

A polícia pode forçar alguém a desbloquear o dispositivo móvel celular em uma busca pessoal?

Já se imaginou em uma situação em que você estava na rua e, durante uma busca, os policiais te obriguem a desbloquear o celular?

A questão tem gerado debates, tanto nas cortes brasileiras como dos Estados Unidos, conforme detalharemos a seguir.

Nos Estados Unidos, durante o início das discussões se a conduta dos policiais violava a quinta emenda, que veda a autoincriminação, os tribunais começaram a entender que as impressões digitais e o reconhecimento facial não se enquadravam no conceito de senha.

É posição da EFF (*Electronic Frontier Foundation*) que a descritografia forçada, seja por senha biométrica ou alfanumérica, deve ser protegida pela quinta emenda porque a descritografia é sempre testemunhal. A recomendação dos especialistas é que jamais se utilizasse apenas a biometria, mas uma senha forte.

No entanto, o entendimento dos tribunais está mudando e alguns julgados já entendem que obrigar o desbloqueio de um dispositivo usando dados biométricos é uma violação dos direitos da quinta emenda. Assim, os mecanismos biométricos de login passam a ter a mesma proteção. Juízes já entendem que impressões digitais e varreduras de rostos não são o mesmo que evidências físicas e, portanto, policiais não têm o direito de forçar suspeitos a se incriminarem.

Nesse sentido, em 2014, no caso *Riley vs. Califórnia*, a

Suprema Corte dos Estados Unidos decidiu pela necessidade de prévia ordem judicial para que a polícia pudesse validamente acessar o conteúdo de aparelhos celulares apreendidos em buscas incidentais e prisões.

Também em 2019, numa decisão histórica, uma juíza da Califórnia determinou que as autoridades não podem obrigar suspeitos a desbloquear o seu próprio smartphone usando impressão digital ou reconhecimento facial. Ainda, declarou que o governo não tinha o direito, mesmo com um mandado, de forçar os suspeitos a se incriminarem, destrancando seus dispositivos com suas características biológicas.

Em relação ao ato de forçar os fabricantes a destravarem os dispositivos, é importante destacar que a Apple e outros fabricantes têm resistido ao desbloqueio forçado.

Em 2016, o FBI, por meio de uma ordem judicial, obrigou a Apple a desbloquear o iPhone de Syed Rizwan Farook, o atirador falecido em um ataque terrorista em dezembro de 2015 em San Bernardino, na Califórnia (EUA).

A Apple alega que utiliza a criptografia para proteger os dados pessoais dos clientes porque acredita que é a única maneira de manter suas informações seguras.

Tim Cook, CEO da Apple, em uma carta aberta (<https://www.apple.com/customer-letter/>), diz que “não tem simpatia por terroristas”, e que a Apple, normalmente, coopera com pedidos oficiais para dados aos quais ela tem acesso. Contudo, o FBI quer que a Apple faça uma nova versão do sistema operacional do iPhone, contornando vários recursos de segurança importantes, e o instale em um iPhone recuperado durante a investigação.

No Brasil, o tema também já chegou nas cortes.

O Supremo Tribunal Federal, iniciou a discussão do Tema 977 da Repercussão Geral: “aferição da licitude da prova produzida

durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime”. O tema está em discussão no Recurso Extraordinário nº 1.042.075, da relatoria do ministro Dias Toffoli, que ainda não foi julgado.

O caso vem do Rio de Janeiro, onde o Tribunal de Justiça absolveu acusado por considerar ilícita a prova produzida após apreensão de seu telefone e acesso ao registro de chamadas e contatos, sem ordem judicial.

No STF, o relator Dias Toffoli entendeu que é lícita a prova obtida com o acesso a registro telefônico ou agenda de contatos do celular mesmo sem autorização judicial, por não configurar ofensa ao sigilo das comunicações, à intimidade ou à privacidade do acusado.

Contudo, há divergência já que os ministros Gilmar Mendes e Edson Fachin entenderam que a verificação dos dados contidos nos celulares depende de “prévia decisão judicial que justifique, com base em elementos concretos”, a necessidade e adequação da medida, bem como “delimite a sua abrangência”.

O caso, no entanto, não enfrenta, diretamente, o acesso forçado de policiais à senha ou a coação para que o suspeito destrave o equipamento.

No Superior Tribunal de Justiça, no Habeas Corpus nº 89.981/MG, a corte entendeu que o acesso a mensagens de WhatsApp, sem autorização judicial, fere o inciso X do art. 5º da Constituição Federal, e no caso determinou o desentranhamento das conversas do mensageiro dos autos.

No mesmo sentido, o STJ decidiu no Recurso em Habeas Corpus nº 101.119/SP, em dezembro de 2019:

RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. PRISÃO EM FLAGRANTE. ACESSO A DADOS CONTIDOS NO CELULAR DO RÉU. AUSÊNCIA

DE PRÉVIA AUTORIZAÇÃO JUDICIAL. ILICITUDE DAS PROVAS OBTIDAS. RECURSO EM HABEAS CORPUS PROVIDO. 1. Os dados armazenados nos aparelhos celulares – envio e recebimento de mensagens via SMS, programas ou aplicativos de troca de mensagens, fotografias etc. -, por dizerem respeito à intimidade e à vida privada do indivíduo, são invioláveis, nos termos em que previsto no inciso X do art. 5º da Constituição Federal, só podendo, portanto, **ser acessados e utilizados mediante prévia autorização judicial, com base em decisão devidamente motivada que evidencie a imprescindibilidade da medida, capaz de justificar a mitigação do direito à intimidade e à privacidade do agente.** 2. No caso, por ocasião da própria prisão em flagrante – sem, portanto, a prévia e necessária autorização judicial -, **o celular do réu foi apreendido, desbloqueado e nele verificada a existência de mensagens de texto que indicavam prévia negociação da venda de entorpecentes, sem, portanto, a prévia e necessária autorização judicial.** A autorização do juiz deferindo a quebra do sigilo das informações e das comunicações (como aplicativos, fotografias e demais dados armazenados nos aparelhos de telefonia apreendido) somente foi feita em momento posterior, já na audiência de custódia e, mesmo assim, sem nenhuma fundamentação concreta que evidenciasse a imprescindibilidade da medida. 3. Pelos documentos constantes dos autos, não se verifica nenhum argumento ou situação que pudesse justificar a necessidade e a urgência, em caráter excepcional, de as autoridades policiais poderem acessar, de imediato (e, portanto, sem prévia autorização judicial), os dados armazenados no aparelho celular do recorrente. Ao contrário, pela dinâmica dos fatos, o que se depreende é que não haveria nenhum prejuízo às investigações se os policiais, após a apreensão do telefone celular, houvessem requerido judicialmente a quebra do sigilo dos dados nele armazenados. 4. A denúncia se apoiou em elementos obtidos a partir da apreensão do celular pela autoridade policial, os quais estão reconhecidamente contaminados pela forma ilícita de sua colheita. Não é possível identificar, com precisão, se houve

algum elemento informativo produzido por fonte independente ou cuja descoberta seria inevitável, porquanto o contexto da abordagem do ora recorrente aliado à quantidade de drogas apreendidas e aos dados obtidos por meio do acesso ao celular do agente é que formaram a convicção do Parquet pelo oferecimento de denúncia pela possível prática do crime previsto no art. 33, caput, da Lei n. 11.343/2006. 5. A própria narrativa da dinâmica dos fatos coloca **sob dúvida o “consentimento” dado pelo réu aos policiais para o acesso aos dados contidos no seu celular, pois é pouco crível que, abordado por policiais, ele fornecesse voluntariamente a senha para o desbloqueio do celular e o acesso aos dados nele contidos.** 6. Recurso em habeas corpus provido, para reconhecer a ilicitude das provas obtidas por meio do acesso ao celular do recorrente, bem como de todas as que delas decorreram e, conseqüentemente, **anular** o Processo n. 0001516-27.2018 ab initio, sem prejuízo de oferecimento de nova denúncia, desde que amparada em elementos informativos regularmente obtidos. Em consequência, fica determinado o relaxamento da prisão cautelar imposta ao réu, por excesso de prazo.

(RHC 101.119/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, SEXTA TURMA, julgado em 10/12/2019, DJe 13/12/2019)

É importante mencionar que o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece os princípios, garantias e deveres para o uso da internet no Brasil, dispõe, no art. 7º, que: “O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.”

Na persecução penal, o acesso a dados pessoais de indiciados demonstra-se importante, principalmente nos crimes praticados

por organizações criminosas. Essa situação, inclusive, é uma exceção da aplicabilidade da Lei Geral de Proteção de Dados (LGPD), que prevê, nos termos do art. 4º, III, que a Lei não se aplica ao tratamento de dados pessoais realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Por outro lado, como visto, apesar da LGPD não se aplicar, deverão ser observadas as normas constitucionais e processuais penais. Neste sentido, não nos parece lícito que policiais não só acessem conteúdos privados em dispositivos móveis, sem ordem judicial expressa, como também que constriam ou forcem um indiciado a destravar o equipamento para fins de acesso ao conteúdo ali armazenado.

