que notre cadre de responsabilité peut fournir une réponse satisfaisante à la problématique cyberphysique,

---

[486] *Létourneau c. JTI-Macdonald Corp.*, préc., note 484, para 227 ; J.-L. BAUDOUIN, P. DESLAURIERS et B. MOORE, préc., note 148, par. 2-354.

[487] O.Q.L.F., préc., note 64, « journalisation » : « Enregistrement, dans un journal, d'événements se produisant dans un système informatique. […] La journalisation permet de conserver la trace de certains événements en vue de vérifications ultérieures et de reconstituer des informations et des traitements après une panne ou un autre dysfonctionnement. » (Nos soulignés). ; B. WALKER SMITH, préc., note 57, p. 52 : « *Data will be essential to many of these claims. Specific information about the [car] crash may be stored in components of the automated driving system that are on the vehicule […]* ».

[488] B. WALKER SMITH, préc., note 57, p. 52.

notamment en fournissant une conception appropriée du défaut de sécurité informationnelle et en prenant en compte les particularités du domaine.

Nous convenons cependant qu'il n'est pas parfait, et qu'il subsiste des difficultés. La question du développeur tiers est le premier exemple qui vient en tête, mais nous n'avons pas abordé le problème posé par l'apprentissage automatisé. Il arrive, par exemple, que les modèles de comportement développés à l'aide de cette technique de l'intelligence artificielle soient si complexes que même leurs concepteurs ne les comprennent pas[489]. Comment peut-on alors espérer déterminer, dans une procédure judiciaire, si ce type d'algorithme comporte un défaut de sécurité ayant causé le préjudice physique ? Dans tous les cas, il est inévitable que la preuve à faire par la victime soit tout de même bien technique, sans même aborder la question du partage de responsabilité.

D'autres problèmes découlent, en outre, de la structure du régime lui-même. Nous avons vu que l'obligation de renseignement à l'égard des nouveaux défauts ne prend naissance qu'au moment où le fabricant en prend connaissance. Cet aspect de subjectivité jeté au sein de l'ensemble peut avoir pour effet de récompenser le fabricant qui négligerait de se tenir au courant des nouveaux développements en cybersécurité, qui sont légion. Peut-être est-ce là un effet involontaire du régime mis en place par le C.c.Q.

En vrai, sans doute serait-il tout de même pertinent que le législateur se prononce sur ces questions épineuses. Sans même traiter de la question par l'entremise d'une loi à caractère général, il pourrait d'abord légiférer sur certains des domaines d'application les plus sensibles des S.C.P., comme en santé ou dans le domaine des transports (en visant les véhicules autonomes, par exemple). Ce faisant, il se joindrait au rang des juridictions qui commencent à prendre des actions législatives relativement à la problématique cyberphysique[490].

---

[489] Richard DANZIG, « An Irresistible Force Meets a Moveable Object: The Technology Tsunami and the Liberal World Order », (2017) 5-1 *Lawfare Research Paper Series*, p. 5 : *« Moreover, as unsupervised machine learning grows more prevalent, machine decision-making moves beyond our comprehension. In this situation, if we are to benefit from the machine's work, it is not only its development but also its output that becomes unsupervised. For example, when a NY hospital fed clinical data to a central computing system, administrators were surprised to find that the system provided sounder than human predictions of schizophrenia in patients. Hospital administrators cannot determine the computer's basis for these judgments.* » (Nos soulignés).

[490] Voir par exemple le projet de loi américain au niveau fédéral : H.R. 3388 – SELF DRIVE act, 115th Congress (2017-2018). Il est intéressant de constater, à l'article 5 (1) (consulté le 12 décembre 2017), que le fabricant a

Finalement, bien que la question du préjudice physique causé par un bris de sécurité informationnel puisse être appréhendée par les principes de base en droit de la responsabilité québécois, il reste d'autres questions de la problématique cyberphysique qui ne seront peut-être pas aussi facilement traitables. Nous pensons notamment aux questions qui peuvent être liées à l'éthique, notamment celles qui découle de savoir quand l'algorithme devra décider s'il doit mettre en danger le conducteur d'une voiture autonome ou un piéton, lorsqu'une conduite sécuritaire n'est plus possible. Les questions relatives à la protection de la vie privée sont aussi importantes. Assurément, la question que nous avons abordée dans ce mémoire n'est pas la seule qu'on pourrait soulever.

l'obligation de se doter d'une politique de cybersécurité qui traite, notamment, des mesures à prendre pour assurer la sécurité physique : « *SEC. 5. […] a) Cybersecurity Plan.—A manufacturer may not sell, offer for sale, introduce or deliver for introduction into commerce, or import into the United States, any highly automated vehicle, vehicle that performs partial driving automation, or automated driving system unless such manufacturer has developed a cybersecurity plan that includes the following: (1) A written cybersecurity policy with respect to the practices of the manufacturer for detecting and responding to cyber attacks, unauthorized intrusions, and false and spurious messages or vehicle control commands. This policy shall include— (A) a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands; and (B) a process for taking preventive and corrective action to mitigate against vulnerabilities in a highly automated vehicle or a vehicle that performs partial driving automation, including incident response plans, intrusion detection and prevention systems that safeguard key controls, systems, and procedures through testing or monitoring, and updates to such process based on changed circumstances. (2) The identification of an officer or other individual of the manufacturer as the point of contact with responsibility for the management of cybersecurity. (3) A process for limiting access to automated driving systems. (4) A process for employee training and supervision for implementation and maintenance of the policies and procedures required by this section, including controls on employee access to automated driving systems.* » À l'instar du cadre de responsabilité que nous avons dégagé dans ce mémoire, la solution proposée dans ce projet de loi emprunte les méthodes de la cybersécurité des données en les adaptant à la nature cyberphysique du problème. De nombreux états américains ont également des instruments législatifs relatifs aux véhicules autonomes. À cet égard, voir : NATIONAL CONFERENCE OF STATE LEGISLATURES, *Autonomous Vehicles Legislative Database*, 2017, en ligne : <http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx> (consulté le 12 décembre 2017).

Conclusion

Les S.C.P. sont des systèmes formés par la mise en synergie de trois éléments : les composantes physiques, les composantes virtuelles, et une connectivité aux réseaux numériques. Ils ont pour vocation première non pas le simple traitement de données, mais l'action directe sur le monde physique. Ceci les place à la frontière entre le monde physique et le monde numérique. Leur qualification juridique reflète cette dualité : ce sont généralement des biens meubles qui portent, du point de vue de la L.C.C.J.T.I., des documents technologiques. Ils sont appelés à trouver application dans une foule de domaines – presque dans toutes les sphères de l'activité humaine – et leur déploiement est en croissance.

Leur nature cyberphysique rend cependant possible qu'ils causent un préjudice physique en raison d'un bris de sécurité informationnelle, et ce danger est aggravé par leur connectivité aux réseaux (surtout à Internet). L'exemple de l'exploitation des véhicules que nous avons présenté en introduction de ce mémoire met en exergue les dangers que cette dynamique peut représenter, mais d'autres situations peuvent aussi être envisagées, comme celle d'un préjudice qui découlerait d'un bogue informatique du dispositif médical implanté dans le corps d'un patient. Évidemment, le droit doit se pencher sur les incidences de telles hypothèses.

