Commerce électronique : certaines lois et règles que vous devez connaître

7 mai 2020

Auteur

André Vautour

Associé, Avocat

Diverses manières de faire du commerce électronique

Le commerce électronique prend plusieurs formes : il est dit « direct », lorsque le contrat de vente ou de service est conclu électroniquement et que le produit ou le service est également livré électroniquement (par exemple, la conclusion en ligne d'un contrat d'abonnement à une publication uniquement disponible en ligne), et « indirect » lorsque le contrat de vente ou de service est conclu électroniquement et que le bien est un bien matériel ou que le service est rendu autrement qu'en ligne. Le commerce électronique peut se faire entièrement en ligne ou de manière hybride lorsque le vendeur exerce ses activités à la fois en ligne et au moyen de magasins traditionnels.

Il est « fermé », lorsqu'il intervient entre un nombre de participants relativement peu élevé qui ont déjà des liens contractuels ou professionnels entre eux. Il peut intervenir entre une entreprise et un consommateur, on l'appelle alors B2C, ou entre une entreprise et une autre entreprise, on dit alors qu'il est B2B.

Le commerce électronique pose des défis particuliers pour les entreprises et si ces défis ne sont pas adéquatement relevés, ils sont susceptibles d'exposer l'entreprise à des responsabilités additionnelles nouvelles. Ces défis font en sorte que le commerce électronique peut être particulièrement risqué pour les entreprises néophytes qui s'y lancent sans être adéquatement préparées.

Par exemple, certaines données personnelles des clients, telles que leur nom et leur adresse et leur numéro de carte de crédit, devront nécessairement être mises en la possession directe du commerçant ou encore en sa possession indirecte par le biais d'un fournisseur de plateforme de

commerce électronique. L'utilisation de ces données personnelles est soumise aux dispositions des lois sur la protection des renseignements personnels et, de plus, comme elles ont une grande valeur pour des voleurs ou des fraudeurs potentiels, elles devront être protégées. Le commerçant pourrait aussi être victime de commandes frauduleuses ou encore de paiements effectués au moyen de cartes de crédit dont les numéros ont eux-mêmes été volés.

Pour mieux contrôler ses risques, l'entreprise néophyte peut donc avoir intérêt à faire affaire avec des fournisseurs de plateformes de commerce électronique déjà établies, telles Shopify, BigCommerce, Squarespace ou encore GoDaddy, lesquelles ont mis en place des infrastructures robustes à l'intention de leurs clients. Malgré tout, l'entreprise devrait tout de même « faire ses devoirs » avant de choisir l'une ou l'autre des plateformes de commerce électronique établies. Ainsi, l'entreprise devrait se renseigner quant aux modalités de la convention de services qu'elle conclura avec le fournisseur choisi et, en particulier, quant aux services offerts (ce qui comprend aussi la manière dont la plateforme traite les retours et la rétrofacturation), quant à la façon dont la plateforme protège ses clients en cas de vol de données ou de fraude, quant aux frais facturés, etc.

De plus, dans tous les cas, que l'entreprise fasse ou non affaire avec un fournisseur de plateforme de commerce électronique, elle devrait s'assurer de ne conserver sur ses propres serveurs et ordinateurs que l'information absolument nécessaire et éviter, autant que possible, de conserver une fois la transaction complétée des données personnelles appartenant à un client, comme son nom, son adresse et son numéro de carte de crédit.

L'entreprise qui décide de se lancer dans le commerce électronique doit aussi être consciente de certains aspects juridiques particuliers liés, d'une part, aux particularités du commerce électronique lui-même et, d'autre part, au fait que sa clientèle peut se trouver n'importe où dans le monde. Pour les fins de cet article, nous allons nous attarder sur les règles applicables à tous les types de commerces électroniques; un futur article traitera des règles particulières prévues à la *Loi sur la protection du consommateur*.