REFERÊNCIAS

<https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/?sh=1f66cf842b76>

[https://gizmodo.uol.com.br/fbi-ajuda-apple-atirador-base-naval-eua/#:~:text=Em%202016%2C%20o%20FBI%20conseguiu,%2C%20na%20Calif%C3%B3rnia%20\(EUA\)](https://gizmodo.uol.com.br/fbi-ajuda-apple-atirador-base-naval-eua/#:~:text=Em%202016%2C%20o%20FBI%20conseguiu,%2C%20na%20Calif%C3%B3rnia%20(EUA))

<https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898>

AUTORES

JOSÉ ANTÔNIO MILAGRE

(<https://app.exeed.pro/holder/badge/55319>) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo). Mestre e Doutorando em Ciência da Informação pela UNESP. Pós Graduado em Gestão de Tecnologia da Informação. Advogado com atuação em Direito Digital. Perito

Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP. Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários à Lei 12.975/2014 e Manual de Crimes Informáticos).

LAURA SECFÉM RODRIGUES

Advogada. Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

EMILY LUCILA DE OLIVEIRA

Consultora especializada em Privacidade e Proteção de Dados. Gerente de Direito Digital na José Milagre & Associados. Atuação em assessment e planos de adequação para empresas e órgãos públicos do Brasil, Vice-Diretora do IDCI – Instituto de Defesa do Cidadão na Internet, entidade focada na preservação dos direitos dos usuários de internet e titulares de dados pessoais.

Como implementar a LGPD na prática em 2021: 20 passos essenciais para adequação de empresas e negócios

Implantar a LGPD não se resume em criar uma “Política de Privacidade”!

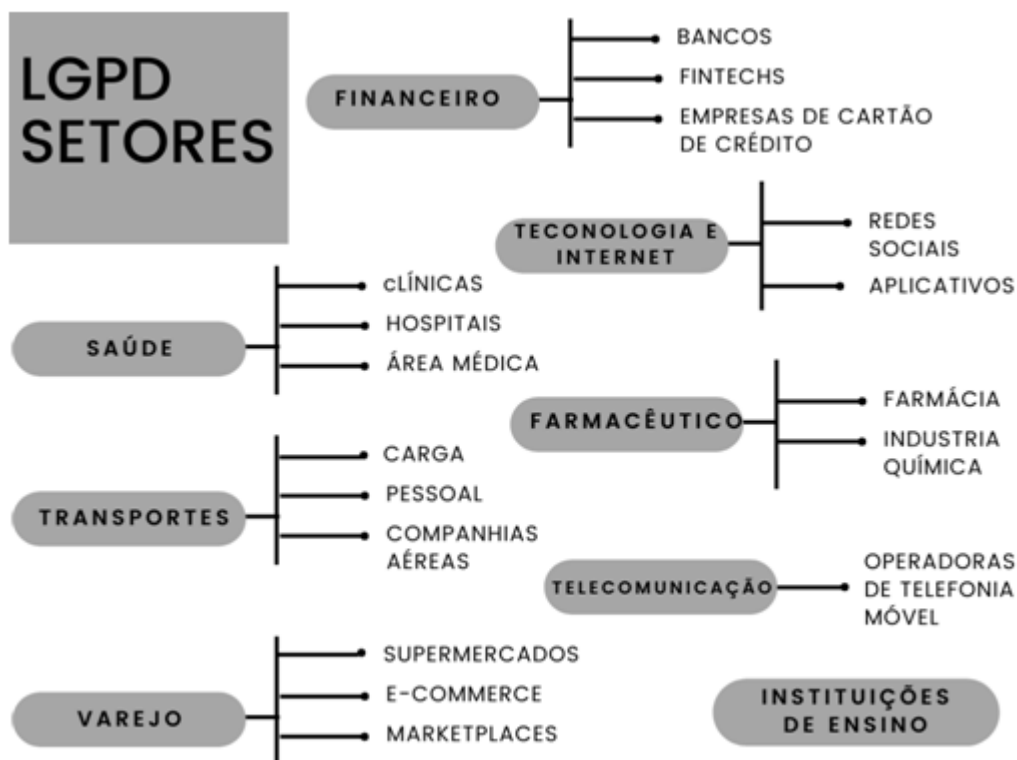
A Lei Geral de Proteção de Dados (Lei nº 13.709/18) já está em vigor desde setembro de 2020, trazendo direitos aos titulares de dados pessoais e deveres aos agentes de tratamento, sejam controladores ou operadores de dados pessoais.

Como estamos discorrendo de uma norma pendente de diversas regulamentações e fixações de posicionamentos por parte da Autoridade Nacional de Proteção de Dados (ANPD), muitos subjetivismos são considerados quando o tema é afirmar que se está em conformidade com a Lei, bem como quais os meios para que isso aconteça.

Porém, ao contrário do que parece, adequar-se à LGPD é muito mais do que mudar a política de privacidade da empresa. Envolve o desenvolvimento da cultura da privacidade nos processos corporativos, um programa de governança que trate de um sistema de gestão da privacidade da informação, com revisões de posturas, ações e processos.

É notório que empresas dos mais variados setores devem comprovar adequação à norma, sobretudo porque o tratamento de dados pessoais, hoje, é realidade nos negócios. Assim, preparamos 20 passos de adequação que auxiliarão empresas e negócios no processo de conformidade.

A adequação à LGPD deve ocorrer em diversos setores, incluindo, mas não se limitando a:



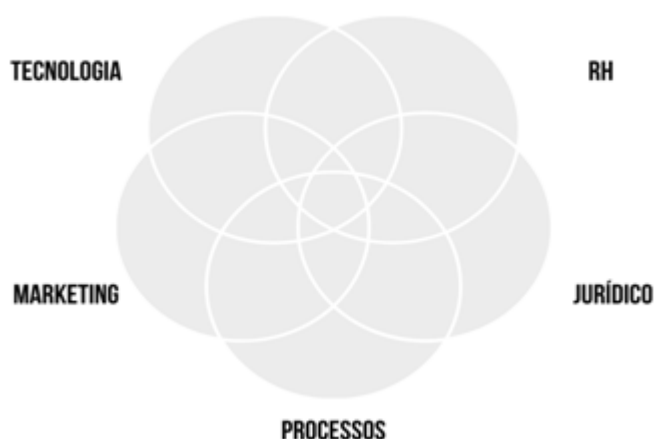
Conquanto alguns segmentos, naturalmente, em decorrência de suas atividades, acabam por tratar mais dados sensíveis e tenham processos mais críticos, nenhuma empresa deve ignorar a Lei, considerando ainda que as punições começam a ser aplicadas em agosto de 2021.

1. Quais áreas envolver?

Como visto, da mesma forma que a LGPD não é apenas uma Política de Privacidade, também não é somente uma revisão de regras do *firewall*, criptografia da base de dados ou implantação de permissionamentos de acesso ou política de mesa limpa.

É preciso deixar claro que a adequação da LGPD envolve inúmeras competências, ligadas comumente às áreas de tecnologia, como segurança da informação, jurídico, compliance

e time de processos ou projetos. Além disso, é o conjunto de ações, melhores práticas e processos que indicarão a maturidade do seu negócio em proteção de dados pessoais, e não apenas uma ação isolada de uma área específica da empresa.



Neste sentido, um processo de adequação deve considerar o apoio de todas as áreas e *keyusers*, que são definidos como peças-chave no projeto de adequação.

2. Realize a reunião de *Kick-Off* e crie o Comitê de Proteção de Dados

O início do projeto de adequação envolve a apresentação da equipe que será responsável pelos esforços.

Neste momento, é importante a participação de todos que serão canalizadores do projeto junto aos setores e áreas do negócio e que atuarão no *Assessment* inicial, ou seja, a fase em que se avaliará a empresa ou a instituição no que diz respeito à sua maturidade de controles envolvendo proteção de dados.

Na reunião, é apresentado como funcionará o programa, cronogramas, as próximas etapas e uma estimativa de esforço inicial para que as equipes se planejem (esta estimativa pode modificar-se após a avaliação).

Assim, é formalizada a abertura do projeto. Uma exposição é feita com os colaboradores para a conscientização sobre o projeto que se inicia. Além disso, dos *keyusers* poderá sair os nomes das pessoas que integrarão o comitê de proteção de dados na empresa, que se recomenda seja constituído logo no início do projeto.

