Divisão da Sociedade da Informação

Anexo à resposta ao Ofício nº 259/2015/GAB-SAL-MJ (Processo nº 08027.000032/2015-11)

Informações recebidas de Embaixadas do Brasil no exterior

CANADÁ

"Encaminha a seguir panorama da regulamentação jurídica do uso da Internet e da proteção de dados pessoais no Canadá, com base em pesquisa legislativa e contatos junto ao Ministério dos Negócios Estrangeiros, Comércio e Desenvolvimento.

I. Há regulamentação acerca do uso da Internet?

Por decisão política deliberada, o uso da Internet não é objeto, no Canadá, de regulamentação exaustiva, seja por lei, seja por normas administrativas. Com efeito, o único diploma legal vigente a respeito da matéria é a Lei C-28, de 2010, popularmente conhecida como Lei Canadense Anti-Spam ("Canadian Anti-Spam Law").

Aplicam-se, no entanto, à Internet, dispositivos da Lei de Telecomunicações ("Telecommunications Act"), promulgada em 1993. A seção 2 do diploma confere à Comissão Canadense de Telecomunicações, Rádio e Televisão (Canadian Radio-television and Telecommunications Commission – CRTC) competência para regulamentar tecnologias de comunicação supervenientes à promulgação da lei - entre as quais se inclui, em sua dimensão comercial, a Internet.

As atividades normativas da CRTC são, contudo, restringidas por aquela mesma lei federal, que, em sua seção 7, alínea "f", consagra o princípio do minimalismo regulatório: "[a política canadense de telecomunicações tem como objetivo] (f) estimular o crescente recurso às forças de mercado para a oferta de serviços de telecomunicações e garantir que a regulamentação, quando necessária, seja eficiente e efetiva."

Fundamentando-se nesse princípio, a CRTC, em 1999, por meio do documento intitulado "Novos meios de comunicação" ("New media"), firmou posição de abster-se de regulamentar o uso da Internet no país. De acordo com o órgão, os objetivos expressos na Lei de Telecomunicações e na Lei de Radiodifusão ("Broadcasting Act"), de 1991, estavam sendo atendidos pelos serviços de Internet, tal como oferecidos em condições de livre mercado. A política de supervisão não legiferante estabelecida há dezesseis anos permanece em vigor.

I.a. Há previsão de garantia da neutralidade da rede?

Não. Como afirmado no item acima, conserva-se deliberadamente quadro de desregulamentação do setor de prestação de serviços de Internet no país.

Cabe registrar, de qualquer modo, que a CRTC promoveu debates públicos sobre o

tema entre novembro de 2008 e fevereiro de 2009. Não houve publicação subsequente de relatório ou de normativa.

Em 2008, dois projetos de lei que acolhiam a garantia de neutralidade da rede foram apresentados por parlamentares de oposição na Câmara dos Comuns, mas não foram levados adiante após a dissolução da 39ª sessão do parlamento.

I.b. São previstas exceções ao princípio da neutralidade?

Não aplicável.

I.c. O provimento de acesso gratuito a determinadas aplicações é visto como violação da neutralidade?

Não aplicável.

II. Há legislação disciplinando a coleta, a guarda, o armazenamento e o tratamento de dados pessoais?

Sim. O Canadá possui duas leis federais a regulamentar a coleta, a guarda, o armazenamento e o tratamento de dados pessoais: (i) a "Lei de Privacidade" ("Privacy Act"), em vigor desde 1985, que se aplica a ministérios e órgãos do governo federal expressamente relacionados em seu Anexo de Instituições ("Schedule of Institutions"), e (ii) a "Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos" ("Personal Information Protection and Electronic Documents Act" - PIPEDA), sancionada em 2000, que se aplica a organizações do setor privado.

1) Lei de Privacidade

A Lei de Privacidade, norma federal de direito público, possui três disposições fundamentais: (i) assegura ao cidadão o direito de ter acesso a dados pessoais a seu respeito em poder do governo federal; (ii) impõe ao governo federal a obrigação de implementar políticas e práticas probas de coleta, guarda, utilização e divulgação de informações pessoais sob seu controle; e (iii) cria o Escritório do Comissário para a Proteção da Vida Privada ("Office of the Privacy Commissioner"), subordinado diretamente ao parlamento, para garantir o cumprimento da norma e dirimir conflitos.

