LEI GERAL DE PROTEÇÃO DE DADOS E AS INVESTIGAÇÕES CORPORATIVAS

Fernanda Maia

Remilina Yun

Rafael Siqueira

Thiago Braga

Maria L. Gándara

Mariana Moura

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL

Tudo o que amplia o debate sobre as causas e efeitos do risco comportamental é o início da mudança que queremos.

Nós acreditamos que o conhecimento é a base para empoderar as pessoas e transformar o ambiente empresarial de dentro para fora, com técnica e rigor científico. Por isso, um dos pilares do IPRC tem a ver com conteúdo, que ora é feito dentro de casa, ora surge por meio de parcerias, como é o caso deste livro que você tem em mãos.

Criado por advogados, consultores e especialistas em Segurança de Informação, o e-book *"Lei Geral de Proteção de Dados e as Investigações Corporativas"* analisa os reflexos da nova LGPD no cenário brasileiro e mostra o caminho legal a ser seguido pelas organizações que fazem monitoramento, inspeção e investigação de dados.

O livro também explica a importância da cultura, da transparência e da atuação das pessoas no que diz respeito à segurança de informações.

Esperamos que a sua leitura seja agradável, didática e dinâmica. E que, ao terminar o livro, você possa compartilhar com seus colaboradores e terceiros o conhecimento adquirido.

Um abraço

IPRC
INSTITUTO DE PESQUISA DO
RISCO COMPORTAMENTAL

Nota de Agradecimento

Esse e-book foi desenvolvido a partir de uma iniciativa que começou em Agosto/2018, o grupo LGPD Acadêmico, o qual é composto por voluntários do Brasil inteiro, apaixonados pelo mundo da privacidade e com objetivo comum – aprender e compartilhar.

Assim, seguimos com os agradecimentos ao amigo Dirceu Santa Rosa por ter nos inseridos ao seleto grupo de proteção de dados.

Ao Renato Santos, amigo, professor e mentor que instiga nossa paixão e curiosidade sobre a conduta humana.

Ao IPRC por ser incubadora desse material, abrindo as portas para iniciativa desse grupo.

Ao Marcel Leonardi por ser sempre solícito e paciente em ensinar e atender aos pedidos de duas pessoas que o admiram muito.

Remi e Fernanda

SUMÁRIO *executivo*

- O presente e-book possui uma visão teórica e prática das alterações que a nova Lei Geral de Proteção de Dados, nº 13.709/18, trouxe no cenário de investigações corporativas;

- Nessa perspectiva, o início do trabalho, realizado por diversos profissionais relacionados às áreas abordadas, teve por ponto de partida a análise do reflexo da nova legislação no cenário brasileiro, enquadrando os princípios da privacidade junto com a legalidade do monitoramento, inspeção/ investigação dos dados.

- Na sequência - e com um olhar prático - este e-book desmembra o passo a passo da investigação corporativa a partir do canal de denúncia, do background checking e da apuração da denúncia (registro, apuração de dados, investigação, entrevistas e relatórios), sempre sob a luz da nova legislação e apresentando as novidades da lei, por exemplo, como será a atuação do encarregado (Data Protection Officer) nas investigações.

Autores

Reflexo da Proteção de Dados nas Investigações Corporativas

Fernanda Maia

Advogada atuante na área de Direito Digital, Proteção de Dados e Tecnologia

in/fernanda-maia-2305b0aa/

Rafael Siqueira

Advogado Especialista em Direito Digital, Segurança de Informação e Compliance

in/rafael-siqueira-bb180720/

Remilina Yun (Remi)

Advogada e Auditora Interna Especialista em Gestão de Riscos, Compliance e Investigação Forense

in/remiyun/

Thiago Braga

Consultor de Privacidade e Proteção de Dados, Especialista em Segurança de Informação e Gerenciamento de Projetos

in/thiago-braga-infosec/

Colaboradores

Reflexo da Proteção de Dados nas Investigações Corporativas

Maria Laura Gándara

Revisora e Tradutora formada pela PUC

Mariana Moura

Bacharel em Comunicação Social com habilitação em Publicidade e Propaganda pelo Centro Universitário Belas Artes e designer gráfica

in/mariana-moura-9b3590b5/

Reflexo da LGPD nas Investigações Corporativas elaborada por Fernanda Maia, Rafael Siqueira, Remilina Yun (Remi) e Thiago Braga; está licenciado com uma licença Creative Commons - Atribuição 4.0 Internacional.

Índice

Introdução

Fernanda Maia

Investigação é um processo privado, derivado de um conjunto de diligências realizadas dentro de uma organização, que procura apurar sobre a existência de algum ato ou fato que viole suas normas ou políticas internas e/ou legislação vigente.

A eficácia em uma investigação está na capacidade de proteger os interesses da organização e seus acionistas por meio da prevenção e detecção de má conduta e de uma razoável garantia de que as atividades da organização estejam de acordo com as leis e regulamentações aplicáveis além de, também, identificar as áreas de melhoria para as operações internas.

A investigação ocorre a partir de uma análise de dados coletados pela organização em diversas frentes, tais como e-mails corporativos, entrevistas exploratórias e/ou confirmatórias, análise documental, *background check*, avaliação do *lifestyle* (estilo de vida), entre outros, sendo também realizadas a coleta de dados sensíveis.

Este e-book tem o objetivo de discorrer a respeito das alterações que o setor das investigações corporativas sofrerá a partir da vigência da nova Lei Geral de Proteção de Dados nº 13.709/18, sancionada no dia 14/08/2018, atualmente em vacatio legis, e que entrará em vigência em 16 de agosto de 2020.

Tratando-se da regulamentação de proteção de dados no aspecto jurídico brasileiro, a nova lei atingirá diretamente a estrutura das investigações internas, que são baseadas nos dados coletados e tratados pela própria empresa.

Logo, para realizar esta análise, é preciso entender, primeiramente, os limites entre as normas de proteção de dados e as normas de investigações internas, dissecando as nuances das fases da investigação, da coleta dos dados e seus tratamentos.

Sob essa perspectiva, o presente e-book discorrerá sobre os reflexos da regulamentação geral de proteção de dados (regulamentação europeia utilizada como base para o texto da lei brasileira que está em vigor desde 25/05/2018) para então aprofundar nas fases da investigação, sempre analisado à luz da Lei Geral de Proteção de Dados, conhecida hoje como LGPD.

Desmistificação: LGPD x Investigações Corporativas

Fernanda Maia

O artigo 4º da LGPD prevê as hipóteses de exclusão de sua aplicabilidade. Um dos apontamentos é: "atividades de investigação e repressão de infrações penais."

A interpretação deste dispositivo é taxativa, o que significa que essa exclusão de aplicabilidade da LGPD é, única e exclusivamente, para situações de investigação criminal, o que não atinge as investigações corporativas.

O parágrafo 2º deste artigo aponta o cenário em que uma pessoa jurídica privada se valerá dessa exceção. Todavia, esta pessoa jurídica precisará atuar no auxílio de uma investigação criminal feita pelo poder público e, portanto, estará realizando os serviços para fins públicos.

O antigo "Article 29 Data Protection Working Party", órgão consultivo constituído por um representante da autoridade de proteção de dados de cada Estado-Membro da UE, da **Autoridade Europeia para a Proteção de Dados** e da Comissão Europeia, possui entendimentos consolidados referentes às investigações corporativas e o não enquadramento na exceção supracitada. Assim, para monitoramento de dados de funcionários e investigações internas corporativas, a base legal de tratamento aplicável seria o legítimo interesse.

