TRADUÇÃO

Proteção cibernética de informações pessoais em um sistema multidimensional

ZHOU Yuexin

Tradução:

Liu Yi

Talitha Saez Cardoso

V. 1 / N. 2 / DEZEMBRO DE 2020
PÁGINAS 297 A 309

Proteção cibernética de informações pessoais em um sistema multidimensional

ZHOU Yuexin*

Apresentação dos tradutores

Não é preciso mencionar os diversos momentos em que a China exerceu fascínio sobre o Ocidente, desde os primeiros contatos registrados ao longo da história, para justificar a relevância de artigos acerca da complexa interdependência entre internet e sociedade na China contemporânea. O texto a seguir foi publicado originalmente em inglês, no entanto é possível notar a influência da língua chinesa na maneira especial de transmitir ideias e conceitos, uma vez que a língua chinesa tem em vista substancialmente a ação. Com a presente tradução pretendemos revelar uma das múltiplas realidades da China, em matéria de internet e sociedade, não como um Outro idealizado, mas sim como um Outro que nos desafia a pensar.

O artigo selecionado para tradução foi publicado na *Tsinghua China Law Review*, a primeira revista acadêmica em inglês dirigida por estudantes e publicada por uma universidade da China continental, a Universidade Tsinghua (localizada em Pequim e considerada uma das mais seletivas universidades do país). Assim como a Revista Internet & Sociedade, a *Tsinghua China Law Review* promove o pensamento crítico sobre questões de impacto imediato na sociedade contemporânea. Como as publicações da *Tsinghua China Law Review* tratam de questões diversas do direito chinês, nossa seleção priorizou conteúdos diretamente relacionados ao escopo da Revista Internet & Sociedade, ou seja, material sobre diferentes aspectos do contato entre internet e sociedade.

"Proteção cibernética de informações pessoais em um sistema multidimensional", de ZHOU Yuexin, publicado no número 1 do volume 12 da *Tsinghua China Law Review* em 2019, trata da elaboração de regras sobre a proteção de dados pessoais na China. Ao introduzir o peculiar sistema chinês de proteção de dados pessoais, esse artigo nos convida a identificar, enquanto leitores ativos, as possíveis semelhanças e diferenças entre a regulamentação da proteção de dados pessoais no Brasil e na China. O diagnóstico da realidade chinesa feito pela autora, ZHOU Yuexin, expõe tanto o lado positivo como também as inconsistências intrínsecas ao atual sistema chinês de proteção de dados pessoais. Além disso, o artigo é ainda propositivo, conforme as conclusões a que nos conduz a autora.

A recente entrada em vigor das revisões à *Especificação sobre Segurança das Informações Pessoais*, em 1 de outubro de 2020, evidencia a atualidade do tema abordado por ZHOU Yuexin. Dentre as alterações, vale sublinhar aquela que exige o consentimento livre, específico e informado para o processamento de informações pessoais. Ademais, a fim de aperfeiçoar a proteção às informações pessoais processadas por meio de novas tecnologias, como inteligência

artificial, foram incluídas novas exigências. Pelas revisões também foram incluídas regras de compliance análogas àquelas praticadas pela União Europeia. No entanto, a *Especificação* tem uma natureza não vinculativa, o que será devidamente examinado no texto a seguir.

Agradecemos à autora, ZHOU Yuexin, pela autorização para traduzir seu artigo e à equipe da *Tsinghua China Law Review*, especialmente ZIYU Lin, que prontamente nos auxiliou com as autorizações.

* ZHOU Yuexin, graduanda em Direito pela Universidade de Tsinghua. Agradeço a Lin Meng, Song Jinyang e Lin Ziyu pelo feedback atencioso em várias etapas deste artigo, e à equipe do TCLR pela edição cuidadosa. Todos os erros são meus.

Proteção cibernética de informações pessoais em um sistema multidimensional

ZHOU Yuexin*

1. Introdução

Nos últimos dois anos, para garantir a cibersegurança de dados e os direitos legítimos dos cidadãos, a China emitiu uma série de documentos regulamentares para estabelecer o referencial do uso de dados. Com o enfoque global na legislação de ciber proteção de dados, o processo regulatório revelou a tentativa da China de estabelecer seu próprio sistema de proteção cibernética de dados.