Taxe à la consommation

La majorité des États et provinces imposent une taxe à la consommation sur les biens et, parfois, sur les services vendus sur leur territoire. Les lois applicables en matière de taxes à la consommation prévoient généralement que les entreprises qui ont une présence dans le territoire doivent percevoir la taxe applicable et la remettre aux autorités compétentes. Pour une entreprise qui n'a par ailleurs aucune présence dans un territoire, le simple fait d'y vendre un bien n'est en général pas suffisant pour qu'elle doive s'enregistrer auprès des autorités fiscales de ce territoire, percevoir la taxe applicable et la remettre à ces autorités. Il faut toutefois être conscient que la définition de ce qui constitue une présence suffisante pour exiger l'enregistrement de l'entreprise et la perception et la remise de la taxe à la consommation varie d'un territoire à l'autre. L'entreprise qui veut vendre ses biens et services électroniquement doit donc s'assurer d'être au fait des règles applicables en matière de taxes à la consommation dans les principaux territoires où elle vend ses biens ou fournit ses services.

Licences et permis

Bien que pour la grande majorité des biens typiquement vendus en ligne, il n'est pas nécessaire que le fabricant ou le vendeur se procure une licence, un permis ou une autre autorisation gouvernementale, des licences, des permis ou d'autres autorisations peuvent être obligatoire avant de pouvoir vendre en ligne ou autrement, au pays ou à l'étranger, certains produits, particulièrement dans le domaine médical ou pharmaceutique.

Notons qu'une entreprise pourrait avoir le droit de vendre un bien sans licence, permis ou autre autorisation dans un territoire, mais n'aurait pas le droit de le faire dans un autre. Ainsi, si un commerçant veut vendre son produit dans un territoire où un permis, une licence ou une autre

autorisation est nécessaire, il devra s'assurer d'obtenir ce permis ou cette licence avant de procéder à ses ventes.

De plus, dans certains territoires la vente au détail de certains biens doit nécessairement se faire par le biais d'entreprises qui détiennent un monopole d'État. De telles restrictions sont encore la norme au Canada en ce qui concerne les boissons alcoolisées. Ainsi, un résident de l'Ontario ne peut commander directement sur Internet des produits alcooliques auprès d'un producteur de boissons alcooliques d'une autre province et se les faire livrer en Ontario, ce qui empêche un producteur artisanal de boissons alcoolisées québécois de vendre ses produits en ligne à des clients ontariens pour livraison en Ontario.

Expédition

Tous les biens ne peuvent pas être expédiés de la même manière, certains doivent être conditionnés de manière particulière et il est même interdit d'expédier certains autres biens par les moyens ordinaires que sont Postes Canada et les principales sociétés de messagerie.

Par exemple, Postes Canada exige que le poisson, le gibier, la viande, les fruits, les légumes ou autres produits périssables soient conditionnés de façon appropriée et satisfassent à certaines autres exigences.

D'autres produits ne peuvent tout simplement pas être expédiés par la poste. Il en va ainsi des objets classifiés comme matière dangereuse. Dans un tel cas, il faudra faire affaire avec un service de messagerie qui expédie de telles matières.

Enfin, les lois canadiennes interdisent l'exportation de certains biens ou soumettent leur exportateur à l'obtention de permis spéciaux. De la même façon, le commerçant devra s'assurer que les lois du territoire de destination permettent l'importation sur son territoire des biens expédiés. Tous les pays interdisent l'importation de certains biens sur leur territoire ou soumettent leur importateur à l'obtention d'un permis ou d'une licence émis par leur gouvernement.

Restrictions quant à l'âge

En vertu des lois et règlements applicables, certains biens ne peuvent être vendus qu'à des personnes ayant atteint un certain âge ou ne peuvent être vendus à des enfants. Ces restrictions peuvent varier d'un territoire à l'autre. Par exemple, alors que l'âge pour acheter de l'alcool est de 18 ans au Québec, il est de 19 ans ailleurs au Canada et de 21 ans aux États-Unis. Les commerçants qui veulent vendre des boissons alcoolisées en ligne doivent donc tenir compte de ces restrictions. Il en va de même de la vente de tout autre bien assujetti à des restrictions quant à l'âge.