3. Tenha em mente as macrofases do projeto

As macrofases são: ***preparação, organização, implementação, governança, e avaliação e melhoria.***

Na preparação, a empresa é avaliada e a estrutura organizacional inicial é formada para a criação de um programa de proteção de dados.

Na organização, são estabelecidas as estruturas organizacionais, planos de ação e os mecanismos necessários para suportar a privacidade e proteção de dados.

Na fase de implementação, os processos, medidas técnicas e organizativas entram em prática, aqui se inclui *privacyby design*, pseudonimização, anonimização, criptografia, controles de acesso, controles na contratação, segurança da cadeia de suprimentos, segurança física, novas políticas, novos aditivos, ativação de processos e capacitação/conscientização.

Na fase de governança, irá gerenciar aspectos do programa de proteção de dados, requerimentos dos titulares, gerenciará incidentes com dados, a avaliação, análise e gerenciamento de riscos, dentre outras ações.

E, por fim, na fase de avaliação e melhoria, a empresa revisará continuamente os controles e fiscalizará a manutenção do programa nas diversas áreas da empresa.

4. Conduza o *Assessment* Inicial

O *Assessment* Inicial é essencial e insumo para outras fases do processo de adequação, como o *mapping* dos dados e o registro das operações de processamento.

Nesta fase, os *keyusers*, tanto da consultoria LGPD como da empresa, irão avaliar “*in locu*”, mediante respostas de áreas e acessos nos aplicativos e áreas virtuais, as questões envolvendo as políticas, ações e controles existentes.

O objetivo da avaliação é analisar os regulamentos aplicados à empresa, identificando o impacto da privacidade no negócio, bem como entender quais são os dados pessoais tratados e o ciclo de vida deles, isto é, a forma de coleta, armazenamento, classificação e descarte.

5. *Mapping* e Inventário dos dados

A partir do *Assessment*, fase intimamente ligada, ainda, na macrofase de preparação é realizado o mapeamento e o

inventário de dados.

Data mapping ou mapeamento de dados é uma atividade de catalogação de todo o fluxo de dados pessoais que são objeto de qualquer operação de tratamento. O mapping pode ser mantido em sistemas eletrônicos, visto que facilita a tomada de decisões e a manutenção de registros.

Lembrando que o mapeamento de dados será um organismo vivo e deverá ser mantido sempre pela organização para cada novo ciclo de vida ou processo que faça o tratamento de dados pessoais.

Junto ao *data mapping*, é importante manter o inventário de dados que objetiva entender com detalhes a variedade dos dados tratados na empresa e categorizá-los, mensurar os riscos existentes e seus impactos, e servir como base para elaborar planos de ação mais direcionados e efetivos. É algo mais técnico, relacionado à granularidade de estruturas de campos.

Templates de Mapping podem ser encontrados em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>

6. *Gap Analysis*

A minha experiência em adequação de grandes varejos e redes sociais tem demonstrado que o *mapping*, se a estimativa de esforço não for bem direcionada, é uma das etapas mais demoradas do processo de adequação. Isso se deve também ao

fato de que diversos times, de outras inúmeras áreas de negócios, devem ser acionados para auxiliar o processo.

No entanto, quando adequadamente realizado, pode expor severas deficiências na empresa, como tratamentos irregulares, vulnerabilidades, bases legais equivocadas, ausência de definições claras quanto à retenção de dados, dentre outros riscos.

Neste momento, pós mapping, realizamos um relatório de *Gaps*, que são importantes insumos para os próximos passos, como o plano de ação e implementação.

7. Programa de proteção de dados e plano de ação

Na fase de preparação, também é importante a concepção do programa de proteção de dados.

Embora seja um conjunto de ações e práticas, recomendo sempre a documentação dele, constantemente revista, bem como a criação de um plano de ação com metas de implementação e ajustes. A empresa precisará definir:

- Periodicidade do **Status Report** do projeto;
- Como será o processo e sistemas que suportarão o armazenamento da documentação relativa à conformidade;
- Um plano de conscientização que preveja recorrência, ações, comumente prevendo atividades durante o ano;
- Um planejamento de ações “vivas” que serão mantidas e deverão ser atualizadas pós-consultoria.

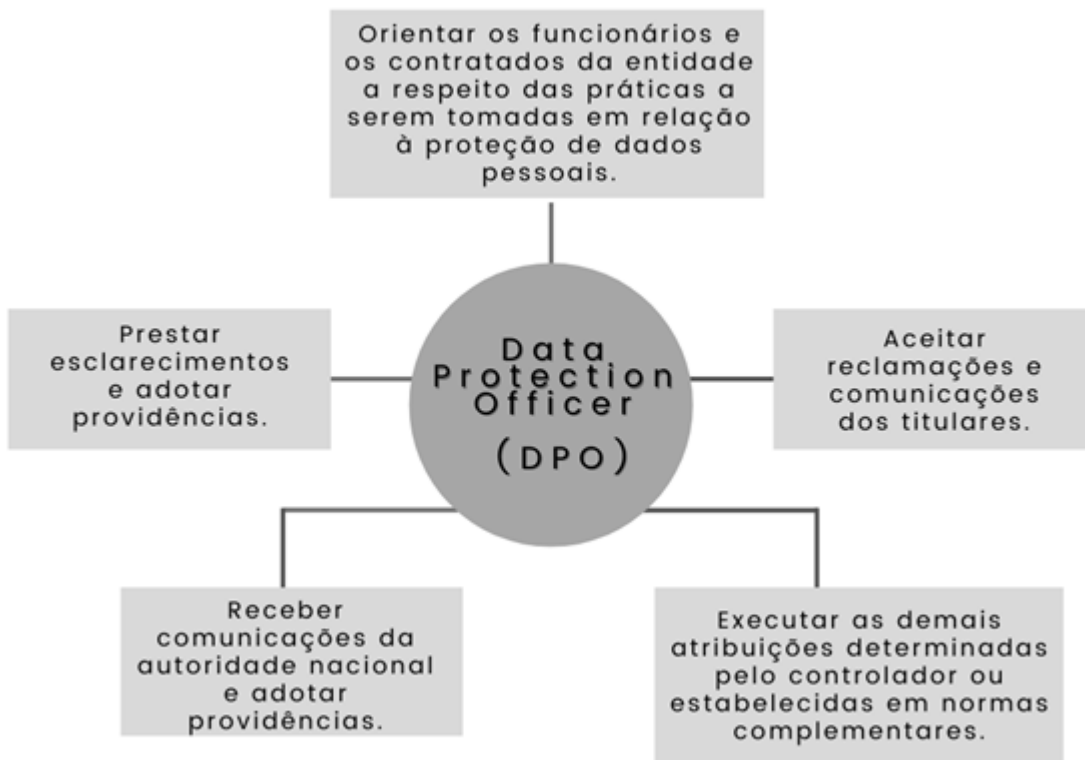
Documentamos estes itens, para que fiquem claros para os responsáveis pelo Comitê de Proteção de Dados e neste sentido eles terão um plano de ação definido.

8. Matriz de responsabilidades

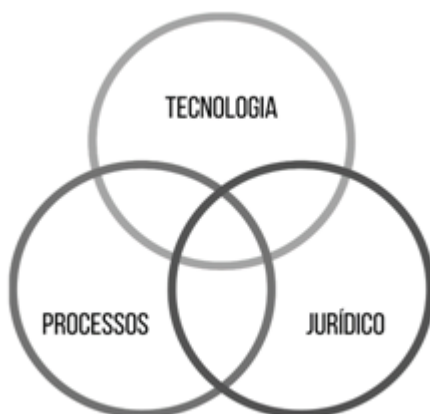
Já na fase de organização, é muito importante o estabelecimento da matriz de responsabilidades pela proteção de dados e privacidade. Nesta fase, também se define como manter os programas, as políticas e os controles de proteção de dados, além de definir e implementar como será mantido o envolvimento dos níveis táticos, operacionais e estratégicos da empresa.

9. Estabeleça o *Data Protection Officer* (DPO)

Na fase de organização é que estabeleceremos também o encarregado de proteção de dados, conhecido como Data Protection Officer (DPO), que desempenhará, dentre algumas atividades:



Mais uma vez, aqui, sobre as competências do DPO, entendo que este deva ter conhecimentos complementares, incluindo, mas não se limitando a conhecimento das áreas tecnologia, processos e jurídico:



10. Estabelecimento dos processos

É preciso criar, estabelecer e realizar a manutenção dos processos e procedimentos que garantam que as pessoas estão atuando nas melhores práticas de proteção de dados.

Assim, a elaboração de um plano de comunicação das ações, mudanças, novos ou atualização de processos existentes para considerar dados pessoais como “contratação de fornecedores”, “admissão”, “avaliação de riscos a privacidade”, planos de treinamentos, dentre outros, devem ser alinhados neste momento, não só com a criação de processos com fluxos claros, mas com o preparo dos profissionais que atuarão nas áreas e manterão estes “organismos vivos”. É importante integrar as ações de proteção de dados pessoais no dia a dia corporativo.