Au meilleur de notre connaissance, la perspective d'un préjudice physique prenant naissance dans la sphère virtuelle est inédite en droit québécois de la responsabilité. Ce dernier peut-il fournir une réponse satisfaisante à ce nouveau problème ? En règle générale, on peut certes reprocher au droit de répondre avec lourdeur aux problématiques complexes et changeantes qui émergent des technologies de l'information. Or, nous estimons que ceci n'empêche pas les principes juridiques de base de fournir une réplique adéquate à la situation envisagée.

À cette fin, nous avons présenté deux cadres de responsabilité, issus chacun d'un des domaines d'opération des S.C.P. (physique et virtuel) afin de pouvoir en dégager par la suite un cadre de responsabilité applicable au fabricant de tels systèmes dont la faille de sécurité informationnelle aurait causé un préjudice physique. Il s'agit de la responsabilité du fabricant mis en place par l'article 1468 C.c.Q. et celui de l'obligation de sécurité informationnelle. Une fois les principes et le vocabulaire de ce dernier domaine présentés, nous avons brièvement

dépeint certains des enjeux en cybersécurité qui grèvent les S.C.P. – et qui expliquent l'intérêt d'une étude juridique à ce sujet. Ce sont la gravité amplifiée des dommages potentiels d'un bris de cybersécurité en raison de répercussions dans le domaine physique (et non plus seulement dans la sphère informationnelle), les nouvelles vulnérabilités entraînées par la nature cyberphysique de ces systèmes, et l'attrait nouveau qu'ils peuvent représenter pour les acteurs malicieux qui chercheraient à les exploiter.

Une fois ce portrait tracé, nous avons vu quels étaient les effets du cyberphysique sur les cadres présentés dans l'abstrait. Le cadre de la responsabilité du fabricant de l'article 1468 C.c.Q. s'adapte assez bien aux S.C.P. Il vise sans difficulté les biens meubles grevés d'un défaut de sécurité, en laissant une grande marge de manœuvre à la forme que peut prendre ce défaut. Il est suffisamment flexible pour viser les différents acteurs impliqués dans la mise en marché d'un S.C.P., notamment le développeur logiciel responsable de la conception de son programme interne et responsable, pour l'essentiel, de mettre en place les mesures de sécurité informationnelle appropriées au sein du système. En outre, ce régime offre au fabricant des moyens d'exonération qui semblent appropriés compte tenu de l'impossibilité d'assurer une sécurité parfaite en matière informationnelle. Mais certains moyens d'exonération, comme celui du risque de développement, ont également l'effet positif d'inciter le fabricant à mettre en place les meilleures méthodes de sécurité connues, au-delà de ce qui sera strictement nécessaire, dans l'espoir de garder ouverte cette avenue d'exonération.

Or, la flexibilité inhérente des termes très généraux « défaut de sécurité » retrouvés à l'article 1469 C.c.Q. nous cause problème en ce qu'elle ne nous fournit aucun guide pour savoir à quoi ressemblerait ce défaut dans la sphère informationnelle. Ce vide conceptuel n'est pas comblé par la jurisprudence ou la doctrine québécoise, qui n'a pas encore eu à se pencher sur une telle question.

L'obligation de sécurité informationnelle, elle aussi, est affectée par la nature cyberphysique des objets à l'étude dans ce mémoire. Bien qu'elle fournisse un cadre conceptuel capable d'appréhender le défaut de sécurité informationnel, elle ne s'applique que malaisément lorsqu'il s'agit de sanctionner un préjudice physique causé à un tiers. Nous croyons cependant que les principes de base de la sécurité informationnelle peuvent s'adapter pour traiter d'un problème cyberphysique. Les attributs de l'information à protéger, représentés par l'acronyme

D.I.C.A.I., sont transformés par la vocation des S.C.P. d'agir sur le monde physique. Il découle en effet de cette vocation que le but de la sécurité informationnelle devient non pas de protéger seulement l'information, mais d'abord et surtout la sécurité physique des personnes et des biens. À cette fin, la confidentialité de l'information est reléguée au second rang parmi les attributs D.I.C.A.I., et l'intégrité et la disponibilité des systèmes règnent en maîtres.

Ces observations ainsi faites, nous avons en main les outils pour construire un cadre de responsabilité extracontractuel applicable au fabricant d'un S.C.P. dont le produit aurait causé un préjudice en raison d'un défaut de sécurité informationnel. À notre avis, le régime de l'article 1468 C.c.Q. est mieux adapté pour traiter d'une telle question, et le cadre de l'obligation de sécurité informationnelle peut nous servir afin de définir le défaut de sécurité informationnel au sens de l'article 1469 C.c.Q. Il en découle alors que toute personne impliquée dans la fabrication d'un S.C.P. doit se demander, sans égard à la nature numérique ou physique de son apport, si sa contribution est assez importante pour être visée par le régime de l'article 1468 C.c.Q. Dès lors, elle doit prendre toutes les mesures de sécurité informationnelle raisonnables afin d'éviter que ne se glisse un défaut de sécurité informationnel dans le produit en question. En surface, cela sera similaire aux mesures employées dans le domaine de la cybersécurité « traditionnelle » – excepté pour ce qui est de la finalité des mesures employées, c'est-à-dire préserver la sécurité des personnes et des biens.

Le cadre de responsabilité que nous avons dégagé, croyons-nous, a l'avantage de se reposer sur une assise ayant fait ses preuves et fournissant des recours aux victimes dans un objectif de protection du consommateur. Là où il ne savait pas fournir de réponses, nous sommes allés puiser dans un réservoir conceptuel pertinent, sans qu'il ait été nécessaire de proposer de toutes pièces une nouvelle règle de droit. À notre avis, cela démontre que le droit québécois de la responsabilité dispose d'assez de ressources pour traiter de la problématique cyberphysique émergente de façon assez satisfaisante, bien que certaines questions subsistent.

Évidemment, les tribunaux feront peut-être une autre interprétation du défaut de sécurité informationnel que nous, que ce soit sur sa nature, sur les mesures qu'il exige qu'on mette en place, ou sur les personnes qui peuvent être impliquées dans son sillage. Compte tenu de la place croissante que les S.C.P. sont appelés à prendre dans la vie quotidienne au fil des prochaines décennies, le silence jurisprudentiel à cet égard ne saurait se prolonger très longtemps. Sans

doute finirons-nous par avoir un flot de décisions judiciaires traitant de la question qui nous a intéressés ici, et peut-être aussi une précision législative qui, somme toute, pourrait n'être pas superflue, du moins dans certains domaines.