A lei define "informação pessoal" como qualquer dado a respeito de um indivíduo identificável, armazenado sob qualquer forma, incluindo informações sobre idade, escolaridade e histórico médico e criminal. Estipula-se que informações pessoais devem ser coletadas e empregadas por órgãos do governo federal apenas na medida em que guardem relação direta com política ou atividade da instituição. Sempre que possível, a fonte da informação deve ser o próprio indivíduo interessado, a quem deve ser comunicado o propósito ao qual se destina o dado colhido. Para fins de transparência e de publicidade, as instituições do governo têm o dever de divulgar índices que relacionem os bancos de dados pessoais arquivados.

O princípio que estrutura a Lei da Privacidade pode ser assim enunciado: informações pessoais sob controle do governo federal não devem ser utilizadas, sem o devido consentimento do indivíduo ao qual dizem respeito, para fins outros que não aqueles para os quais foram coletadas. Deve-se garantir, ademais, que aqueles fins sejam compatíveis com políticas e atividades inerentes à instituição federal.

Todo indivíduo tem o direito de demandar acesso a informações pessoais a seu respeito que estejam sob poder de órgãos federais. Caso se verifiquem inexatidões nos dados registrados pela instituição, pode-se exigir a correção das falhas. Na hipótese de o cidadão não se conformar com a resposta fornecida pela instituição, pode-se apresentar reclamação perante o Escritório do Comissário para a Proteção da Vida Privada. Adicionalmente, pode-se ajuizar ação perante a justiça federal.

Registre-se, finalmente, que o Escritório do Comissário pode submeter órgãos federais a exame de auditoria abrangente de suas práticas de gestão de dados pessoais.

2) Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos (PIPEDA)

A "Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos" ("Personal Information Protection and Electronic Documents Act" - PIPEDA), norma federal de direito privado, vigora em todas as províncias que não tenham leis próprias a regulamentar a matéria de modo "substancialmente semelhante" ao daquela norma federal. No momento, as províncias de Alberta, da Colúmbia Britânica e do Québec possuem leis a respeito do tema. Nessas unidades da federação, a vigência da PIPEDA restringe-se a setores sujeitos a regulação federal exclusiva (como o bancário, o de transportes e o de telecomunicações), bem como a pessoas físicas e jurídicas que, no curso de atividades comerciais, transmitem informações pessoais para outras províncias ou para o exterior.

A PIPEDA, sancionada em 2000 e emendada pela última vez em julho de 2014, determina que a coleta, o uso e a divulgação ("disclosure") de dados pessoais, para fins comerciais, devem estar amparadas no consentimento do indivíduo. Consagra-se o direito de a pessoa ter acesso a dados pessoais guardados por uma organização e contestar sua exatidão, se necessário. Informações pessoais podem ser utilizadas apenas para os fins para os quais foram coletadas. Se uma organização deseja empregar os dados com objetivo diverso, deve obter consentimento expresso do indivíduo. As organizações devem estar aptas a demonstrar aos interessados que protegem dados pessoais com salvaguardas apropriadas.

Cabe esclarecer que o conceito de "organização" adotado pela PIPEDA inclui associações, cooperativas, pessoas físicas e sindicatos, na medida em que desempenhem atividades de natureza comercial. Tais atividades são definidas como "atividades regulares ou atos isolados que se revestem de caráter comercial por sua própria natureza, incluindo a venda, a permuta e o arrendamento de listas de doadores, de membros e de arrecadadores de fundos" (parte 1, seção 2, inciso 1).

A lei federal citada estatui que "dado pessoal" deve ser entendido como qualquer

informação factual ou subjetiva, gravada ou não, que diga respeito a um indivíduo identificável. Estão excluídos do alcance normativo dessa definição os seguintes dados: (i) nome, cargo, endereço e telefone de trabalho de empregados da organização; (ii) informações coletadas, guardadas ou divulgadas por uma pessoa para fins estritamente particulares; (iii) informações em poder de uma organização para propósitos jornalísticos, artísticos ou literários.

