MATERIAL DE APOIO

WORKSHOP SUPER SEMANA LGPD

Riosoft®

LGPD ADVANCE

POR QUAL MOTIVO O BRASIL SE ADEQUOU À LEI DE PROTEÇÃO DE DADOS?

O Brasil é signatário de tratados internacionais (Convenção Americana sobre Direitos Humanos, na Convenção Europeia de Direitos Humanos, bem como na Declaração Universal de Direitos Humanos) que preconizam que países adequados à lei somente poderão se relacionar comercialmente com países que também possuam tal regulamento.

Assim, o Brasil estava perdendo espaço comercial por não possuir uma lei de proteção de dados. Quando a GDPR (*General Data Protection Regulation)* entrou em vigor, no ano de 2018, a pressão por uma regulamentação parecida no Brasil tornou-se um importante tópico para o país, até porque a lei europeia também afetaria o país na transferência de dados.

E diante de todas as possibilidades, nasceu a LGPD, Lei Geral de Proteção de Dados, que é explicitamente baseada na versão europeia, embora possua suas próprias características para se adaptar ao cenário brasileiro.

TRÂMITES DA LGPD

A LGPD foi publicada em 15 de agosto de 2018 e entraria em vigor 18 meses depois de sua publicação. Posteriormente, a Lei n. 13.853/2019 ampliou esse prazo de *vacatio legis* para 24 meses, o que significa que a LGPD deveria ter entrado em vigor em 16 de agosto de 2020. Antes dessa última data, porém, foi publicada a Medida Provisória n. 959/20 que, dentre outros assuntos, previa que a LGPD passaria a valer apenas em 03 de maio de 2021.

Além da Medida Provisória, outro dispositivo legal tratava da questão da vigência da LGPD: no dia 03 de abril de 2020 o Senado votou o projeto de lei n.1179/20, que institui normas transitórias para a regulação de relações jurídicas de direito privado durante a pandemia.

Na discussão desse projeto de lei, o Senado emitiu um parecer, aprovado na primeira votação, para que ocorresse uma prorrogação escalonada na LGPD. Em 01 de janeiro de 2021 a norma entraria em vigor e, em 1º de agosto de 2021, entrariam em vigor os artigos relativos às punições e sanções às transgressões à norma.

A Medida Provisória 959/2020 - PLV 34/2020

É preciso compreender a Medida Provisória 959/20. Ela trata de dois temas:

- Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020;
- Adia para 03 de maio de 2021 a entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais - LGPD.

No dia 26 de agosto o Senado transformou essa Medida Provisória no Projeto de Lei de Conversão 34/2020 e, antes de sua votação, o presidente do Senado, observando o regimento da Casa, considerou *prejudicado* o artigo 4º do texto, exatamente o artigo

que adiava o início da vigência da LGPD para o ano seguinte. Se o presidente do Senado *rejeitasse* formalmente o artigo, o texto seria devolvido para a Câmara. Havia, enfim, nítido interesse político em iniciar a vigência da lei.

Quando o presidente da República sancionou o projeto de lei de conversão, que tratava sobre o tema da MP 959/20 (PLV 34/2020), foi definido, portanto, que a maior parte da LGPD entraria em vigor, não existindo mais debate em relação ao adiamento da LGPD.

APLICABILIDADE DA LEI

A LGPD foi criada especificamente para o controle e proteção de dados pessoais. Ela busca garantir todos os direitos possíveis dos titulares, além de dar o máximo de autonomia, não excluindo situações específicas.

Sendo assim, a LGPD influencia todas as partes envolvidas, mas tem uma proposta genuína: tornar a proteção dos dados pessoais uma corresponsabilidade entre titular e organizações que os coletam, oferecendo mais autonomia aos titulares sem interferir no cumprimento de obrigações.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

De um dia para o outro (do dia 26 de agosto para o dia 27 de agosto de 2020) foi criada a ANPD (Agência Nacional de Proteção de Dados), via Decreto e vinculada à Presidência. A inexistência da autoridade fiscalizadora era um entrave para a vigência da LGPD e era pleiteada e cobrada por entidades setoriais, advogados e associações da iniciativa privada. De fato, a LGPD sem fiscalização traria insegurança jurídica, especialmente em razão da lei de caráter inédito no país.

A decisão pelo Decreto - publicado no Diário Oficial da União do dia 27 de agosto - foi criticada por especialistas, pois a intenção inicial era que o órgão fosse criado nos moldes das agências reguladoras, não atrelada ao Executivo Federal, o que compromete a expertise técnica e a neutralidade política do órgão.

O decreto aprova a estrutura de cargos e define as funções da ANPD, dentre elas regular a lei, observando a aplicação correta dos artigos e definindo as eventuais punições em caso de descumprimento. Também será competência da ANPD orientar a sociedade e mediar eventuais conflitos entre as empresas e os clientes.

A autoridade ficará sob responsabilidade da Casa Civil e o ministro da pasta indicará o conselho diretor da autoridade, que será composto por cinco membros, nomeados pelo presidente.

O decreto é, sim, um passo importante para a completude da ANPD, mas a organização de seu quadro de pessoal e regras só entram em vigor na data de publicação da nomeação do diretor-presidente da ANPD no DOU (Diário Oficial da União).

A PEC 17/19

A existência da PEC 17/19 não pode ser esquecida. A proposta de Emenda à Constituição n° 17, de 2019, acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

O texto foi aprovado por unanimidade pela comissão na Câmara, na forma de substitutivo pelo relator, o deputado Orlando Silva, cujo texto, além de determinar que a proteção de dados seja um direito fundamental, prevê a criação de um órgão responsável pela fiscalização do setor. Nos termos da PEC, esse órgão regulador – no caso, a ANPD, será uma "entidade independente, integrante da administração pública federal indireta, submetida a regime autárquico especial" e terá as mesmas atribuições de uma agência reguladora.

Ou seja, a PEC 17/19 pode federalizar as demandas sobre proteção de dados e privacidade no Brasil e alterar a estrutura da ANPD de órgão da administração direta para uma agência/autarquia autônoma.

Esse texto foi enviado à Câmara, que, em 14 de maio deste ano, ou seja, já depois da edição da mencionada Medida Provisória, decidiu pela não prorrogação da lei de dados, mas apenas dos artigos relativos às punições e sanções.

Devolvido para o Senado, e após as discussões e debates sobre a questão da manutenção do antigo parecer, apresentou-se um destaque pelo líder do PDT, no qual decidia-se pela *prorrogação apenas* dos artigos relativos às penalidades. O destaque foi aprovado por 62 votos a 15.

O projeto de lei n.1179/20 gerou, enfim, a lei n.14.010, de 10 de junho de 2020, que prevê que *apenas* os artigos 52, 53 e 54 da Lei n.13.709/18, ou seja, os artigos sobre as sanções administrativas previstas, entrarão em vigor no dia 1º de agosto de 2021.

AGENTES DA LGPD

TITULAR DE DADOS: Consoante prescreve o art. 5º, V, da Lei 13.709/18, o titular dos dados pessoais é a *"pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"*. O dado pessoal, por sua vez, é definido como *"informação relacionada à pessoa natural identificada ou identificável"* (art. 5º, I, LGPD).

Assim, a pessoa que está lendo este material de apoio é um titular de dados pessoais e, portanto, poderá exercer seus direitos perante o controlador de dados, nos termos do art. 18 da Lei Geral de Proteção de Dados. Vale esclarecer que o controlador de dados é definido pela lei como *"pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"* (art. 5º, VI, LGPD). Para facilitar a compreensão do tema, partiremos de uma situação hipotética.

Imagine que você, há alguns anos, tenha realizado cadastro na rede social "XX" e forneceu dados como estado civil, ano de nascimento, CPF, RG e endereço. Não bastasse isso, postou uma bela foto de perfil, adicionou seu número de celular, conta de e-mail, bem como marcou sua posição política e religião no perfil. Passados

alguns anos, muita coisa mudou. Você já não mora no mesmo lugar, o estado civil mudou, sua própria aparência mudou. Entretanto, algumas coisas permanecem iguais, como seu número de celular e posição política. Todos estes dados continuam em poder do controlador, ou seja, da rede social “XX”, ainda que a rede não esteja mais ativa.

CONTROLADOR: Como vimos, nos termos da própria lei, o controlador é “pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais”. Seria a figura equivalente ao responsável GDPR, ou seja, a empresa que demanda o tratamento, podendo ela mesma realizá-lo ou contratar um operador (que veremos logo a seguir). A lei brasileira, no entanto, traz uma peculiaridade: o controlador pode sim, ser pessoa natural – na GDPR essa classificação é limitada a pessoa jurídica. De certa forma, é um viés interessante, já que inibe condutas criminosas como colocar “laranjas” desempenhando o papel de controlador. Caso a pessoa física desrespeite a lei, haverá sanções também.

Cabe ao controlador, por óbvio, seguir o disposto na LGPD, devendo realizar o tratamento de acordo com os princípios ou orientar corretamente o operador, para que este realize um tratamento lícito. Um ponto interessante é a responsabilidade do controlador de elaborar o relatório de impacto (nas hipóteses aplicáveis). Ele responde pelos danos patrimoniais, morais, individuais ou coletivos, tal como violações à legislação (dever de reparação). Ainda, responde solidariamente pelos danos causados pelo operador, se diretamente envolvido no tratamento que resultar em danos.