Este comentário apresentará brevemente o desenvolvimento e o *status quo* da proteção cibernética de dados na China. A parte I introduz o desenvolvimento regulatório da proteção cibernética de dados, impulsionado por três regulamentos. A Parte II, a seguir, completa a tendência regulatória manifestada pelos três documentos e discute o sistema multidimensional organizado por eles, incluindo o motivo para estabelecer esse sistema e como ele funciona, e a tensão entre inovação e proteção da privacidade subjacente a esse sistema. O presente texto conclui que há problemas ao executar esse sistema. Também serão fornecidas sugestões para resolver tais problemas.

2. A tendência regulatória em proteção cibernética de informações pessoais

Em 1 de maio de 2018, entrou em vigor a Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais (doravante denominada "Especificação") emitida pela Administração de Normalização da China.[1] Em 19 de abril de 2019, o Ministério da Segurança Pública da China divulgou a versão final da Diretriz para Proteção e Segurança de Informações Pessoais na Internet (doravante denominada "Diretriz") como uma reafirmação e validação da Especificação. Em 28 de maio de 2019, o Proposta de Medidas sobre Administração de Segurança de Dados (doravante denominadas "Medidas") foi emitido pela Administração do Ciberespaço da China, em conjunto com uma consulta pública.[2] Depois de formalmente emitidas, as Medidas, diferentemente da Especificação e da Diretriz, se tornariam um regulamento vinculativo.

A. Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais

Como critério nacional recomendado, a Especificação é principalmente uma diretriz voluntária, não juridicamente vinculativa para os tribunais nem obrigatória para as empresas. No entanto, constitui a referência para a coleta de dados sob a Lei de Cibersegurança da República Popular da China de 2016 (doravante

denominada "Lei de Cibersegurança").[3]

Também deve ser observado que a Especificação nunca é apenas uma versão prática e detalhada da Lei de Segurança Cibernética. Ela avança, adicionando requisitos mais rigorosos sobre a coleta de dados. Esse desenvolvimento progressivo distingue especialmente os pontos a seguir.

Primeiramente, comparado com a Lei de Cibersegurança, o escopo de informações pessoais é ampliado na Especificação devido a um método de definição diferente. O artigo 76 da Lei de Cibersegurança define informações pessoais como todos os tipos de informações registradas em formato eletrônico ou outro, que podem ser usadas para verificar a identidade pessoal de uma pessoa física.[4] As informações pessoais sob esta definição incluem, entre outras, nome, data de nascimento, número de identidade, informações biométricas, endereço e número de telefone. Mesmo que seja declarado que a lista acima é inesgotável, o escopo das informações pessoais é, sem dúvida, reduzido a um escopo limitado pela maneira como é definido. A Especificação, em contrapartida, define informações pessoais como informações que incluem tanto a identidade de uma pessoa quanto suas atividades.[5] Nesse sentido, informações como endereço de IP são incluídas e protegidas.[6] Além disso, a Especificação adiciona uma nova categoria de informações pessoais sensíveis, incluindo, mas não se limitando ao número de identificação pessoal, informações de transações e informações de crianças menores de 14 anos. Informações pessoais sensíveis são previstas para dispor de um nível maior de proteção.[7]