Reflexo da Proteção de Dados nas Investigações Corporativas

Fernanda Maia

Nas rotinas cotidianas de organizações, a figura do risco sempre se faz presente, pois as organizações estão lidando cada vez mais com temas relacionadas **à *corrupção, abusos, fraudes, ética, compliance, entre outros.*** Cada tema envolve, direta ou indiretamente, a reputação das empresas, então se cada setor não estiver sempre alinhado com as legislações vigentes, melhores práticas e normas internas de cada organização e da sociedade, pode se deparar com diversos riscos para seus negócios e imagem.

RISCO: *evento futuro identificado, ao qual é possível associar uma distribuição de probabilidades de ocorrência.* ***Incerteza****: evento futuro identificado, ao qual não é possível associar uma distribuição de probabilidades de ocorrência.* ***Ignorância****: eventos futuros que, no momento da análise, não poderão sequer ser identificados, muito menos quantificados* ***(M. Faber, R. Manstetten e J. Proops, Ecological Economics: Concepts and Methods, 1996, pp. 209-211.)***

O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite de risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

De acordo com o Código das Melhores Práticas de Governança Corporativa do IBGC:

Os riscos a que a organização está sujeita devem ser gerenciados para subsidiar a tomada de decisão [...]. Os agentes de governança têm responsabilidade em assegurar que toda a organização esteja em conformidade com os seus princípios e valores, refletidos em políticas, procedimentos e normas internas, e com as leis e os dispositivos regulatórios a que esteja submetida" (IBGC, Código das Melhores Práticas de Governança Corporativa, 5ª edição, 2015, p. 91.).

Os agentes envolvidos nos processos, que procuram minimizar e mitigar os riscos, realizam ações preventivas, corretivas e detectivas como, por exemplo, investigações corporativas onde analisam, armazenam, trocam, coletam, entre outras ações, diversos dados, sejam pessoais (por exemplo: funcionários), ou da pessoa jurídica em si.

Na sociedade brasileira o tratamento de dados pessoais é uma realidade que até pouco tempo não possuía regulamentação específica. Contudo, em 14/08/2018, foi sancionada a LGPD que procurou regulamentar a troca, os tratamento e tudo mais que pode envolver dados.

Vale salientar que antes do surgimento da LGPD era possível encontrar em algumas leis definições sobre dados pessoais e tratamentos, como no Decreto do Marco Civil da Internet nº 8771/16, (artigos 13 e 14) e no Marco Civil da Internet (artigo 7º).

Os requisitos, relativos à regulamentação europeia, afetam as investigações já na fase inicial, onde é realizada a solicitação dos dados necessários, visto que a revisão, divulgação e/ou transferência desses dados, seja para empresas afiliadas, fornecedores ou autoridades forenses de TI , devem sempre ser justificadas, assim como o tratamento desses dados, que deve acontecer sempre de forma transparente, informando os titulares sobre sua utilização.

O processamento à luz da regulamentação, tanto europeia quanto brasileira, é limitado ao "necessário" para atingir o fim desejado, o que, na prática, implica em uma filtragem cuidadosa dos dados.

Ambas as regulamentações irão afetar a investigação quanto ao papel do encarregado de proteção de dados ou DPO (Data Protection Officer) que deverá ser informado de todo o passo a passo da utilização e zelar pelo respeito aos princípios e direitos previstos na lei.

A LGPD traz um cenário de adaptações para as investigações corporativas, as quais deverão observar os princípios previstos no art. 2º, como, por exemplo, o respeito à privacidade, desenvolvimento econômico e tecnológico e à inovação, entre outros, e enquadrado o tratamento em uma das dez hipóteses legais previstas no art. 7º.

Do Direito à privacidade e viabilização jurídica de monitoramento, inspeção/ investigação

Rafael Siqueira & Fernanda Maia

O empregador deve garantir o uso adequado das informações e dos recursos de tecnologia de sua propriedade ou sob sua responsabilidade em razão da lei vigente.

Em seus Artigos 927, 932, III, 933 e 1.016, o Código Civil Brasileiro **estabelece que o empregador é responsável pela reparação civil dos atos praticados por seus funcionários, mesmo que não haja culpa de sua parte:**

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL

Art. 927

Aquele que, por ato ilícito ***(arts. 186 e 187)****, causar dano a outrem, fica obrigado a repará-lo. (...)*

Art. 932

São também responsáveis pela reparação civil: (...)

III

O empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele; (...)

Art. 933

As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos. (...)

Art. 1.016

Os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções.

Ainda, em complemento ao texto legal, o Supremo Tribunal Federal explicitou em sua Súmula nº 341 que "*é presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto*".

Entretanto, para a validade legal da inspeção de dispositivos, há direitos que precisam ser respeitados. A privacidade é o principal direito fundamental que limita a prática da inspeção do dispositivo pelo empregador. Antes da lei nº 13.709/18, a doutrina e jurisprudência produziram alguns conceitos para o termo "privacidade", sendo um deles o controle sobre informações e dados pessoais. Portanto, entende-se a privacidade como a "reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que extensão informações a seu respeito são comunicadas a terceiros" (LEONARDI, 2012, p. 67).

Assim, a violação da privacidade configura violação a direito fundamental protegido pela Constituição Federal (art. 5º, X e XII), pelo Código Civil (art. 21) e, como previamente citado, pela Lei Geral de Proteção de Dados Pessoais.

Sobre as questões éticas e legais, podemos citar a doutrina de João Carlos Leal Júnior et al. que afirma:

> *Assim, vale dizer que o empregador tem o direito de monitorar a forma como se desenvolve o serviço de seus empregados, para que reste adimplida a obrigação nascida com o contrato de trabalho, garantindo-se o regular funcionamento de sua empresa. Em contrapartida, a fiscalização do trabalho do funcionário deve respeitar como um* ***todo seus direitos da personalidade, como a intimidade e a privacidade, não sendo permitido o monitoramento abusivo ou de caráter oculto****. Ademais, o rigor excessivo na vigilância autoriza o empregado a rescindir seu contrato e a pleitear indenização judicialmente." (grifo nosso).*

No mesmo sentido, a doutrina de Patrícia Peck Pinheiro, que afirma:

> *A privacidade é um tema importantíssimo para a gestão legal da Segurança da Informação, com efeitos em diversas esferas. Em princípio, há alguns aspectos que precisam ser observados, sob pena de se cometerem infrações legais no gerenciamento e proteção dos ativos da empresa. Esses aspectos consistem em observar: a vida privada (assuntos de cunho pessoal), a interceptação (sigilo e confidencialidade tanto da pessoa física como da jurídica), a prova obtida por meio ilegal ou legal e o anonimato.*

Assim sendo, por mais que o empregador seja responsável e deva zelar pelo uso adequado de seus recursos, a privacidade é um direito que deve ser respeitado.