OPERADOR: Caso o controlador deseje que um terceiro realize o tratamento dos dados, será preciso contratar um operador: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. Esta figura seria o equivalente ao subcontratante da GDPR (é o processador dos dados pessoais).

O operador deve seguir as diretrizes trazidas pelo controlador e tratar os dados de acordo com as políticas de privacidade referentes e ao ordenamento jurídico. Ele ainda responde pelos danos patrimoniais, morais, individuais ou coletivos, tal como violações à legislação (dever de reparação) – assim como o controlador. Responde solidariamente caso descumpra a legislação (equiparando-se ao controlador, caso não tenha seguido as instruções deste).

ENCARREGADO: O encarregado é definido pela lei como a “pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados”. Equipara-se à figura do já conhecido DPO, da GDPR, e tem como responsabilidade legal estabelecer comunicação com os titulares e a autoridade nacional, fornecendo esclarecimentos, providências e orientações internas. Na redação original da lei brasileira, havia a exigência de que o encarregado fosse pessoa física, mas a redação foi alterada com a MP 869/2018.

Na LGPD, pelo menos por enquanto, o encarregado deve ser indicado pelo controlador, não havendo previsão expressa de indicação por parte do operador. Ainda que o encarregado seja uma figura de destaque em ambas as legislações, é importante lembrar que, em momento algum, há previsão do encarregado responder legalmente. Entende-se, portanto, que cabe ao controlador a sua fiscalização – podendo o encarregado ser seu funcionário ou prestador de serviços por meio

contratual –, pois a interessada pelo adequado desenvolvimento das atividades do encarregado é a própria empresa que o contratou. Assim, a responsabilidade, em caso de incidente, é do controlador ou operador (a depender do caso concreto), mas jamais do DPO/encarregado.

CLASSIFICAÇÃO E DIFERENÇA ENTRE DADOS PESSOAS E DADOS SENSÍVEIS

DADOS PESSOAIS: Além dos conceitos legislativos nacionais, é oportuno ainda colacionar a definição adotada pelo regulamento da União Europeia sobre o tema, cujo art. 4º, I conceitua "dado pessoal" como qualquer informação relativa a uma pessoa natural identificada ou identificável, o assim chamado "titular de dados".

O art. 5º, inciso I, da LGPD conceitua dados pessoais como "informação relacionada à pessoa natural identificada ou identificável." São exemplos: dados cadastrais, data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos de consumo, entre outros. Ou seja, desde o número dos seus documentos até as páginas curtidas e os perfis seguidos nas redes sociais podem ser considerados dados pessoais.

O QUE SÃO DADOS SENSÍVEIS?

O artigo 5º da LGPD define como sensível o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".
Em outras palavras, os dados pessoais sensíveis são aqueles relacionados a aspectos muito íntimos do titular. Como a sua divulgação pode gerar prejuízo ou constrangimento em algumas circunstâncias, há regras específicas para o seu recolhimento.

QUANDO AS EMPRESAS PODEM SOLICITAR UM DADO SENSÍVEL?

Existe uma seção na LGPD para tratar apenas da manipulação de dados sensíveis. Ela esclarece que só pode haver o recolhimento de informações dessa natureza quando o titular consentir para uma finalidade específica ou para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Em suma, apesar da sensibilidade exigida para lidar com essas informações, existem muitos casos em que o titular pode ter seus dados colhidos sem nem saber disso, principalmente se esse processo estiver ligado a alguma ação governamental.

As condições citam ainda a possível anonimização dos dados sensíveis, isto é, a ocultação do nome e de outros dados que ajudem no reconhecimento do titular. Essa seria uma forma de aplacar os prejuízos que a exposição dessas informações pode causar. O artigo 12 até detalha que “os dados anonimizados não serão considerados dados pessoais para os fins desta Lei”.

CICLO DE VIDA DOS DADOS

A Lei Geral de Proteção de Dados (LGPD) determina que uma pessoa natural ou jurídica, de direito público ou privado, deve deixar claro para qual finalidade utilizará dados pessoais, solicitar o consentimento de seus titulares e realizar o devido tratamento dos dados.

Entender e classificar corretamente os dados se torna um processo importante para estar em conformidade com a lei, através da implementação de políticas, processos e programas apropriados para gerenciar a forma de coletar, processar, analisar, armazenar, compartilhar, reutilizar e eliminar esses dados.

Diante desse contexto, a Gestão do Ciclo de Vida dos Dados deve ser incorporada ao negócio, considerando a finalidade do fornecimento de seus bens e serviços.

A COLETA: A coleta dos dados nada mais é do que o meio pelo qual esses dados entram na sua empresa. Em relação aos colaboradores, por exemplo, eles podem ser adquiridos desde o site da empresa, nas já comuns áreas de “trabalhe conosco”, até mesmo quando se recebe os currículos, tanto de forma física como virtual. Isso pode acontecer seja por e-mail ou até por empresas terceiras especializadas em realizar a pré-seleção do candidato.

Outro exemplo se dá ao pedir que o colaborador forneça os dados dos seus filhos menores para o cumprimento de determinadas exigências ou para o fornecimento do plano de saúde como benefício, por exemplo.

O USO: Os exemplos citados acima listam dados que serão repassados, cada um a seu destino competente. Contudo, ter os dados dos familiares do seu colaborador para a inclusão em um plano de saúde não justifica que os encarregados pela expedição, por exemplo, tenham acesso a essas informações. As regras sobre o uso exigem que seja feita a adequação da utilidade daquele dado concreto e que ele sirva apenas àquele fim.

No caso da certidão de nascimento do filho do colaborador por exemplo, fica a cargo da empresa garantir o acesso destes dados ao pessoal autorizado e a elaboração de travas dali para frente, garantindo que apenas o pessoal competente tenha acesso ao seu uso.

O COMPARTILHAMENTO: O terceiro ponto do ciclo de vida é o compartilhamento. Ele pode existir tanto internamente, entre os setores da empresa, quanto externamente à empresa, como os dados enviados para o plano de saúde, por exemplo. Tal compartilhamento também deve ser observado rigorosamente para ter a certeza de que apenas o destino competente tenha o acesso. Também é de

responsabilidade da empresa que mais nenhum outro departamento consiga se interpor nesse trânsito dos dados.

O ARMAZENAMENTO: Depois do compartilhamento, a próxima obrigação se dá no que toca ao armazenamento destes dados. Será realizado um backup na nuvem ou até mesmo em um servidor local? Quais pessoas terão acesso? É de extrema importância que existam travas para que seus colaboradores não mandem esses dados para um lugar pouco seguro. Não é incomum que aconteça que esses tipos de informações sejam enviadas a um computador doméstico em que familiares acabem por acessá-los.

Esta regra também vale para documentos impressos. Por muitas vezes o arquivamento deste material é feito de forma negligente, muitas vezes sendo reaproveitados erroneamente como rascunho, por exemplo.

O DESCARTE: Por fim, a última parte do ciclo de vida dos dados é o descarte. Uma política correta para este procedimento é muito importante. Será que esses dados ficarão para sempre no seu servidor ou na sua nuvem? Se este arquivo for físico, por quanto tempo ficarão guardados antes de serem excluídos? Para a construção dessa política, devem ser levadas em conta as leis específicas que obriguem a retenção de determinados documentos ou informações por um período específico de tempo.

Dessa forma, tal política não exige que todos os dados sejam deletados imediatamente após a utilização, mas sim que sejam criadas regras que deixem claro qual é o documento, qual é o dado que lá consta e onde e por quanto tempo o mesmo será armazenado, pois só assim será possível elaborar corretamente a maneira mais eficiente de descarte dos dados.

HIPÓTESES DE TRATAMENTO DOS DADOS

MEDIANTE O FORNECIMENTO DE CONSENTIMENTO PELO TITULAR: Esta possivelmente é a base legal de tratamento de dados mais difundida pelos consultores e estudiosos do tema em geral, mas ao mesmo tempo a mais problemática de se realizar a gestão. A LGPD exige que o consentimento seja ser fornecido por escrito ou por outro meio que demonstre a manifestação inequívoca de vontade do titular.

Quando o consentimento se der por escrito, ele deverá constar em uma cláusula destacada das demais contratuais, que não pode ser genérica, justamente para que seja comprovado que aquele consentimento foi dado para uma finalidade específica de tratamento.

Porém, o maior problema em tratar dados pessoais com base no consentimento do titular é o fato de que ele é considerado um autorizador temporário, uma vez que pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Em outras palavras, caso uma empresa colete dados através do consentimento dos titulares desses dados, será necessário dispor de algum tipo de plataforma que permita a exclusão dos dados após a requisição do titular e que mantenha evidência dessa exclusão para fins de comprovação posterior, caso necessário. Tudo de forma gratuita.

Portanto, recomenda-se que a coleta de dados se dê com base no consentimento somente de forma residual, caso não seja possível o tratamento de dados através de alguma das outras 9 bases legais expostas ao longo deste texto.

PARA O CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR: A 2ª base legal para tratamento de dados pessoais prevista pela LGPD é o cumprimento de obrigação legal ou regulatória pelo controlador. Este é um autorizador da LGPD que possibilita que a lei não entre em conflito com outras legislações vigentes em nosso país, o que acabaria por gerar uma discussão sobre a possibilidade ou não do titular de dados registrar reclamação contra um tipo de tratamento de dados que estivesse em discordância com outra determinação legal.