Em segundo lugar, as regras de consentimento prévio das pessoas estão detalhadas na Especificação. O artigo 41 da Lei de Cibersegurança obrigava as companhias de Internet a obter consentimento prévio para qualquer coleta de informações.[8] Com base nessa definição, a Especificação categoriza ainda mais os requisitos para diferentes tipos de coleta de informações. Quanto à coleta direta, onde o coletor de dados é o usuário direto dos dados, a entidade coletora deve notificar as pessoas sobre o tipo de informação que está sendo coletada e a maneira detalhada de usá-la. Após a notificação, é necessário o consentimento expresso do indivíduo para a coleta.[9] Quanto à coleta indireta, onde o coletor coleta dados pessoais de outros coletores de dados, o coletor deve confirmar a legitimidade da coleta original de informações. E o consentimento expresso do indivíduo para o compartilhamento de informações também é obrigatório.[10] Além disso, ao coletar informações de menores de 14 anos, é necessário o consentimento explícito de seus pais.[11] Quanto à coleta de informações pessoais sensíveis, é necessário o consentimento prévio detalhado, voluntário e explícito.[12] Se os usuários se recusarem a fornecer voluntariamente essas informações, a eles não poderia ser negado o acesso às "funções essenciais do negócio" fornecidas pela entidade coletora, a qual protege os usuários de serem forçados a fornecer informações importantes. Note-se que, o nome da pessoa não é classificado como informação sensível.[13] Isso permite que o registro do nome real exigido pela Lei de Cibersegurança, a qual estipula que, se uma pessoa não fornecer um nome real, ela não poderá obter acesso a todos os serviços[14]. Mas como o nome da pessoa não está previsto, um nível mais alto de proteção exige justificativa[A], pois o uso indevido do nome individual causaria risco de identidade, o que atende a definição de informações pessoais sensíveis.[15] O motivo da exclusão do nome individual não é claro na Especificação. E isso pode desencadear a confusão de que seja apenas para observar o requisito de registro de nome real estabelecido na Lei de Cibersegurança.

Em terceiro lugar, a Especificação estabelece o princípio de minimização. Este é um esclarecimento do princípio da necessidade no Artigo

41 da Lei de Cibersegurança. Embora o princípio da necessidade proíba apenas a coleta irrelevante dos serviços prestados pelos operadores de rede,[16] o princípio da minimização admite apenas informações pessoais diretamente relacionadas à execução das funções comerciais dos produtos ou serviços que não poderiam ser obtidas de outra forma. Ao dizer "minimização", a Especificação examina não apenas os recursos das informações, mas também a quantidade e a frequência das coletas. Também deve ser o mínimo para realizar as funções operacionais dos produtos ou serviços.[17]

Pode-se concluir que a Especificação visa promover a implementação da Lei de Cibersegurança. Mas também faz sua própria evolução com base na Lei de Cibersegurança, que assinala um controle mais detalhado e rígido sobre a coleta de informações.

B. Diretriz para Proteção e Segurança de Informações Pessoais na Internet

Quase um ano após o lançamento da Especificação, a Diretriz foi emitida em seguida pelo Ministério da Segurança Pública, que é o principal executor da lei para combater crimes cibernéticos e proteger a segurança cibernética. A Diretriz é importante e referência para os operadores de rede por implementar a Lei de Cibersegurança.

Referindo-se à Especificação como sua "fonte indispensável",[18] a Diretriz compartilha com ela o mesmo uso de termos e certas regras básicas, por exemplo, o princípio da minimização, entre outros.

Mas a Especificação também faz seu próprio progresso, por exemplo, estabelecendo a estrutura básica do regulamento em medidas técnicas, que não está incluída nos documentos normativos anteriores. De acordo com a lei de segurança cibernética, os operadores de rede devem tomar medidas técnicas e outras medidas necessárias para garantir a segurança das informações pessoais coletadas por eles e evitar vazamentos, danos e perdas de informações.[19] Esse requisito geral de fato proporciona uma certa margem de manobra. Mas na Seção 5 da Diretriz, todo um sistema para salvaguardar a segurança dos dados é estabelecido.[20] Condições detalhadas direcionadas a diferentes estágios da transmissão de dados, incluindo a segurança de telecomunicações e segurança de rede, segurança perimetral, segurança do ambiente de computação e segurança de aplicativos e dados, garantem a confidencialidade dos dados em grande medida. Essa é definitivamente uma extensão da Lei de Cibersegurança e abrange o que ainda é deixado em branco na Especificação.

Deve-se notar que, embora o conceito de "informações pessoais sensíveis" não seja levantado na Diretriz, a Diretriz também estabelece um padrão rígido para a coleta e o uso de informações sigilosas. Particularmente, os operadores de rede não devem coletar ou processar informações confidenciais como raça, etnia, opiniões políticas ou crenças religiosas em larga escala. A coleta de informações biométricas pessoais em sua forma original também deve ser evitada.[21] Esse novo requisito é levantado pela Diretriz pela primeira vez.