En attendant, le fabricant aura toujours avantage à privilégier la sécurité de ses produits. D'une part, sans même avoir besoin de savoir quelle sera la solution précise qui sera privilégiée par les tribunaux, sans doute peut-il estimer certain que sa responsabilité peut être engagée en raison d'un préjudice physique causé par l'emploi de mauvaises pratiques en sécurité informationnelle. Mais, d'autre part, les incidences d'un bris de cybersécurité ne sont pas seulement économiques ou juridiques : elles sont également préjudiciables à l'image de marque d'une entreprise[491]. Au-delà d'éviter de se retrouver dans une situation où ses produits mal sécurisés ont causé un préjudice à ses clients, une entreprise aurait avantage à assurer une bonne sécurité afin de bénéficier d'une réputation plus favorable que ses compétiteurs[492].

Il reste que, par-delà du droit, la sécurité des S.C.P. ne sera pas toujours facile à maintenir. Tel que nous l'avons vu, ce sont des systèmes complexes et il est difficile de prévoir comment ils peuvent être exploités ou faire l'objet d'une défaillance. La littérature technique a par ailleurs souligné le besoin de recherche supplémentaire à cet égard.

Mais, comme nous l'avons dit en introduction de ce mémoire, nous avons été en mesure d'aborder une étroite portion seulement des questions associées au paradigme cyberphysique des technologies de l'information. Au-delà des confins du droit privé, les S.C.P. posent d'importants enjeux de sécurité nationale, surtout lorsqu'ils sont utilisés à titre d'infrastructures :

> « *[…] new security audits are starting to reveal the vulnerability of major critical infrastructures. In a recent security audit, the Tennessee Valley Authority (TVA), the nation's largest public power company, was*

[491] HANOVER RESEARCH, *The Emergence of Cybersecurity Law*, février 2015, p. 5, en ligne : <https://sm.asisonline.org/ASIS%20SM%20Documents/The-Emergence-of-Cybersecurity-Law.pdf> (consulté le 12 décembre 2017).
[492] C. SUNDT, Chris, « Information security and the law », *Information Security Technical Report 2*, (2006), p. 1.

found to be vulnerable to cyber attacks that could sabotage their control systems. »[493]

Plus funestement encore, les S.C.P. pourraient être aussi appelés à jouer un rôle dans les conflits armés du 21e siècle. Émergent alors d'importantes questions juridiques, par exemple celle de l'imputabilité des décisions prises par les algorithmes et mises en action par un S.C.P. sur le champ de bataille, qui risquent de pousser les cadres existants à leurs limites[494].

La problématique cyberphysique n'est qu'une des tendances susceptibles d'avoir des effets importants sur le droit dans l'avenir[495]. Les avancées technologiques continueront d'avoir des incidences majeures sur la société en lui apportant des transformations peut-être profondes[496]. Celles-ci pourraient se faire non sans heurts, alors que l'automatisation promet de faire disparaître de nombreux emplois[497]. Assurément, traiter de questions de ce genre demande une expertise dans plusieurs domaines et requiert désormais la coopération de chercheurs de plusieurs champs distincts. Ces enjeux risquent d'impliquer des juristes pour longtemps encore.

---

[493] A. A. CARDENAS et al., préc., note 61 ; UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, *Information Security. TVA Needs to Address Weaknesses in Control Systems and Networks*, 2008, en ligne : <https://www.gao.gov/products/GAO-08-526> (consulté le 12 décembre 2017). Voir aussi, à cet égard : U.S. DEPARTMENT OF HOMELAND SECURITY, *The Future of Smart Cities: Cyber-Physical Infrastructure Risk*, 2015, en ligne : <https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf> (consulté le 12 décembre 2017).

[494] Voir par exemple : Dustin A. LEWIS, Gabriella BLUM et Naz K. MODIRZADEH, « War-Algorithm Accountability », (2016), en ligne : <https://ssrn.com/abstract=2832734> (consulté le 12 décembre 2017).

[495] Voir, pour une analyse de certaines des autres tendances possibles : Benoît DUPONT, « L'environnement de la cybersécurité à l'horizon 2022. Tendances, moteurs et implications », Note de recherche no. 14, (2012), en ligne : <http://benoitdupont.openum.ca/files/sites/31/2015/07/Dupont-2012-Cybersécurité-2022-note-14.pdf> (consulté le 12 décembre 2017).

[496] Voir à cet égard par exemple : R. DANZIG, préc., note 489.

[497] Vincent DEL GIUDICE et Wei LU, « America's Rich Get Richer and the Poor Get Replaced by Robots », (26 avril 2017) *Bloomberg*, en ligne : <https://www.bloomberg.com/news/articles/2017-12-18/finance-gurus-devise-funky-workarounds-to-loss-of-salt-deduction> (consulté le 12 décembre 2017).

Bibliographie

LÉGISLATION ET RÉGLEMENTATION

Législation canadienne fédérale

Code criminel, L.R.C. (1985), c. C-46

Loi sur l'accès à l'information, L.R.C. (1985), c. A-1

Loi sur l'emballage et l'étiquetage des produits de consommation, L.R.C. (1985), c. C-38

Loi sur l'indemnisation du dommage causé par les pesticides, L.R.C. (1985), c. P-10

Loi sur la protection des renseignements personnels et documents électroniques, L.C. (2000), c. 5

Loi sur la responsabilité en matière maritime, L.C. 2001, c. 6

Loi sur la responsabilité nucléaire, L.R.C. (1985), c. N-28

Loi sur les produits dangereux, L.R.C. (1985), c. H-3

Législation québécoise

Code civil du Québec, L.Q. 1991, c. 64

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

Loi sur l'assurance automobile, L.R.Q., c. A-25

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., ch. P-39.1

Loi sur la protection du consommateur, L.R.Q., c. P-40.1

Loi sur le régime des eaux, L.R.Q., c. R-13

Loi sur les accidents de travail, L.R.Q., c. A-3

Législation et instruments étrangers et internationaux

44 U.S.C. § 3542

Convention des Nations Unies relative aux contrats de vente internationale de marchandises, 11 avril 1980

Directive de la Communauté Économique Européenne du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux, (85/374/CEE), Journal officiel n° L 210 du 07/08/1985 p. 0029 - 0033

H.R. 3388 – SELF DRIVE Act, 115th Congress (2017-2018)

JURISPRUDENCE

Accessoires d'auto Vipa c. *Therrien*, [2003] R.J.Q. 2390 (C.A.)

Allstate du Canada, compagnie d'assurances c. *Assurance royale du Canada*, [1994] R.J.Q. 2045 (C.S.)

Baldor Electric Company c. *Delisle*, 2012 QCCA 1004

Bédard c. *Location Val-d'Or inc.*, J.E. 85-1029 (C.S.)

Cigna du Canada c. *A.C.F. Grew Inc.*, [1993] R.R.A. 295

Cohen v. *Coca-Cola Ltd.*, 1967 R.C.S. 469

Compagnie d'assurances Wellington c. *Canadian Adhesives Ltd.*, [1997] R.R.A. 635

Connolly c. *Seven-up Canada Inc.*, J.E. 85-909 (C.S.)