No caso de uma obrigação decorrente de lei acarretar em um tratamento de dados pessoais por parte de uma empresa, essa estará autorizada a tratá-los de modo a cumprir a dita exigência legal ou regulatória.

Exemplificando, seria o caso de uma empresa transmitir os dados dos empregados constantes de seus registros internos de RH à Secretaria Especial do Ministério da Economia (antigo Ministério do Trabalho), a fim de cumprir com a entrega da Relação Anual de Informações Sociais (Rais). Nesse caso, os empregados não podem opor resistência ao compartilhamento de dados, uma vez que é necessário para o cumprimento de uma obrigação legal/regulatória por parte do controlador.

PELA ADMINISTRAÇÃO PÚBLICA, PARA O TRATAMENTO E USO COMPARTILHADO DE DADOS NECESSÁRIOS À EXECUÇÃO DE POLÍTICAS PÚBLICAS PREVISTAS EM LEIS E REGULAMENTOS OU RESPALDADAS EM CONTRATOS, CONVÊNIOS OU INSTRUMENTOS CONGÊNERES, OBSERVADAS AS DISPOSIÇÕES DO CAPÍTULO IV DESTA LEI: Durante o trabalho de consultoria para adequação à LGPD, uma das principais dúvidas que surgem é: essa lei se aplica ao tratamento de dados pessoais realizado por parte da Administração Pública? O inciso III do art. 7º da LGPD responde a esta pergunta. Sim, órgãos da administração pública precisam se adequar e cumprir a lei ao tratarem e compartilharem dados pessoais para execução de politicas públicas ou respaldadas em contratos, convênios ou instrumentos congêneres, sem a necessidade de consentimento dos titulares.

Contudo, a Administração Pública é obrigada a fornecer ao titular dos dados informações claras e inequívocas sobre a base legal para o tratamento dos dados, a finalidade e quais os procedimentos utilizados ao longo do ciclo de vida do dado dentro dos sistemas da Administração Pública.

A Administração Pública somente não estará obrigada a cumprir com as exigências da LGPD no caso de tratamento de dados feito exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão de infrações penais.

Vale ressaltar que os serviços notariais e de registro exercidos em caráter privado por delegação do Poder Público, terão o mesmo tratamento dispensado aos órgãos públicos, sendo necessário fornecer acesso aos dados por meio eletrônico para a Administração Pública.

Uma grande diferença da aplicação da LGPD aos órgãos públicos para o âmbito privado diz respeito às penalidades aplicadas. Para a Administração Pública, não há a previsão de sanção pecuniária, mas apenas a advertência, a publicitação da infração, bloqueio ou eliminação dos dados pessoais a que se refere a infração, sem prejuízo das sanções previstas no Estatuto do Servidor Público Federal, na lei de Improbidade Administrativa e na lei de acesso à informação.

PARA A REALIZAÇÃO DE ESTUDOS POR ÓRGÃO DE PESQUISA, GARANTIDA, SEMPRE QUE POSSÍVEL, A ANONIMIZAÇÃO DOS DADOS PESSOAIS: Também é

permitido o tratamento de dados pessoais para a realização de estudos por órgãos de pesquisa, de modo que, sempre que possível, esses dados devem ser anonimizados[1], a fim de garantir a privacidade dos titulares e evitar possíveis vazamentos, considerando a utilização de técnicas razoáveis na ocasião do tratamento.

Os órgãos de pesquisa já utilizam algumas práticas com o intuito de anonimizar os dados pessoais. Isso é feito, por exemplo, em pesquisa para apuração de intenção de votos em uma eleição, na qual há a proporção de votação para cada candidato de acordo com sexo, escolaridade, região geográfica, classe social, etc.. O resultado da pesquisa é cumprido, ao ponto que é praticamente impossível saber quem foram as pessoas que demonstraram aquelas intenções.

QUANDO NECESSÁRIO PARA A EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO DO QUAL SEJA PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS: A 5ª base legal autorizadora do tratamento de dados pessoais é a necessidade para execução de um contrato ou de procedimentos preliminares relacionados a um contrato que o titular dos dados figurará como integrante.

Nesse caso, o tratamento de dados se dará a pedido do próprio de titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares. Essa hipótese se assemelha um pouco com o tratamento de dados via consentimento, com a diferença de que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a vigência do contrato.

Um exemplo seria a contratação, por parte de um titular de dados, de um serviço cujo objeto principal é o tratamento de dados pessoais, tal como acontece com a inserção de dados em um serviço de armazenamento em nuvem.

PARA O EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL, ESSE ÚLTIMO NOS TERMOS DA LEI Nº 9.307/96 (LEI DE ARBITRAGEM): Outra base legal possível de ser utilizada pelo controlador é o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Esse autorizador garantido pela LGPD é uma decisão acertada com o intuito de garantir o direito de produção de provas de uma parte contra a outra em um processo judicial (na maioria das vezes), administrativo ou arbitral, este último nos termos da Lei de Arbitragem. Permitir que uma das partes se oponha a este tipo de tratamento de dados seria cercear o direito de defesa da outra em um processo e infringir os preceitos constitucionais da ampla defesa e do contraditório.

PARA A PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO: Ademais, a LGPD também admite o tratamento de dados com o intuito de proteger a vida ou a incolumidade física do titular dos dados ou de terceiros. Trata-se de um autorizador legal cujo objetivo é garantir a proteção de bens de elevado interesse público, tais como a vida e a incolumidade física, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento dos dados nesta situação.

Esta é uma base legal autorizadora para o tratamento de dados pessoais tão específica que, até mesmo o art. 11, II, da LGPD estabelece que dados pessoais

[1] Dado anonimizado é aquele em que não é possível identificar o seu titular.

sensíveis poderão ser tratados sem o fornecimento de consentimento do titular, caso sejam indispensáveis para a proteção da vida ou da incolumidade física do titular ou de terceiro, haja vista o interesse público envolvido neste tipo de tratamento.

Um exemplo deste tipo de tratamento de dados: imagine uma pessoa inconsciente dando entrada em um hospital que nunca esteve na vida após sofrer um grave acidente. Nesse caso, o novo hospital precisará de todo o histórico médico do paciente, constante em outro hospital que ele costuma frequentar. Nesse caso, o médico que irá atendê-lo está autorizado a requisitar a documentação ao outro hospital, que poderá compartilhar toda a documentação que disponha daquele paciente.

PARA A TUTELA DA SAÚDE, EXCLUSIVAMENTE, EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA: Seguindo a mesma ideia da base legal mencionada no item anterior, a LGPD também autoriza o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

É também uma base legal que tem como plano de fundo o interesse público no tratamento dos dados pessoais, sendo objeto de regras específicas dentro da própria LGPD quando o controlador atuar na área da saúde. Provavelmente será um dos itens de maior debate ao longo da formação e consolidação da consciência de proteção de dados na sociedade brasileira.

Da mesma forma que o item anterior, esta também é uma base legal autorizadora para o tratamento de dados pessoais bastante específica, em que o art. 11, II, f da LGPD estabelece que dados pessoais sensíveis poderão ser tratados sem o fornecimento de consentimento do titular, caso sejam indispensáveis para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Uma especificidade do tratamento com base neste inciso é a autorização do art. 11 da referida lei para a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde nos casos de prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, com objetivo de obter vantagem econômica, desde que em benefício dos interesses dos titulares de dados, sendo vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. Qualquer outro tipo de comunicação ou uso compartilhado de dados referentes à saúde é categoricamente vedado pela LGPD.

QUANDO NECESSÁRIO PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO, EXCETO NO CASO DE PREVALECEREM DIREITOS E LIBERDADES FUNDAMENTAIS DO TITULAR QUE EXIJAM A PROTEÇÃO DOS DADOS PESSOAIS: Após o consentimento, a 2ª base legal autorizadora de tratamento de dados mais propagada é o legítimo interesse do controlador ou de terceiros. No entanto, assim como o consentimento, esta base legal é potencialmente problemática, sendo recomendado utilizá-la somente quando não houver outra base legal aplicável ao caso, pela nebulosidade e fragilidade que envolve o tema.

Além de ser um tanto quanto difícil apontar, neste momento, o que seria o “legítimo interesse” do controlador ou de terceiro, uma vez que não há uma previsão legal no

ordenamento jurídico brasileiro a respeito da definição deste termo, é sempre muito importante sopesar até que ponto o legítimo interesse do controlador ou de terceiro sobrepõe o do titular dos dados ou fere alguma outra disposição expressa da LGPD.

O art. 10 da LGPD determina que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: 1) apoio e promoção de atividades do controlador e 2) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Portanto, para que se possa utilizar esta base legal como autorizadora para o tratamento de dados é necessário identificar um interesse inequivocamente legítimo, demonstrar que o tratamento de dados é necessário para se atingir tal objetivo e tomar o devido cuidado para não violar nenhum dispositivo legal ou nenhum direito do titular daqueles dados.