Em vista disso, um sistema de proteção abrangente é estabelecido sob a Especificação e a Diretriz. As cláusulas e princípios gerais da Lei de Cibersegurança são mais praticáveis com o complemento desses dois documentos normativos. No entanto, ainda existem diferenças entre eles, o que pode representar alguns obstáculos à implementação. Um exemplo óbvio é a definição de diferentes exceções

ao consentimento obrigatório da coleta de informações. Onze tipos de exceções são listados como exceções ao consentimento do usuário na Especificação,[22] mas apenas três na Diretriz, dois dos quais se sobrepõem à Especificação[23] e a tecnologia de *profiling* de usuário totalmente automática para marketing de precisão, ranking de resultados de pesquisa, notícias *push* personalizadas, publicidade direcionada e outros aplicativos de valor agregado é uma nova exceção definida na Diretriz.[24] Embora a Diretriz inclua menos cláusulas de exceção, a permissão geral do uso de dados sem consentimento, no contexto da tecnologia automática de criação de perfil de usuário em aplicativos com valor agregado, confere às empresas espaço para realizar uma determinada parte dos negócios. Outras diferenças dos dois documentos estão centralizadas na categoria de informações pessoais e na exigência de medidas técnicas. A inconsistência dos dois documentos gera confusão conforme explicado a seguir. Esse problema será discutido mais detalhadamente na próxima seção deste comentário.

C. Proposta de Medidas sobre Administração de Segurança de Dados

Emitido pela Administração do Ciberespaço da China em 28 de maio de 2019, o Proposta de Medidas acabou de encerrar seu período de comentários abertos e está prestes a ser lançado oficialmente, sendo que irá adquirir força legal na qualidade de regulamentos oficiais para o segmento. As Medidas, cristalizando as lições adquiridas com a implementação dos documentos normativos anteriores, também compartilham o mesmo conteúdo, em certa medida, com a Especificação, dando assim efeito jurídico ao quadro voluntário anterior. O lançamento do Proposta de Medidas pode ser considerado como uma confirmação dos esforços contínuos para obter experiência na implementação da proteção de dados cibernéticos.

As Medidas introduzem regulamentos semelhantes sobre aviso e consentimento, direitos do titular dos dados, recomendações personalizadas e publicidade direcionada, compartilhamento de informações pessoais e resposta a incidentes.[25]

No entanto, as Medidas também introduzem novos requisitos para "dados importantes", que são definidos como "dados que podem afetar diretamente a segurança nacional, a segurança econômica, a estabilidade social, a saúde pública e a segurança uma vez divulgados". Uma lista inesgotável de dados importantes inclui informações governamentais não publicadas, informações relacionadas a uma grande população, saúde genética, geografia e recursos minerais. Tanto a coleta quanto o processamento de dados importantes são rigidamente controlados. Antes da coleta de dados para uso comercial, os operadores de rede são obrigados a arquivar suas práticas de coleta de dados no escritório local de administração do ciberespaço.[26] E após a coleta, medidas como classificação, backup e criptografia devem ser tomadas para fortalecer a proteção de dados importantes.[27] Ao publicar, compartilhar ou negociar com dados importantes, além de avaliar o risco de segurança, as empresas também devem solicitar a permissão do órgão regulador do segmento.[28]

As Medidas, no geral, advêm da Especificação e, portanto, também estão intimamente relacionadas com a Lei de Cibersegurança. As orientações fornecidas ilustram a conformidade das empresas com o ordenamento jurídico.

3. Proteção de dados em um sistema multidimensional

A. Visão geral da proteção cibernética de informações pessoais

De acordo com o debate acima, a China se dedicou a criar e melhorar seu próprio sistema de proteção de dados. Com a Lei de Cibersegurança como base geral, os três documentos normativos oferecem parâmetros de referência mais detalhados sob a perspectiva de diferentes reguladores. Como a Especificação e a Diretriz carecem de força legal, elas formulam principalmente uma estrutura voluntária como referência para empresas, já as Medidas podem servir como uma diretriz mais importante para complementar a aplicação da Lei de Cibersegurança.

Porém, como todos esses documentos são elaborados por órgãos reguladores das operadoras de rede, existe realmente um forte incentivo à conformidade, devido aos poderes de investigação dessas autoridades sobre as violações de dados pessoais, o que poderia levar a sanções administrativas. Por exemplo, em 2019, o Ministério da Segurança Pública, o emissor da Diretriz, iniciou a campanha "Network Clearing 2019", que visava controlar os aplicativos que utilizavam indevidamente dados pessoais. Sanções administrativas e multas podem ser aplicadas às empresas infratoras. Os documentos normativos elaborados por eles podem refletir o critério de sua ação nos termos da Lei de Cibersegurança.

