

Informações sobre regulamentação de Internet

Resposta ao Ofício nº259/2015/GAB-SAL-MJ (Processo nº 08027.000032/2015-11)

Informações recebidas de Embaixadas do Brasil no exterior

DINAMARCA

1. Após consulta a jornalistas, a órgão de direito dos consumidores e órgãos públicos que tratam da regulamentação do uso da tecnologia da informação, seguem, a seguir, comentários sobre a regulamentação do uso da Internet e a proteção de dados pessoais na Dinamarca.

I. Contexto:

2. Como membro da União da Europeia, a Dinamarca segue as diretivas da UE sobre o tema, em particular a 95/46/EC, de 1995, bem como participa ativamente do debate para reformular a diretiva às necessidades atuais.

3. Não há legislação específica sobre neutralidade da rede no país. A classe política dinamarquesa parece preferir que o tema seja legislado no ambiente europeu e não meramente nacional, tanto para evitar tornar as empresas locais menos competitivas como por perceber que a legislação nacional apenas não seria eficaz num ambiente de rede internacionalizado.

4. O debate sobre a neutralidade da rede vê, por um lado, o risco de que o fornecimento de "serviços especializados" (como, exemplo, velocidade diferenciada para serviços de interesse do provedor) prejudique empresas iniciantes no mercado (start-ups) e assim, comprometa a concorrência e a inovação. Já representantes da indústria argumentam que um marco regulatório rígido e a proibição ao fornecimento de velocidades diferenciadas poderiam deter o desenvolvimento de serviços com necessidades especiais de conexão e velocidade, tal como a assistência médica pela Internet, que já é utilizada pelo setor público dinamarquês.

II. Órgãos com competência para regulamentação do uso da Internet e de dados pessoais:

5. A Agência Dinamarquesa de Proteção de Dados (Datatilsynet) é entidade do Ministério da Justiça encarregada da supervisão da lei de processamento de dados pessoais. Possui um conselho e um secretariado. O Conselho é composto por seis membros e um presidente escolhidos pela Ministra da Justiça. O secretariado conta com um diretor e 35 funcionários (advogados, consultores de segurança de TI, funcionários encarregados da administração e estudantes assistentes). Em 2014, a Agência contou com orçamento de DKK 21,6 milhões (US\$ 3,2 milhões).

6. A Agência orienta autoridades, empresas e cidadãos, reage a denúncias e realiza visitas de inspeção anuais a autoridades públicas e empresas privadas que tenham recebido

aval para processar dados pessoais. Caso descubra violações à legislação específica (descrita a seguir), seja por denúncia ou inspeção anual, poderá notificar ou banir a empresa, além de notificar a polícia para início de investigação criminal (fonte: <http://www.datatilsynet.dk/english/the-danish-data-protection-agency/introduction-to-the-danish-data-protection-agency/>).

7. Vinculada ao Ministério dos Negócios, a Autoridade para Negócios (Danish Business Authority ou Erhvervsstyrelsen, em dinamarquês) exerce funções de autoridade reguladora independente nas telecomunicações e Internet, inclusive administração de frequências. Como autoridade reguladora, a Autoridade é independente do Ministro dos Negócios nas suas decisões.

8. A Agência para Digitalização, do Ministério da Fazenda, foi estabelecida em 2011, para coordenar o processo de digitalização necessário para modernizar o Estado do bem estar social (previdência e outros benefícios sociais), bem como outros processos de digitalização no setor público. A meta é a de que 80% da comunicação entre o Estado e as pessoas físicas e jurídicas na Dinamarca seja “online” já em 2015. A Agência coordena-se com entidades municipais e autarquias e preside o Fórum de Segurança da Informação, que assessora o Conselho de Tecnologia da Informação do governo dinamarquês. Participam do Fórum cerca de 30 entidades governamentais, com 4-6 reuniões ao ano que tratam de aspectos tais como: aplicação do padrão ISO de segurança da informação; acompanhar o desenvolvimento da gestão da segurança da informação por autoridades públicas; determinar e intercambiar boas práticas e propor melhorias à Agência para Digitalização, que preside o Fórum. Desde janeiro de 2014, todas as instituições governamentais do país estão obrigadas a seguir o padrão internacional de segurança da informação ISO/IEC 27001.

III. Legislação sobre a proteção de dados pessoais:

9. A Dinamarca adota a Diretiva europeia sobre a proteção de dados (95/46/EC). Há negociação em andamento para unificar a proteção de dados na UE através de uma lei única (General Data Protection Regulation, GDPR). Em julho de 2000, entrou em vigor a lei nacional 429 (Persondataloven ou Lei sobre processamento de dados pessoais) que implementa a Diretiva no país. Versão em inglês da lei dinamarquesa está disponível em <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/>.

10. "Cookie-bekendtgørelse" é uma instrução normativa relativa à demanda de autorização expressa pelo usuário final para uso de "cookies" e acesso ou armazenamento de dados pessoais. A autoridade reguladora Erhvervsstyrelsen emitiu um guia de 40 páginas sobre a aplicação dessa instrução, destinado a usuários e empresas. A versão em inglês do guia, em PDF, está disponível em <https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf>.

11. A lei Persondataloven (a) cobre todo o tipo de dado pessoal, em princípio apenas de pessoa física, em casos especiais poderá cobrir alguns dados de pessoas jurídicas. A norma

sobre uso de "cookies" (b) tem por objeto o acesso a dados do terminal do usuário, pessoa física ou não.