PARA A PROTEÇÃO DO CRÉDITO, INCLUSIVE QUANTO AO DISPOSTO NA LEGISLAÇÃO PERTINENTE. A 10ª e última base legal possível de utilização para se realizar o tratamento de dados pessoais é a proteção do crédito, em observância às regras específicas para este tema.
O objetivo do legislador foi evitar que titulares de dados pessoais se utilizem de uma brecha legislativa para criar mecanismos que os livrem de cobranças por dívidas contraídas.
Seria inimaginável pensar em um titular de dados requerendo a exclusão dos mesmos dos cadastros do SPC e Serasa, por exemplo, sob a alegação de que não autorizou o referido tratamento ou que violaria a sua privacidade, safando-se, assim, de instrumentos para efetivar a cobrança do crédito.

DIREITOS DO TITULAR

Como já deve ser amplamente conhecido hoje, a Lei Geral de Proteção de Dados garante essencialmente, no artigo 18, 10 direitos a todos os titulares de dados pessoais:

CONFIRMAÇÃO E ACESSO: Você pode solicitar a confirmação da existência de um tratamento e acesso aos seus dados pessoais, a razão pelas quais eles são armazenados, a origem da informação e quais os critérios de uso da empresa. Aqui também é possível descobrir quando seus dados não estão presentes na organização.

CORREÇÃO: Você tem o direito de solicitar que dados incompletos, desatualizados ou incorretos sejam prontamente corrigidos.

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO: Será possível solicitar que os dados sejam totalmente desvinculados das informações de reconhecimento pessoal (anonimização), suspensão temporária da operação de tratamento dos dados ou a exclusão de algo específico ou um conjunto de coisas dentro do banco de dados de uma organização, especialmente quando considerados desnecessários para a utilização da empresa.

PORTABILIDADE: É possível solicitar a transferência de dados pessoais para outro fornecedor, serviço, produto (e até mesmo internacionalmente).

REVOGAÇÃO DE CONSENTIMENTO: É possível revogar a qualquer momento o consentimento de uso de seus dados pessoais tratados, pois mesmo após a autorização você ainda possui os mesmos poderes sobre eles.

ELIMINAÇÃO: Sim, você pode manifestar o direito de pedir para que seus dados pessoais tratados, mesmo após consentimento anterior, sejam eliminados.

COMPARTILHAMENTO: Você tem o direito de obter informações sobre todas as entidades – públicas ou privadas com os quais suas informações pessoais são compartilhadas.

EXPLICAÇÃO: Você tem o direito de obter informações sobre as possibilidades e consequências de não fornecer o consentimento sobre determinadas ações de tratamento de dados pessoais.

OPOSIÇÃO: Você pode negar o tratamento dos dados pessoais quando o processo é realizado de maneira ilegal – fora de *compliance* com a LGPD.

REVISÃO DE DECISÃO AUTOMATIZADA: O titular dos dados pessoais tem o direito de solicitar informações sobre os critérios e processos utilizados na tomada de decisão da estrutura automatizada. Decisões como definição de perfil profissional, de consumo e de crédito são algumas das que afetam diretamente os interesses do titular.

Os direitos do titular são limitados, portanto seus dados pessoais ainda podem ser tratados sem autorização quando são necessários para a execução de contratos para o cumprimento de alguma obrigação legal, segredo comercial e industrial.

PRINCÍPIOS DA LEI

Para facilitar o reconhecimento de boas condutas e também das práticas que são inadequadas no dia a dia dos negócios, separamos aqui os 10 princípios que norteiam a LGPD e que devem ser respeitados:

1- FINALIDADE
A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais.
Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular.
Além disso, a empresa não está autorizada a modificar a finalidade durante o tratamento. Se sua startup solicita o e-mail do cliente para a finalidade específica de *login* na plataforma, você não pode utilizar automaticamente esse mesmo e-mail para enviar publicidade ou ofertas.

2- ADEQUAÇÃO
Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa. Ou seja, sua justificativa deve fazer sentido com o caráter da informação que você pede.
Por exemplo: se o seu negócio é um e-commerce de produtos eletrônicos, dificilmente será justificável pedir dados de saúde aos usuários. Então, se não é compatível, o tratamento se torna inadequado.

3- NECESSIDADE
As startups e empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades. Procure fazer uma ponderação entre o que é realmente essencial para o seu negócio e o que é apenas conveniente.
Lembre-se que quanto mais dados você tratar, maior será a sua responsabilidade, inclusive em casos de vazamentos e incidentes de segurança.

4- LIVRE ACESSO
A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito.
Além disso, devem ser especificadas questões como: o que a empresa faz com as suas informações, de que forma o tratamento é realizado e por quanto tempo.

5- QUALIDADE DOS DADOS
Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.

6- TRANSPARÊNCIA
Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.
Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta. Se você repassa dados pessoais para terceiros, inclusive para operadores que sejam essenciais para a execução do serviço, o titular precisa saber.

7- SEGURANÇA
É responsabilidade da empresa buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por *hackers*.
Além disso, devem ser tomadas medidas para solucionar situações acidentais, como destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.

8- PREVENÇÃO
O princípio da prevenção objetiva que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as empresas devem agir antes dos problemas e não somente depois.

9- NÃO DISCRIMINAÇÃO
Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico.

10- RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS
Além de se preocupar em cumprir integralmente a Lei, a empresa deve ter provas e evidências de todas as medidas adotadas, para demonstrar a sua boa-fé e a sua diligência.

EXCEÇÕES

Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019) Vigência.

MULTAS E SANÇÕES

A maior parte dos dispositivos da Lei Geral de Proteção de Dados só passa a vigorar em agosto de 2021, exceto a criação da ANPD. O regulamento define direitos e deveres das empresas, órgãos públicos e cidadãos no que se refere à proteção de dados pessoais. Além disso, estabelece as responsabilidades no caso de infração da lei. Veja as principais punições:

REPARAÇÃO DE DANOS: O responsável por manipular os dados (operador) ou por tomar decisões relativas a eles (controlador) deve reparar eventuais danos ao titular

das informações. No caso do operador dos dados, a responsabilidade é solidária, exceto se ele descumprir ordens explícitas do controlador (tomador de decisões).

SANÇÕES ADMINISTRATIVAS: Tanto o operador quanto o controlador dos dados podem sofrer punições administrativas, aplicadas pela ANPD. As sanções vão de simples advertências a multas, que podem ser de 2% do faturamento da empresa, limitadas a R$ 50 milhões. A definição da metodologia de cálculo do valor das multas será regulamentada pela ANPD.

SANÇÕES ADMINISTRATIVAS, CIVIS OU PENAIS: Os agentes de tratamento de dados que infringirem a lei também estão sujeitos a punições nas esferas administrativas, civis e penais. Tanto órgãos públicos quanto entidades privadas podem ser punidas.

Em decorrência dessas punições, as empresas e os governos terão que tomar muito cuidado com os dados de seus clientes. Estima-se que nem todas as instituições estarão aptas a cumprir os requisitos do regulamento, sobretudo as empresas menores, que terão dificuldades em contratar um ou mais profissionais para fazer o tratamento de dados.

FUNÇÕES DO ENCARREGADO

O Encarregado tem um cargo estratégico na governança dos dados. Além de interagir com o Poder Público e com os titulares dos dados. A própria LGPD, em seu art. 5º, inciso VIII, define o Encarregado como o profissional indicado pelos agentes de tratamento de dados (Controlador e Operador) para “atuar como canal de comunicação entre o controlador, os titulares dos dados e Autoridade Nacional de Proteção de Dados”. Mas suas atribuições vão além. O Encarregado precisa estar ciente sobre o ciclo de vida dos dados pessoais dentro de uma empresa, orientar a organização e os colaboradores na implantação da gestão do Programa de Privacidade e assegurar que as atividades de tratamento desses dados estejam adequadas aos dispositivos da LGPD, garantindo a conformidade e o nível de segurança adequados, além de esclarecer à ANPD e a outros órgãos sobre como se dá o tratamento dos dados.

Pela LGPD, a função de Encarregado pode ser exercida por pessoa física ou jurídica externa à organização. E, nesse momento inicial de vigência da LGPD, essa alternativa pode ser fundamental para a estruturação da governança interna na proteção de dados.

Ter um profissional externo, o chamado DPO as a Service ou Encarregado terceirizado, implica em atuação imparcial e redução de custos para as empresas, podendo ser uma vantagem competitiva. Outro ponto de destaque é que o DPO externo poderá atuar como elemento certificador da conformidade dos atos de tratamento da empresa após a implementação, além de atuar como peça chave para garantir a conformidade durante a implementação nas empresas que ainda não concluíram seus processos.

O ideal é que a empresa busque no mercado um Encarregado que reúna conhecimentos multidisciplinares inerentes à função. Deve ter um perfil profissional que una conhecimentos jurídicos, tecnológicos e práticos quanto à proteção de dados. No futuro, é possível que a Autoridade Nacional de Proteção de Dados venha a regulamentar requisitos mínimos para a função de Encarregado.

SEGURANÇA DA INFORMAÇÃO PRINCÍPIOS

Segurança da Informação trata da proteção de informações, sistemas, recursos e demais ativos contra desastres e erros (intencionais ou não). Trata também da manipulação não autorizada e proteção de vários tipos de ameaças para garantir a continuidade do negócio. A informação que possui valor deve ser devidamente protegida não importando os meios pelos quais é compartilhada ou armazenada.

