

## **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**

#### **ALEMANHA**

1. “A regulamentação do funcionamento e do uso da Internet na Alemanha apoia-se em conjunto bastante amplo e heterogêneo de normas, que disciplinam desde questões mais gerais de direito constitucional, civil, comercial e penal, até campos mais específicos como, por exemplo, a proteção de dados pessoais, o direito autoral e telecomunicações. A matéria também envolve a interação de diferentes esferas de competência (a comunitária, a federal e a estadual), o que adiciona complexidade ao assunto.

2. O Governo alemão está envolvido no momento em diversas iniciativas para atualizar a regulamentação de temas digitais, tanto no âmbito da União Europeia, quanto internamente. No plano doméstico, debate-se, por exemplo, a implementação da Agenda Digital 2014-2017, aprovada em agosto último, que visa incentivar o desenvolvimento do setor de TI na Alemanha, inclusive com mudanças regulatórias (informações em inglês podem ser acessadas em [www.bmwi.de/EN/Topics/Technology/digital-agenda](http://www.bmwi.de/EN/Topics/Technology/digital-agenda)).

3. O Governo alemão também debate projetos de lei, como a Lei de Segurança das Tecnologias de Informação ("IT-Sicherheitsgesetz"), que pretende definir padrões mínimos de segurança e requisitos de fornecimento de informações para operadores de "infraestruturas críticas". Discute-se, ademais, de forma mais preliminar, a adoção de possível nova legislação geral para "mídias" (rádio, televisão e multimídia, inclusive a Internet).

4. Vários dos pontos em debate no processo de regulamentação do Marco Civil da Internet são questões igualmente atuais na Alemanha, onde também se reconhece a necessidade de se adequar a legislação às novas demandas impostas pelo crescimento das tecnologias de informação e telecomunicação. Alguns temas são considerados controversos e seguem na pauta de debate do Governo alemão, como a neutralidade da rede, a retenção de registros de conexão e limites para a coleta e o tratamento de dados pessoais na Internet. A seguir, comentários a respeito, com base em informações colhidas junto a diferentes fontes oficiais públicas e profissionais da área.

#### **NEUTRALIDADE DA REDE**

5. Não há, na Alemanha, garantia legal expressa da neutralidade da rede. A Lei de Telecomunicações ("Telekommunikationsgesetz", TKG) autorizou o Governo Federal a publicar, com o consentimento do Parlamento e do Conselho Federal, decreto para estabelecer "a não discriminação na transmissão de dados e no acesso e na utilização de conteúdos", e para "impedir a deterioração arbitrária de serviços e a imposição de barreira ou de redução de velocidade do

tráfego nas redes". O artigo, porém, nunca foi regulamentado.

6. A neutralidade de rede é tratada na Alemanha, em certa medida, como questão de qualidade de serviço. A Bundesnetzagentur, agência reguladora encarregada, entre outras tarefas, de defender a concorrência no campo das telecomunicações, elenca entre suas atribuições contribuir para a "neutralidade da rede" por meio de estudos de qualidade dos servidores e da promoção da transparência. Em sua página, a agência federal esclarece que a TKG lhe fornece os instrumentos para "garantir aos usuários a possibilidade de utilizar os serviços e aplicações de sua escolha" e que "a agência sempre sublinhou, no que diz respeito à neutralidade da rede, que a Internet se desenvolve de forma dinâmica". Para o órgão, a transparência permite que usuários "saibam quando seus provedores de serviço favorecem ou prejudicam certas formas de tráfego, para que possam decidir se querem sancioná-los por meio da troca para um meio de acesso neutro".

7. Nesse contexto, tampouco existem restrições ao provimento de acesso gratuito a determinadas aplicações da Internet. A prática do chamado "zero-rating" é bastante difundida no setor de Internet móvel. A oferta de Internet por linhas terrestres, por sua vez, parece ser menos afetada. Em 2013, a Deutsche Telekom chegou a anunciar planos de limitar a banda de usuários de Internet a cabo que ultrapassassem certo volume de dados, excluindo dessa provisão serviços oferecidos pela companhia e por empresas parceiras. A proposta foi abandonada, porém, diante de pressões políticas e de decisão judicial que não dizia respeito diretamente a questões de neutralidade da rede (decidiu-se que a empresa não poderia limitar o volume de dados de planos anunciados como "flatrate").

