No Brasil, a tutela da privacidade e da proteção de dados pessoais está salvaguardada em dois dispositivos jurídicos: na Constituição Federal e no Código Civil. No caso da CF/88:

> **Art. 5°**. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

Por sua vez, o Código Civil (Lei 10.406/2002) prevê, em seu art. 21:

> **Art. 21.** A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma (Vide ADIN 4815).

Com o advento das **novas tecnologias de informação e comunicação (TIC)** e a aceleração dos processos na sociedade capitalista contemporânea, podemos dizer, hoje, que a produção de bens, o comércio e as finanças têm se digitalizado. Nesse contexto, não apenas as relações econômicas, mas também as pessoais, são marcadas pelo uso da tecnologia, motivo pelo qual à sociedade atual é dada a alcunha de **sociedade da informação**. Em razão desse aumento no fluxo de informações e uso dos dados pessoais com valor de mercadoria, não bastaram à regulamentação os dispositivos acima citados, sendo necessária uma legislação específica para **sopesar a proteção dos dados e a liberdade de expressão**.

Marcos normativos no ordenamento jurídico brasileiro

No Brasil, existem alguns marcos normativos importantes sobre esse tema, quais sejam:

- Lei nº 12.414/2011 (Lei do Cadastro Positivo);
- Lei nº 12.965/2014 (Marco Civil da Internet), que regula, em seu art. 3º, o uso da internet com base nos princípios da proteção da privacidade e dos dados pessoais; e
- Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet.

Antes de prosseguir, importante mencionar alguns **aspectos relevantes do Marco Civil da Internet**. O primeiro deles é a previsão de que sempre que estivermos diante de **operações de coleta, armazenamento, guarda e tratamento** de registros que envolvam dados pessoais, **aplica-se a legislação brasileira** e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, desde que preenchidos os seguintes requisitos:

- a) qualquer das operações ocorra em território nacional;
- b) quando pelo menos um dos terminais esteja localizado no Brasil; e
- c) quando houver oferta de serviço ao público brasileiro ou quando pelo menos um integrante do mesmo grupo econômico que realiza essas operações possuir estabelecimento no Brasil.

Como podemos ver, esses requisitos são abrangentes e alargaram o âmbito de atuação da legislação brasileira na proteção de dados.

Além disso, o Marco Civil da Internet menciona **direitos e garantias** gerais dos usuários da internet, sendo que o art. 7º direciona alguns deles à proteção da privacidade e dos dados pessoais, quais sejam:

- a) a **inviolabilidade da intimidade e da vida privada**, sua proteção e indenização pelo dano material ou moral em decorrência de sua violação;
- b) a **inviolabilidade e sigilo do fluxo de suas comunicações pela internet**, salvo por ordem judicial, na forma da lei;
- c) **inviolabilidade e sigilo de suas comunicações privadas armazenadas**, salvo por ordem judicial;
- d) o **direito a informações claras e completas** sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais. Neste caso, os dados pessoais somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação, ou quando este uso esteja previsto nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
- e) deve haver o **consentimento expresso** sobre coleta, uso, armazenamento e tratamento de dados pessoais, devendo ocorrer de forma destacada das demais cláusulas contratuais; e
- f) devem ser **excluídos definitivamente** os dados pessoais que forem fornecidos a determinada aplicação de internet pelo usuário, que fará esse requerimento ao término da relação entre as partes.

Há, contudo, a ressalva de que existem hipóteses de guarda obrigatória previstas no Marco Civil da Internet e na lei que dispõe sobre a proteção de dados pessoais (LGPD).

Guarda e Disponibilização

O Marco Civil da Internet prevê que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem preservar a intimidade, a vida privada, a honra e a imagem das pessoas direta e indiretamente envolvidas.

Nosso ordenamento adota o **modelo de retenção**, e não o de preservação de dados. Isso significa que a nossa lei obriga que os provedores guardem por algum período estes registros digitais, e não que a guarda apenas ocorra quando há ordem expressa para tanto.