Conformité aux normes PCI-DSS

Les entreprises émettrices de cartes de crédit que sont American Express, Discover Financial Services, JCB International, MasterCard et Visa ont constitué en 2006 le Conseil des normes de sécurité PCI pour uniformiser les règles et les normes applicables aux paiements effectués au moyen de leurs cartes de crédit.

Pour atteindre cet objectif, le conseil a adopté une série de règles, mieux connues sous leur acronyme anglais PCI-DSS (Payment Card Industry Data Security Standard), auxquelles doivent adhérer tous les marchands qui souhaitent recevoir des paiements par carte de crédit, y compris les paiements directs en ligne. Ainsi, tout marchand qui souhaite traiter des paiements par carte de crédit sur son site Internet doit, à moins de faire affaire avec une plateforme de paiement elle-même conforme, se conformer aux normes PCI-DSS, et ce, peu importe la taille de son entreprise.

Les normes PCI DSS spécifient les 12 conditions de conformité suivantes, regroupées dans six groupes appelés « objectifs de contrôle ». Le tableau qui suit, tiré du document intitulé « Industrie

des cartes de paiement (PCI) — Norme de sécurité des données — Conditions et procédures d'évaluation de sécurité[1], résume la teneur de ces normes.

Objectif de contrôle	Conditions du PCI DSS
Création et gestion d'un réseau et d'un système sécurisé	1. Installer et gérer une configuration de pare-feu pour protéger les données du titulaire de carte 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
Protection des données de titulaire de carte	3. Protéger les données de titulaires de carte stockées 4. Crypter la transmission des données du titulaire sur les réseaux publics ouverts
Gestion d'un programme de gestion des vulnérabilités	5. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus 6. Développer et maintenir des systèmes et des applications sécurisés
Mise en œuvre de mesures de contrôle d'accès strictes	7. Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître 8. Identifier et authentifier l'accès à tous les composants du système 9. Restreindre l'accès physique aux données du titulaire de carte
Surveillance et test réguliers des réseaux	10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données du titulaire de carte 11. Tester régulièrement les processus et les systèmes de sécurité
Gestion d'une politique de sécurité des informations	12. Gérer une politique qui adresse des informations de sécurité pour l'ensemble du personnel

Bien que les normes PCI-DSS soient obligatoires, seules Visa et MasterCard exigent que les commerçants et fournisseurs de services qui acceptent les cartes Visa et MasterCard soient en

conformité avec ces normes. L'entreprise qui ne serait pas conforme à ces normes engage sa pleine responsabilité si une fraude, associée à un vol des données du titulaire de la carte, a lieu. De plus, dans le cas d'une faille de sécurité, toutes les entreprises exposées qui ne sont pas conformes aux normes PCI-DSS devront payer une amende. Il incombe aux commerçants et aux fournisseurs de services de réaliser, de démontrer et de maintenir leur conformité par le biais d'une validation annuelle.

Des fournisseurs offrent leurs services aux entreprises pour leur permettre de se conformer aux normes PCI-DSS et il existe aussi des outils utiles sur Internet pour leur permettre de s'assurer qu'elles sont conformes à ces normes[2].

Par ailleurs, une entreprise qui ne désire pas passer à travers le processus de conformité aux normes PCI peut toujours décider de faire affaire avec une passerelle de paiement qui elle, sera conforme à ces normes[3].

---

1. PCI Security Standards Council, « Industrie des cartes de paiement (PCI) — Norme de sécurité des données — Conditions et procédures d'évaluation de sécurité » (Version 3.2.1, mai 2018), en ligne (pdf) : *Site officiel du conseil de normes de sécurité PCI*
2. Une recherche au moyen des mots clés « PCI DSS conformité » ou « PCI DSS conformity » renvoie à une grande partie de ces outils.
3. Une recherche au moyen des mots clés « PCI DSS passerelle de paiement » renvoie également à plusieurs fournisseurs de telles passerelles.