Covertite Ltd. c. *Fonds d'indemnisation des victimes d'accidents d'automobiles*, [1965] C.S. 140

Danson c. *Château Motors Ltd.*, 1976 C.P.

Desjardins Assurances générales c. *Venmar ventilation inc.*, 2014 QCCS 3653

Duteau c. *Service agricole de l'Estrie*, 2013 QCCS 50

Gagnon c. *Ratté*, [1996] R.R.A. 766 (C.S.)

Gauvin v. *Canada Foundries & Forgings Ltd.*, 1964 C.S. 160

General Motors Products of Canada Ltd v. *Kravitz*, [1979] 1 R.C.S. 790

General Steel Wares Ltd. c. *Raymond*, 1978 C.A. 288

Gougeon c. *Peugoet Canada ltée*, 1973 C.A. 824

Imbeault c. *Bombardier inc.*, 2006 R.R.A. 462 (C.S.)

Installations électriques R. Théberge inc. c. *Rainville (Paré, Tanguay, notaires, s.e.n.c.)*, 2015 QCCQ 5590

Ladouceur c. *Brasserie Labatt ltée*, B.E. 99BE-779 (Q.C.p.c.)

Lebel c. *2427-9457 Québec inc.*, 2007 QCCS 4644

Létourneau c. *JTI-Macdonald Corp*, 2015 QCCS 2382

London & Lancashire Guarantee & Accident Co. v. *Cie F.X. Drolet*, 1944 S.C.R. 82

Lower St. Lawrence Power Co. c. *Immeuble Landry Ltée*, [1926] R.C.S. 655

Monsanto Oakville Ltd v. *Dominion Textile Co.*, 1985 B.R. 339

Montreal Light, Heat and Power Consolidated c. *Westmount (City of)*, [1926] R.C.S. 515

Pharand Ski Corp. c. *Alberta*, 1991 CarswellAlta 85 (ABQB)

Pomerleau c. *East Broughton Station (Mun. du village d')*, [1965] C.S. 337

Québec (Procureur général) c. *Labrador Welding Ltd.*, [1972] C.S. 426

R c. *Stewart*, [1988] 1 R.C.S. 963

Ross v. *Dunstall*, (1921) 62 S.C.R. 393

St-Laurent (Cité de) c. *Commission hydroélectrique de Québec*, [1978] 2 R.C.S. 529

Trudel v. *Clairol Inc.*, 1975 2 R.C.S. 236

Véranda Industries inc. c. *Beaver Lumber Co.*, [1992] R.J.Q. 1763 (C.A.)

Wabasso Ltd. c. *National Drying Machinery Co.*, 1981 1. R.C.S. 1554

DOCTRINE

Monographies et ouvrages collectifs

BAUDOUIN, J.-L. et Y. RENAUD, *Code civil du Québec annoté*, 19e éd., Montréal, Wilson & Lafleur, 2016

BAUDOUIN, J.-L., P. DESLAURIERS et B. MOORE, *La responsabilité civile*, 8e éd., Montréal, Éditions Yvon Blais, 2014

CÔTÉ, P.-A., *Interprétation des lois*, 4e éd., Montréal, Les Éditions Thémis, 2009

DESLAURIERS, J., *Vente, louage, contrat d'entreprise ou de service*, 2e éd., Montréal, Wilson & Lafleur, 2013

JOBIN, P.-G., *La Vente*, 3e éd., Cowansville, Éditions Yvon Blais, 2007

KARIM, V., *Les Obligations*, 4e éd., Vol. 1, Montréal, Wilson & Lafleur, 2015

LAFOND, P.-C., *Droit de la protection du consommateur : Théorie et pratique*, Montréal, Éditions Yvon Blais

LAMONTAGNE, D.-C., *Biens et propriété*, 7e éd., Montréal, Éditions Yvon Blais, 2013

MINISTÈRE DE LA JUSTICE, *Commentaires du ministre de la Justice, Le Code civil du Québec*, tome 1, Québec, Les Publications du Québec, 1993

VERMEYS, N. W., *Droit codifié et nouvelles technologies : le Code civil*, Montréal, Éditions Yvon Blais, 2015

VERMEYS, N. W., *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010

Articles de revue et études d'ouvrages collectifs

ARBOUR, M.-E., « Itinéraire du risque de développement à travers des codes et des constitutions », dans B. MOORE (dir.), *Mélanges Jean-Louis Baudouin*, Cowansville, Éditions Yvon Blais, 2012

ARBOUR, M.-E., « Portrait of Development Risk as a Young Defence », (2014) 59-4 *McGill Law Journal* 915

ARBOUR, M.-E., « Sécurité des produits, santé des consommateurs, responsabilités et constitutions : synergies comparées », (2013) 7-2 *Revue de droit et santé de McGill* 169

BERNARDOT, A. et R. KHOURI, *La responsabilité du centre hospitalier et du fabricant résultant du fait d'appareils médicaux défectueux*, (1980) 26 *McGill Law Journal* 978

BICH, M.-F., « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans S.F.P.B.Q., *Développements récents en droit de la propriété intellectuelle*, Cowansville, Éditions Yvon Blais, 2003

DANZIG, R., « An Irresistible Force Meets a Moveable Object: The Technology Tsunami and the Liberal World Order », (2017) 5-1 *Lawfare Research Paper Series*

DE RICO, J.-F. et D. JAAR, « Le cadre juridique des technologies de l'information », dans S.F.P.B.Q., vol. 298, *Développements récent en droit criminel (2008)*, Cowansville, Éditions Yvon Blais

DUPONT, B., « L'environnement de la cybersécurité à l'horizon 2022. Tendances, moteurs et implications », Note de recherche no. 14, (2012), en ligne : <http://benoitdupont.openum.ca/files/sites/31/2015/07/Dupont-2012-Cybersécurité-2022-note-14.pdf>

DUPONT, B., « L'évolution du piratage informatique : De la curiosité technique au crime par sous-traitance », dans ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION (dir.), *Le respons@able 2.0 : Acteur clé en AIPRP*, Cowansville, Québec, Éditions Yvon Blais, en ligne : <http://benoitdupont.openum.ca/files/sites/31/2015/07/Dupont-2010-Les-pirates-informatiques_0.pdf>

FORRAY, V., « Peut-être. Incertitude du risque et dialectique de la responsabilité », (2014) 59-4 *McGill Law Journal* 847

FRÉCHETTE, P., « Fait des biens », dans JurisClasseur Québec, coll. « Droit civil », *Obligations et responsabilité civile*, fasc. 19, Montréal, LexisNexis Canada, feuilles mobiles

HAANAPPEL, P., « La responsabilité civile du manufacturier en droit québécois », (1980) 25 *McGill Law Journal* 365

HANOVER RESEARCH, *The Emergence of Cybersecurity Law*, février 2015, en ligne : <https://sm.asisonline.org/ASIS%20SM%20Documents/The-Emergence-of-Cybersecurity-Law.pdf>

LEWIS, D. A., G. BLUM et N. K. MODIRZADEH, « War-Algorithm Accountability », (2016), en ligne : <https://ssrn.com/abstract=2832734> (consulté le 12 décembre 2017).