11. Políticas de Privacidade, Proteção de Dados e Contratos

Já na fase de implementação, um item atinente ao jurídico/compliance diz respeito à política de privacidade e proteção de dados pessoais.

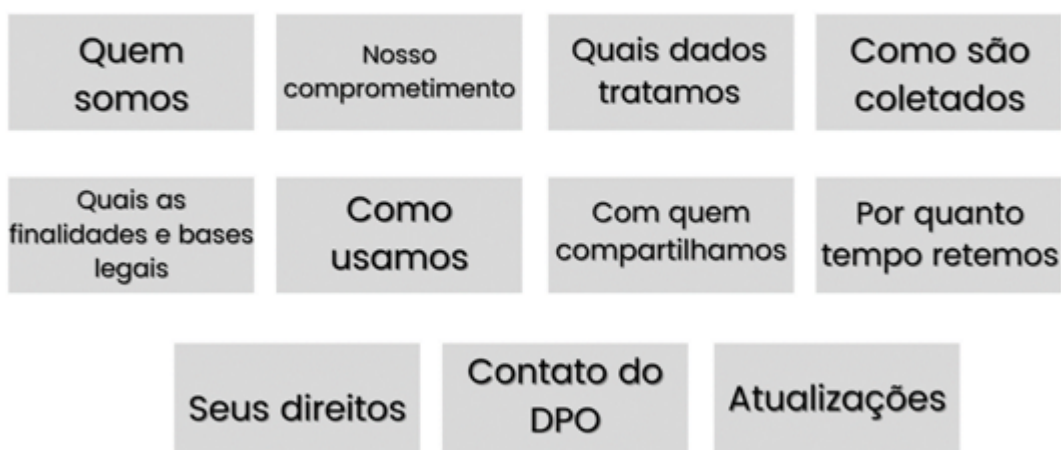
A política de privacidade é um documento externo, destinado ao público em geral. O seu objetivo é regulamentar o comprometimento da empresa em relação à proteção de dados pessoais, e deixar claro como realiza o tratamento dos mesmos.

É de boa prática que a partir da política de privacidade, estabelecem-se também tabelas e matrizes sobre dados tratados, finalidade e base legal.

Além disso, é importante destacar o contato com o encarregado de proteção de dados, para que o titular possa enviar

requerimentos e sanar dúvidas em relação à proteção de dados.

Tópicos de uma Política de Privacidade



Por sua vez, a política de proteção de dados é um documento interno, destinado à empresa, colaboradores, terceiros, e demais envolvidos no processo de tratamento de dados.

Trata-se de uma política que poderá ser regulamentada ou estratificada em outras normas e procedimentos. As normas estão relacionadas às regras básicas do que deve ser feito para observar determinado controle definido na política da organização. Já os procedimentos, detalham como deve ser implantado o controle.

Esta política prevê o que a empresa espera de profissionais e prestadores, inclusive prevendo sanções por descumprimento.

A política de privacidade e política de proteção de dados pessoais demonstram a transparência da empresa quando do tratamento de dados pessoais, observando o princípio da transparência, nos termos do art. 6º, VI, da LGPD.

Além disso, é importante a revisão jurídica dos contratos para que prevejam cláusulas que estabeleçam os deveres em relação ao tratamento de dados pessoais.

O esforço jurídico, neste momento, comumente se dá na elaboração de:

- Aditivos contratuais;
- *Data Processing Agreements*;
- Termos de comprometimento das empresas com a Política de Proteção de Dados.

12. Processo para aprovação de tratamento de dados pessoais

Qualquer nova operação, lançamento, *feature*, tela, sistema, ação, produto na empresa e que envolva o tratamento de dados pessoais deverá passar por um processo para análise e aprovação.

Comumente, este processo conduzirá os demandantes a necessidade de um Relatório de Impacto a Proteção de Dados (RIPD) ou não, de acordo com o que for identificado e critérios que devem ser transmitidos ao Comitê de Proteção de Dados.

Caso a empresa tenha decidido realizar o tratamento de dados, esta deverá seguir outro processo, o de privacidade por design. Pode ser necessário, neste aspecto, revisar bases legais ou revalidar consentimentos para tratamento de dados. Alguns itens e questionamentos revistos no conceito de privacidade por design de um novo serviço/processo/operação envolvem:

- É possível anonimizar os dados?
- É possível realizar o processo ou atingir as finalidades com menos dados pessoais?
- Quais técnicas de pseudonimização e criptografia disponíveis?
- O controle de acesso aos dados foi revisto?
- Revisão de interface para ativação de opções de privacidade por padrão;
- Como garantir os direitos dos titulares?

13. Implementação de medidas técnicas e organizativas

Na macrofase de implementação, inicia-se a adoção de medidas técnicas e organizativas para proteção de dados.

Como medidas organizativas, podemos citar, por exemplo, a classificação da informação, políticas e conscientização. Já as medidas técnicas envolvem controles, implementações e ações destinadas ao atendimento de diretrizes de segurança da informação aplicáveis aos dados, como criptografia, sistemas de proteção de dados, logging das atividades, dentre outros.

Recomenda-se, nesta fase, observar os requisitos e as diretrizes da norma ABNT ISO 27701 (Sistema de Gestão da

Privacidade da Informação), sobretudo, os requisitos e as diretrizes adicionais para controladores e processadores de dados.

A empresa não precisará implementar todos os controles, mas deverá selecionar adequadamente os necessários para proteção da sua atividade justificando a seleção. *Backups*, anonimização, registros de eventos, logs, revisões de minimização são executadas nesta fase.

14. Execute o plano de treinamento

A capacitação é uma boa prática e faz parte de um programa de proteção de dados. Ela envolve conteúdos direcionados às áreas específicas e insere elementos de conscientização para riscos envolvendo o tratamento de dados pessoais, levando em conta as atividades dos prestadores, colaboradores e terceiros. São ações comuns “ataques simulados”, treinamentos, cartazes, quizzes, questionários e outras formas de aumento da consciência sobre ameaças cibernéticas. Lembrando que “ações educativas” são previstas com boas práticas de governança no art. 50 da LGPD.

15. Processo para recebimento de solicitações e resposta a titulares

Esse é um dos passos prioritários de adequação. A empresa precisa disponibilizar para os titulares de dados um canal de contato para que possam realizar requerimentos e solicitações relativas a seus direitos previstos na norma.

Os direitos dos titulares de dados estão previstos no art. 18 da LGPD, que também assegura o direito de peticionar em face do controlador de dados pessoais, para exercitar os referidos direitos:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII – informação das entidades públicas e privadas com as

quais o controlador realizou uso compartilhado de dados;

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

- 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
- 2º O titular pode opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
- 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

Importante destacar que este requerimento será exercido sem custo algum ao titular de dados pessoais, nos prazos e termos que serão previstos em regulamento. A boa prática recomenda, inclusive, que o titular sempre seja informado do prazo para atendimento a sua solicitação.

Conforme previsto na LGPD, a confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular em formato simplificado, imediatamente; ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os

segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. A Legislação prevê, ainda, que os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

Neste contexto, é importante que a empresa entenda que não basta um formulário de contato ou um ajuste no SAC, mas efetivamente um processo interno que trate os requerimentos envolvendo dados pessoais, com papéis e responsabilidades definidas.

Nem sempre a empresa poderá atender os requerimentos dos titulares, mas é importante que esteja preparada, com uma boa fundamentação legal para explicar os motivos e que jamais deixe os requerimentos sem resposta.

É de suma importância manter os registros de todas as solicitações. A boa prática também vem prevista no controle A.7.3.9 da ISO 27701, destinado aos controladores, estabelecendo-se que *“A organização deve definir e documentar políticas e procedimentos para tratamento e respostas, a solicitações legítimas dos titulares de dados pessoais”*.

16. Plano de resposta a incidentes

Do mesmo modo, é importante já na macrofase de governança, que o agente de tratamento de dados pessoais estabeleça um plano e processo de resposta a incidentes envolvendo dados pessoais.

Este poderá estar integrado ao processo já praticado pelo time

de resposta a incidentes de segurança da informação, caso o processo já exista.

Um processo claro de como saber o que fazer e como agir diante de incidentes que comprometam dados pessoais é fundamental, até mesmo porque a LGPD estabelece em seu art. 48 que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Neste aspecto, cumpre destacar a Diretriz 6.13 da norma ISO 27701 que dispõe, dentre outros pontos que:

1. a) Convém que a empresa estabeleça responsabilidades e procedimentos para identificação e registro de violações de dados pessoais;
2. b) Procedimentos relativos à notificação para as partes envolvidas e autoridades, considerando a legislação;
3. c) Realize uma análise crítica, como parte de um processo de gestão da segurança da informação, para avaliar se medidas foram tomadas adequadamente.