Assim sendo, não é difícil concluir que esse sistema fornece às empresas mais instruções para conformidade. Como a Lei de Cibersegurança visa proteger a soberania geral da rede, não é uma regulamentação conclusiva e completa dos direitos dos indivíduos, como proteção de dados e privacidade.[29] O sistema suplementar definitivamente beneficiará a implementação da Lei de Cibersegurança e, inevitavelmente, trará uma certa inconsistência e confusão quanto ao que seguir. Como documentos diferentes categorizam as informações pessoais de maneiras diferentes e estipulam diferentes níveis de proteção, as empresas podem ter dificuldade em seguir todas as instruções ao mesmo tempo. E, como mencionado acima, as cláusulas de exceção também diferem em cada documento. Isso pode ser difícil para as empresas quando elas precisam de justificação jurídica. E se elas precisam seguir todas as instruções, parece necessário ter um único regulamento geral em vez de dispersos.

Consequentemente, ao emitir vários documentos normativos complementares à Lei de Cibersegurança, a China estabeleceu um sistema multidimensional singular de proteção de dados. Os documentos, emitidos em diferentes etapas, podem ser uma ferramenta experimental que se adapta às mudanças rápidas da Internet. Mas também levanta outros problemas. Discussões adicionais se reúnem neste sistema único.

B. Um sistema multidimensional: melhor ou pior?

Como ilustrado acima, a China emprega um sistema multidimensional para regulação cibernética. Este item se concentrará no motivo pelo qual a China estabelece esse sistema específico na regulamentação de dados e em como ele poderia funcionar de maneira estável e eficaz.

B1. A compreensão do sistema: lições da prática

A Lei de Cibersegurança foi publicada no final de 2016, exatamente no período em que a China entrou na era do "4G +",[30] e a Internet estava começando a desempenhar um papel mais fundamental na vida cotidiana dos cidadãos. Além disso, 2016 também testemunha o nascimento de uma nova geração de tecnologia da informação e comunicação, representada por big data, inteligência, Internet móvel e computação em nuvem, que apenas havia começado a se integrar completa e profundamente em todos os campos da economia e da sociedade. Isso desencadeou uma preocupação com a possibilidade de a privacidade ser invadida pela difusão da tecnologia.

Nesse contexto, a Lei de Cibersegurança foi considerada importante e necessária. No entanto, nesse ponto, o formulador de políticas dificilmente poderia prever o futuro com o rápido desenvolvimento da tecnologia. Consequentemente, a linguagem da Lei de Cibersegurança é bastante geral, de modo a incluir o maior número possível de probabilidades, para que pudesse responder a condições futuras. Ao oferecer princípios básicos para o ambiente saudável da Internet, em vez de orientações detalhadas para as empresas, a Lei de Cibersegurança oferece aos tribunais um espaço mais flexível para a discricionariedade.

Com o lançamento do Regulamento Geral Europeu sobre a Proteção de Dados (doravante denominado "GDPR") publicado em maio de 2018, reguladores em todo o mundo aceleraram o processo da regulamentação de dados. Nesse contexto, nasceu a Especificação, que também é conhecida como a versão chinesa do GDPR. Nesse estágio inicial, a Especificação ofereceu aos operadores de rede uma expectativa razoável e instruções a serem seguidas. Também faz sentido o motivo pelo qual a Especificação é apenas um critério recomendado, pois serve como referência experimental e modelo de prática para empresas. O resultado do desenvolvimento do setor sob estas diretrizes gerais pode ser importante e referência para documentos normativos futuros. Obrigações muito rígidas para os operadores de rede podem dificultar o processo de inovação.

Portanto, ao abordar os problemas no mercado chinês da Internet em rápida mudança, os reguladores precisam de mais experiência experimental e estrutura flexível, em vez de políticas discricionárias. A experiência adquirida com a implementação da Especificação e os consecutivos documentos normativos preencheram a lacuna entre política e realidade, e poderia ser a base para a elaboração de uma diretriz com força jurídica.