Para que seja possível manter a proteção diante das ameaças internas e externas. Existem alguns princípios fundamentais da segurança da informação, a saber: **confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade ou não repúdio**.

CONFIDENCIALIDADE: Garantia de que o acesso à informação é restrito aos seus usuários legítimos. É a proteção dos dados contra o acesso não autorizado. Inclui medidas para proteger a privacidade.

A violação da confidencialidade pode assumir muitas formas. Permitir que alguém olhe por cima do seu ombro na tela do computador enquanto você tem dados sigilosos sendo exibidos, pode ser uma quebra de confidencialidade. Se um *laptop* contendo informações importantes sobre os funcionários de uma empresa for roubado ou vendido, isso também poderá ferir o princípio.

INTEGRIDADE: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais. A informação deve ser correta e sem erros.

A integridade significa que os dados não podem ser modificados sem autorização. A integridade é violada quando um funcionário acidentalmente ou com intenção maliciosa exclui arquivos de dados importantes, quando um vírus infecta um computador, quando um funcionário é capaz de alterar seu próprio salário em um banco de dados de folha de pagamento, etc.

DISPONIBILIDADE: Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de maneira oportuna, ou seja, determina que os recursos estejam disponíveis para acesso, sempre que solicitado.

Para que qualquer sistema de informação atenda ao seu propósito, as informações devem estar disponíveis quando necessário. Isso significa que os sistemas de computação usados para armazenar e processar dados, controles de segurança usados para protegê-los e os canais de comunicação usados para acessá-los, devem estar funcionando corretamente.

Os sistemas de alta disponibilidade visam permanecerem sempre disponíveis, evitando interrupções no serviço devido a quedas de energia, falhas de *hardware* e atualizações do sistema.

AUTENTICIDADE: Significa garantir que um usuário é de fato quem alega ser, ou seja, que a informação pertence à fonte anunciada. Origem e destino verificam a identidade da outra parte envolvida na comunicação.

NÃO REPÚDIO OU IRRETRATABILIDADE: É a capacidade do sistema de provar que um usuário executou uma determinada ação. Só se pode garantir o não repúdio quando houver autenticidade e integridade.

VULNERABILIDADES

A fórmula mais importante quando falamos em segurança da informação é: **risco = impacto*probabilidade** (risco em segurança da informação é igual ao impacto vezes a sua probabilidade). Seu principal objetivo é mitigar e diminuir a probabilidade de que um ataque ou ciberameaças sejam bem-sucedidos, de tal forma que o risco seja erradicado do ambiente. E, caso um ataque seja bem sucedido, que o impacto seja mínimo.

Por isso, é fundamental conhecer os 7 principais tipos de vulnerabilidades:

FÍSICAS: Instalação predial, controle de acesso, data center, etc.. Tudo que envolve controle de acesso às instalações do ambiente corporativo.

NATURAIS: Desastres como incêndios, quedas de energia, etc.. Para tudo o que pode tirar o seu ambiente de produção do funcionamento adequado. A pergunta que deve ser feita é: existe um plano de contingência?

HUMANAS: Falta de treinamento e alinhamento com as políticas de segurança da empresa, vandalismo e até mesmo sabotagem. Um colaborador descontente pode, sim, ser uma ameaça.

HARDWARE: Depreciação do ativo, má instalação, etc.. Tudo o que envolve um ativo ou item de configuração que pode causar um ponto de vulnerabilidade ao ambiente, causando a indisponibilidade do acesso ao ambiente de produtividade da empresa e impactando diretamente no andamento das atividades.

SOFTWARE: Este também é um dos principais pontos de vulnerabilidade dentro das empresas. Um *software* ou sistema operacional desatualizado pode causar grande impacto aos negócios. Citando um exemplo simples, o recente ataque global de *ransomware*, que atingiu mais de 100 países, ocorreu por falta de atualização de pacotes de segurança no sistema operacional de computadores e ambientes de redes. As perguntas que precisam ser feitas aqui são: os softwares utilizados na empresa estão homologados? Foram desenvolvidos através de padrões de qualidade adequados?

MÍDIAS DIGITAIS: *Pendrives* e hds externos são ótimos exemplos. A utilização de qualquer dispositivo externo não autorizado por vários motivos podem comprometer a confidencialidade, integridade e disponibilidade dos sistemas, que são os pilares que sustentam a segurança da informação. Por motivos óbvios, a utilização destes dispositivos requer atenção para se evitar o vazamento de informações confidenciais, bem como danos ao computador, dependendo da qualidade do dispositivo e do seu conteúdo (arquivos infectados com vírus).

COMUNICAÇÃO: O meio de comunicação adotado pela empresa também pode ser um tipo de vulnerabilidade já que a utilização de softwares não homologados - como Skype, WhatsApp, MSN, aplicativos de mensagens instantâneas alternativos - podem comprometer a segurança na comunicação, acarretando seríssimos problemas relacionados à vazamento de informações sensíveis e até mesmo fraudes.

TIPOS DE ATAQUES

Uma vez que já nos apropriamos das principais vulnerabilidades corporativas, quais seriam **os principais tipos de ataques** que as explorariam?

DOS: negação de serviço, uma falha recorrente e explorada por hackers. Em diversos artigos em nosso blog explicamos sobre este ataque, que tira o acesso do usuário a um determinado serviço.

SQL* INJECTION:* injeção de código malicioso em aplicações que utilizam banco de dados SQL.

PRIVILEGE ESCALATION*:* através de códigos maliciosos é possível aumentar privilégios de acesso, como administradores de um determinado computador ou até mesmo do ambiente de redes, podendo executar *softwares* maliciosos e coletar informações sensíveis da empresa.

DUMPSTER DIVING*:* a forma incorreta no descarte de informações corporativas é uma vulnerabilidade que requer muita atenção. Assim como deve acontecer com documentos físicos, o mesmo cuidado deve ser adotado nos meios digitais. Por exemplo: no caso do descarte de um computador que parou de funcionar, é importante saber que existem formas de recuperação das informações contidas no hd deste computador. O descarte de e-mails deve ser tratado de forma especial.

MALWARE

O QUE SÃO *MALWARES*?

Malware, ou “software malicioso,” é um termo mais amplo que descreve qualquer programa ou código malicioso que seja prejudicial aos sistemas. Hostil, intrusivo e intencionalmente prejudicial, o *malware* invade, danifica ou desabilita computadores, sistemas de computador, redes, *tablets* e dispositivos móveis, geralmente assumindo o controle parcial das operações de um dispositivo. Assim como a gripe para os humanos, ele interfere no funcionamento normal.

Malware é uma maneira de ganhar dinheiro à sua custa de forma ilícita. Embora *malware* não possa danificar o *hardware* físico dos sistemas e equipamentos de rede (com uma exceção conhecida— consulte a seção Google Android abaixo), ele pode roubar, criptografar ou excluir seus dados, alterar ou sequestrar funções essenciais do computador e espionar a atividade de seu computador sem seu conhecimento ou permissão.

COMO POSSO IDENTIFICAR SE HOUVE INFECÇÃO POR *MALWARE*?

O *malware* pode se revelar através de muitos comportamentos atípicos diferentes. Aqui estão alguns sinais típicos de que você tem malware em seu sistema:
- Seu computador se torna mais lento. Um dos principais efeitos do *malware* é reduzir a velocidade de seu sistema operacional, seja ao navegar na Internet ou ao usar os aplicativos locais.
- Uma torrente de anúncios irritantes que não deveriam estar ali invadem sua tela. Anúncios em janelas pop-up inesperadas são um sinal típico de uma infecção por *malware*. Eles são associados especialmente com uma forma de *malware* conhecida

como *adware*. Além disso, os pop-ups geralmente são acompanhados de outras ameaças de *malware* ocultas. Assim, se você vir algo como “PARABÉNS, VOCÊ GANHOU UMA CONSULTA GRATUITA COM UM MÉDIUM!” em uma pop-up, não clique nela. Independente do prêmio gratuito oferecido pelo anúncio, o preço será alto.

- Seu sistema desliga repetidamente, congela ou exibe BSOD (Tela Azul), o que pode ocorrer em sistemas Windows após um erro fatal.

- Você nota uma perda misteriosa de espaço em disco, provavelmente, causada por um *malware* invasor gigantesco que se oculta em seu disco rígido. Há um aumento estranho na atividade da sua Internet do sistema.

- O uso de recursos de seu sistema está estranhamento alto e a ventoinha de seu computador gira em plena velocidade — sinais de atividade de *malware* consumindo recursos do sistema em segundo plano.

- A página inicial do navegador mudou sem sua permissão. De forma semelhante, os links em que você clica o encaminham a um destino indesejado na internet. Isto geralmente indica que você clicou em uma janela do tipo “parabéns”, que baixou algum software indesejado. Também é possível que seu *browser* fique lento ou extremamente lento.

- Novas barras de ferramentas, extensões ou *plugins* aparecem inesperadamente em seu navegador.

- Seu produto antivírus para de funcionar e você não consegue atualizá-lo, ficando desprotegido contra o *malware* furtivo que desabilitou o antivírus.

- Por fim, há também o ataque de malware dolorosamente óbvio e intencionalmente nem um pouco sorrateiro. Isto é muito comum com *ransomware*, o qual se apresenta e informa que está com seus dados e exige um resgate para devolver seus arquivos.