Para que se possa afastar a expectativa de privacidade do colaborador no que tange ao uso dos recursos tecnológicos e informações de propriedade ou sob a responsabilidade do empregador, e a fim de garantir a proteção e segurança das informações e demais ativos corporativos, **é necessário garantir a ciência pelo colaborador do monitoramento realizado nos recursos tecnológicos.**

Nesse sentido, é possível citar a doutrina de Patrícia Peck Pinheiro acerca da validade do monitoramento, conforme segue:

> *Por isso a orientação legal é que seja feito sempre o aviso prévio expresso no próprio ambiente quanto este não for privativo ou estiver sujeito ao monitoramento, visto que a proteção deste direito tão fundamental irá atrair a presunção de privacidade quanto não tiver sido feita previsão clara em contrário ou não se tratar de um ambiente notadamente público.*
> *O aviso serve para validar a captação de dados, imagens e áudios das pessoas que ali transitarem, seja em um contexto presencial e/ou digital. Para o uso do conteúdo capturado posteriormente como prova, é fundamental que haja legitimidade e legalidade da captura.*
> *(...)*
> *No caso da empresa, se ela deixa claro que o e-mail corporativo é de sua propriedade, que o ambiente é monitorado, inserindo essa informação nos rodapés de e-mails para dar publicidade inequívoca, possui uma política clara, então o uso de dados coletados nessa caixa postal corporativa não gerará problemas legais. Mas se tais etapas não forem cumpridas, não há presunção de propriedade da empresa; a presunção é de privacidade e vai favorecer a parte desprotegida, que na maioria dos casos é o empregado.*

Tanto a ciência do monitoramento quanto a possível inspeção de dispositivo podem ser incluídas em contrato de trabalho, de prestação de serviços e em normas específicas, seja para colaboradores, seja para terceiros segundo Patrícia Peck Pinheiro:

> *Os empregados cujo vínculo empregatício é regido pela CLT (Consolidação das Leis do Trabalho) e os empregados temporários podem ser advertidos do monitoramento pelo Contrato de Trabalho ou pela Política de Segurança. É interessante vincular a Política de Segurança da Informação ao Contrato de Trabalho, pois dessa forma o empregado não poderá alegar desconhecimento da referida Política de Segurança.*

> *Já para os demais colaboradores, que sejam prestadores de serviços que apresentem nota fiscal, pode haver a apresentação da Política de Segurança da Informação (PSI), caso exista, e se possível, um anexo ao contrato de prestação de serviços, ou a inserção da cláusula de monitoramento no próprio NDA ou Termo de Confidencialidade.*

Entretanto, por mais que seja dada ciência ao colaborador e que este seja instruído a somente utilizar o equipamento corporativo para os fins da empresa, deve-se tomar medidas para evitar que sejam consultadas informações de cunho particular, pois poderia haver afronta à Lei Geral de Proteção de Dados, nº 13.709 de 2018. Neste ponto, Patrícia Peck Pinheiro explica:

> *No entanto, apesar do aviso, a "câmera" não escolhe o que está gravando. Por isso, pode ocorrer que o monitoramento acabe gerando acesso a conteúdo de ordem particular, íntima e pessoal que estejam trafegando no e-mail corporativo ou que tenham sido salvos ou armazenados nos computadores ou servidores da empresa.*
>
> *Por esse motivo o monitoramento deve ser realizado por uma equipe treinada, e ocorrer de modo centralizado, com procedimentos-padrão, nas quais o relatório de monitoramento deve ser utilizado apenas para fins de investigação de casos específicos, em que se demonstre infração ao código de conduta, prática de ilícito ou crime, ou mediante solicitação das Autoridades Competentes.*

Como já mencionado, a legislação brasileira agora possui a LGPD que regulamenta tratamento indevido de dados pessoais o que poderá resultar em multas expressivas e sanções administrativas.

Neste sentido, há que se apontar as hipóteses nas quais é possível que seja realizado o tratamento de dados pessoais. Primeiramente, cabe a definição de dado pessoal, bem como a definição de tratamento, controlador e operador como dispõe o artigo 5º da LGPD.

Dado Pessoal:

informação relacionada a pessoa natural identificada ou identificável;

Controlador:

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador:

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Tratamento:

toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Restando claras as definições acima, é necessário esclarecer que em uma relação de "Empregador e Empregado", apenas o consentimento do titular do dado, ou seja, do empregado, não será considerado suficiente, mesmo com a previsão legal do inciso I, artigo 7º da LGPD, tendo em vista a subordinação direta que existe entre as Partes, que pode afetar a validade do consentimento.

Assim, para tratar dados neste contexto é importante considerar outras hipóteses de tratamento previstas no artigo 7º, lembrando que não existe hierarquia entre elas.
Dessa maneira, na investigação corporativa a base que melhor se adequa é a do Legítimo Interesse, prevista no inciso IX do art. 7º e definida no artigo 10º conforme segue:

Art. 10.

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:

I

Apoio e promoção de atividades do controlador; e

II

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, nos termos desta Lei.

§ 1º

Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º

O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º

A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

Importante ressaltar que, para justificar o uso do legítimo interesse, é necessário realizar um teste de três partes - ICO, 2017 que são:

TESTE DE EQUILÍBRIO

(*equilibrá-lo contra os interesses, direitos e liberdades do indivíduo*)

TESTE DE NECESSIDADE

(*mostrar que o tratamento é necessário para alcançá-lo*)

TESTE DE PROPÓSITO

(*identificar um interesse legítimo*)

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL

Finalmente, em última análise, caso haja acesso a conteúdos privados encontrados nos dispositivos e/ou ambiente lógico corporativos, e o empregador deseje fazer uso destas informações, deve comprovar o legítimo interesse de modo, a fundamentar o tratamento de dados pessoais para as finalidades de investigações corporativas.

Desta maneira, para o presente tratamento é necessário cautela para não excedê-lo e ultrapassar a finalidade definida a priori, a fim de não coletar mais dados do que o necessário como, por exemplo, dados sensíveis que possam violar o direito de privacidade e intimidade do empregado, devendo, neste caso, o empregador realizar o imediato descarte seguro, sob pena de incidir em sanções que variam desde a aplicação de advertência e multa até o bloqueio ou a suspensão do tratamento.

Canal de Denúncia

Remilina Yun (Remi)

Como é sabido, a Lei de Anticorrupção ou Lei da Empresa Limpa (**Lei Federal nº. 12.846/2013**) e o decreto que a regulamenta (**Decreto Federal nº. 8.420/2015**) não obrigam as organizações a ter um canal de denúncias, que é um dos pilares de um programa de compliance.

Entretanto, o estabelecimento de um programa de compliance efetivo, incluindo um canal de denúncias, não é só um diferencial competitivo, mas também um meio preventivo e detectivo de não conformidades, desde um assédio moral até um caso de corrupção.

Além disso, quanto à aplicação de penalidades, a lei em seu artigo 7º dispõe inúmeros fatores que serão levados em consideração para a aplicação das sanções, sendo uma delas o inciso VIII - *a existência de mecanismos e procedimentos internos de integridade, auditoria e* ***incentivo à denúncia de irregularidades***

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL

e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;

Segundo o Decreto nº 8.420/2015, especificamente em seu capítulo IV, foram estabelecidos os parâmetros de avaliação dos programa de integridade, sendo um dos critérios a existência de "***canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciantes de boa-fé***".

Com a LGPD, não se vislumbra um caminho diferente; ao contrário: em respeito aos direitos dos titulares de dados, identifica-se uma necessidade de criação de um canal de comunicação entre o controlador e os titulares de dados.

Contudo, a lei não especifica o formato e/ou estrutura deste canal, cabendo, assim, à Autoridade Nacional de Proteção de Dados essa responsabilidade (ANPD).