MÄKINEN, J., « Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things », (2015) 24-3 *Information & Communications Technology Law* 262

NEVEJANS, N., « Les robots : tentative de définition », dans A. BENSAMOUN (dir.), *Les Robots, objets scientifiques, objets de droits*, Paris, Éditions Mare & Martin, 2016

O'BRIAN, M., « The Internet of Things : The Inevitable collision with Product Liability », (2015) *The Licensing Journal*

PAEZ, M. et M. LA MARCA, « The Internet of Things: Emerging Legal Issues for Business », (2016) 43 *Northern Kentucky Law Review* 29

PEPPET, S. R., « Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent », (2014) 93 *Texas Law Review* 85

RABKIN, J. et A. RABKIN, « Naviguating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea », (2013) 14-1 *Chicago Journal of International Law* 197

RICHARDS, N. M. et W. D. SMART, « How should the law think about robots? », (2013), en ligne : <https://ssrn.com/abstract=2263363>

ROBINSON, W. K., « Patent Law Challenges for the Internet of Things », (2015) 15-4 *Wake Forest Journal of Business and Intellectual Property Law* 655

SAMARCQ, N. et L. MASSON, « Les agissements en ligne des salariés : un risque majeur pour les entreprises », (2006) *Juriscom*, en ligne : <http://www.juriscom.net/documents/resp20060605.pdf> (lien non accessible)

SNELL, J. et C. LEE, « The Internet of Things Changes Everything, or Does It? – Your Handy Guide to Legal Issue-Spotting in a World Where Everything Is Connected », (2015), 32-11 *The Computer & Internet Lawyer*

VERMEYS, N. W., J. M. GAUTHIER et S. MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », *Document de travail du Labortoire de Cyberjustice* No. 11, 2014

VERMEYS, N.W., K. BENYEKHLEF et V. GAUTRAIS, « Réflexions juridiques autour de la terminologie associée aux places d'affaires électroniques », (2004) 38 *Revue juridique Thémis* 641

VÉZINA, N. et F. MANIET, « La sécurité du consommateur au Québec… deux solitudes : mesures préventives et sanctions civiles des atteintes à la sécurité », (2008) 49-1 *Les cahiers de Droit* 57

VÉZINA, N., « Dualité de régimes et interdiction d'options », dans JurisClasseur Québec, coll. « Droit civil », *Obligations et responsabilité civile*, fasc. 16, Montréal, LexisNexis Canada, feuilles mobiles

VÉZINA, N., « L'exonération fondée sur l'état des connaissances scientifiques et techniques, dites du 'risque de développement' : regard sur un élément perturbateur dans le droit québécois de la responsabilité du fait des produits », dans P.-C. LAFOND (dir.), *Mélanges Claude Masse : En quête de justice et d'équité*, Cowansville, Éditions Yvon Blais, 2003

VÉZINA, N., « Obligation d'information relative à un bien dangereux et obligation de sécurité : régime général et droit de la consommation », dans JurisClasseur Québec, coll. « Droit des affaires », *Droit de la consommation et de la concurrence*, fasc. 4, Montréal, LexisNexis Canada, feuilles mobiles

WALKER SMITH, B., « Automated Driving and Product Liability », (2017) *Michigan State Law Review* 1

WALTZMAN, H. W. et L. SHEN, « The Internet of Things », (2015) 27-7 *Intellectual Property & Technology Law Journal* 19

WEBER, R. H., « Internet of Things – New security and privacy challenges », (2010) 26 *Computer Law & Security Review* 23

Dictionnaires

BLUM, C., (dir.), *Le Nouveau Petit Littré*, Paris, Éditions Garnier, 2009

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Le grand dictionnaire terminologique », en ligne : <http://www.granddictionnaire.com/index.aspx>

ROBERT, P., J. REY-DEBOVE et A. REY (dir.), *Le Nouveau Petit Robert*, Paris, Dictionnaires Le Robert, 2010

LITTÉRATURE TECHNIQUE

AHMADI, H. et al., « The Sparse Regression Cube: A Reliable Modeling Technique for Open Cyber-Physical Systems », (2011) *Proceeding sof the IEEE/ACM Second International Conference on Cyber-Physical Systems* 87

ALEMZADEH, H. et al., « Analysis of Safety-Critical Computer Failers in Medical Devices », (Juillet-Août 2013) *IEEE Security and Privacy* 14

ATZORI, L., A. IERA et G. MORABITO, « The Internet of Things: A Survey », (2010) 54-15 *Computer Networks*

BAHETI, R. et H. GILL, « Cyber-physical Systems », dans T. SAMAD et A. ANASWAMY (dir.), *The Impact of Control Technology*, IEEE Control Systems Society, 2011, en ligne : <http://ieeecss.org/general/impact-control-technology>

BERGER, C. et B. RUMPE, « Autonomous Driving—5 Years after the Urban Challenge: The Anticipatory Behicule as a Cyber-Physical System » (2014) *Proceedings of the INFORMATIK 2012*

BHATIA, G., K. LAKSHMANAN et R. RAJKUMAR, « An End-to-End Integration Framework for Automotive Cyber-Physical Systems Using SysWeaver », (2010) *Proceedings of the AVICPS*

BILGE, L., et T. DUMITRAS, « Before We Knew It. An Empirical Study of Zero-Day Attacks in the Real World », (2012) *Proceedings of the 2012 ACM conference on Computer and communications security*

BLACK, P.E., K. A. SCARFONE et M. P. SOUPPAYA, « Cyber Security Metrics and Measures », dans *Wiley Handbook of Science and Technology for Homeland Security*, (2009), John Wiley & Sons Inc., Hoboken (N.J.), p. 6., en ligne : <https://www.nist.gov/publications/cyber-security-metrics-and-measures>

BOOS, D. et al., « Controllable accountabilities: The Internet of Things and its challenges for organisations », (2013) 32-5 *Behaviour & Information Technology* 449

CARDENAS, A. A. et al., « Challenges for Securing Cyber Physical Systems », (2009) *Workshop on Future Directions in Cyber-physical Systems Security*, en ligne : <https://chess.eecs.berkeley.edu/pubs/601/cps-security-challenges.pdf>

CARDENAS, A. A., S. AMIN et S. SASTRY, « Secure Control: Towards Survivable Cyber-Physical Systems », (2008) *The 28th International Conference on Distributed Computing Systems Workshops* 495

CHEN, T. M. et S. ABU-NIMEH, « Lessons from Stuxnet », (2011) 44-4 *Computer* 91

COMMITEE ON NATIONAL SECURITY SYSTEMS, *National Information Assurance Glossary*, 2010, en ligne : <https://www.hsdl.org/?view&did=7447>

CONTI, M. et al., « Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence », (2012) 8 *Pervasive and Mobile Computing*

CORONADO, A. J., et T. L. WONG, « Healthcare Cybersecurity Risk Management: Keys to an Effective Plan », (2014) *Horizon*