Mesmo que pareça que tudo está funcionando bem em seu sistema, não seja complacente. Um malware potente pode se ocultar em seu computador, fazer suas atividades sujas sem despertar nenhum alerta, à medida que rouba suas senhas, arquivos sensíveis ou usa seu computador para se difundir para outros computadores.

COMO FUI INFECTADO COM *MALWARE*?

As principais formas de infecção por *malware* são as duas maneiras mais comuns pelas quais ele acessa seu sistema — a Internet e o e-mail. Em outras palavras, você pode ser infectado a qualquer momento enquanto esteja conectado on-line.

O *malware* pode penetrar em seu computador quando você navega em websites submetidos a *hack*, ao clicar em demos de jogos, ao fazer o *download* de arquivos de música infectados, ao instalar novas barras de ferramentas de um provedor desconhecido, ao configurar um *software* de uma fonte arriscada, ao abrir uma anexo de e-mail malicioso ou, basicamente, ao baixar qualquer coisa da Internet para um dispositivo que não tenha um aplicativo de segurança antimalware de qualidade.

Aplicativos maliciosos podem se esconder em aplicativos legítimos, especialmente quando são baixados de websites ou de mensagens ao invés de uma app store. Aqui é importante verificar as mensagens de alerta ao instalar aplicativos, especialmente se pedirem permissão para acessar suas informações de e-mail ou outras informações pessoais.

ENGENHARIA SOCIAL

Engenharia social é termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Por meio da engenharia social, os criminosos cibernéticos usam a interação humana para manipular o usuário a divulgar informações confidenciais. Como a engenharia social se baseia na natureza humana e nas reações emocionais, os invasores utilizam várias táticas para tentar enganá-lo on-line e off-line.

***BAITING* (ISCAS):** Seres humanos são criaturas curiosas e essa característica é essencial neste cenário. O criminoso cibernético deixará um dispositivo, como um pen drive, infectado com *malware* à vista em um local público. Alguém encontrará o dispositivo e o conectará em seu computador para ver o que ele contém, e assim o *malware* se injeta no computador.

***PHISHING*:** O truque mais antigo de todos e ainda o mais bem-sucedido. Os criminosos cibernéticos tentarão usar diferentes métodos para convencê-lo a divulgar informações. A tática de intimidação parece ser a mais popular entre os criminosos, pois apresenta uma situação urgente ao usuário, normalmente envolvendo uma conta bancária ou outra conta on-line. Essa tática conta com decisões precipitadas do usuário, tomadas sob efeito do medo, e baseadas em suas emoções e não na racionalização da situação.

Outras versões desses e-mails aparentam ser de uma pessoa de autoridade, como um diretor da empresa em que você trabalha, solicitando seu nome de usuário e senha para que ele possa acessar um sistema. As pessoas naturalmente atendem a solicitações enviadas por um colega de trabalho, principalmente se vierem de um departamento superior na hierarquia da empresa.

O senso de urgência é também uma tática popular usada no *phishing*. Você já deve ter recebido inúmeros e-mails divulgando ofertas de produtos com descontos, em quantidades limitadas. O desconto parece excelente e o usuário se sente pressionado a agir com urgência, tomando decisões impulsivas e sem muito controle.

ENVIO DE SPAM AOS CONTATOS E *HACKING* (VIOLAÇÃO) DE EMAILS: Dar atenção a mensagens enviadas por pessoas que conhecemos faz parte da nossa natureza. Se a minha irmã me envia um e-mail com o assunto "Confira este site que eu achei, é fantástico!", não pensarei duas vezes antes de abri-lo. Exatamente por isso esses criminosos buscam endereços de email e senhas. Uma vez obtidas essas credenciais, eles passam a controlar a conta e logo enviarão spam a todos os contatos do catálogo de endereços do usuário. O objetivo principal é espalhar *malware*, convencer as pessoas a divulgar seus dados pessoais e outros.

PRETEXTOS: Pretextos são histórias elaboradas inventadas pelos criminosos para criar uma situação que vai "fisgar" suas vítimas. Muitas vezes são histórias tristes sobre alguém perdido em um país estrangeiro ou que precise de ajuda em um momento difícil. Essas situações apelam para a inclinação humana natural de ajudar aqueles que necessitam. Pretextos são normalmente usados em conjunto com os outros métodos, pois a maioria dessas situações precisam de uma história para atrair

a atenção das vítimas ou para reforçar a história personificada pelo criminoso em uma chamada telefônica.

QUID PRO QUO: "Tomar uma coisa por outra". Seduzindo o usuário com prêmios ou descontos em produtos de luxo, este golpe oferece aos usuários "alguma coisa", mas só depois que eles preencherem um formulário que solicita todas as suas informações pessoais. Esses dados serão, então, usados para o roubo de identidade.

***SPEAR PHISHING*:** Um parente mais complexo do *phishing*, *spear phishing* é uma campanha direcionada a funcionários de uma determinada empresa da qual o criminoso pretende roubar dados. O criminoso escolherá um alvo dentro da empresa e fará uma pesquisa on-line sobre essa vítima, coletando informações pessoais e interesses com base em suas pesquisas na Internet e perfis de mídias sociais. Depois de conhecer melhor sua vítima, ele passará a enviar e-mails que parecerão especificamente relevantes a ela, a fim de convencer a vítima a clicar em um link malicioso que hospeda um *malware* ou a fazer o *download* de um arquivo malicioso. É claro que todo mundo confere seus e-mails pessoais ou mídias sociais enquanto trabalha na rede da empresa e é com essa prática que o criminoso cibernético conta. Depois que o usuário for enganado com sucesso, o *malware* é instalado no computador e ligado à rede da empresa, o que o ajudará a se propagar facilmente a outros computadores ligados à mesma rede.

***VISHING*:** O *vishing* é, de todos esses métodos, o que envolve mais interações humanas. O criminoso liga para o funcionário de uma empresa fingindo ser uma pessoa confiável ou um representante do seu banco ou de uma instituição parceira da empresa em que você trabalha e tenta, durante a conversa, obter informações da vítima. Em outra ligação subsequente, ele finge ser um colega de trabalho que perdeu sua senha, solicitando a senha da vítima ou pode também fazer uma série de perguntas para verificar a sua identidade.

A engenharia social pode ser executada de duas formas: um ataque único, como um e-mail de *phishing* ou, de uma forma mais complexa, normalmente direcionada a instituições. Esses dois métodos são chamados de *hunting* (caça) e *farming* (cultivo).

***HUNTING*:** Hunting é a versão curta desses ataques. Normalmente os criminosos cibernéticos usam *phishing*, *baiting* e *hacking* de e-mails com o objetivo de extrair o máximo possível de dados de suas vítimas, com o mínimo de interação possível.

***FARMING*:** Um tipo de crime mais elaborado no qual o criminoso procura uma maneira de estabelecer um relacionamento com a vítima. Normalmente ele analisa o perfil das vítimas em mídias sociais e tenta estabelecer um relacionamento com ela, com base nas informações obtidas em sua pesquisa. Esse tipo de ataque depende também do pretexto, pois o criminoso tenta enganar a vítima pelo máximo de tempo que for possível, a fim de extrair o máximo de dados possíveis.

A engenharia social está em toda parte, on-line e off-line. Ela tem uma alta taxa de sucesso porque conta com um elemento contra o qual não é possível instalar um software de segurança: o ser humano. A melhor defesa contra esses tipos de ataques é se informar e se manter consciente sobre os sinais para os quais estar sempre alerta.

RISCOS

ESPIONAGEM INDUSTRIAL: A espionagem é a prática de obter informações de caráter secreto ou confidencial sobre governos, organizações, empresas ou até mesmo pessoas físicas, sem autorização destes, para alcançar certa vantagem política, econômica, tecnológica ou social. A prática manifesta-se geralmente como parte de um esforço organizado e, em relação a empresas, tem-se a prática de espionagem industrial.

Contudo, a espionagem não tem um tratamento específico na legislação brasileira, sendo tratada de maneira esparsa na legislação penal, geralmente referenciada à espionagem militar, isto é, ao acesso e apropriação desautorizada de informações e dados atinentes à defesa. Entretanto, os efeitos jurídicos da espionagem não se cingem à esfera do direito penal, podendo também repercutir em outras instâncias do direito, como a civil e a administrativa.

Em relação a estes casos, tem-se a Lei nº 9.279/1996 (Lei da Propriedade Industrial) que protege segredos industriais, reputando concorrência desleal do seu uso desautorizado. A legislação impede, de forma ampla, o uso de dados de natureza confidencial que tenham sido obtidos durante relação contratual ou empregatícia, ou que tenham sido obtidos de forma ilícita ou fraudulenta (artigo 195, incisos XI e XII).

Temos, assim, uma legislação que oferece proteção aos segredos industriais e que permite que qualquer tipo de informação possa ser considerado como tal, desde que não seja pública, tenha relevância comercial e tenha sido objeto de medidas para resguardar sua confidencialidade. Dentre as informações mais comumente incluídas nesse rol, destacam-se listas de clientes, fornecedores, documentos contábeis, fiscais, financeiros, remuneração de funcionários, manuais, especificação de produtos, fórmulas, entre outros.