Dos Direitos do Titular de Dados Pessoais:

Confirmar a existência de tratamento;

Acessar os dados;

Correção de dados incompletos, inexatos ou desatualizados;

Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;

Portabilidade dos dados a outro fornecedor de produto ou serviço, mediante requisição expressa;

Eliminação dos dados tratados com o consentimento do titular;

Informações das entidades públicas e privadas com as quais o controlador realizou o compartilhamento de dados;

Informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

Revogação do consentimento;

Revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem interesse do titular;

Além da ausência de definições quanto ao formato de canal a ser implementado pelas organizações, identifica-se também a falta de dispositivos quanto à comunicação de um incidente de segurança relativos aos dados pessoais cujo titular, terceiros, entre outras partes interessadas tenham conhecimento ou suspeita.

Mas, independentemente das lacunas a serem preenchidas pela interpretação da LGPD pela ANPD, é defensável a adoção de um canal similar ao canal de denúncias ou ouvidoria, pois caberá ao controlador responder a qualquer tempo, mediante requisição do titular de dados quanto aos seus direitos como dispõe o artigo 18, exceto pela confirmação de existência ou o acesso a dados pessoais que dever ser providenciado em até 15 (quinze) dias, contados da data do requerimento que segue disposto no artigo 19, inciso II da LGPD.

Ainda, em analogia aos pilares de um programa de compliance, a LGPD determina adoção de medidas preventivas quanto a ocorrência de danos em virtude do tratamento de dados pessoais, bem como utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Assim, como não é obrigatório o estabelecimento de programa de compliance, incluindo um canal de denúncias, também o artigo 50 da LGPD apenas faculta aos agentes de tratamento a adoção de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos - incluindo reclamações e petições de titulares -, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Importante ressaltar que mesmo se tratando de uma faculdade dos agentes de tratamento, a adoção de políticas de boas práticas e de governança serão avaliadas pela ANPD em conjunto com as peculiaridades da infração cometida na aplicação de sanções, tal como previsto pelo artigo 52, § 1º, inciso IX da LGPD, resultando, assim, em uma possível atenuante.

Ainda que não seja mandatória para as organizações a existência de um canal de denúncias, percebe-se claramente que o legislador forneceu, tanto na Lei de Anticorrupção quanto na LGPD, incentivos diretos para que as instituições disponibilizem essa ferramenta aos seus públicos, tanto internos quanto externos.

No primeiro momento, tal necessidade estará atrelada às operações do controlador, não existindo, porém, qualquer impedimento para que o operador também estabeleça um canal próprio para recebimento de tais incidentes.

Tendo em vista que não restam dúvidas quanto à necessidade de um canal de comunicação entre os agentes de tratamento e titulares de dados pessoais, a dúvida que paira é sobre a necessidade, ou não, de estabelecer um canal apartado do canal de denúncia ou ouvidoria já existente na organização, uma vez que o estabelecimento de novas estruturas enseja custos e despesas adicionais.

O que podemos esclarecer é que a adoção, ou não, de um novo canal de comunicação depende da estrutura e *core business* da organização, sendo em alguns casos recomendado manter um canal independente para tratamento apenas de incidentes de segurança relativos a dados pessoais e, em outros casos, valer-se de uma estrutura já existente, capacitando os postos de trabalho por meio de conhecimento específico e técnico para a apropriada classificação do chamado e o atendimento aos direitos dos titulares.

Por fim, independentemente da estrutura estabelecida, é fundamental que o encarregado pelo tratamento de dados pessoais devidamente nomeado pela organização tenha a responsabilidade de gerir as demandas, prestando esclarecimentos e adotando as providências aplicáveis como dispõe o artigo 41, §2º, inciso I da LGPD.

Desta maneira, dentro da estrutura do canal de denúncia ou ouvidoria, é necessário deixar claro o papel e a responsabilidade do encarregado, assegurando-se a confidencialidade dos procedimentos, desde o recebimento da suposta irregularidade até sua apuração e/ou providência adotada, resguardando-se, acima de tudo, sua independência em relação aos responsáveis pela apuração.

Da Apuração de Denúncia

Remilina Yun (Remi)

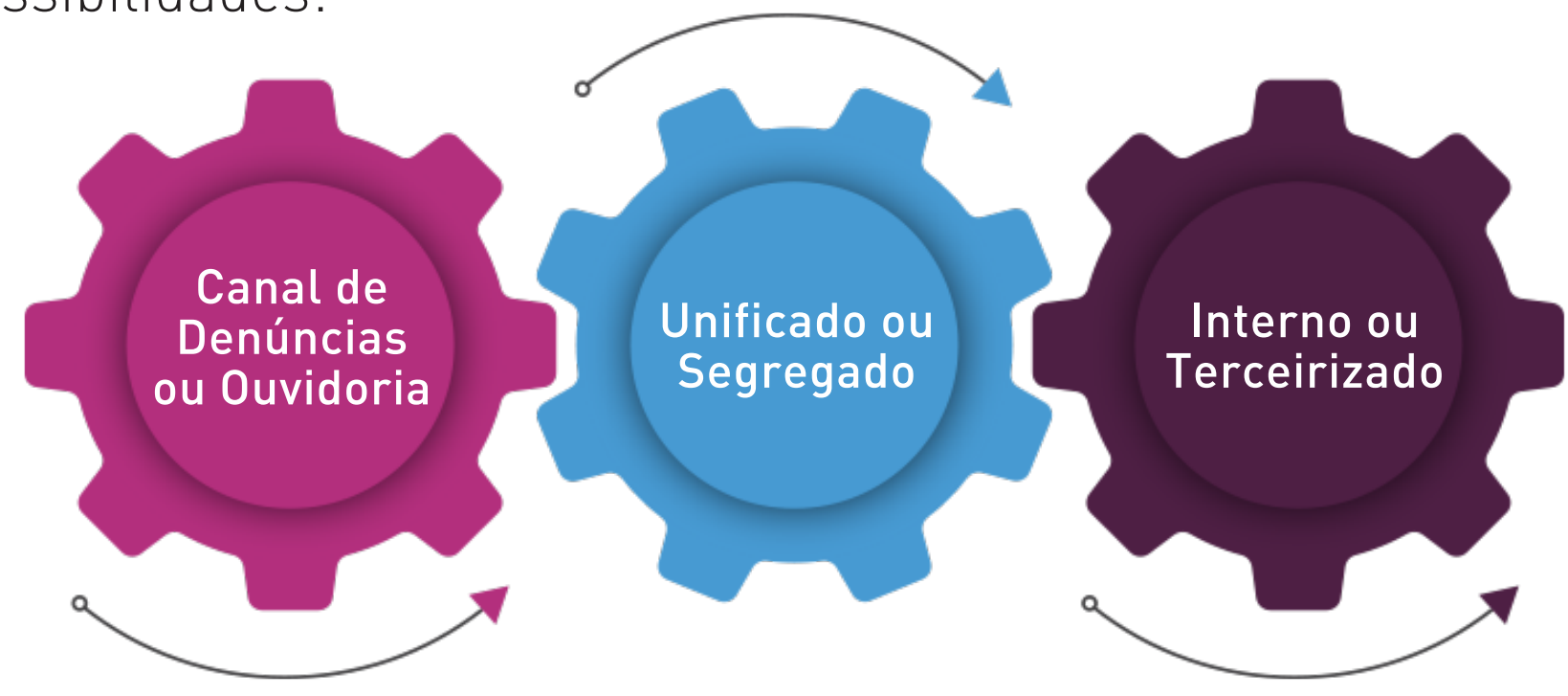
Ainda que não seja mandatória para as organizações a existência de um canal de denúncias, percebe-se claramente que o legislador forneceu, tanto na Lei de Anticorrupção quanto na LGPD, incentivos diretos para que as instituições disponibilizem esses tipos de canais de comunicação aos seus públicos, tanto internos quanto externos.