B2. A tensão entre inovação e proteção da privacidade

A tensão entre inovação e proteção da privacidade também desencadeia o desenvolvimento desse sistema multidimensional.

A indústria da Internet é dinâmica. Portanto, o processo de elaboração de regras é sempre acompanhado pelo teste de equilíbrio entre segurança nacional, privacidade e inovação. Tais lutas podem ser claramente observadas a partir das normas. Por exemplo, o artigo 7.4 da Especificação dispõe que, quando um sujeito de informações pessoais, cujos dados são coletados, solicita acesso a informações que não forneceu voluntariamente, os controladores de informações pessoais podem considerar a solicitação de maneira abrangente, levando em consideração os riscos. ou danos aos direitos e interesses legais do sujeito que possam resultar da não resposta à solicitação, viabilidade técnica, custo e outros fatores na execução da solicitação. E depois que a decisão é tomada,

uma explicação da decisão deve ser fornecida.[31] Este é um acordo entre os interesses das empresas e a privacidade pessoal. Já no GDPR, os operadores devem fornecer os dados solicitados pelos usuários, embora possam cobrar por isso. Esta é uma parte importante do direito de acesso. Da mesma forma, na Diretriz, informações confidenciais como raça, etnia, opiniões políticas ou crenças religiosas não devem ser coletadas ou processadas em larga escala, mas isso é notavelmente fraco em comparação ao GDPR, que proíbe o processamento de dados sensíveis como um todo.[32]

Não é difícil concluir que os regulamentos de dados pessoais estejam cheios de testes de ajuste com base no objetivo do governo. Os detalhes de uma regra podem ser o jogo de interesse entre o coletor de informações e o titular dos dados. O sistema multidimensional realmente ajuda na realização do ajuste. Na falta de experiência acumulada na jurisprudência e no entendimento do setor, é difícil para os tribunais nacionais explicar e esclarecer melhor as regras gerais definidas na Lei de Cibersegurança. Por exemplo, para interpretar "ética nos negócios", "boa fé" e "responsabilidades sociais",[33] é sem dúvida necessária uma observação e um entendimento abrangentes do ecossistema do setor.

No entanto, se o papel do preenchimento de lacunas finalmente recair sobre os tribunais, que carecem da experiência real desse setor em desenvolvimento, o equilíbrio pode não ser perfeito. Portanto, o processo de elaboração de regras detalhadas pode assumir esse papel. Com rodadas de discussão sobre a Especificação, Medidas e Diretrizes, especialistas de todas as áreas podem ser reunidos para descobrir a solução. O processo de implementação desses documentos também pode ser uma boa chance para os tribunais domésticos observarem os resultados e obterem entendimento. Somente dessa maneira os julgamentos, especialmente aqueles relativos às cláusulas gerais da Lei de Cibersegurança, alcançam o objetivo de proteger os direitos e interesses dos cidadãos, pessoas jurídicas e outras organizações, e promover o desenvolvimento sólido da informatização econômica e social, conforme estabelecido no Artigo 1 da Lei de Cibersegurança.[34]

4. Conclusão

Este artigo se concentra basicamente no desenvolvimento da regulamentação chinesa sobre a proteção de dados pessoais no contexto da Lei de Cibersegurança. Além das inovações regulatórias e um padrão mais rígido para a coleta de dados, esse processo caracteriza o estabelecimento de um sistema multidimensional de proteção de dados.

Este sistema traz os benefícios de testar e ganhar experiência; no entanto, também sofre de uma inconsistência interior inevitável. O sistema misto e pouco claro pode afetar negativamente a realização do objetivo definido nesses documentos. Porque se as empresas não estiverem dispostas a seguir as regras, nenhuma experiência poderá ser adquirida. Portanto, é urgente configurar um sistema geral integrado de informações pessoais. O sistema multidimensional só pode ser utilizado temporariamente. Portanto, o artigo solicita uma reconciliação do sistema e uma legislação única integrada, que possa beneficiar as empresas da indevida carga de compliance.

Notas da autora

1 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018).

