ASPECTS JURIDIQUES DE LA CYBERSÉCURITÉ

RICHARD WILLEMANT /// Avocat aux Barreaux de Paris et du Québec, Agent de marques, WILLEMANT AVOCATS

STEPHANIE FOULGOC /// Avocate aux Barreaux de Paris et du Québec

La cybersécurité peut être conçue, d'un point de vue juridique, comme la sécurité juridique dans le cyberespace. Elle désigne ainsi l'ensemble des règles qui protègent les biens et les personnes (incluant les organisations et les États) contre les atteintes qui peuvent leur être portées au moyen des technologies. La notion de cybersécurité est donc vaste et ne se limite pas aux seuls mécanismes de sécurité des systèmes d'information. Le présent article a pour objet d'aborder trois aspects juridiques essentiels de la cybersécurité des entreprises, à savoir les obligations légales en matière de cybersécurité des données, la protection du patrimoine immatériel et informationnel et les mécanismes de protection contre les cyberattaques visant les personnes.

LES OBLIGATIONS LÉGALES EN MATIÈRE DE CYBERSÉCURITÉ DES DONNÉES

La cybersécurité des systèmes d'information et des données concerne tous les acteurs de l'économie : entités publiques ou privées, PME ou grandes entreprises, et ce, que les informations concernées soient celles de l'entreprise ou de tiers.

En Europe, le nouveau règlement européen sur la protection des données personnelles du 27 avril 2016 (et dont l'application s'étend au Canada si les services fournis pour lesquels des données sont traitées visent expressément des résidents de l'Union européenne) met à la charge du responsable du traitement de données et de ses sous-traitants d'importantes obligations en matière de sécurité. Ce règlement prévoit en outre un mécanisme de notification des autorités nationales de protection des données personnelles en cas de piratage informatique. En fonction de la nature de l'attaque et des risques d'atteintes pour les personnes dont les données ont été piratées, l'entité visée par le piratage peut également être contrainte d'en informer les personnes concernées. Par ailleurs, en application du Code de la défense français, les opérateurs dits « d'importances vitales » (dans le domaine de la santé, de l'activité militaire, etc.) se voient quant à eux appliquer des obligations renforcées pour faire face à la cybermenace, comprenant notamment la mise en œuvre de systèmes qualifiés de détection d'évènements susceptibles d'affecter la sécurité de leurs systèmes d'information.

Au Canada, les enjeux sont les mêmes. En application de la Loi fédérale sur la protection des renseignements personnels et des documents électroniques, les opérateurs économiques qui exploitent des renseignements personnels doivent prendre des mesures de sécurité adaptées au degré de sensibilité des données. Ces mesures doivent être à la fois matérielles (sécurisation des locaux), administratives (procédures de restriction des accès aux informations) et techniques (utilisation de mots de passe et de chiffrement). Une procédure de notification des atteintes a également été adaptée, mais elle n'est pas encore en vigueur, dans l'attente de règlements d'application. Par ailleurs, dans le cadre d'une Stratégie de cybersécurité du Canada mise en place de 2010 à 2015, d'importantes réflexions ont été menées sur les obligations en matière de sécurité des systèmes du gouvernement, mais également s'agissant des « cybersystèmes essentiels » des secteur publics et privés. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) coordonne les actions et obligations de chacun en matière de Cybersécurité.

LA PROTECTION DU PATRIMOINE IMMATÉRIEL

Les faits de vol de données qui constituent le patrimoine ou l'outil de travail d'une entreprise sont de plus en plus fréquents et ont émaillé l'actualité ces derniers années. Ces agissements causent un préjudice économique considérable et nuisent à l'image des sociétés victimes. Au-delà des mesures techniques de prévention, le premier mécanisme de protection juridique du patrimoine informationnel ou immatériel de toute organisation est de nature pénal, au travers des infractions informatiques.