Esses direitos não devem ser interpretados de maneira taxativa, pois os titulares que tiverem conhecimento ou suspeita de um incidente de segurança relativo aos seus dados pessoais têm a prerrogativa de relatar o problema a um canal oficial e competente pertencente a um dos agentes de tratamento para adoção das medidas apropriadas.

Esses incidentes podem ter por objetivo a prática de fraude, espionagem, desvio, falha ou evento indesejado ou inesperado

que tenham probabilidade de comprometer ou ameaçar a segurança da informação, cujos princípios se resumem na ***Confidencialidade, Integridade e Disponibilidade (CID).***

Assim, independente do formato do canal a ser adotado, o titular de dados ou denunciantes de boa-fé devem ter acesso a um canal aberto que possa reportar irregularidades. Abaixo algumas possibilidades:



Independentemente do formato do canal adotado pela organização, o processo de apuração ou avaliação das irregularidades reportadas deve seguir alguns protocolos, sendo indiferente a natureza da não conformidade ou violação.

Do Recebimento de Irregularidade

Tratando-se de canal de denúncia ou ouvidoria, terceirizada ou não, a organização é responsável por definir canais específicos para recebimento de irregularidades, tais como o *hotline* (0800), formulário, e-mail, caixa postal, etc. Essas irregularidades podem estar relacionadas a uma conduta inadequada (assédio moral, por exemplo) até um incidente de segurança, tal como o vazamento de informações confidenciais.

Importante ressaltar que as diretrizes quanto às informações a serem coletadas, principalmente no que se referem aos "dados pessoais e dados sensíveis", devem estar pré-definidos por meio de questionários e/ou instruções, a fim de respeitar o princípio da necessidade ou minimização de dados (***Data Minimization***), coletando-se apenas dados pessoais que sejam essenciais para finalidade estabelecida, apuração factual da denúncia.

Ao lado, seguem algumas informações/questionamentos realizados para contextualizar a irregularidade relatada pelo Denunciante(s):

Denúncia identificada ou anônima?

Você é colaborador da organização?

Qual a natureza da irregularidade?

Detalhar onde ocorreu;

Descrever a irregularidade;

Como tomou conhecimento da irregularidade?

Quando aconteceu a irregularidade?

Há quanto tempo essa irregularidade tem ocorrido?

Por que a irregularidade ocorreu?

Se for possível mensurar, qual o valor envolvido?

Quem está envolvido diretamente ou indiretamente na irregularidade?

Indique provas/ evidências se existirem e onde podem ser encontradas;

Neste processo em questão não se aplica a minimização da coleta de dados, pois não estamos falando em dados pessoais, mas apenas em detalhamento da irregularidade reportada que, com estes dados, possibilitará a condução da investigação da maneira mais factual possível.

Do Registro

Quando iniciamos o registro da irregularidade, precisamos distingui-la em duas frentes: Incidente de Segurança de Informação (ISI) ou Condutas e Fraudes (C&F).

Quando adentramos nas irregularidades de C&F, seu registro precisa ser efetuado, respeitando-se o processo de anonimização dos dados das partes, ora Denunciante(s) e ou Denunciado(s), entre outros, a fim de embasar a investigação.

O registro em questão pode ser acompanhado de um número sequencial que muitos denominam como *CASE CODE* (Código do Caso), acompanhado de um *CODE NAME* (Nome do Código).

Para se atender aos dispositivos legais da LGPD e as boas práticas, os nomes estabelecidos (*Code Name*) não devem gerar qualquer tipo de associação e/ou identificação da natureza da denúncia, assim como das partes envolvidas.

No registro, é de suma importância definir campos que possam gerar métricas para organização, respeitando-se a confidencialidade e o sigilo das informações coletadas no ato do recebimento das informações.

Abaixo seguem algumas informações que são registradas normalmente:

- Tipo de denúncia: identificada ou anônimo;
- Denúncia identificada: nome, email ou telefone/ celular;
- Natureza da denúncia: assédio, fraude, furto, etc;
- Conteúdo da denúncia;
- Partes envolvidas: nome, empresa, posição, função, etc;

Quando a irregularidade for relativa a Incidente de Segurança de Informação (ISI), deve-se ter à disposição estrutura e equipe capacitada com conhecimento técnico para avaliação e conseguinte registro do relato, como segue abaixo:

1. Identificação de Incidentes

reconhecer a natureza dos incidentes identificados por sistemas de monitoramento ou reportados por meio de diferentes canais.

2. Registro de Chamada

registrar o conteúdo do incidente com o objetivo de criar histórico para eventual consulta quanto ao status de resolução.

3. Categorização da Chamada

classificação quanto ao registro, distinguindo-a em demanda operacional ou incidente. Caso a requisição seja um dos direitos do titular de dados, a mesma deve ser atendida em 15 (quinze) dias, o que torna necessária uma equipe específica para esse tipo de atendimento.

4. Priorização de Incidentes

avaliação através de uma matriz de risco, cujos critérios comumente utilizados são impacto e urgência, ou seja, um incidente urgente é aquele que precisa ser atendido imediatamente por conta da sua gravidade ou para fins de atendimento do prazo legal. Já um incidente impactante é aquele que pode gerar grandes riscos ao negócio.

5. Diagnóstico Inicial de Incidentes

avaliar o incidente reportado,
buscando-se uma solução efetiva.

6. Escalada de Incidentes

direcionamento ao nível competente para tratamento do incidente de acordo com a sua criticidade, por exemplo, caso o primeiro nível não tenha conhecimento técnico para resolução do incidente, será delegado para segundo nível competente.

7. Resolução de Incidentes

comunicação para a parte interessada com a solução adotada, registrando, assim, todas as informações relevantes sobre o incidente e sua resolução.

8. Fechamento do Chamado

encerramento do chamado que deve ser documentado para eventuais consultas.

Da distribuição e definição de stakeholder

- De posse do registro das informações, a irregularidade reportada deve ser investigada por pessoas competentes que possuam habilidades técnicas necessárias para uma apuração apropriada dos fatos, assegurando-se a total imparcialidade do investigador.

- A distribuição das referidas informações deve ser feita de maneira a evitar qualquer vazamento e/ou compartilhamento indevido do conteúdo, a fim de evitar retaliação e/ou prejuízo às partes envolvidas. Isso é possível quando o stakeholder tem ciência de seu papel na investigação por meio de políticas claras ou advertências dentro das comunicações, como e-mails.

- A boa prática recomenda que tal distribuição seja definida de maneira colegiada dependendo da natureza e da gravidade do assunto num comitê composto por pessoas multidisciplinares e estratégicas da organização, a fim de dar a devida *accountability* e *enforcement* da investigação a ser conduzida.

- Quando se tratar de incidente de segurança de informação relativo a dados pessoais, o principal stakeholder é o encarregado de proteção de dados que tem o papel e a responsabilidade de acompanhar, avaliar e revisar o processo de apuração, bem como a solução adotada, para realizar a comunicação junto ao titular de dados e/ou ANPD, razão pela qual deve ser assegurada a sua independência em relação aos responsáveis pela apuração.