Já na jurisprudência, constata-se que, caso seja comprovada a prática de espionagem industrial, o ensejo a uma ação de indenização é plenamente possível.

Verificada a prática do ato ilícito, a Lei de Propriedade Industrial oferece os instrumentos necessários para fazer cessar imediatamente a violação, como também para obter reparação pelos danos sofridos. Além disso, a possibilidade de que haja uma decisão liminar para impedir ou coibir tal prática é expressamente prevista, bem como a respectiva indenização pelos prejuízos causados (artigo 209 e 210 da referida lei).

VAZAMENTO DE INFORMAÇÕES

Vazamento de dados é um incidente de segurança que expõe publicamente informações sensíveis que podem ser vistas, copiadas, roubadas, transmitidas ou usadas sem acesso autorizado.

Surpreendentemente, as principais causas de vazamentos não são apenas ataques cibernéticos como *malware*, *phishing*, *spyware*, *ransomware*, etc., mas também falhas simples de configurações de segurança que poderiam ser corrigidas, evitando, assim, enormes prejuízos de reputação e perdas financeiras para as empresas vazadas. Outras causas podem incluir funcionários insatisfeitos ou mal-intencionados, erros não intencionais de funcionários, falta de conhecimento técnico ou *expertise* para proteger os dados ou o ambiente.

Apesar de serem difíceis de detectar, o melhor a fazer para mitigar o iminente risco é implementar gestão de risco para detecção, contenção e comunicação no caso de um vazamento. Quanto mais rápida sua detecção menor o prejuízo.

As regulamentações de privacidade de dados como LGPD e GDPR requerem que as empresas informem os clientes e procurem remediar o vazamento de dados assim que eles ocorram. Os prejuízos de um vazamento de segurança não são apenas financeiros, mas também ocasionam perda de reputação cada vez mais evidente.

Isso torna essencial para organizações terem um programa de gestão de segurança da informação baseado em frameworks como ISO 27.001, NIST CyberSecurity Framework e CIS. Esses *frameworks* sugerem a adoção de controles e processos que permitem avaliar continuamente a segurança do ambiente organizacional e de todos envolvidos com a operação da empresa, sejam colaboradores, fornecedores e parceiros de negócio.

Além disso, sugerem a criação de procedimentos para incidentes de segurança da informação, de forma que todos os responsáveis por segurança e tecnologia na empresa, saibam como proceder em caso de um vazamento de dados.

INDISPONIBILIDADE

Alguns dos fatores que causam a indisponibilidade podem ser combatidos por meio de planejamento e monitoramento constante. Outros, porém, são gerados a partir de ações externas e o que resta ao empresário é tentar agir o mais rápido possível para devolver normalidade às operações. Entre esses fatores, estão:

ACIDENTES E DESASTRES NATURAIS: enchente, incêndio, tempestade ou terremoto no local onde estão instalados os Data Centers pode ser uma catástrofe para qualquer empresa que não tenha um plano de recuperação de desastres. *Backup* em outros lugares físicos ou na Nuvem são algumas opções para recuperar os dados que foram perdidos por esses motivos.

FALHAS NOS SERVIÇOS DE TERCEIROS: quando um prestador de serviços em TI tem algum dano que possa interferir no sistema do cliente, no mínimo deve oferecer suporte para que a situação se normalize.

ERROS NO SCRIPT: esses erros podem causar perda de acesso do usuário por meio de *login* e senha, mesmo que o SQL esteja intacto. A solução é encontrar o erro o mais rápido possível e dispor de ferramentas para reorganizar as funções e implementar melhorias.

ESCOLHA DE SISTEMA ERRADO PARA O DATA CENTER: centro de dados é onde se concentram os servidores, equipamentos de armazenamento e processamento de informações, além de switches e roteadores. O que significa que deve ficar o mais distante possível de falhas.

ROUBO DE IDENTIDADE

A definição de roubo de identidade é **a aquisição não consensual das informações pessoais confidenciais de alguém**. Simplificando, é quando alguém rouba seus dados pessoais, por exemplo, seu CPF ou outro número de identificação, as

informações do seu cartão de crédito, a data do seu aniversário etc.. Normalmente, os ladrões de identidade usam essas informações para compras, obter crédito ou realizar outras ações indesejadas em seu nome.

Roubo de identidade e fraude de identidade são dois conceitos intimamente relacionados e confundidos com frequência, mas não são exatamente iguais. O roubo de identidade refere-se ao ato de adquirir os dados pessoais confidenciais de alguém sem o consentimento dela. Para definir fraude de identidade, precisamos ver o que as pessoas podem fazer com essas informações. Assim, o roubo de identidade torna-se fraude de identidade quando o ladrão usa seus dados pessoais para realizar ações indesejadas em seu nome. Atualmente, a fraude de identidade se tornou uma forma comum de crime cibernético. Esses são só alguns exemplos do que um ladrão de identidade pode fazer quando comete uma fraude com seus dados pessoais:

- Esvaziar sua conta bancária;
- Abrir novas linhas de crédito;
- Fazer compras com seus cartões de crédito;
- Obter documentos legais em seu nome;
- Abrir contas bancárias e pedir empréstimos;
- Usar seu seguro de saúde para receber tratamento;
- Apresentar declarações fiscais e solicitar restituições;
- Controlar suas contas de mídia social.

Para obter detalhes pessoais, os criminosos cibernéticos têm várias ferramentas à disposição. Aqui, veremos como eles cometem roubo de identidade e o que é considerado roubo de identidade no mundo on-line atual.

- Navegação desprotegida;
- Vazamentos de dados;
- Dados pessoais na *dark web*;
- *Software* malicioso;
- Ataques de *phishing* e *pharming*;
- Invasão de Wi-Fi;
- Invasão de e-mail.

MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

PRÁTICAS PARA UMA POLÍTICA DE SENHAS EFICAZ

POLÍTICA DE SENHAS: A maioria das violações de *hackers* é feita a partir de senhas corporativas legítimas consideradas fracas. O sequestro de dados feito por *ransomwares* foi um dos ataques mais frequentes nos últimos dois anos. Sua causa, quase sempre, foi por comportamento inadequado no ambiente de trabalho.

Casos como esses, reforçam a importância de garantir que os usuários da rede corporativa realizem acessos seguros aos dados da empresa. A política de senhas surge nesse cenário para resolver a situação.

CRIAÇÃO DE SENHAS FORTES: O primeiro passo parece óbvio, mas no dia a dia corrido das empresas, muitos funcionários acabam criando senhas fracas para não se esquecerem delas. No entanto, isso pode causar grandes problemas.

Senhas fáceis, que possuem dados como datas de nascimento, endereços ou outras informações pessoais dos usuários podem ser facilmente descobertas por criminosos. Por esse motivo, é fundamental que funcionários criem senhas fortes e sem dados importantes sobre si para dificultar o trabalho dos *hackers*. Estabelecer um número mínimo de dígitos, como de 8 caracteres, por exemplo, pode ajudar.

UTILIZAÇÃO DE CARACTERES DIFERENTES: Essa prática é complementar à apresentada anteriormente. A utilização de palavras únicas ou até mesmo frases curtas não garantem a segurança da senha.

NÃO UTILIZAR A MESMA SENHA EM TODAS AS CONTAS: Outro grande erro cometido por muitos usuários em busca de agilidade é utilizar a mesma senha para todos os seus *logins* ou apenas trocar algumas letras ou números no final. Nesses casos, quando uma invasão acontece, a empresa pode sofrer com um efeito dominó, em que diversos acessos daquele usuário serão invadidos.

TROCA PERIÓDICA DAS SENHAS: Além da utilização de padrões mais complexos para garantir a proteção das senhas, é necessário tomar outra medida para reforçar a segurança. É preciso aplicar uma regra para todos os usuários, solicitando que a senha seja alterada a cada período estabelecido. Desse modo, os usuários adquirem o hábito de atualizar suas chaves de acesso, limpando um possível rastro que poderia permitir a entrada de desconhecidos.

UTILIZAR SOFTWARES PARA GUARDAR SENHAS: Muitos usuários não seguem essas práticas por não conseguirem se lembrar de senhas extensas e que precisam ser trocadas com frequência. No entanto, isso não é necessário. É possível utilizar *softwares* de gerenciamento de senhas. Eles permitem que os usuários salvem suas senhas de forma segura.

IMPLEMENTAÇÃO DE SISTEMAS DE BLOQUEIO DE CONTAS: Outra prática importante que deve fazer parte das políticas de senha de seus clientes é o bloqueio de contas caso haja algum problema. Caso alguém tente entrar no sistema com o *login* de algum funcionário, ou algum dispositivo conectado seja roubado, é preciso que o acesso seja bloqueado imediatamente para evitar o acesso de terceiros.

Para evitar riscos desnecessários, a empresa deve implementar um sistema capaz de bloquear o acesso às contas depois de um certo número de tentativas. Por meio desse tipo de sistema, a TI é notificada por e-mail, relatando as tentativas mal sucedidas e, assim, pode tomar as medidas necessárias.

CONSCIENTIZAÇÃO DOS FUNCIONÁRIOS: Não basta estabelecer diversas regras de proteção se elas não são seguidas. É necessário conscientizar todos os usuários sobre a importância da política de senhas e de segui-la. Para isso, as empresas devem oferecer treinamentos sobre segurança, promover reuniões para abordar o assunto, tirar dúvidas, indicar as melhores práticas, entre outras ações. Os colaboradores devem saber que o compartilhamento de suas senhas, mesmo com membros de seu time de trabalho, é proibido.