8. Conhecido especialista e ativista alemão, em conversa com colaborador meu, avaliou haver, na prática, certo respeito ao princípio da neutralidade da rede no provimento de acesso à Internet por linhas terrestres na Alemanha. Tal situação resultaria, porém, essencialmente da concorrência entre os diferentes provedores, uma vez que não há quadro legal para se impedir certas práticas. Por diferenças regulatórias e de mercado, observa-se no setor de telefonia móvel situação distinta, não só com o amplo recurso ao "zero-rating", mas também com a oferta de contratos que muitas vezes desautorizam o uso da conexão para VoIP, P2P, "Instant Messaging" e "Tethering".

9. No acordo para a formação do atual Governo alemão, assinado no fim de 2013, a coalização CDU/CSU-SPD estabeleceu entre seus objetivos regulamentar o artigo sobre neutralidade da rede da TKG e esforçar-se no âmbito comunitário para "ancorar legalmente" o princípio da neutralidade da rede. O acordo de governo trata "o transporte sem discriminação de todos os pacotes de dados" como princípio fundamental para garantir a inclusão, a diversidade de pensamento, a inovação e a livre concorrência na Internet; o texto defende, ainda, a neutralidade em ferramentas de busca, de modo que "todas as ofertas de conteúdo sejam apresentadas sem discriminação". A coalizão trabalharia, ademais, para proibir a "Deep Packet Inspection" (DPI) a fim de impedir a discriminação de serviços e o monitoramento de usuários.

10. Nos últimos meses, contudo, diferentes representantes do Governo alemão - entre eles a própria Chanceler Federal, Angela Merkel - têm dito que a neutralidade da rede deve vir acompanhada de garantias para certos "serviços especiais". As declarações têm sido

interpretadas como desvio das propostas do acordo de coalizão, que diz, inclusive, que a neutralidade da rede não deve ser prejudicada por uma "míriade de `managed services`".

## **PROTEÇÃO DE DADOS NA INTERNET**

11. Como resultado de diferentes processos históricos e culturais, a Alemanha desenvolveu arcabouço legal no campo da proteção de dados pessoais reconhecido como pioneiro e entre os mais robustos do mundo. Vale notar, por exemplo, que a Lei de Proteção de Dados do estado federal de Hesse, que entrou em vigor em 1970, é considerada a primeira lei formal de proteção de dados do mundo.

12. O principal instrumento legal na Alemanha sobre a matéria é a Lei Federal de Proteção de Dados (Bundesdatenschutzgesetz, BDSG), que entrou em vigor em 1979 e já passou por diversas revisões, inclusive para se adequar à diretiva europeia 95/46/EC. Versão em inglês da BDSG pode ser acessada em [www.gesetze-im-Internet.de/englisch\\_bdsng/](http://www.gesetze-im-Internet.de/englisch_bdsng/). Cada estado federal conta, ademais, com leis próprias de proteção de dados pessoais, as quais visam regulamentar primariamente o processamento e uso de dados pelas autoridades públicas estaduais. De modo geral, a BDSG estabelece regras para o processamento e uso de dados por autoridades públicas federais e por instituições privadas, razão pela qual se reveste de especial relevância para o setor digital.