Levantamento de Dados

Para buscar a veracidade ou não do fato denunciado, é necessário conduzir algumas pesquisas, como verificar *lifestyle* e antecedentes (background check) do Denunciado, bem como analisar registros internos, que podem ser desde registros internos do colaborador (medidas disciplinares, promoções, férias, jornada de trabalho, etc.), a arquivos de dados do Outlook (PST) e similares, históricos de conversas de meios internos de comunicações da organização, entre outros.

Importante destacar que as informações oriundas das ferramentas internas são propriedade da organização, mas esta diretriz deve estar disposta de maneira clara numa política interna, a fim de dar ciência a todas as partes envolvidas.

Condução de Entrevistas

- A condução de entrevistas é essencial para a integridade e transparência objetivada numa apuração/investigação. Ela pode ser conduzida de duas maneiras: exploratória ou confirmatória.

- A exploratória tem como finalidade questionar e/ou esclarecer processos, atividades e situações específicas, para o melhor entendimento do evento denunciado. Já a entrevista confirmatória normalmente é conduzida quando já se tem certos indícios ou provas quanto ao fato denunciado, ou seja, materialidade e autoria, concedendo, assim, a oportunidade do entrevistado, ora Denunciado, de apresentar a sua versão ou de se buscar a confissão do ato praticado.

- Dificilmente se faz coleta de dados pessoais do entrevistado, mas toda e qualquer informação obtida nessa fase deve ser devidamente registrada e arquivada para evitar qualquer tipo de vazamento ou extravio de informações.

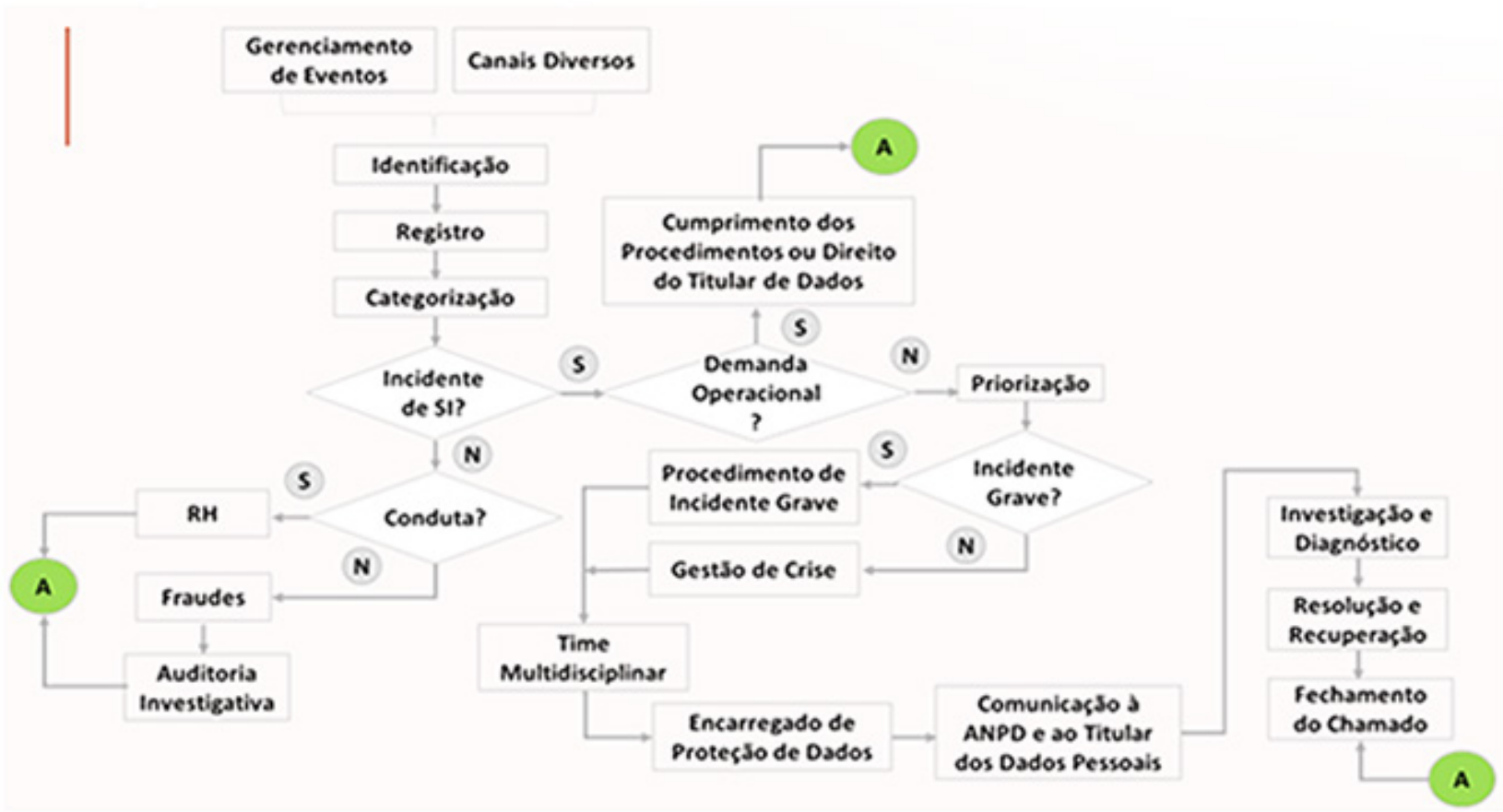
Elaboração de Relatório

Ao concluir o levantamento de informações, uma vez conduzidas as entrevistas, faz-se necessária a elaboração do relatório de maneira coerente, cronológica e devidamente referenciada, por exemplo com anexos e/ou evidências, para facilitar o entendimento do comitê competente quanto ao resultado da investigação, bem como das medidas recomendadas, sejam elas de natureza disciplinar ou até mesmo desligamento.

Recomenda-se que no relatório, em um primeiro momento, faça-se menção das partes envolvidas e, ao discorrer sobre os fatos apurados, utilize-se nomenclaturas genéricas como “DENUNCIADO A / DENUNCIADO B” ou DENUNCIADO 1 / DENUNCIADO 2, a fim de evitar exposição desnecessária. Da mesma maneira, não se recomenda fazer identificação das pessoas que corroboraram os fatos investigados nas entrevistas para não se criar rótulos/ estereótipos quanto ao que foi relatado.

Por fim, no relatório deve estar destacado em negrito uma das classificações definidas na Política de Acesso às Informações, estabelecidas pela organização, que normalmente se enquadram em quatro categorias: confidencial, sigiloso, secreto e restrito.

Fluxograma - Recebimento de Irregularidades



Background Check

Rafael Siqueira & Fernanda Maia

Com o advento da LGPD, ficam agora definidos em lei tanto os conceitos de dados pessoais quanto as bases legais para o tratamento de dados pessoais, entre as quais estão o consentimento e o interesse legítimo na captura de dados pessoais.

A execução do chamado *background check* (investigação de antecedentes) surgiu com a necessidade da realização de averiguações prévias antes da concretização de algumas decisões que poderiam influenciar a empresa, como seus funcionários, dentro de investigações corporativas. Assim, o principal objetivo é o de conhecer e avaliar com profundidade todas as informações úteis para se preservar os valores internos da empresa.

IPRC
INSTITUTO DE PESQUISA DO
RISCO COMPORTAMENTAL

Profissionais de compliance e auditorias investigativas podem se utilizar do *background check*, pelo qual são levantados dados não somente de empresas como também de indivíduos, os quais podem eventualmente ser dados pessoais protegidos pela Lei Geral de Proteção de Dados. Com isso, é necessário compreender como a nova legislação irá afetar, na prática, essas utilizações, que se não forem enquadradas nas hipóteses legais de tratamento serão consideradas ilegais.