O anexo 1 da PIPEDA institui princípios para proteção de informações pessoais, a ser observado por todas as organizações submetidas àquela norma. Os dez princípios que o compõem são sintetizados a seguir:

a) Responsabilidade - as organizações são responsáveis pelos dados pessoais sob seu controle e devem designar um ou mais funcionários para garantir o cumprimento dos princípios insculpidos na PIPEDA. Devem, ademais, elaborar e aplicar políticas e práticas de proteção dos dados.

b) Identificação dos fins para a coleta de dados - os fins a que se destina a coleta de dados devem ser identificados e documentados antes de as ações serem realizadas.

c) Consentimento - toda pessoa deve ser informada da coleta, da utilização e da comunicação de dados pessoais. Seu consentimento deve ser obtido, exceto quando impróprio.

d) Limitação da coleta - a organização deve coletar apenas os dados estritamente necessários para seus propósitos, agindo de maneira honesta e lícita.

e) Limitação da utilização, da comunicação e da guarda - dados pessoais devem ser utilizados apenas para os fins para os quais foram coletados e devem permanecer em poder da organização apenas pelo tempo necessário para a consecução daqueles fins.

f) Exatidão - os dados pessoais devem ser tão exatos, completos e atualizados quanto necessário para os propósitos aos quais se destinam.

g) Medidas de segurança - dados pessoais devem ser protegidos por medidas de segurança compatíveis com seu grau de sensibilidade.

h) Transparência - a organização deve estar apta a prestar informações específicas sobre suas políticas e práticas relativas à gestão de dados pessoais.

i) Acesso a informações pessoais - mediante pedido do interessado, a organização tem o dever de prestar informações sobre a existência, a utilização e a divulgação de dados pessoais em seu poder. Deve-se franquear ao solicitante pleno acesso a tais dados.

j) Contestação do cumprimento da norma - todo indivíduo deve poder submeter uma reclamação contra o descumprimento dos princípios enunciados ao funcionário encarregado, na organização, de garantir sua observância. Deve-se investigar os fatos indicados na reclamação e tomar medidas para sanar possíveis falhas. Deve-se, ademais,

informar o interessado da existência de outros canais para interposição de reclamações.

II.a. De que maneira os provedores de conexão e de aplicações de Internet comprovam o cumprimento dessa legislação?

Os provedores não têm o dever de comprovar, "a priori" ou regularmente, o cumprimento da legislação federal. A demonstração de observância da PIPEDA dá-se, sempre, de maneira motivada, seja pela apresentação de reclamação concreta por um indivíduo, seja pela instauração de processo de auditoria pelo órgão de fiscalização, o Escritório do Comissário de Privacidade do Canadá ("Office of the Privacy Commissioner of Canada" - OPC). Assim sendo, a comprovação de cumprimento da lei guarda estreita relação com a apuração de violações - tema abordado no item abaixo.

II.b. De que maneira são apuradas as violações a essas regras?

Todo indivíduo tem legitimidade para apresentar reclamação contra a violação das regras da PIPEDA perante o Escritório do Comissário de Privacidade do Canadá. Cabe ressaltar que o órgão de controle emprega, preferencialmente, abordagem cooperativa para resolução dos conflitos. A utilização de recursos como a mediação e a conciliação é estimulada em todas as fases da investigação.

A reclamação é encaminhada a um Agente de Resolução Rápida ("Early Resolution Officer") nas hipóteses de (i) referir-se a questão objeto de investigações pretéritas do OPC; (ii) aludir a tema de que a organização já tenha prestado contas, de maneira satisfatória, no passado; ou (iii) exibir baixo grau de complexidade.

Nos demais casos, o OPC, estando convencido da existência de indícios substantivos de infração, abre processo de investigação.

O Comissário, por meio de um investigador devidamente designado, notifica a organização da abertura do processo e do teor da reclamação e abre uma primeira possibilidade de apresentação de defesa. O funcionário da organização encarregado de assegurar o cumprimento da PIPEDA é informado dos procedimentos seguintes da investigação, incluindo a intenção do órgão de visitar a organização. São realizadas reuniões entre o Escritório do Comissário e representantes da organização, e são compulsados documentos originais pertinentes. Dá-se, em todo o processo, oportunidade para a organização sanar a falha apontada pela reclamação.

Os resultados da investigação são submetidos ao gabinete do Comissário de Privacidade, que analisa os autos e publica um relatório final. Na hipótese de as partes não terem resolvido voluntariamente o conflito, o Comissário poderá decidir (i) fixar prazo para que a organização adote medidas aptas a sanar a violação apontada pela reclamação; (ii) cobrar explicações adicionais sobre eventual inação da organização; ou (iii) encaminhar o caso para a Justiça Federal.