2 Shuju Anquan Guanli Banfa Zhengqiu Yijian Gao (数据安全管理办法征求意见稿) [Projeto de Medidas sobre Administração de Segurança de Dados] (promulgado pela Administração do Ciberespaço, em 28 de maio de 2019), (CHINALAWINFO).

3 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 76(5) (CHINALAWINFO).

4 *Id*. art. 76(5).

5 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), art. 3.1.

6 *Id*. app. § A.

7 *Id*. sec. 5.5, sec. 6.3.

8 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 41 (CHINALAWINFO).

9 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), art. 5.3.

10 *Id*.

11 *Id*. art. 5.5 (c).

12 *Id*. art. 5.5 (a), art. 5.5 (b).

13 *Id*. app. § B.

14 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 24 (CHINALAWINFO).

15 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), app. § B.

16 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 41 (CHINALAWINFO).

17 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), art. 5.2.

18 Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Diretriz para Proteção e Segurança de Informações Pessoais na Internet] (promulgada pelo Ministério da Segurança Pública em 10 de abril de 2019, em vigor a partir de 10 de abril de 2019), sec.2 (CHINALAWINFO).

19 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 42 (CHINALAWINFO).

20 Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Diretriz para Proteção e Segurança de Informações Pessoais na Internet] (promulgada pelo Ministério da Segurança Pública em 10 de abril de 2019, em vigor a partir de 10 de abril de 2019), sec. 5 (CHINALAWINFO).

21 Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Diretriz para Proteção e Segurança de Informações Pessoais na Internet] (promulgada pelo Ministério da Segurança Pública em 10 de abril de 2019, em vigor a partir de 10 de abril de 2019), sec. 6.1 (CHINALAWINFO).

22 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), art. 5.4.

23 Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Diretriz para Proteção e Segurança de Informações Pessoais na Internet] (promulgada pelo Ministério da Segurança Pública em 10 de abril de 2019, em vigor a partir de 10 de abril de 2019), sec. 6.6(b), 6.7(b) (CHINALAWINFO).

24 *Id.* Sec. 6.3(c).

25 *China Releases Draft Measures for Data Security Management*, INSIDE PRIVACY NET (28 de maio de 2019), https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administra tion-of-data-security/.

26 Shuju Anquan Guanli Banfa Zhengqiu Yijian Gao (数据安全管理办法征求意见稿) [Projeto de Medidas para a Administração da Segurança de Dados] (promulgado pela Administração do Ciberespaço, em 28 de maio de 2019), art.15 (CHINALAWINFO).

27 *Id.* art. 19.

28 *Id.* art. 28.

29 Sarah Wang Han; Abu Bakar Munir, *Information Security Technology – Personal Information Security Specification: China's Version of the* GDPR, 4 Eur. Data Prot. L. Rev. 535, 538 (2018).

30 *2016 Nian Zhonguo Hulianwang Chanye Zongshu Yu 2017 Nian Fazhan Qushi* (2016年中国互联网产业综述与2017年发展趋势) [*Visão geral do setor de Internet da China em 2016 e tendências de desenvolvimento em 2017*], XINHUA NET (06 de janeiro de 2017), http://www.xinhuanet.com//info/2017-01/06/c_1359612 49.htm.

31 Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 _个人信息安全规范) [Especificação sobre Segurança das Tecnologias da Informação e Segurança das Informações Pessoais] (promulgada pela Administração de Normalização, em 29 de dezembro de 2017, em vigor a partir de 1º de maio de 2018), art. 7.4.

32 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados), art. 9, 2016 O.J. (L 119) 1, 38.

33 Wangluo Anquan Fa (网络安全法) [Lei de Cibersegurança] (promulgada pelo Comitê Permanente do Congresso Nacional do Povo, em 7 de novembro de 2016, em vigor a partir de 1º de junho de 2017), art. 9 (CHINALAWINFO).

34 *Id*. art. 1.

Nota dos tradutores

A O governo chinês basicamente obriga todo mundo a fornecer nome real (normalmente junto com número de identidade) ao acessar a internet bem como outros serviços e conteúdos digitais. A justificativa oficial disso é pela segurança nacional e combate aos crimes, mas é de entendimento comum que isso também serve para facilitar a censura. A maioria dos sites e fornecedores de serviços e conteúdos digitais são obrigados a coletar estes dados pessoais e entregá-los ao governo quando exigido.