Assim, analisando as 10 hipóteses do tratamento de dados, disponíveis no artigo 7º, e conforme já expressado neste e-book, a base que melhor se aplica para legalizar o *background check* é o legítimo interesse, observados os requisitos necessários, assim como a realização e documentação do teste de três fases.

O conceito de “banco de dados” também foi trabalhado pela LGPD, que o define como “conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico”. A utilização de dados pessoais encontrados em banco de dados, para ser considerada lícita e com o menor risco possível, precisará observar algumas garantias, incluindo a qualidade dos dados armazenados.

Para realizar o armazenamento de dados pessoais, o operador/controlador responsável pelo banco de dados precisará obedecer os parâmetros da lei, ou seja, enquadrar o tratamento em uma das 10 hipóteses legais. Quando terceiros quiserem utilizar as informações disponibilizadas publicamente, deve compreender que os dados pessoais publicamente disponíveis não deixam de ser dados pessoais, sendo necessário, mesmo assim, enquadrar o tratamento em uma das 10 bases legais já citadas.

A simples utilização, para uma investigação corporativa ou para a realização de um *background check*, de informações disponíveis em bancos de dados que não estejam em conformidade com a LGPD pode tornar todo o processo de investigação ilegal, seguindo a teoria do princípio do direito penal “fruto da árvore envenenada”. Assim, a partir do momento em que se utilizam dados pessoais tratados em desconformidade com a legislação para a construção de um *background check*, esse processo encontra-se “contaminado” por esta ilegalidade, resultando na ilegalidade desse procedimento.

Governança de Dados

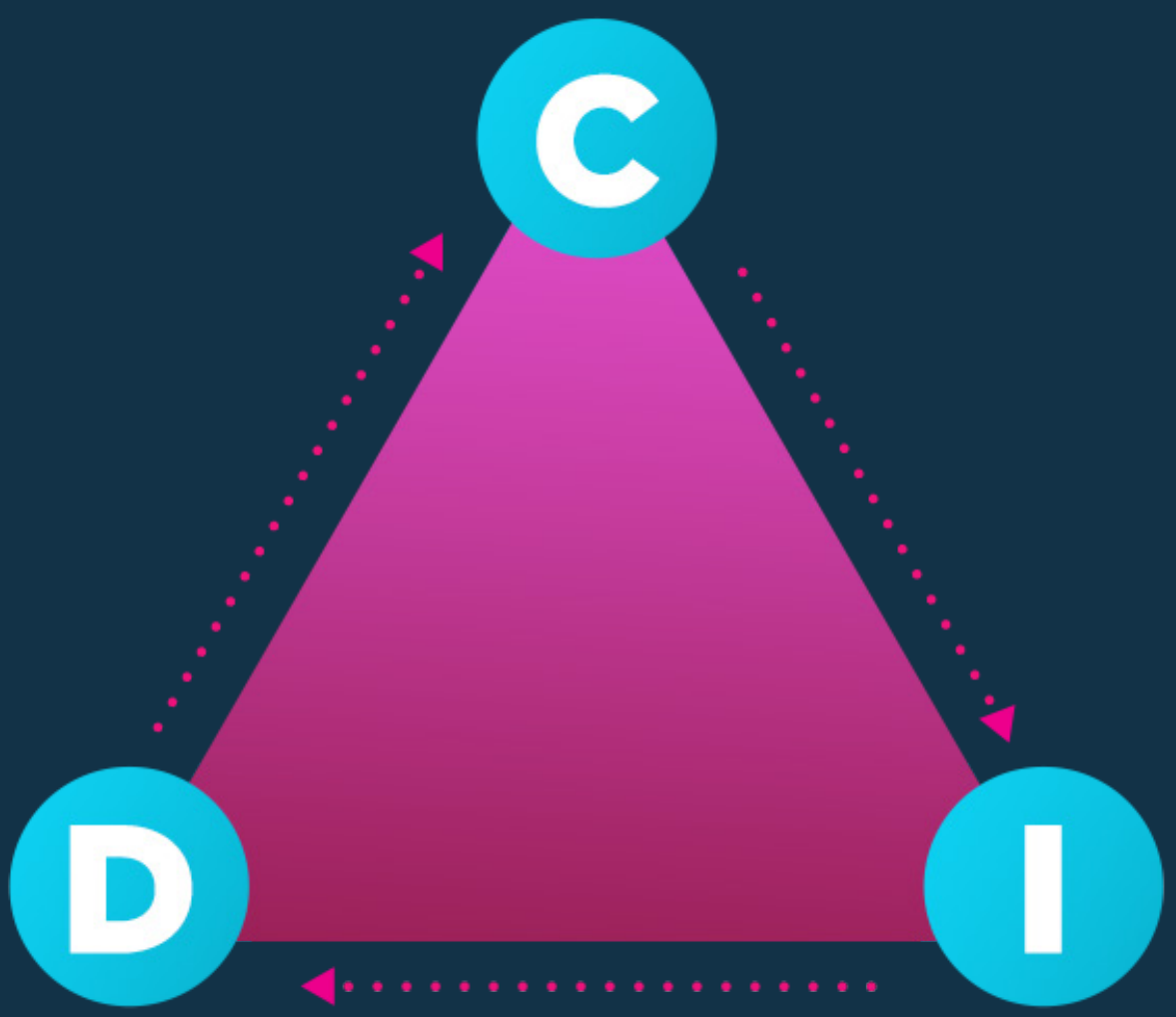
Thiago Braga, Remilina Yun (Remi) e Fernanda Maia

O conceito de "banco de dados" também foi trabalhado pela LGPD, que a define como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". A utilização de dados pessoais encontrados em banco de dados, para ser considerada lícita e com o menor risco possível, precisará observar algumas garantias, incluindo a qualidade dos dados armazenados.

Consequentemente, os investimentos em processos e ferramentas devem ser feitos de maneira proporcional ao impacto que cause ao negócio. Por essa razão, a manutenção dos dados deve ser observada pelos três pilares da Segurança da Informação:

CONFIDENCIALIDADE

Que o dado não esteja disponível ou seja revelado a indivíduos, entidades ou processos não autorizados;



DISPONIBILIDADE

Estar acessível e utilizável quando solicitado por uma entidade autorizada ou parte interessada.