Assim, a comunicação aos envolvidos e à Autoridade Nacional de Proteção de Dados (ANPD) deverá se dar nos moldes do art. 48 da LGPD e prever:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;

- os motivos da demora, no caso de a comunicação não ter sido imediata; e
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Vale mencionar que cláusulas que cubram a notificação de violação de dados pessoais sejam previstas para operadores de dados pessoais, a fim de que estes deem ciência aos controladores tão logo constatem um incidente.

Em todos os casos, é importante observar o controle 6.13.1.7 da ISO 27701, com o estabelecimento de um processo para coleta de evidências em casos envolvendo incidentes com dados pessoais.

17. Auditoria de risco e maturidade em proteção de dados

Nesta fase, é relevante conduzir uma auditoria independente envolvendo a implantação dos processos e a maturidade do sistema. É preciso olhar para o mercado, verificar o que os concorrentes estão implantando, priorizando, como a Autoridade de Proteção de Dados está agindo, avaliar o *baseline* do início do projeto e verificar o que, de fato, está implementado e funcionando desde então.

Aqui, a auditoria tem a função de avaliar o estágio de adequação e os riscos residuais. Para condução dela, alguns *frameworks* podem ser utilizados, como o *Privacy Maturity Model*.

: https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

18. Mantenha a documentação de privacidade organizada e atualize os termos

Um dos princípios previstos na LGPD é o da responsabilização e prestação de contas, que prevê a demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Neste sentido, todas as ações aqui trazidas, que podem conduzir a empresa para a conformidade, precisam ser gravadas, registradas, testadas e sua documentação organizada.

Além disso, o sistema de gestão da proteção de dados é um organismo vivo, com constantes atualizações, o que demandarão a revisão e custódia constante de registros e documentos relativos. *Softwares* de gestão de documentos, consentimento, logging, gestão de versão de políticas, dentre outros, podem auxiliar nestas atividades. Também, algumas suítes de sistemas de gestão da proteção de dados já centralizam a gestão dos documentos, o que pode facilitar.

19. Monitorar o sistema, Leis e relatar as desconformidades

Como visto, um sistema de gestão da privacidade da informação é algo vivo, ativo, em constante atualização. Documentos, práticas e ações devem ser revistos constante e periodicamente.

O DPO, com apoio do Comitê Interno de Proteção de Dados, tem esta tarefa de coordenar as atualizações, monitorar o sistema,

acompanhar a evolução de entendimentos, legislativa e regulatória e zelar para que os processos internos estejam em conformidade, relatando desconformidades e adotando medidas para adequação, no âmbito de suas competências.

Análises críticas e técnicas de compliance são práticas previstas no controle 6.15.2.4 da ISO 27701 e envolvem, inclusive, monitoramentos contínuos e testes específicos de vulnerabilidade e invasão, como os *pentests*, ou testes de reversão de anonimização, técnicas que também são consideradas boas práticas para “se comprovar” a segurança de sistemas que tratam dados pessoais, tendo-se em mente que nos termos da LGPD, tratamento irregular não é só aquele que deixa de observar a legislação, mas que não fornece a segurança que o titular dele poderia esperar.

20. Atue nas prioridades enquanto desenvolve as outras frentes!

Alguns itens são considerados prioritários no processo de adequação. Significa dizer que enquanto a empresa avança nas fases-macro, pode ter um olhar especial para estes itens, considerados prioritários. Dentre as prioridades estão:

- constituição do comitê de proteção de dados;
- nomeação de um DPO;
- estabelecimento do plano de ação e programa de proteção e dados;
- criação do processo e área para requerimentos do titular;
- revisão das políticas de privacidade;
- avaliação inicial de segurança.

Outras atividades ainda podem ser listadas como prioritárias, de acordo com contexto e atividades de tratamento. Seja como for, é importante avançar nas ações de adequação, considerando que a Lei já está em vigor e as penalidades podem ser aplicadas a partir de agosto 2021.

Conclusões

Como visto, negligenciar a adequação do negócio à LGPD pode ser um erro e irá interferir nas negociações realizadas, visto que os produtos e serviços deverão ostentar um padrão de segurança e proteção de dados esperados. Além disso, com o avanço da tecnologia, amplificam-se os riscos e elevam-se as preocupações quanto a encontrar soluções de segurança adequadas.

Porém, seguindo as ações descritas neste guia, é possível avançar rumo à conformidade, realizando as ações necessárias e que atendem boa parte dos requisitos legais, com economia e eficiência.

O presente artigo elenca 20 passos que, se adotados, cobrem, significativamente, parte das ações ligadas ao processo de adequação.

Adequar-se é necessário. A adequação à LGPD não deve ser encarada somente como um rito obrigatório, mas como uma oportunidade de inovação e mudança de cultura, a fim de elevar o padrão da empresa, gerando valores sólidos voltados à proteção de dados pessoais.

Canvas compliance model

Elaboramos um mapa em formato Canvas, que traz um modelo mental de questões que a empresa deve fazer, e com isso, não negligenciar nenhuma ação necessária para que siga nas fases da adequação, descritas no mapa. O modelo auxilia empresas a seguirem uma sucessão ordenada de atos para a correta implementação. Para requerer o seu se inscreva no canal @josemilagre e conecte-se conosco. Acesse também nosso grupo de DPOs no Facebook <https://www.facebook.com/groups/lgpdbrasil/>

Como implementar a LGPD? CyberExperts Consultoria

A CyberExperts Consultoria é referência em projetos de adequação de negócios à LGPD, bem como na implementação de Sistemas de Gestão de Proteção de Dados, em conformidade com a ISSO 27701. Também oferecemos programas de conscientização e capacitação para empresas e órgãos públicos. O PrivacyOfficer é um programa de DPO *as a service*, para auxiliar negócios e agentes de tratamento nas questões envolvendo proteção de dados.

Solicite uma apresentação gratuita sobre a adequação LGPD aplicável ao seu negócio, ou conheça nossos treinamentos na área de proteção de dados: Acesse: www.cyberexperts.com.br

Sobre o autor: **José Antonio Milagre** (<https://app.exeed.pro/holder/badge/55319>) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo), Mestre e Doutorando em

Ciência da Informação pela UNESP, Pós Graduado em Gestão de Tecnologia da Informação, Advogado com atuação em Direito Digital, Perito Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários a Lei 12.975/2014 e Manual de Crimes Informáticos).

Algumas participações na imprensa:

<https://ww1.folha.uol.com.br/cotidiano/2018/07/comissao-da-cmara-aprova-juizado-especial-para-crime-cibernetico.shtml>

<https://oglobo.globo.com/economia/tecnologia/como-voce-era-ha-10-anos-brincadeira-no-facebook-pode-trazer-riscos-sua-privacidade-23377262>

<https://cio.com.br/quando-os-algoritmos-falham-e-o-combate-as-fakenews-causa-outros-danos/>

Colaboradora: **Laura Secfém Rodrigues**. Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

© 2021

Crimes Digitais, a Omissão das Operadoras de Telefonia Móvel e a Impunidade

Conforme o disposto no Marco Civil da Internet (Lei nº 12.965/14), qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Do mesmo modo, os provedores de telefonia móvel são responsáveis pela guarda dos chamados registros de conexão, sendo eles 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.

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 com segurança, pelo prazo de 1 (um) ano, nos termos do Marco Civil da Internet. De outra ordem, não se impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

Como previsto no Marco Civil da Internet:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

A prática de inúmeros crimes cibernéticos vem sendo estimulada por condutas negligentes das operadoras de telefonia móvel. O golpe da clonagem de Chip, o “*sim swap*” figurou como um dos principais golpes de 2018 a 2020 e, nitidamente, reflete a falha das operadoras de telefonia em checar a autenticidade de pessoas que solicitam trocas de chips, a partir de dados coletados de clientes.

O resultado são inúmeros processos movimentando o Poder Judiciário, sendo que muitos responsabilizam as operadoras por não adotarem os critérios de segurança para avaliar a integridade de uma solicitação.

Mas não é só neste fato que as operadoras vêm protagonizando condutas impensadas e que prejudicam cidadãos e vítimas de

crimes digitais. Como se sabe, o cadastramento de chips pré-pagos é obrigatório no Brasil, considerando que, do contrário, seriam usados (como foram) por pessoas má intencionadas para acesso à rede e prática de crimes, sem que fossem identificadas.

O Judiciário já entende que a não adoção de procedimentos para verificação do cadastro de quem solicita um plano ou chip pode responsabilizar o provedor de telefonia.

Igualmente, encontramos decisões que condenam as operadoras por não apresentarem dados cadastrais, ligados a um número telefônico, permitindo que um criminoso cibernético jamais seja identificado.