UTILIZAÇÃO DE SOFTWARES DE MONITORAMENTO: Para contar com uma política de senhas eficaz, é preciso que a TI tenha o registro de todos os acessos ao sistema. Por isso, cada *login* deve ser utilizado unicamente pelo colaborador em questão. Há *softwares* desenvolvidos especialmente para auxiliar no gerenciamento de senhas. Eles permitem que a TI tenha uma visão geral do nível de segurança de cada senha, monitoramento dos usuários com acessos privilegiados, entre outras funções.

Assim, é possível garantir que todos os usuários estão utilizando seus *logins* corretamente.

Ao estabelecer uma política de senhas, o ambiente de trabalho de seus clientes se torna mais seguro. Portanto, não perca tempo e coloque-as em prática em sua revenda de TI e também auxilie seus clientes na adoção de todas as medidas citadas.

POLÍTICA DE BACKUP

Para proteger os dados de forma eficiente, é necessária a elaboração de uma política de *backup*, na qual constará todas as decisões sobre o armazenamento de dados.

A política de *backup* é imprescindível para as atividades do setor de TI. Nela deverão constar os dados prioritários que devem ser copiados, possíveis riscos que a empresa está sujeita, medidas que deverão ser tomadas, etc.. Todas essas tarefas precisam manter a empresa competitiva, sem aumentar os custos.

POLÍTICA DE PRIVACIDADE

Também chamada de termos e condições de segurança por alguns sites, a política de privacidade refere-se às práticas e processos adotadas por um site, app ou outro tipo de provedor de aplicação para tornar transparente sua relação com o usuário. Basicamente, ela informa ao usuário todos os direitos, garantias, formas de uso, dados recolhidos, processamento e descarte dessas informações pessoais.

Normalmente, esses sites e provedores de aplicação pedem que o usuário, ao preencher seu cadastro ou iniciar o uso da plataforma, **demonstre seu expresso consentimento e concordância com esses termos.** É uma maneira não apenas de informar ao usuário o que será feito com seus dados, como também isentar o provedor de qualquer responsabilidade decorrente da falta de consentimento.

Um dos principais aspectos de qualquer política de privacidade **diz respeito aos dados de identificação dos usuários.** Hoje em dia, com plataformas cada vez mais múltiplas e conectadas, isso vai muito além de um nome e sobrenome. Dados de identificação também podem ser o número de seu documento de identidade, CPF, e-mail, *username*, imagem pessoal, número de IP (*internet protocol*) de seu computador ou dispositivo de acesso à internet (*tablet*, *smatphone*, etc.).

Todas essas informações servem para a identificação dos usuários de sites e aplicativos, por isso **devem ser tratadas com cuidado e confidencialidade por parte das empresas** afinal, o vazamento desses dados podem ter consequências graves não apenas para o usuário, mas também para os provedores de serviços.

Sites de e-commerce são os que mais necessitam dos endereços de seus usuários para a realização de cadastros. Esses dados são utilizados não apenas para a entrega de produtos e para a prestação de serviços, como também para a **emissão de documentos fiscais, especialmente em transações que envolvem o recolhimento de impostos.** É preciso saber se o usuário é pessoa física ou jurídica, e onde sua sede ou residência está localizada. Além do endereço, sites de e-commerce também exigem com frequência o compartilhamento de dados bancários de seus usuários, seja para o estabelecimento de débito automático na prestação de serviços contínuos, seja para a realização de transações bancárias, como pagamentos e transferências por meio de cartão de crédito, por exemplo.

Lembre-se que os dados bancários não são fornecidos apenas por quem tem que realizar um pagamento pela internet. Muitas vezes, sites e apps de economia de compartilhamento (Airbnb, Uber, etc..), compra e venda de produtos entre consumidores e até mesmo empresas digitais de finanças (fintechs), também recolhem os dados pessoais de seus usuários para realizar depósitos. Esses dados bancários são essenciais para o modelo de negócio dessas empresas, mas devem constar também na política de privacidade.

POLÍTICA DE CONFIDENCIALIDADE

O **termo de confidencialidade** ou Acordo Secreto ou Acordo de Não Divulgação é um acordo de caráter tipicamente empresarial que tem como objetivo assegurar que determinadas informações estratégicas sejam mantidas em sigilo. Também conhecido como **NDA – *Non Disclosure Agreement*** – ou acordo de sigilo, é um documento jurídico acertado por duas ou mais partes.

O **NDA** se tornou bastante recorrente no atual cenário, marcado por projetos e inovação tecnológica. Fundamentado em um **termo de acordo entre partes,** o **termo de confidencialidade** evita que os envolvidos ou até mesmo terceiros divulguem informações importantes sobre uma empresa, transação, contrato ou processo.

Para muitos profissionais da área jurídica, a confidencialidade é um aspecto indispensável no dia a dia dos empresários, visto que o **termo de confidencialidade** caracteriza-se como um instrumento de proteção de informações sigilosas e estipula regras de conduta e atuação entre as partes envolvidas.

Mas como funciona o **termo de confidencialidade?** Basicamente, estabelece-se um contrato legal que protege os direitos das partes envolvidas. Ao assinar este **termo de confidencialidade**, as partes estão impedidas de divulgar ou se beneficiar de uma informação considerada confidencial e de extrema importância para os negócios de uma companhia.

Um exemplo para entender a importância de **um termo de confidencialidade** é o caso de empresas de tecnologia, **startups**, pesquisadores ou empreendedores que, durante algum processo de negociação, não querem que a sua ideia, produto ou serviço seja divulgado para outras pessoas. Para proteger este material sigiloso, assina-se um **termo de acordo entre as partes** que evitará o vazamento de informações.

Do mesmo modo, se o sigilo das informações estratégicas é muito importante para o sucesso de uma empresa, esta precisa de proteção, ou seja, de um **termo de confidencialidade**. Se a empresa estiver negociando com outra para o desenvolvimento de um projeto inovador, o **NDA** pode assegurar que informações substanciais sobre ideias ou processos não sejam divulgados antes mesmo do fechamento do contrato.

CRIPTOGRAFIA

O termo Criptografia surgiu da fusão das palavras gregas "Kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de regras que visam codificar a informação de forma que só o emissor e o receptor consiga decifrá-la. Para isso, várias técnicas são usadas e, ao passar do tempo, modificadas, aperfeiçoadas, sendo que novas outras surgem, de maneira que fiquem mais seguras.

Na computação, a técnica usada é a de chaves, as chamadas "CHAVES CRIPTOGRAFICAS". Trata-se de um conjunto de bit's baseado em um algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave diferente e incompatível com a do emissor, ela não conseguirá ter a informação.

A primeira técnica de criptografia usava apenas um algoritmo de decodificação. Assim, bastava o receptor do algoritmo para decifrá-la. Porém, se um intruso conhecesse esse algoritmo, poderia decifrar a informações caso capturasse os dados criptografados. Ainda existe outro problema, imagine: Se a pessoa A tivesse que enviar uma informação para a pessoa B, e a pessoa C tivesse que receber uma informação da pessoa A, mas a pessoa C não pode saber a informação passada a pessoa B, mas para a pessoa B e a pessoa C obterem a informação precisariam ter o algoritmo, assim precisaríamos ter mais de um algoritmo.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Por meio do uso da criptografia você pode: Proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda; criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas; proteger seus *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias; proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas.

Você já deve ter ouvido chave de 64 bit's, chave de 128 bit's e assim por diante. Esses valores expressam o tamanho das chaves. Quanto mais bits's forem usados, mais seguro será o código. Por exemplo, se for usado um algoritmo oito bit's, apenas 256 chaves poderão ser utilizadas (2 elevado a 8). Por isso, sabemos que esse código é inseguro, pois uma pessoa pode gerar 256 combinações diferentes. Agora, faça a conta da chave 128 (2 elevado a 128). O resultado é um número de chaves extremamente elevado.

FIREWALL

Na informática, os *firewalls* são aplicativos ou equipamentos que ficam entre um link de comunicação e um computador, checando e filtrando todo o fluxo de dados. Esse tipo de solução serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade deles.

Os firewalls em forma de *hardware* são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais. A vantagem de usar equipamentos desse tipo é que o *hardware* é dedicado, em vez de compartilhar recursos com outros aplicativos. Dessa forma, o *firewall* pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

ANTIVÍRUS

São aplicativos que detectam programas maliciosos e são capazes de removê-los ou colocá-los em quarentena. Normalmente agem de forma preventiva, detectando ameaças antes mesmo que elas sejam instaladas e comecem a agir, mas também são capazes de remediar os problemas após a infecção.

Um antivírus roda constantemente no computador, sempre atento aos arquivos que são baixados da internet e ao uso de dispositivos como pendrives, dois dos principais caminhos pelos quais os programas maliciosos se propagam.

Esses programas são extremamente úteis e, na maioria dos casos, indispensáveis. É muito fácil contaminar o computador navegando na internet, ao abrir páginas suspeitas ou baixar arquivos infectados, e um antivírus eficaz estará sempre atento, em busca de arquivos perigosos.