Au Canada, le Code criminel punit l'infraction de méfait à l'égard des données informatiques. Sont ainsi incriminés les actes de destruction

ou de modification de données, ainsi que tous les actes de nature à entraver ou empêcher l'accès ou le fonctionnement normal d'un système d'information en empêchant un emploi légitime des données.

En France, le code pénal réprime les atteintes aux systèmes de traitement de données, en punissant l'accès ou le maintien frauduleux dans un système d'information, l'entrave ou le faussement d'un tel système, mais également le fait d'y introduire frauduleusement des données. Le législateur français a ajouté les faits d'extraction, de détention, de reproduction et de transmission frauduleuses de données parmi ces infractions informatiques.

Dans ce contexte, les Tribunaux français ont récemment reconnu l'infraction de vol de données, quand bien même elles n'auraient pas été copiées sur un support électronique qui aurait lui-même fait l'objet d'une soustraction comme l'exigeaient antérieurement les juges en considérant que le vol n'était applicable qu'aux choses corporelles.

La protection juridique du patrimoine immatériel des entreprises passe également par les mécanismes de lutte contre la contrefaçon, c'est-à-dire contre toutes les atteintes aux droits de propriété intellectuelle afférents au patrimoine des entreprises (droits d'auteur, marques, dessins et modèles, brevets). Les technologies de l'information facilitent grandement ce type de délit, par la reproduction des œuvres protégées, l'utilisation sans autorisation de marques enregistrées ou encore la reproduction de modèles protégés. Les innovations matérielles prennent aujourd'hui le relais, notamment les imprimantes 3D qui rendent encore plus aisées les reproductions illicites et constituent un nouveau défi pour les titulaires de droits. Les systèmes juridiques français et canadien incluent tout un ensemble de mesures juridiques de poursuite des atteintes contrefaisantes, que ce soit sur le terrain civil ou le terrain pénal, notamment en France par le biais des saisies-contrefaçon, dont les ordonnances Anton Piller sont l'équivalent canadien.

LES MÉCANISMES DE PROTECTION CONTRE LES CYBERATTAQUES VISANT LES PERSONNES

Le droit français et le droit canadien comprennent des mécanismes de protection des individus contre les atteintes personnelles causées aux moyens des technologies de l'information. Il existe ainsi toute une série d'infractions pénales et de procédures permettant d'obtenir le retrait de contenus illicites publiés sur internet, qu'il s'agisse de contenus à caractère pédopornographique, d'incitation à la haine raciale, d'apologie de crime contre l'humanité, de terrorisme, d'atteinte à la vie privée ou encore d'usurpation d'identité.

Dans le monde des affaires, l'une des cyberattaques les plus redoutables est celle qui porte atteinte à la réputation d'une entreprise ou d'un individu, en raison de la rapidité de diffusion des informations et des difficultés à en obtenir la suppression.

Il existe heureusement des systèmes juridiques de défense de l'e-réputation (diffamation, d'injure ou de dénigrement des produits ou services). Ils supposent néanmoins la mise en place d'une veille efficace et de réagir rapidement dès la survenance des faits, afin de contenir autant que possible la diffusion des propos litigieux et d'en obtenir le retrait effectif.

Photo : Krimar, shutterstock.com

Dans ce contexte, la Cour de Justice de l'Union européenne a reconnu en 2014 un véritable « droit à l'oubli » permettant à toute personne de s'opposer au traitement de ses données sur internet lorsque celles-ci sont non pertinentes, obsolètes ou inappropriées, en sollicitant le déréférencement sur les moteurs de recherche des résultats associés à ces données.

Au Canada, la constitutionnalité d'un tel mécanisme est discutée, dans la mesure où il revient à un acteur privé (moteur de recherche) de se faire juge de la balance des intérêts en présence (protection des renseignements personnels contre droit à l'information et liberté d'expression). Néanmoins, une réflexion sur les nouveaux défis que pose cette disponibilité numérique de données est menée actuellement par le Commissariat à la protection de la vie privée du Canada.