13. O acompanhamento e o controle da implementação da BDSG é responsabilidade da Representante Federal para Proteção de Dados e Liberdade de Informação (BfDI, na sigla em alemão), que é designada pelo Parlamento, por indicação do Governo Federal. O cargo é atualmente ocupado pela Senhora Andrea Voßhoff, que tem independência oficial no desempenho de suas funções, mas está sob a supervisão legal do Governo Federal e sob a supervisão administrativa do Ministério do Interior. A BfDI, que tem sede em Bonn, conta com o apoio de cerca de 90 funcionários, divididos em 9 departamentos, além de outros órgãos de assessoria, e seu orçamento em 2014 foi de 9 milhões de euros. Suas atribuições, que estão descritas na BDSG, incluem aconselhar e controlar autoridades e órgãos federais, empresas de telecomunicação e de correio. Qualquer pessoa podem recorrer à BfDI se considerar que seus direitos pessoais de proteção de dados foram violados.

14. O sistema alemão, porém, é bastante complexo, e a BfDI não é a única instituição responsável por supervisionar e controlar a implementação das regras de proteção de dados. Cada estado federal alemão tem seu próprio Representante para Proteção de Dados, bem como competência para regular como será feito o controle de proteção de dados de suas instituições e das empresas com sede em seu território. A maior parte dos estados encarrega seus Representantes para Proteção de Dados com essas tarefas, mas alguns recorrem a órgãos distintos. A Baviera, por exemplo, além de um Representante, tem uma agência especial responsável apenas pela supervisão de instituições privadas. O estado federal de Schleswig-Holstein, por sua vez, encarrega uma instituição independente com a responsabilidade de supervisão.

15. Estas Autoridades de Supervisão, cujas atribuições estão descritas na BDSG (seção 38), têm diferentes mecanismos de controle a sua disposição. Pequenas empresas e instituições, por exemplo, são obrigadas a se registrar antes de iniciar procedimentos de

coleta e processamento de dados. Empresas ou instituições com número maior de funcionários ou que queiram realizar processamento automático de dados devem, por sua vez, designar um Oficial para Proteção de Dados, cuja responsabilidade é verificar a implementação interna das leis de proteção de dados. As Autoridades de Supervisão também têm o poder de realizar inspeções in loco das empresas para monitorar o processamento de dados e apurar infrações (o que por vezes é feito em cooperação com outras Autoridades e agências).

16. Ainda que a legislação alemã sobre a matéria seja considerada avançada, a complexidade do sistema de supervisão e controle da proteção de dados na Alemanha enseja algumas críticas importantes. Há críticas, por exemplo, no sentido de que, na prática, não haveria controle efetivo do armazenamento e processamento de dados em provedores de acesso à Internet e em empresas da área, uma vez que as Autoridades de Supervisão não contariam com os recursos materiais e pessoais necessários para isso.

17. Nos 16 "Länder" (estados) alemães, as Autoridades de Supervisão contam com cerca de 400 funcionários, que normalmente também são responsáveis por acompanhar a aplicação das leis de acesso à informação. Dentro desse universo, apenas parte dos funcionários trabalha com temas de TI: entre suas muitas tarefas está supervisionar o setor de "cloud computing", verificar se os provedores e empresas adotam os padrões mínimos de segurança exigidos pela BDSG (seção 9 e anexo da lei) e analisar software e aplicativos (inclusive "apps" móveis). As Autoridades também produzem inúmeras "checklists" e folhetos informativos para auxiliar instituições e empresas na aplicação prática da lei.

18. De modo a dirimir algumas limitações de pessoal, e de forma consistente com a natureza digital das atividades de algumas empresas, a Agência Estadual para Supervisão da Proteção de Dados da Bavária (BayLDA) tem, desde 2012, realizado também "inspeções online", pela qual se avalia, por exemplo, a segurança de servidores de e-mail e o uso adequado de ferramentas como Google Analytics e Adobe Analytics. Estima-se que inspeções do gênero serão cada vez mais utilizadas.

19. Outro aspecto que desperta críticas com relação à supervisão da proteção de dados na Alemanha é a independência "limitada" da BfDI. A questão, porém, deixa de ser grande óbice com a aprovação, no fim de 2014, de nova "lei para o fortalecimento da independência da BfDI", que estabelece que o órgão será elevado em 2016 ao status de "autoridade federal superior autônoma". Com a mudança, a BfDI deixará de estar sob a supervisão legal do Governo e sob a supervisão administrativa do Ministério do Interior. Deverá permanecer apenas o controle parlamentar e judicial da instituição. No plano dos "Länder", todavia, a independência institucional, bem como material e de pessoal, continua a ser uma questão importante.