CÔTÉ, A.-M., M. BÉRUBÉ et B. DUPONT, « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », (2016) *Réseaux*, p. 203-224

CYBER PHYSICAL SYSTEMS PUBLIC WORKING GROUP (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), *Framework for Cyber-Physical Systems*, Release 1.0, 2016, en ligne : <https://pages.nist.gov/cpspwg/>

DeSMIT, Z. et al., « Cyber-Physical Vulnerability Assessment in Manufacturing Systems », (2016) 5 *44th Proceedings of the North American Manufacturing Research Institution of SME* 1060

EVANS, D., « The Internet of Things : How the Next Evolution of the Internet is Changing Everything », (avril 2011) *Cisco Internet Business Solutions Group White Paper*, en ligne : <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>

FEDERAL TRADE COMMISSION, *Internet of Things: Privacy & Security in a Connected World*, F.T.C. Staff Report, 2015, p. 1, en ligne : <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

FERNANDES, E., J. JUNG et A. PRAKASH, « Security Analysis of Emerging Smart Home Applications », (2016) *2016 IEEE Symposium on Security and Privacy (SP)*

FREI, S. et al., « Large-Scale Vulnerability Analysis », (2006) *Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense*, p. 131-138

FU, K. et J. BLUM, « Controlling for Cybersecurity Risks of Medical Device Software », (2013) 56-10 *Communications of the ACM*

GOUVERNEMENT DU QUÉBEC, « Guide pour l'élaboration d'une politique de sécurité de l'information numérique et des échanges électroniques », S*tandards du gouvernement du Québec pour les ressources informationnelles (SGQRI 34)*, Version 1.0, Juillet 2003

GUBBI, J. et al., « The Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions », (2013), 29-7 *Future Generation Computer Systems* 1645

GUTTMAN, B. et E. A. ROBACK (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY), *An Introduction to Computer Security*: *The NIST Handbook*, Gaithersburg, N.I.S.T., 1995

HALPERIN, D. et al., « Pacemakers and Implantable Cardiac Defibrillators : Software Radio Attacks and Zero-Power Defenses », (2008) *2008 IEEE Symposium on Security and Privacy*

HERZBERG, B., D. BEKERMAN et I. ZEIFMAN, « Breaking Down Mirai: An IoT DDoS Botnet Analysis », (26 octobre 2016), en ligne : <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>

HP, *Security of the IoT*, 2015, p. 1, en ligne : <http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf>

HUANG, H. et al., « Integrating neuromuscular and cyber systems for neural control of artificial legs », (2010) *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems* 129

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, « P2413 », en ligne : <https://standards.ieee.org/develop/project/2413.html>

INTERNATIONAL TELECOMMUNICATION UNION, « The Internet of Things – Executive Summary », (2005) *ITU Internet Reports*, p. 8, en ligne : <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>

JAIN, H. A., M. LUK, and A. PERRIG, « Don't sweat your privacy: Using humidity to detect human presence », (2007) *Proceedings of 5th International Workshop on Privacy in UbiComp (UbiPriv'07)*

JHA, S. K. et G. SUKTHANKAR, « Modeling and Verifying Intelligent Automotive Cyber-Physical Systems », (2011) *Proceedings of the NIST/NSF/USCAR Workshop on Developing Dependable and Secure Automotive Cyber-Physical Systems from Components*

KHAITAN, S. K. et J. D. McCALLEY, « Design Techniques and Applications of Cyberphysical Systems: A Survey », (2015) 9-2 *IEEE Systems Journal*

KIM, K.-D. et P. R. KUMAR, « Cyber-Physical Systems: A Perspective at the Centennial », (2012) 100 *Proceedings of the IEEE*

KOPETZ, H., *Real-Time Systems*, Springer, 2011

KOSCHER, K. et al., « Experimental Security Analysis of a Modern Automobile » (2010) *2010 IEEE Symposium on Security and Privacy*

KUEHN, A. et M. MUELLER, « Analysing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities », (2014) *2014 TPRC Conference Paper*, en ligne : <https://ssrn.com/abstract=2418812>

LARSON, U. E. et D. K. NILSSON, « Securing vehicules against cyber attacks », (2008) *CSIIRW'08: Proceedings of the 4th annual workshop on Cyber security and information intelligence research*

LEE, E. A., « Cyber Physical Systems: Design Challenges », (2008) *11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*

LEE, E. A., « Cyber-Physical Systems – Are Computing Foundations Adequate? », (2006) *Position Paper for NSF Workshop on Cyber-Physical Systems: Reserach Motivation, Techniques and Roadmap*, en ligne : <https://ptolemy.eecs.berkeley.edu/publications/papers/06/CPSPositionPaper/>

LEE, I. et O. SOKOLSKY, « Medical Cyber Physical Systems », (2010) *47th Design Automation Conference (DAC '10)* 743

LEE, J., B. BAGHERI et H.-A. KAO, « A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems » (2015) 3 *Manufacturing Letters* 18

LIU, C. L. et James W. LAYLAND, « Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment », (1973) 20-1 *Journal of the Association for Computing Machinery*

McFARLANE, D. et al., « Auto ID systems and intelligent manufacturing control », (2003) 16 *Engineering Applications of Artificial Intelligence*

McGREGOR, J. D., D. P. GLUCH et P. H. FEILER, « Analysis and Design of Safety-critical, Cyber-Physical Systems », (2016) 36-2 *ACM SIGAda Ada Letters*

MEIJER, H., J.-H. HOEPMAN, B. JACOBS et E. POLL, « Computer Security Through Correctness and Transparency », dans K. de LEEUW et J. BERGSTRA (dir.), *The History of Information Security: A Comprehensive Handbook*, Elsevier B.V., 2007

MILLER, C. et C. VALASEK, *Remote Exploitation of an Unaltered Passenger Vehicule*, 2015, en ligne : <http://illmatics.com/Remote%20Car%20Hacking.pdf>

MIORANDI, D. et al., « Internet of things: Vision, applications and research challenges » (2012) 10 *Ad Hoc Networks* 1497

MOHURLE, S., et M. PATIL, « A Brief Study of Wannacry Threat : Ransomware Attack 2017 », (2017) 8-5 *International Journal of Advanced Research in Computer Science*.