Sobre o tema, cumpre colacionar as seguintes decisões:

EMENTA: JUIZADO ESPECIAL. CONSUMIDOR. TELEFONIA. PRELIMINARES. LEGITIMIDADE PASSIVA DO WHATSAPP. ILEGITIMIDADE PASSIVA DA OPERADORA DE TELEFONIA. PRELIMINARES REJEITADAS. CLONAGEM DE LINHA TELEFÔNICA. FALHA NA PRESTAÇÃO DOS SERVIÇOS. DANO MORAL CONFIGURADOS. [...] 3. Por outro lado, a empresa de telefonia recorrente se mostra parte legítima para figurar no polo passivo da ação, tendo em vista ser a responsável direta pela disponibilização e manutenção da linha telefônica do recorrido, que foi alvo de clonagem. [...] 4. Verifica-se dos documentos juntados aos autos que o autor/recorrido foi vítima de ações de estelionatários, por meio de técnica conhecida como SIM SWAP, que consiste no repasse pela operadora do número de telefone do usuário para um novo chip, que está em posse de criminosos, possibilitando a invasão de aplicativos de trocas de mensagens, internet banking e também acesso a informações privativas. Esta técnica pode ser empregada a

partir do fornecimento de dados pessoais do usuário pelo estelionatário para o atendente da operadora, convencendo-o a operar a troca do chip do celular, ou ainda, com a participação de criminosos dentro da própria operadora, com a troca da linha telefônica diretamente nos sistemas da empresa de telecomunicações. 5. Em ambas as hipóteses, está configurada a falha na prestação dos serviços de telefonia celular, uma vez que a fragilidade da segurança da empresa, no caso, possibilitou a ação de criminosos que utilizaram a linha telefônica do autor para enviar mensagens falsas para seus contatos, conforme noticiado em ocorrência policial (ID15838538), gerando danos ao consumidor, o que faz incidir o enunciado no art. 14, § 1º, inciso II, do CDC. 6. A fraude operada gerou aborrecimentos, indignação e angústia que refogem aos meros aborrecimentos do cotidiano, sobretudo diante do descuido com os dados do autor, cujo sigilo violado causou-lhe também prejuízos à sua imagem e honra, já que possibilitou que estelionatário, passando-se pelo autor, enviasse mensagens aos seus familiares, amigos e colegas de trabalho pedindo contribuições financeiras, sob a alegação de estar em dificuldades, fatores esses que caracterizam o dano moral e, conseqüentemente, o dever de indenizar [...]

(TJDFT, [Acórdão 1276175](#), Processo 07292427920198070016, Relatora: SONÍRIA ROCHA CAMPOS D'ASSUNÇÃO, j. 14/8/2020).
(g.n.)

EMENTA: RECURSO INOMINADO. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS E MATERIAIS. PRELIMINARES DE INCOMPETÊNCIA E DE ILEGITIMIDADE PASSIVA AFASTADAS. SERVIÇOS DE TELECOMUNICAÇÃO. GOLPE DE CLONAGEM DE CHIP. SIM SWAP. ILÍCITO CARACTERIZADO PELA AUSÊNCIA DE SEGURANÇA NO SISTEMA DA OPERADORA. CULPA EXCLUSIVA DE TERCEIRO NÃO VERIFICADA. DANOS MORAIS CONFIGURADOS EM DECORRÊNCIA DA INEFICIÊNCIA DOS SERVIÇOS PRESTADOS PELA TIM. QUANTUM INDENIZATÓRIO ARBITRADO EM R\$ 4.000,00 QUE COMPORTA MAJORAÇÃO PARA R\$ 8.000,00. RECURSO RECLAMADA CONHECIDO E DESPROVIDO. RECURSO RECLAMANTE CONHECIDO

E PROVIDO. (TJPR, Processo 0085357-55.2018.8.16.0014, Relatora: Juíza Manuela Tallão Benke, j. 19/06/2020). (g.n)

EMENTA: APELAÇÃO CÍVEL. AÇÃO INDENIZATÓRIA POR DANOS MATERIAIS E MORAIS, COM PEDIDO DE ANTECIPAÇÃO DE TUTELA. SERVIÇO DE TELEFONIA MÓVEL. FRAUDE. CLONAGEM DE CHIP DO CELULAR DO PRIMEIRO AUTOR, ORA APELADO, QUE PERMITIU O ENVIO DE MENSAGENS PELO FALSÁRIO A AMIGOS E PARENTES DO PROPRIETÁRIO DA LINHA, OPORTUNIDADE EM QUE A SEGUNDA AUTORA FOI LEVADA A DEPOSITAR QUANTIA EM DINHEIRO NA CONTA CORRENTE DO GOLPISTA PENSANDO ESTAR AJUDANDO SEU PRIMO. SENTENÇA DE PROCEDÊNCIA DO PEDIDO EXORDIAL ATACADA POR RECURSO DE APELAÇÃO DA RÉ.

EXTORSÕES FEITAS VIA WHATSAPP QUE SEGUEM UM MÉTODO DENOMINADO SIM SWAP, TÉCNICA QUE CONSISTE EM TRANSFERIR A LINHA DO CHIP DE UM USUÁRIO PARA UM CHIP EM BRANCO. GOLPE QUE FREQUENTEMENTE ENVOLVE UM FUNCIONÁRIO DA OPERADORA QUE TENHA ACESSO AOS SISTEMAS QUE, EM CONLUÍO COM O FRAUDADOR, PERMITE A TROCA DA LINHA NO CHIP OU DECORRE DA UTILIZAÇÃO DE DOCUMENTOS FALSOS, QUANDO O FALSÁRIO SE FAZ PASSAR PELO PROPRIETÁRIO DA LINHA E SOLICITA JUNTO À OPERADORA A HABILITAÇÃO DA LINHA DO CONSUMIDOR NO CHIP EM BRANCO. PATENTE A OCORRÊNCIA DE FRAUDE NA HIPÓTESE EM TELA A ENSEJAR A FALHA DA EMPRESA QUE NÃO SE CERCOU DE CUIDADOS PARA EVITAR QUE SITUAÇÕES COMO A NARRADA NOS PRESENTES AUTOS ACONTEÇAM. CLONAGEM DO TELEFONE CELULAR QUE DEMONSTRA A VULNERABILIDADE DO SERVIÇO PRESTADO PELA CONCESSIONÁRIA, SENDO CERTO QUE SEUS RISCOS NÃO PODEM SER TRANSFERIDOS AOS CONSUMIDORES, DEVENDO A EMPRESA ASSUMIR A RESPONSABILIDADE PELAS SUAS CONSEQUÊNCIAS, BEM COMO, OS PREJUÍZOS SOFRIDOS. [...]. RECURSO DESPROVIDO (TJRS, Proc. 0068797-30.2017.8.19.0001, Des. AUGUSTO ALVES MOREIRA JUNIOR, j. 28/05/2019) (g.n)

Apesar de o Marco Civil da Internet impor alguns deveres e o

Judiciário amadurecer ao tratar da responsabilidade dos provedores de conexão na apuração da autoria, novos desafios surgem diariamente e clamam a atenção de autoridades de aplicação da lei, sob pena de se privilegiar um ambiente anônimo e perigoso.

As linhas pré-pagas são comercializadas de acordo com a Resolução da Anatel nº 477/07. É sabido que é responsabilidade dos titulares efetuar o cadastramento das linhas pré-pagas. No Brasil, a Lei nº 10.703/2003 estabelece este dever de cadastramento. **Ocorre que um criminoso pode se valer de um chip pré-pago ativado, sem qualquer cadastro, por alguns dias, até que a operadora suspenda o número. E isto, infelizmente, vem ocorrendo com frequência.**

É neste lapso que o anonimato pode ser “garantido”. Na chamada ***lacuna do ciclo de ativação***, que pode durar dias. Um apagão na coleta de dados mínimos necessários. Um criminoso digital não precisa de mais de algumas horas para acessar a rede, criar contas em redes sociais e serviços e/ou publicar conteúdos ofensivos. Imagine então, podendo utilizar um chip por 24 horas, sem qualquer cadastro, até que o mesmo seja suspenso ou cancelado?

Desse modo, em inúmeros processos no Judiciário brasileiro, para apuração de titulares de linhas telefônicas, operadoras estão usando justificativa de que ***“não possuem em seus sistemas os dados cadastrais relacionados à linha telefônica”***. Ainda, chegam a afirmar que apresentaram os dados cadastrais que possuíam, ou seja, nada.

Para determinados casos, crimes e golpes envolvendo o comunicador WhatsApp, mais uma razão para que WhatsApp INC não

ofereça resistência a apresentar os registros de acesso a aplicação de usuários, a partir de números fornecidos em juízo, pois, além dos casos de chips criados em nome de terceiros, pode ocorrer de a operadora de telefonia não ter nenhum dado de cadastro do chip, pela lacuna no ciclo de ativação, sendo os dados do comunicador a única forma para se tentar apurar a autoria de crimes de informática, ataques, ameaças, golpes...