20. Como lei geral sobre a proteção de dados na Alemanha, a BDSG também tem implicações importantes para a proteção dos dados e da privacidade do consumidor. Nela estão consolidados princípios fundamentais como o de que só podem ser colhidos e processados dados com a autorização do indivíduo, e o de que toda pessoa tem direito a ter acesso a seus próprios dados armazenados por uma instituição. A BDSG também regulamenta a transferência de dados para terceiros. Vale notar, ainda, que, com a formação

do atual Governo, em 2013, a proteção do consumidor foi incluída no portfólio do Ministério da Justiça, que também tem certas competências sobre questões de proteção de dados e segurança da Internet. Espelhando a já mencionada complexidade do sistema alemão de proteção de dados, porém, também a proteção do consumidor é objeto de extenso e heterogêneo conjunto de leis. Há, na Alemanha, ampla rede de centrais de proteção do consumidor, as quais não estão vinculadas ao Governo alemão.

## **DEVER DE GUARDA DE REGISTROS DE ACESSO E CONEXÃO**

21. A Alemanha não possui, atualmente, legislação que prevê o dever de guarda de registros de acesso a aplicações de Internet ou de registros de conexão. Em cumprimento das diretrizes 2006/24/EG da União Europeia, o Parlamento Federal alemão chegou a aprovar legislação sobre o tema, a qual entrou em vigor em 1/1/2008, estabelecendo a retenção de dados telefônicos e de conexão por seis meses para uso, em caso de necessidade, das autoridades judiciais ou dos serviços de inteligência alemães.

22. A lei dizia respeito a dados coletados, processados ou utilizados pelos serviços de telecomunicação no provimento de seus serviços. Para os serviços de telefonia, isso implicava, por exemplo, os números de telefone da pessoa que faz e da pessoa que recebe uma chamada, os horários de início e fim da conversa, o número de série do telefone celular e do chip telefônico, bem como a estação telefônica utilizada. No campo da Internet, especificamente, a lei previa a retenção de endereços de IP utilizados para conexões e informações sobre o tráfego de e-mails (IPs, endereços, datas e horários), entre outros metadados.

23. O dever de guarda de dados de acesso a aplicações de Internet não estava previsto na lei de 2008. A questão tampouco parece figurar no atual debate sobre retenção de dados na Alemanha. A guarda do registro de acesso a aplicações chegou a ser discutida no país, mas propostas nesse sentido não chegaram a obter apoio suficiente e foram posteriormente abandonadas.

24. A elaboração e aprovação de lei sobre retenção de dados foi acompanhada de grande controvérsia na Alemanha. O próprio BfDI criticou a norma desde o princípio, antes mesmo de sua adoção, qualificando a retenção abrangente e irrestrita de dados como desproporcional e anticonstitucional. Entre os problemas apontados pelo BfDI estava a possibilidade teórica de que os dados pudessem ser utilizados para construir perfis sociais e de deslocamento dos usuários da Internet. Críticos da lei também argumentavam que a população não pode ser considerada "suspeita a priori", e que tampouco havia risco concreto a ser dirimido.

25. O BfDI também relatou ter verificado dificuldades substanciais na implementação prática da lei de 2008. Levantamentos junto aos serviços de telecomunicação demonstraram à época que estes retinham regularmente mais dados do que o que legalmente previsto. Ademais, na avaliação do órgão, a legislação falhava ao não garantir nível adequado de segurança dos dados armazenados.

26. Ainda no início de 2008, em resposta a ação legal conjunta apresentada por mais de

35 mil apelantes contra a lei alemã de retenção de dados, a Corte Constitucional Alemã adotou medidas cautelares que limitaram fortemente a possibilidade de utilização dos dados de conexão retidos. Em março de 2010, o tribunal declarou as provisões da lei de retenção de dados como inconstitucionais e consequentemente nulas.