MOORE, G. E., « Cramming More Components onto Integrated Circuits », *Electronics*, 19 avril 1965, pp. 114-117, réimprimé dans *Proceedings of the IEEE*, Vol. 76, No. 1, janvier 1998

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Guide for Conducting Risk Assessments*, SP 800-30 Revision 1, 2012, p. B-7, en ligne : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Managing Information Security Risk*, Special Publication 800-39, 2011, en ligne : <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, 2013, en ligne : <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

NATIONAL RESEARCH COUNCIL, *Interim Report on 21st Century Cyber-Physical Systems Education*, Washington (D.C.), The National Academies Press, 2015

NATIONAL SCIENCE FOUNDATION, *Cyber-Physical Systems (CPS) Program Solicitation NSF 17-529*, en ligne : <https://www.nsf.gov/pubs/2017/nsf17529/nsf17529.pdf>

NUR, A. Y. et M. E. TOZAL, « Defending Cyber-Physical Systems Against DoS Attacks », (2016) *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*

PENDLETON, M. et al., « A Survey on Systems Security Metrics », (2017) 49-4 *ACM Computing Surveys*

PIETERS, W., « The (Social) Construction of Information Security », (2011) 27 *The Information Society* 326

PISTER, K. S. J., « Smart Dust », *BAA 97-43*

POOVENDRAN, R., « Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds », (2010) 98-9 *Proceedings of the IEEE* 1363

PSANNIS, K. E., S. XINOGALOS et A. SIFALERAS, « Convergence of Internet of things and mobile cloud computing », (2014) 2 *Systems Science & Control Engineering: An Open Access Journal*, 476

QU, F., F.-Y. WANG et L. YANG, « Intelligent Transportation Spaces : Vehicules, Traffic, Communications and Beyond », (novembre 2010) *IEEE Communications Magazine* 136

RAD, C.-R. et al., « Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture », (2015) 6 *Agriculture and Agricultural Science Procedia* 73

RAJKUMAR, R. et al., « Cyber-Physical Systems: The Next Computing Revolution », (2010) *Proceedings of the 47th Design Automation Conference*

RINGERT, J. O., B. RUMPE et A. WORTMANN, « A Requirements Modeling Language for Component Behavior of Cyber Physical Robotics Systems », dans Norbert SEYFF et Anne KOZIOLEK (dir.), *Modelling and Quality in Requirements Engineerings: Essays Dedicated to Martin Glinz on the Occasion of His 60th Birthday*, Monsenstein und Vannerdat, 2012

SARMA, S., D. L. BROCK et K. ASHTON, « The Networked Physical World », (2000) *Auto-ID Center White Paper*

SATYANARAYANAN, M., « Pervasive Computing: Vision and Challenges », (2001) 8-4 *IEEE Personal Communications* 10

SCHNEIER, B., *Secrets and Lies. Digital Security in a Networked World*, 15th Anniversary Edition, Indianapolis, John Wiley & Sons, Inc., 2015

SHI, J., J. WAN et H. YAN, « A Survey of Cyber-Physical Systems », (2011) *Proceedings of the International Conference on Wireless Communications and Signal Processing, Nanjing, China, November 9-11*

SHIRNER, G. et al., « The Future of Human-in-the-Loop Cyber-Physical Systems », (Janvier 2013) *Computer*

STOJMENOVIC, I. et F. ZHANG, « Inaugural issue of 'cyber-physical systems' », (2015) 1-1 *Cyber-Physical Systems*

SUNDT, C., « Information Security and the Law », (2006) 2 *Information Security Technical Report*

TAN, L. et N. WANG, « Future Internet: The Internet of Things », (2010) *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*

THORN, P. R. et C. A. MACCARLEY, « A spy under the hood : Controlling risks and automotive EDR », (2008) *Risk Management*

U.S. DEPARTMENT OF HOMELAND SECURITY, *The Future of Smart Cities: Cyber-Physical Infrastructure Risk*, 2015, en ligne : <https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf>

UNION INTERNATIONALE DES COMMUNICATIONS « Y2060 », en ligne : <https://www.itu.int/rec/T-REC-Y.2060-201206-I/fr>

VOAS, J., « Networks of 'Things' », *NIST Special Publication 800-183*, 2016, p. 2, en ligne : <http://dx.doi.org/10.6028/NIST.SP.800-183>

WAN, J. et al., « Context-Aware Vehicular Cyber-Physical Systems with Cloud Support : Architecture, Challenges, and Solutions », (août 2014) *IEEE Communications Magazine* 106

WANT, R., B. N. SCHILIT et S. JENSON, « Enabling the Internet of Things », (janvier 2015) *Computer* 28

WEISER, M., « The Computer for the 21st Century », (septembre 1991) *Scientific American*

WHITE, J. et al., « R&D Challenges and Solutions for Mobile Cyber-Physical Applications and Supporting Internet Services, (2010) 1-1 *Journal of Internet Services and Applications*, 45

WOLF, M., A. WEIMERSKIRCH et C. PAAR, « Security in automotive bus systems », (2004) *Proceedings of the Workshop on Embedded Security in Cars 2004*

WOLF, M., A. WEIMERSKIRCH et T. WOLLINGER, « State of the art : Embedding security in vehicules », (2007) *EURASIP Journal on Embedded Systems*

YAN, H. H., J. F. WAN et H. SUO, « Adaptive Resource Management for Cyber-Physical Systems », (2012) 157/158 *Applied Mechanics and Materials* 747

YE, X., J. ZHAO, Y. ZHANG et F. WEN, « Quantitative Vulnerability Assessment of Cyber Security for Distribution Automation Systems », (2015) 8 *Energies* 5266

YENIARAS, E. et al., « Towards A New Cyber-Physical System for MRI-Guided and Robot-Assisted Cardiac Procedures », (2010) *Proceedings of the 10th IEEE International Conference on Information Technology and Applications in Biomedicine*

ZHANG, Y. et al., « Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data », (2015) *IEEE Systems Journal*

ZHAO, Y., « Telematics: safe and fun driving », (2002) 17-1 *Intelligent Systems*

ZORZI, M. et al., « From Today's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View », (décembre 2010) *IEEE Wireless Communications* 44

RESSOURCES ÉLECTRONIQUES ET ARTICLES DE JOURNAUX

ABRAMS, R., « Target Puts Data breach Costs at $148 Million, and Forecasts Profit Drop », (5 août 2014) *The New York Times*, en ligne : <https://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html>

BERNARD, T. S. et al., « Equifax Says Cyberattack May Have Affected 143 Million in the U.S. », (7 septembre 2017) *The New York Times*, en ligne : <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>

BIT DEFENDER, « Bug bounty programs triple in 2017; $742 payout per vulnerability », 30 juin 2017, en ligne : <https://www.bitdefender.com/box/blog/iot-news/bug-bounty-programs-triple-2017-742-payout-per-vulnerability/>

BOUDETTE, N. E., « 5 Things That Give Self-Driving Cars Headaches », (4 juin 2016) *The New York Times*, en ligne : <https://www.nytimes.com/interactive/2016/06/06/automobiles/autonomous-cars-problems.html?_r=0>

CIEPLY, M., et B. BARNES, « Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm », (30 décembre 2014) *The New York Times*, en ligne : <https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html>

CIMPANU, C., « Hacking of Another Four IoT Devices Reinforces Belief that IoT is Insecure », (30 mars 2016) *Softpedia News*, en ligne : <http://news.softpedia.com/news/hacking-of-another-four-iot-devices-reinforces-belief-that-iot-is-insecure-502350.shtml>

CIMPANU, C., « Hacking of Another Four IoT Devices Reinforces Belief that IoT is Insecure », (30 mars 2016) *Softpedia News*, en ligne : <http://news.softpedia.com/news/hacking-of-another-four-iot-devices-reinforces-belief-that-iot-is-insecure-502350.shtml>