Portanto, embora a manutenção dos registros de acesso a aplicação ou conexão sejam uma obrigação do Marco Civil da Internet, os dados cadastrais das linhas pré-pagas são definidos em Lei Federal, e, muito embora, as operadoras dependam do cadastramento por seus assinantes, não podem permitir linhas ativas anônimas, ainda que por curtos períodos de tempo, o suficiente para a prática cibernética delitativa e sem formas de rastreamento.

O lapso de anonimato no ciclo de ativação de uma linha pré-paga pode incentivar a prática de crimes digitais, impedir a apuração da autoria e, nitidamente, favorecer a impunidade. As operadoras não podem apresentar relatórios em branco, após ordem judicial, dizendo que “apresentaram o que tinham”.

Anatel, Legislativo e Judiciário precisam atentar para este risco, com urgência, adotando medidas que impeçam que as operadoras acobertem maus usuários, sem qualquer consequência.

Currículos:

José Antonio Milagre, Perito especialista em Crimes

Cibernéticos, Analista de Sistemas, Diretor da consultoria CyberExperts, Advogado especialista em Direito Digital e Proteção de Dados, Mestre e Doutorando em Ciência da Informação pela UNESP, DPO EXIN, Presidente da Comissão de Direito Digital Regional Vila Prudente da OAB/SP e Membro da Diretoria do Instituto de Defesa do Cidadão na Internet – IDCI Brasil. <https://www.direitodigital.adv.br> Instagram: @drjosemilagre

Laura Secfém Rodrigues: Graduada em Direito, pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE). Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Atuação em assessment e planos de adequação para empresas e órgãos públicos do Brasil.

Emily Lucila de Oliveira. Consultora especializada em Privacidade e Proteção de Dados. Gerente de Direito Digital na José Milagre & Associados. Atuação em assessment e planos de adequação para empresas e órgãos públicos do Brasil, Vice-Diretora do IDCI – Instituto de Defesa do Cidadão na Internet, entidade focada na preservação dos direitos dos usuários de internet e titulares de dados pessoais.

FAKE NEWS! Vulnerabilidades do armazenamento da cadeia de

contatos dos serviços de mensageria (PL 2630)

O Especialista e Perito em crimes cibernéticos, José Milagre, fala à Folha SP sobre os malefícios da medida e a importância dos provedores na contribuição para identificar os criminosos.

Acompanhe

em:

<https://www1.folha.uol.com.br/poder/2020/07/regra-para-armazenar-cadeia-de-mensagens-do-whatsapp-pode-ser-ineficaz-em-projeto-de-fake-news-no-congresso.shtml?fbclid=IwAR3KjFnigHxi3nmZPjVDwgAiKYfFTj50paQdRNQdUqRILfcCR58TJ80TPMY>

O Especialista em Crimes Cibernéticos e Perito Digital, José Milagre, fala à CNN Brasil sobre o vazamento de dados no MS.

Em um bate papo com a Jornalista [Monalisa Perrone](#), para o “E tem mais”, o Especialista em Crimes Cibernéticos e Perito Digital, José Milagre, fala sobre o vazamento de dados no Ministério da Saúde.

No mesmo ano em que entra em vigor a Lei Geral de Proteção de Dados, o Ministério da Saúde protagonizou dois grandes vazamentos de informações pessoais de pacientes. O primeiro deles revelou os dados de 16 milhões de pessoas que tiveram Covid-19, entre eles o presidente Jair Bolsonaro e o governador do Estado de São Paulo, João Doria. O segundo foi ainda maior, e tornou públicas informações como nome, endereço e até RG de mais de 200 milhões de brasileiros cadastrados no SUS.

Afinal de contas, como instituições públicas e privadas podem ser responsabilizadas pelo vazamento de dados? Elas já respondem à lei de proteção de dados?

Para saber como agir, caso tenha seus dados vazados, acesse:

https://www.cnnbrasil.com.br/tecnologia/2020/12/10/nova-lei-de-protecao-de-dados-e-a-vulnerabilidade-das-informacoes-na-rede?fbclid=IwAR1j8nffcT-1k3L86035x_z4bMsWQSLUKCx6mNW2_m4Mm1kefMjcPIQ6wJY

Home Office causa aumento de crimes digitais no Brasil

Com a pandemia muitas empresas migraram de seus ambientes corporativos para os chamados Home Office, ou Teletrabalho, no entanto, esta nova realidade trás vulnerabilidade aos dados

empresariais que ficam a mercê dos criminosos.

Saiba os detalhes para proteger sua empresa acessando:
<https://www.gazetasp.com.br/brasil/2020/12/1080963-brasil-sofr-eu-mais-de-34-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2020.html>

Vendas pela internet podem facilitar fraudes na Black Friday; veja como evitar

Você costuma fazer compras pela internet? Sabe como conferir a autenticidade dos sites? Como se proteger para não cair em golpes? O Especialista em Direito Digital e Crimes cibernéticos, José Antonio Milagre, fala sobre os cuidados que devem ser adotados durante as compras e o cenário atrativo para os criminosos durante o período de grandes descontos, como a Black Fryday.

Saiba mais em:
<https://jovempan.com.br/noticias/brasil/vendas-pela-internet-podem-facilitar-fraudes-na-black-friday-veja-como-evitar.html>

O novo sistema de transferência bancária está dando o que falar! Já cadastrou a sua chave Pix? O Especialista, José Milagre da dicas para fazê-lo com tranquilidade

O Especialista em Crimes Digitais e Perito em Informática falou ao Gazeta do Povo sobre o novo sistema de transferência bancário, o Pix, você já está por dentro desta nova tecnologia? O Especialista fala sobre a segurança da ferramenta e como se proteger dos golpes que podem surgir.

Para saber mais detalhes acesse:
<https://www.gazetadopovo.com.br/economia/chave-pix-armadilhas-no-uso-de-dados/>

Black Friday 2020: Especialista em crimes

digitais, José Antonio Milagre, orienta como evitar golpes virtuais e como agir caso tenha sido vítima.

Mais uma BlackFriday se aproxima e com ela o oportunismo de criminosos cibernéticos, que usam de técnicas variadas para aplicação de golpes, explorando muitas vulnerabilidades dos consumidores virtuais, que desatentos, acabam fornecendo dados pessoais ou comprando em páginas falsas, que são criadas apenas pelo período necessário para tirar o dinheiro do consumidor. Esta edição, porém, promete ser maior por conta do isolamento social diante da COVID-19. Segundo a Ebit Nielsen, as vendas devem crescer 27% em comparação com a edição de 2019.

Os criminosos digitais têm criado “lojas iscas”, normalmente hospedadas em servidores no exterior. Do mesmo modo, ocultam os dados do registrante, por meio de registros “*domain by proxy*”, tudo para dificultar a investigação de quem está por trás do e-commerce “simulado”.

Rapidamente investem em anúncios nos buscadores e outros métodos de impulsionamento, incluindo redes sociais e rapidamente ficam bem ranqueados na rede. A vítima então se depara com o anúncio, normalmente com preço fora do comum. Se não se atentar para elementos visuais da página ou dados de contato da loja, acaba acreditando que está fazendo um bom negócio, e nunca mais verá seu dinheiro.

As lojas falsas, normalmente se valem de depósito bancário ou boletos, que dificultam o cancelamento das compras ou o rastreamento do dinheiro. Assim, todo o cuidado é pouco no período de promoções, já que o crime digital brasileiro explora momentos de grande mobilização digital para auferir lucro, lesando pessoas.

O advogado e perito especialista em crimes cibernéticos, José Antonio Milagre, CEO da CyberExperts e Diretor do Instituto de Defesa do Cidadão na Internet (IDCI) apresenta estratégias para se proteger de golpes digitais e dá dicas sobre como agir, caso tenha sido vítima de fraudes e crimes cibernéticos na BlackFriday.