27. Apesar de teoricamente não ter considerado a retenção de dados "per se" como inconstitucional, a Corte Constitucional estabeleceu que as medidas até então em vigor feriam o princípio da proporcionalidade e não poderiam ser implementadas por período tão longo e sem objetivos definidos. Já se antecipando a eventuais desdobramentos do assunto, a decisão de 2010 estipulou que eventual nova legislação sobre retenção de dados para fins de investigação, apesar de não constituir necessidade legal, seria possível se atendidos quatro conjuntos de condições:

i) Segurança de dados - os dados pertinentes devem ser retidos de forma separada dos dados utilizados cotidianamente pelas empresas de telecomunicações, bem como protegidos por criptografia avançada e por um sistema de consultas seguro (por exemplo, com o "Vier-Augen-Prinzip", pelo qual o acesso deve ser controlado por duas pessoas ou instâncias distintas). Deve haver, igualmente, sistema adequado de registro/protocolo do acesso e da eliminação dos dados;

ii) Transparência - o acesso e uso dos dados deve ocorrer, em princípio, de forma aberta. O acesso secreto só pode ser autorizado de forma excepcional e com base em decisão judicial. Mesmo nesse caso, a pessoa afetada deve ser informada posteriormente, tão logo expire o prazo de confidencialidade;

iii) Proteção de direitos - a requisição e a transferência dos dados ao órgão solicitante só pode ser feita conforme decisão judicial, não podendo haver acesso direto aos dados. Deve ser estabelecido, ademais, sistema de controle da legalidade da retenção e do uso dos dados, o qual deve prever também a possibilidade de sanções concretas;

iv) Utilização - os dados retidos só podem ser utilizados de maneira estritamente limitada (para além dos critérios já previstos na lei de 2008). A utilização dos dados só pode ser permitida em caso excepcional, para "ofensas graves" elencadas em uma relação pré-definida. No campo da inteligência e da segurança pública, o recurso aos dados só deve ser permitido diante de evidência de ameaça concreta para interesse público maior (por exemplo, risco de vida).

28. A lei de 2008 estabelecia que as empresas de telecomunicação eram responsáveis por guardar os registros de conexão por seis meses, o que em 2010 continuava a ser exigência legal, não obstante as fortes limitações impostas sobre o uso dos dados. Com a decisão da Corte Constitucional, exigiu-se que esses dados fossem apagados, o que, conforme informações do BfDI, foi feito de forma satisfatória, de modo que, atualmente, não há retenção de dados para fins de investigação. As empresas de telecomunicação continuam a ser autorizadas, contudo, a manter dados necessários para o desempenho de suas funções básicas, como, por exemplo, para fins de cobrança. De modo geral, esses dados pessoais devem ser apagados tão logo sejam desnecessários, idealmente sem exceder uma semana.

29. A anulação da lei de 2008 levou a intensas discussões para a aprovação de novo instrumento legal, de modo a cumprir tempestivamente a diretiva europeia pertinente. Não foi possível, porém, produzir acordo sobre o assunto, e a Alemanha chegou, inclusive, a ser multada em mais de 300 mil euros diários pelo descumprimento das regras comunitárias. Mesmo depois da decisão do Tribunal de Justiça da União Europeia de invalidar a diretiva 2006/24/EG, em abril de 2014, continua bastante vivo o debate sobre retenção de dados na Alemanha. Recentemente, a CDU, partido da Chanceler Angela Merkel, tem redobrado chamados para a elaboração de nova legislação nacional sobre o tema, tendo em conta, inclusive, a perspectiva de poucos avanços nas discussões sobre nova diretiva no âmbito comunitário. O SPD, o outro grande partido que compõe a coalizão de Governo, opõe-se em princípio a tal iniciativa, mas não chega a excluir a possibilidade. Em paralelo, setores do Governo também têm demonstrado abertura quanto à possível adoção de um Registro de Identificação de Passageiros (PNR) na UE.”