A **disponibilização**, por sua vez, pelo provedor, dos dados pessoais que ele guarda, somente pode ocorrer por ordem judicial. Há, contudo, exceções, como os dados meramente cadastrais (nome, endereço, filiação), os quais podem ser solicitados por autoridades administrativas que detenham competência legal para requisição, na forma da lei. Apenas nos casos em que a lei prevê a autoridade administrativa pode fazer essa solicitação. Caso os provedores não obedeçam estas regras, ficam sujeitos à advertência, multa, suspensão e proibição da atividade.

Importante distinguir o que são **dados cadastrais**, **dados de conexão**, **dados de acesso** e **interceptação de conteúdo**. Dados cadastrais são informações mais simples que o usuário do serviço fornece ao provedor para acessá-lo. Já os registros de conexão têm a sua definição no art. 5º, VI do Marco Civil da Internet, e são o conjunto de informações que dizem respeito à conexão que o usuário efetuou, constando a data de início e término da conexão, tempo de duração e endereço de IP do usuário. Estes registros de conexão só podem ser fornecidos por ordem judicial. Em relação aos dados de acesso, estes são muito semelhantes aos dados de conexão, e se referem ao conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet, a partir de um determinado endereço de IP.

> **Art. 5º** Para os efeitos desta Lei, considera-se:
>
> (...)
>
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
>
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

A intercepção de conteúdo, por sua vez, diz respeito ao teor da comunicação em si (o que está sendo falado ou escrito). Esse tipo de informação também só pode ser obtido por meio de ordem judicial, mas em hipóteses muito mais restritas, ou seja, naquelas em que a lei estabelecer a finalidade de investigação criminal ou instrução processual penal. Quando pensamos que os provedores têm o dever de guardar os dados de conexão, estamos nos referindo à possibilidade de apenas individualizar o usuário, o tempo de serviço. Já em relação à interceptação de conteúdo, trata-se de uma hipótese muito mais séria, tendo em vista que a privacidade do usuário está exposta. Por tal motivo, ocorre em casos mais específicos, conforme prevê a CRFB/88:

> **Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

A guarda dos **registros de conexão** deve ocorrer pelo prazo de um ano, que pode ser aumentado a pedido da autoridade policial, administrativa ou do Ministério Público. A disponibilização efetiva, contudo, está adstrita à necessidade de ação judicial. Além disso, a guarda deve ser sigilosa, sendo vedado ao provedor a transferência da responsabilidade pela manutenção de dados dos registros a terceiros. No mais, é vedado aos provedores de conexão guardarem os registros de acesso a aplicações da internet. Isso significa que podem guardar apenas os dados de conexão, e não os acessos específicos. Esta seria a responsabilidade dos provedores de aplicação.

> **Art. 13.** Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
>
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.
>
> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.
>
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

> **Art. 14.** Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Os provedores de aplicação, então, são responsáveis pela guarda de **registro de acesso a aplicações** de internet e devem ser pessoa jurídica em exercício da atividade de forma organizada, profissionalmente e com fins econômicos. Essas pessoas têm o dever de guardar os dados de registro de acesso a aplicações pelo prazo de seis meses, de forma sigilosa, com exceção do que for determinado por ordem judicial. Este prazo também pode ser aumentado a pedido da autoridade policial, administrativa ou do Ministério Público, também vinculada a disponibilização efetiva do conteúdo à autorização judicial. Existem algumas vedações à guarda, como a impossibilidade de guardar registros de acesso de *outras* aplicações de internet sem que o titular dos dados tenha consentido previamente e de dados pessoais que sejam *excessivos* em relação ao serviço proposto pela aplicação.

> **Art. 15.** O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.
>
> § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

> **Art. 16.** Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
>
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

> **Art. 17.** Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

No mais, a Lei nº 13.344/2016 alterou o Código de Processo Penal para trazer um tipo de dado que merece proteção, que são os **dados de localização**. Em alguns casos, mediante autorização judicial, as empresas prestadoras de serviço de telecomunicação são obrigadas a fornecer informações sobre localização de vítimas ou suspeitos. Vale ressaltar que isso não é um permissivo para ter conhecimento do teor das comunicações, apenas os dados de localização.

> **Art. 13-B.** Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.