Tribunais federais são a instância competente para sentenciar a organização a emendar práticas que infringem a PIPEDA e para aplicar penas de indenização em

benefício do indivíduo prejudicado.

Além da apuração pontual de violações da norma federal de proteção de dados pessoais, descrita acima, há previsão legal para exame abrangente das políticas e das práticas de gestão mantidas pelas organizações. Com efeito, a PIPEDA atribui, ao OPC, competência para conduzir auditoria ampla nos casos (i) de apresentação reiterada de reclamações contra práticas da organização; (ii) de recebimento de informações sensíveis de denunciante anônimo, nos termos da seção 27 da parte 1 da PIPEDA; e (iii) de uma questão repercutir nos meios de comunicação.

Por meio de carta, o Comissário notifica a organização da abertura do procedimento de auditoria, que, em linha com a abordagem preferencial do Escritório, se caracteriza pela busca de soluções negociadas. A oitiva coercitiva de testemunhas e a emissão de ordens de produção de provas são utilizadas apenas na hipótese de a organização não se dispor a colaborar.

Ao investigador, é facultado visitar a organização, reunir-se com funcionários e consultar arquivos. O relatório produzido é discutido pessoalmente com o representante da organização, antes de ser encaminhado ao Gabinete do Comissário de Privacidade, que apresenta recomendações finais. De acordo com o interesse da sociedade, os resultados da auditoria podem ser divulgados publicamente.

III. Há previsão de dever de guarda de registros de acesso a aplicações de Internet e de registros de conexão?

Não (vide item I, supra).

III.a. Quem tem o dever de guardar cada um desses registros?

Não aplicável.

III.b. De que maneira é disciplinado o dever de guarda de registros de aplicação e de registros de conexão?

Não aplicável.

IV. Qual é a relação entre a proteção do consumidor e a proteção de dados pessoais? A proteção dos dados e da privacidade do consumidor é realizada por meio de leis e instituições de proteção ao consumidor ou exclusivamente pela legislação referente à proteção de dados?

Não existe, no ordenamento jurídico federal, vinculação específica e objetiva entre proteção do consumidor e proteção de dados pessoais, tendo em vista que (i) a Constituição do Canadá outorga a competência para legislar sobre "direitos civis e de propriedade" às províncias (correspondentes aos Estados, no Brasil); e que (ii) a doutrina e a jurisprudência perfilam entendimento de que aqueles direitos compreendem a proteção do consumidor.

V. O país possui órgão administrativo cuja competência abrange diretamente a aplicação de normas de proteção de dados pessoais?

Sim. O Escritório do Comissário de Privacidade do Canadá ("Office of the Privacy Commissioner of Canada" - OPC) é o órgão responsável pela aplicação das normas de proteção de dados pessoais no país.

Trata-se de órgão independente, que presta contas diretamente à Câmara dos Comuns e ao Senado. A escolha do seu chefe é aprovada pelo Parlamento, com base em indicação feita pelo Gabinete do Primeiro-Ministro.

Seis departamentos subordinam-se ao Gabinete do Comissário de Privacidade, quais sejam:

a) Direção de Investigações ("Investigations Branch"), composto de duas unidades administrativas:

a.1) Direção de Investigações da Lei de Privacidade ("The Privacy Act Investigations Branch"), que recebe e investiga reclamações, no âmbito da Lei de Privacidade, de indivíduos que aleguem não ter acesso a dados pessoais em poder de órgãos de governo, ou que acreditam que seus dados foram coletados, utilizados, divulgados ou manipulados de maneira inapropriada por aqueles órgãos. Esse departamento, ademais, conduz investigações solicitadas diretamente pelo Comissário de Privacidade e recebe notificações de violações de órgãos do governo federal.

a.2) Direção de Investigações da PIPEDA ("The PIPEDA Investigations Branch"), que investiga reclamações no âmbito da Lei de Proteção de Informações Pessoais e de Documentos Eletrônicos. Possui dois escritórios na província de Ontário, nas cidades de Gatineau (na região da capital nacional) e de Toronto. Em Gatineau, o departamento recebe e investiga todas as reclamações de escopo nacional apresentadas por indivíduos ou submetidas pelo Comissário de Privacidade, exceto aquelas oriundas da região metropolitana de Toronto ("Greater Toronto Area" - GTA). O escritório de Toronto, além de investigar reclamações oriundas dessa área metropolitana, organiza atividades de educação pública e promove coordenação com partes interessadas ("stakeholders") nos trabalhos do OPC.