COMMON VULNTERABILITIES AND EXPOSURES, en ligne : <http://www.cve.mitre.org>

DE GRANDPRÉ, H., « Agence du revenu du Canada : 900 NAS volés », (14 avril 2014) *La Presse*, en ligne : <http://www.lapresse.ca/actualites/201404/14/01-4757316-agence-du-revenu-du-canada-900-nas-voles.php>

DEL GIUDICE, V. et W. LU, « America's Rich Get Richer and the Poor Get Replaced by Robots », (26 avril 2017) *Bloomberg*, en ligne : <https://www.bloomberg.com/news/articles/2017-12-18/finance-gurus-devise-funky-workarounds-to-loss-of-salt-deduction>

DYN, « Dyn Statement on 10/21/2016 DDoS Attack », en ligne : <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>

GHEORGE, A., « The Internet of Things: Risks in the Connected Home », *Bit Defender Research Paper*, (2016), en ligne : <http://download.bitdefender.com/resources/files/News/CaseStudies/study/87/Bitdefender-2016-IoT-A4-en-EN-web.pdf>

GOODIN, D., « Samsung Smart Home flaws let hackers make keys to front door », (2 mai 2016) *Ars Technica*, en ligne : <https://arstechnica.com/information-technology/2016/05/samsung-smart-home-flaws-lets-hackers-make-keys-to-front-door/>

GREENBERG, A., « Chrysler Launches Detroit's First 'Bug Bounty' For Hackers », (13 juillet 2016) *Wired*, en ligne : <https://www.wired.com/2016/07/chrysler-launches-detroits-first-bug-bounty-hackers/>

GREENBERG, A., « GM Asks Friendly Hackers to Report Its Cars' Security Flaws », (8 janvier 2016) *Wired*, en ligne : >https://www.wired.com/2016/01/gm-asks-friendly-hackers-to-report-its-cars-security-flaws/>

GREENBERG, A., « Hackers Remotely Kill a Jeep on the Highway – With Me In It », (21 juillet 2015) *Wired*, en ligne : <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

HACKERONE, « The Hacker-Powered Security Report 2017 », en ligne : <https://www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf>

HARROW JR., R. O., « Cyber search engine Shodan exposes industrial control systems to new risks », (3 juin 2012) *The Washington Post*, 3 juin 2012, en ligne : <https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html>

KREBS, B., « The Lingering Mess from Default Insecurity », (12 novembre 2015), en ligne : https://krebsonsecurity.com/2015/11/the-lingering-mess-from-default-insecurity/

LEVY, S., « The Brief History of the ENIAC Computer », *Smithsonian Magazine*, Novembre 2013, en ligne : <https://www.smithsonianmag.com/history/the-brief-history-of-the-eniac-computer-3889120/>

MATHEWS, L., « Infected Vending Machines and Light Bulbs DDoS A University », (13 février 2017) *Forbes*, en ligne : <https://www.forbes.com/sites/leemathews/2017/02/13/infected-vending-machines-and-light-bulbs-ddos-a-university/#4527d87b178f>

MERTL, S., « How cars have become rolling computers », (5 mars 2016) *The Globe and Mail*, en ligne : <http://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/>

MOYE, W. T., « ENIAC: The Army-Sponsored Revolution », Janvier 1996, en ligne : <http://ftp.arl.mil/~mike/comphist/96summary/index.html>

NATIONAL CONFERENCE OF STATE LEGISLATURES, *Autonomous Vehicles Legislative Database*, 2017, en ligne : <http://www.ncsl.org/research/transportation/autonomous-vehicles-legislative-database.aspx>

NATIONAL VULNERABILITY DATABASE, en ligne : <https://nvd.nist.gov/home>

NELSON, P., « Home IoT devices are wide open, security provider discovers », (7 avril 2016) *Network World*, en ligne : https://www.networkworld.com/article/3051691/internet-of-things/home-iot-is-wide-open-security-provider-discovers.html>

OPENSSL, en ligne : <https://www.openssl.org>

PERLROTH, N., « Heartbleed Highlights a Contradiction in the Web », (18 avril 2014) *The New York Times*, en ligne <https://www.nytimes.com/2014/04/19/technology/heartbleed-highlights-a-contradiction-in-the-web.html>

PORUP, J.M., « FDA presses medical device makers to OK good faith hacking », (10 février 2016) *The Christian Science Monitor*, en ligne : <https://www.csmonitor.com/World/Passcode/2016/0210/FDA-presses-medical-device-makers-to-OK-good-faith-hacking>

REIMER, J., « Total Share: 30 Years of Personal Computer Market Share Figures », (15 décembre 2005) *Ars Technica*, en ligne : <https://arstechnica.com/features/2005/12/total-share/> (consulté le 12 décembre 2017).

SÉCURITÉ PUBLIQUE CANADA, *Rapport : sondage auprès des utilisateurs d'Internet au sujet de la cybersécurité*, (2017), en ligne : <*https://www.pensezcybersecurite.gc.ca/cnt/rsrcs/rsrch-fr.aspx*>

SHODAN, en ligne : <https://www.shodan.io>

SMITH, T., « Hacker jailed for revenge sewage attacks », (31 octobre 2001) *The Register*, en ligne : <https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/>

STANISLAV, M., et T. BEARDSLEY, « Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities », (29 septembre 2015) *Rapid7 Report*, , en ligne : <https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>

SYMANTEC, « Zero Day Vulnerability », en ligne : <http://www.pctools.com/security-news/zero-day-vulnerability/>

TECHNOPEDIA, « Software Library », en ligne : <https://www.techopedia.com/definition/3828/software-library>

TIMBERG, C., « Heartbleed bug puts the chaotic nature of the Internet under the magnifying glass », (9 avril 2014) *The Washington* Post, en ligne : <https://www.washingtonpost.com/business/technology/heartbleed-bug-puts-the-chaotic-nature-of-the-internet-under-the-magnifying-glass/2014/04/09/00f7064c-c00b-11e3-bcec-b71ee10e9bc3_story.html>

U.S. FOOD AND DRUG ADMINISTRATION, *Firmware Update to Adress Cybersecurity Vulnerabilities Identified in Abbott's (formely St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication* (29 août 2017), en ligne : <www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm>

WADDEL, K., « Avenging a One-Star Review With Digital Sabotage », (5 avril 2017) *The Atlantic*, en ligne : <https://www.theatlantic.com/technology/archive/2017/04/garadget-sabotage/521937/>

WAR DEPARMENT, BUREAU OF PUBLIC RELATIONS, « Ordnance Department Develops All-Electronic Calculatic Machine », en ligne : <http://americanhistory.si.edu/comphist/pr1.pdf>

ZETTER, K., « It's Insanely Easy to Hack Hospital Equipment », (25 avril 2014) *Wired*, en ligne : <https://www.wired.com/2014/04/hospital-equipment-vulnerable/>

ZETTER, K., « Why Hospitals Are The Perfect Targets For Ransomware », (30 mars 2016) *Wired*, en ligne : <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/>