12. Segundo o capítulo 4 da Persondataloven, dados pessoais coletados não devem ser armazenados não devem possibilitar a identificação do indivíduo por tempo superior ao necessário para cumprir o objetivo da coleta de data. O processamento de dados pessoais depende de consentimento expresso do indivíduo e pode ser permitido em casos específicos, tais como: se estiver vinculado a contrato de que o indivíduo seja parte ou a seu pedido, para cumprir obrigação legal, para proteger interesses vitais do indivíduo, ou em caso de interesse público. Nesse mesmo capítulo, a lei proíbe o processamento de dados pessoais em termos de tipificação racial ou étnica, opiniões políticas, crença ou linha filosófica, participação em sindicato, dados sobre saúde ou comportamento sexual. Ademais, é vedado à empresa privada entregar dados sobre consumidor para terceiras partes para fins de marketing, sem consentimento expresso. A comunicação online não-solicitada pelo consumidor é proibida, segundo a seção 6 da lei sobre propaganda (cuja versão em inglês está disponível no link <http://www.consumerombudsman.dk/~media/Consumerombudsman/dco/Markedsfoeringsloven%20lbkg%202013.pdf>).

IV. Discussão:

13. A Dinamarca é um país altamente digitalizado, com grande uso de aplicativos e da Internet para transações comerciais e bancárias, para relacionamento pessoal e também na relação do cidadão com o Estado. Conforme já mencionado, até o final de 2015, 80% da correspondência entre autoridades públicas e o cidadão deverão eletrônicas.

14. É também característico do país o armazenamento de dados pessoais por autoridades públicas. Por meio do número de registro pessoal, o CPR, as autoridades públicas (inclusive fiscais) conhecem o endereço, a escola dos filhos, o clínico geral, o dentista de cada cidadão, bem como se este recebe algum benefício social. Cada prescrição médica é registrada eletronicamente, de modo que a autoridade de vigilância farmacêutica sabe qual o medicamento, em que dosagem, foi prescrita por qual médico, para qual paciente e vendida por qual farmácia. Assim, circulam dados sensíveis no ambiente das autoridades governamentais, o que tende a aumentar com a decisão de fortalecer-se o governo eletrônico.

15. Diversos escândalos recentes sobre acesso a informações privilegiadas aumentaram a preocupação com a segurança dos dados. Como exemplo, o banco de dados dos clínicos gerais, desde 2007, recebeu permissão para armazenar informações sobre doenças crônicas, para fins de pesquisa epidemiológica. No entanto, em novembro de 2014, foi constatado que o banco de dados passara a armazenar dados sobre muitas outras condições médicas, sem conhecimento do paciente, em clara violação da confidencialidade médico-paciente. O banco de dados não foi desfeito. Em outro caso, de 2012, hackers acessaram sem dificuldade o registro do CPR de toda a população dinamarquesa, mantido por empresa terceirizada, filial de conglomerado estadunidense. O caso levantou o problema da terceirização na manutenção de banco de dados do setor público, com o agravante de que a filial de empresa norte-americana poderia ser acionada por autoridades daquele país a

fornecer informações do banco de dados, sem autorização das autoridades dinamarquesas. Por fim, chamou atenção o escândalo da venda de informações sobre transações em cartão de crédito de celebridades e políticos, em 2014. No caso, registro de transações em cartões de débito e crédito na Dinamarca - monopólio da empresa Nets e cujos dados eram administrados pela IBM - era ilegalmente vazado para o tablóide Se og Hor, que usava os dados para perseguir celebridades dinamarquesas em suas férias.

16. Em reação aos escândalos, duas comissões parlamentares foram instadas a apreciar as muitas falhas de segurança no tratamento de dados pessoais por entidades governamentais e privadas e propor soluções. A assunto ainda está sob deliberação, mas uma das propostas analisadas seria diminuir a necessidade de registro de dados do cidadão, talvez adotando o método "privacy consequence analysis" do Canadá, que contrapõe a conveniência da identificação do cidadão ao direito à privacidade.

17. Outro grave problema identificado é a violação recorrente da lei que rege o uso de "cookies". A televisão pública DR exibiu, em 15/3/2015, o documentário "Privatliv til salg" (A vida privada à venda), que demonstrou como empresas de coletas de dados norteamericanas, as chamadas "databrokers", tinham à disposição dados pessoais sobre mais de 359 mil dinamarqueses, inclusive com nome e endereço postal, além do perfil de comportamento online.

18. No programa, a consultora do órgão de defesa do consumidor Taenk, Anette Høytrup, questionou a eficácia da atual lei sobre cookies. Segundo ela, na prática, a exigência de consentimento expresso é implementada de modo fraco. Se o usuário deseja receber ou contratar um serviço, precisa entrar na página web e aceitar o cookie e, assim, apenas ao visitar a página ele já permite o acesso de terceiros a seu perfil.

19. A lei dinamarquesa proíbe a venda de informações privadas a terceiros, sem consentimento do usuário e obriga o site a informar qual a informação será armazenada, para qual propósito e por quanto tempo. No entanto, foi demonstrado que nem as empresas privadas, nem os sites das autoridades públicas dinamarquesas e nem mesmo as agências com competência para verificar o cumprimento da lei conseguem monitorar os "cookies" ocultos, inseridos por empresas de marketing e de coleta de dados, sem o conhecimento expresso dos detentores principais do site. Esses "cookies" de terceiras partes monitoram o comportamento dos usuários e permitem a elaboração de listas à disposição das "databrokers". Em entrevista ao programa, os órgãos dinamarqueses reconheceram que não estão habilitados a verificar "cookies" que operam à margem da lei, sem o consentimento do usuário.