b) Direção de Auditoria e Inspeção ("Audit and Review Branch"), que realiza auditorias em organizações para avaliar o cumprimento das duas leis de proteção de informações pessoais (recorde-se: Lei de Privacidade: setor público federal; PIPEDA: setor privado). Adicionalmente, o departamento analisa e faz recomendações acerca de relatórios de Avaliação de Impacto sobre a Privacidade ("Privacy Impact Assessment" - PIA, que são preparados por órgãos do governo para identificar possíveis riscos à privacidade originados de propostas de políticas e de leis). Finalmente, o Departamento de Auditoria e Inspeção recebe e avalia revelações ("disclosures") de interesse público de autoria de órgãos do governo.

c) Direção de Comunicações ("Communications Branch"), que se dedica a fornecer

orientações estratégicas para atividades de comunicação e de educação pública executadas pelo OPC. O departamento, ademais, planeja e implementa atividades de comunicação sob as formas de acompanhamento e análise dos meios de comunicação, realização de pesquisas de opinião pública, relações públicas, organização de seminários e manutenção da página do órgão na Internet.

d) Direção de Consultoria Jurídica, Elaboração de Políticas, Pesquisa e Análise de Tecnologias ("Legal Services, Policy, Research and Technology Analysis Branch"), que provê aconselhamento jurídico, elabora políticas e conduz pesquisas em novos temas relativos à privacidade. Compõe-se de três divisões:

d.1) Divisão de Consultoria Jurídica ("Legal Services Division"), que fornece consultoria jurídica em investigações no âmbito da PIPEDA e da Lei de Privacidade, em processos de auditoria e em amparo a outros departamentos do OPC.

d.2) Divisão de Política e Pesquisa ("Policy and Research Division"), que estabelece posições estratégicas acerca de projetos de lei e de programas e iniciativas de governo; apoia os pronunciamentos do Comissário perante o parlamento; provê orientação a iniciativas dos setores público e privado; e conduz pesquisa aplicada em novos temas relativos à privacidade.

d.3) Divisão de Análise de Tecnologia ("Technology Analysis Division"), que identifica e analisa tendências e desenvolvimentos de plataformas eletrônicas; conduz pesquisas para avaliar o impacto da tecnologia sobre a proteção das informações pessoas no mundo digital; e analisa estrategicamente temas afetos a violações de segurança de sistemas do governo e comerciais que armazenem dados pessoais.

e) Direção de Gerência de Recursos Humanos ("Human Resources Management Branch"), que é responsável pela gestão de temas como contratação de pessoal, treinamento, equidade laboral e planejamento de recursos humanos.

f) Direção de Serviços Corporativos ("Corporate Services Branch"), em cujas atribuições incluem-se o planejamento corporativo, a gestão de recursos, a gestão financeira, a gestão de tecnologia da informação e serviços gerais de administração do OPC.

O orçamento do Escritório do Comissário de Privacidade do Canadá, no exercício 2014-15, montou a CAN$ 24.3 milhões (equivalentes a US$ 19.4 milhões). Não está previsto qualquer reajuste para os próximos dois exercícios. Daquele total, CAN$ 12.6 milhões (52%) foram empregados em atividades de fiscalização do cumprimento das normas de proteção de dados pessoais, ou seja, em realização de investigações e de auditorias. CAN$ 4.1 (correspondentes a 17% do total) foram investidos em pesquisa e em desenvolvimento de políticas. CAN$ 3.3 (ou 13%) foram dedicados a atividades públicas de divulgação e de conscientização. Finalmente, CAN$ 9.8 (que representam 40%) foram gastos em manutenção da estrutura do órgão (denominados "serviços internos" – "internal services").

O OPC possui 181 funcionários trabalhando em período integral. Daquele total, 81 trabalham em atividades de fiscalização do cumprimento das normas de proteção de dados pessoais. 29 dedicam-se a ações de pesquisa e de desenvolvimento de políticas; 21, a iniciativas de divulgação junto à sociedade. Finalmente, 50 estão empregados em "serviços internos" de administração.”