Dez estratégias para que não que seja vítima de golpes digitais na BlackFriday:

1) Cuidado com descontos absurdos. Embora seja BlackFriday, 90% de desconto é algo estranho de se ver. Cuidado, confira a média de preço dos produtos. O criminoso vai usar este gatilho para chamar sua atenção;

2) Avalie a reputação da Loja. Em um universo de aproximadamente 1 milhão de lojas virtuais, muitas delas podem ser “lojas iscas”, criadas para ficar no ar por pouco tempo, fazer centenas de vítimas e desaparecer. Portanto, pesquise se a loja tem “histórico”, comentários, outras compras, etc. O Google está aí para isso;

3) Avalie as formas de pagamento. Desconfie de lojas que só oferecem depósito bancário, boleto ou criptomoedas. Estas modalidades podem dificultar o cancelamento da compra ou a

investigação dos destinatários. Opte sempre por meios de pagamento seguros, onde o dinheiro é liberado quando o consumidor declara que recebeu a mercadoria;

4) Busque contatos da loja. Faça contatos prévios com a loja, mas não só por e-mail, busque um contato telefônico, verifique onde está a sede e desconfie de lojas onde o único contato é um telefone celular;

5) Cuidado com ofertas em comunicadores, e-mails e redes sociais. Jamais clique ou acesse lojas virtuais a partir de links, ou ofertas que receber em comunicadores, WhatsApp e redes sociais;

6) Não acesse lojas pelo buscador. Acesse diretamente o site da loja evitando também pesquisar pela loja no buscador. Cuidado com pequenas mudanças no nome do site e avalie se possui certificado digital expedido para o próprio site. Os criminosos digitais podem falsear um link direcionando a vítima para o site errado. Ataque de phishing são muito comuns, com a falsificação de marcas e identidade visual de sites com ofertas de descontos, dentre outras chamadas para pescar consumidores desatentos;

7) Cuidado com códigos enviados para o celular para supostos descontos. Imagine que você recebe uma mensagem que conseguiu um cupom especial para o BlackFriday, mas para que você receba, você precisará informar um código que chegará pelo celular via SMS. Neste exato momento a vítima não ganhou o desconto, mas pode ter permitido a clonagem do WhatsApp ou até mesmo ter o reset de senhas de app's financeiros realizados com sucesso, dando acesso ao criminoso. Não confie jamais nesta abordagem. Não informe a ninguém códigos que receber

pelo celular;

8) Golpes com PIX. Muitos criminosos também poderão explorar este momento envolvendo a novidade, falsear identidade visual de lojas e oferecer produtos com “desconto” para compras com o pix, oferecendo códigos errados ou chaves que direcionarão o pagamento para o fraudador. Muita cautela no uso da nova tecnologia;

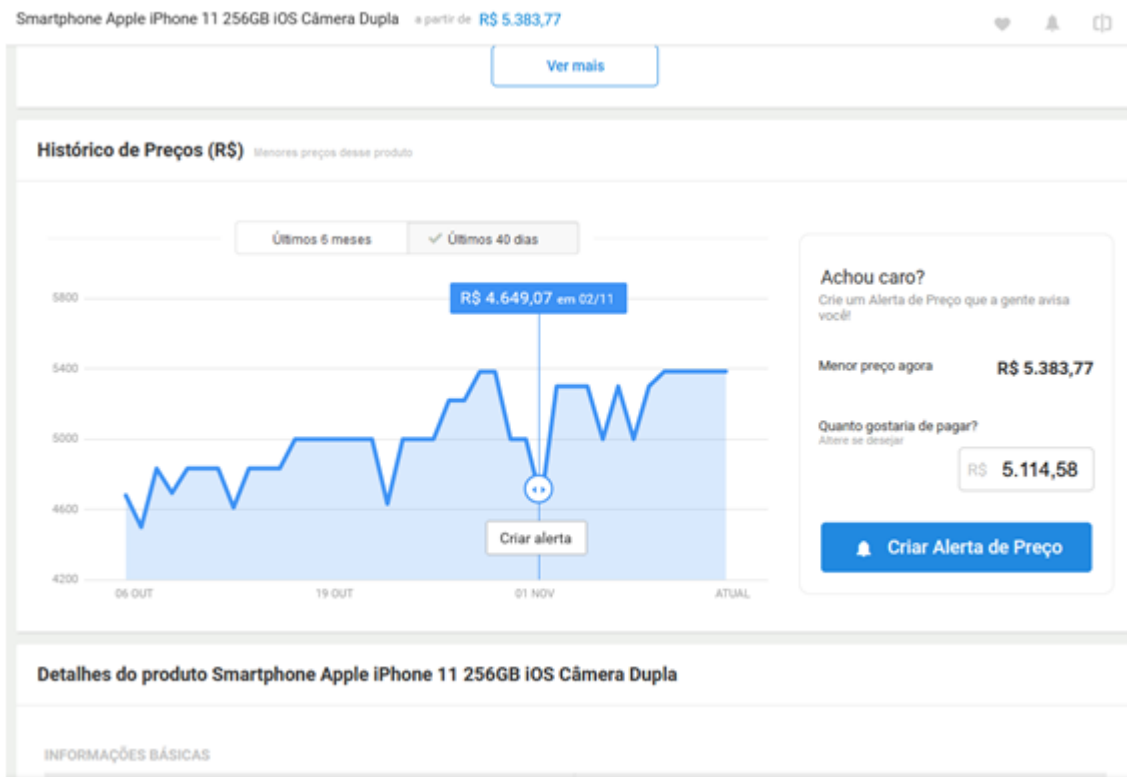
9) Desconfie de dados excessivos. Cheque a política de privacidade do site, se conecte a partir de uma conexão segura, avaliando se o site também tem SSL (https) assegurando proteção contra interceptação de dados e jamais forneça dados mais que necessários para a compra, como “senha do cartão” e outros dados. Mantenha sempre seu sistema operacional atualizado, com firewall e anti-malware ativados;

10) Faça provas de tudo. Guarde provas de toda a compra, salve os códigos, registre prints, e-mails recebidos, se necessário registre em vídeo do processo de compra. Todos estes dados podem ser uteis diante de uma fraude ou golpe, onde a perícia digital poderá identificar a autoria dos criminosos.

Avaliar aspectos de legalidade de um site nem sempre é uma tarefa fácil para o consumidor. Embora a Lei Geral de Proteção de Dados já esteja em vigor (LGPD), já esteja em vigor, muitas lojas ainda não estão em conformidade e não são totalmente transparentes em seus processos.

Outra proteção importante, mas não realizada a golpes digitais, é avaliar as chamadas “fraudes” de lojas que sobem o preço para depois baixarem. Para isso sites como buscapé, zoom

e baixou agora podem auxiliar, pois, apresentam um histórico do preço.



Buscapé mostra preço do Iphone 11 em 02/11 e 14/11 de R\$ 4649,07 por R\$ 5383,00

Caso tenha sido vítima de um golpe digital, o especialista, José Antonio Milagre, recomenda: “Imediatamente *resgate todos os dados da compra, registre um boletim de ocorrência online e procure um especialista em direito digital e crimes cibernéticos para que se incie um processo de apuração da autoria e responsabilização dos criminosos. Em casos de clonagem do chip, pode-se buscar a reparação em face da operadora de telefonia móvel.*”

Do mesmo modo é muito importante contactar o banco com informações sobre a fraude e notificar a loja que eventualmente teve a marca usada para a fraude, para se buscar uma resolução amigável. As lojas podem ser responsáveis, se

não adotavam medidas de segurança da informação ou não monitoravam o uso indevido de suas marcas, permitindo que fossem usadas para fraudes e golpes.

Porém, é importante advertir, se a loja comprovar que não deu causa ou que a despeito de todas as ostensivas demonstrações de segurança, a culpa foi exclusiva do consumidor, esta pode não se obrigada a reparar. Cada caso é um caso, e muitos deles serão apreciados pela Justiça. Por isso, prevenção é a melhor opção, sempre.

O IDCI (Instituto de Defesa do Cidadão e Consumidor na Internet) presta atendimento e apoio a vítimas de golpes e crimes cibernéticos, por seus canais, Siga @idcibrasil no Facebook e Instagram.

Prof. MSc. **José Antonio Milagre**, é Advogado e perito especializado em Direito Digital e Crimes Cibernéticos, Mestre e Doutorando Ciência da Informação pela UNESP, Presidente da Comissão de Direito Digital da OAB/SP Regional da Vila Prudente, Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros “Marco Civil da Internet: Comentários à Lei 12.965/2014” e “Manual de Crimes Informáticos”. Fundador do Instituto de Defesa do Cidadão na Internet – IDCI.

Canais:

<http://www.instragram.com/drjosemilagre>

<http://www.facebook.com/drjosemilagre>

<http://www.youtube.com/josemilagre>

Criminosos fraudam dados para sacar FGTS. Saiba como se proteger com as dicas do Especialista José Milagre

O Especialista em Direito Digital, José Milagre, participou do [Fala Brasil](#) da [Record TV](#), apresentado por [Celso Zucatelli](#), para falar sobre a nova modalidade de crime cibernético. Os criminosos estão fraudando dados em aplicativo do governo para sacar FGTS de beneficiários. Quais os cuidados e como se proteger. A matéria já está no [Portal do R7](#).

Saiba mais
em: <https://recordtv.r7.com/fala-brasil/videos/criminosos-fraudam-dados-em-aplicativo-do-governo-para-sacar-fgts-de-beneficiarios-22102020>