INTEGRIDADE

Garantia de que o dado armazenado ou transferido está íntegro e é apresentado corretamente para quem o consulta;

Manuseio

momento em que a informação é criada e manipulada;

Armazenamento

momento em que a informação é armazenada;

Obrigatórias

aqueles que são necessários na condução dos negócios, por obrigação legal ou por razões operacionais;

Estratégicos

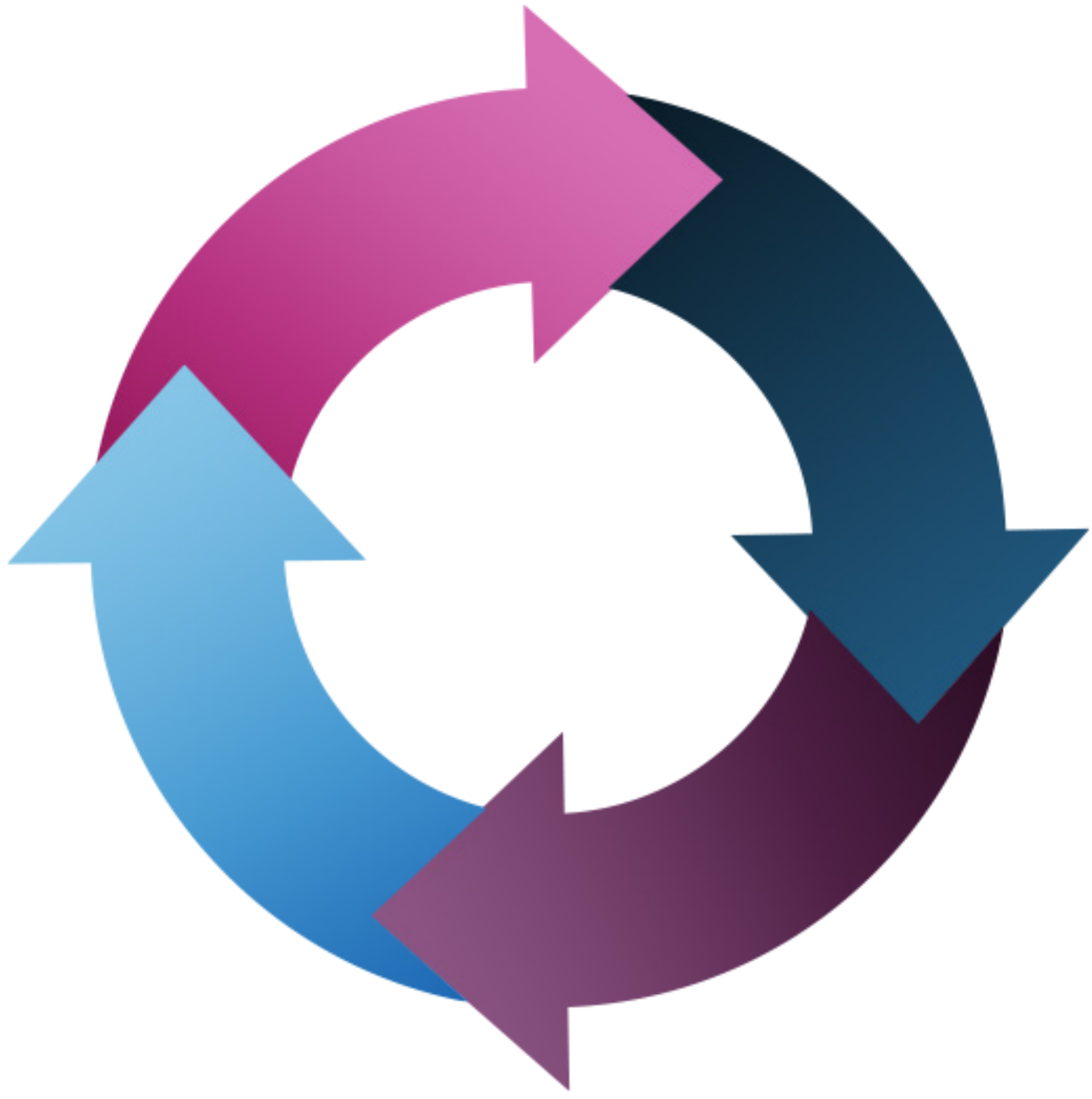
aqueles que são relevantes e devem ser mantidos, mesmo depois de não serem mais considerados necessários para as atividades, com o objetivo de preservar informações estratégicas, confidenciais ou significativas;

Transporte

momento em que a informação é transferida/compartilhada;

Descarte

momento em que a informação é descartada.



As organizações devem manter um inventário de dados atualizado com cada tipo de acesso, entrada e saída, bem como os riscos mapeados através da sua criticidade, probabilidade e impacto para definição das medidas apropriadas de mitigação, aceite ou transferência de risco.

Por fim, o tempo de guarda dos dados não é descrito de maneira taxativa na LGPD. O artigo 40 estabelece que a ANPD poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros. Assim, a recomendação nesse caso é a guarda dos dados em um tempo proporcional e razoável de acordo com a finalidade para a qual ele foi coletado.

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL

Considerações Finais

Fernanda Maia

Como explicado neste e-book, o tratamento de dados na sociedade brasileira é algo recorrente, e apenas foi regulado em agosto de 2018 por meio da LGPD. A importância desse texto legal quanto ao tema de investigação deriva do simples fato de uma investigação acontecer com base na análise e tratamento de dados pessoais coletados por organizações em diversas frentes, como por exemplo e-mails corporativos, entrevistas exploratórias ou confirmatórias, análise documental, background check, construção do lifestyle (estilo de vida), entre outros.

Como explicado neste e-book, o tratamento de dados na sociedade brasileira é algo recorrente, e apenas foi regulado em agosto de 2018 por meio da Lei Geral de Proteção de Dados de nº 13.709/2018. A importância desse texto legal quanto ao tema de investigação deriva do simples fato de uma investigação acontecer com base na análise e tratamento de dados pessoais coletados por organizações em diversas frentes, como por exemplo e-mails corporativos, entrevistas exploratórias ou confirmatórias, análise documental, *background check*, construção do *lifestyle* (estilo de vida), entre outros.

- Profissionais de *compliance*, auditoria interna, jurídicos e RH, entre outros que conduzem investigações internas sobre uma denúncia oriunda de um canal de denúncia, ouvidoria e ou demanda interna da organização, precisam estar preparados quanto às diretrizes dispostas na Lei Geral de Proteção de Dados nº 13.709/18 e a regulamentação europeia - General Data Protection Regulation (GDPR).

- Como explicado neste e-book, o tratamento de dados na sociedade brasileira é algo recorrente e apenas foi regulado em agosto de 2018 por meio da LGPD. A importância desse texto legal quanto ao tema de investigação deriva do simples fato de uma investigação acontecer com base na análise e tratamento de dados pessoais coletados por organizações em diversas frentes, como por exemplo e-mails corporativos, entrevistas exploratórias ou confirmatórias, análise documental, background check, construção do lifestyle (estilo de vida), entre outros.

- Para agir em conformidade com princípios e direitos instituídos pela legislação brasileira, é necessário assegurar a ciência do monitoramento desses dados para os titulares, a fim de garantir a proteção, segurança e legalidade das informações. Todavia, a simples ciência ao colaborador não isenta a organização de tomar medidas preventivas para a utilização dessas informações, visto que a LGPD é clara quanto à necessidade de se demonstrar qual a finalidade específica do tratamento destes dados, com ressalvas que a má utilização ou o excesso dela - fora da finalidade definida – acarretará a aplicação das sanções definidas no texto legal.

- Logo, com as novas diretrizes da LGPD, não se vê outro cenário além da criação de canal para recebimento de manifestações a respeito de potenciais infrações em atividades de tratamento de dados pessoais, com a possibilidade deste canal emitir resposta ao interessado.

- Assim, trabalhando na estrutura do canal de denúncia ou ouvidoria, é importante deixar claro o papel e a responsabilidade da figura do encarregado (responsável por processar as notificações feitas à autoridade reguladora; monitorar as atividades de processamento de dados, além de ser o ponto de contato com a autoridade reguladora em casos de implementação de novas tecnologias e incidentes de vazamentos) para que os titulares de dados tenham acesso a ele.

- Independentemente da estrutura montada para as denúncias, as diretrizes quanto às informações a serem coletadas devem ser pré-definidas por meio de questionários e ou instruções, a fim de tornar possível o início de uma condução de investigação. Desta forma, recebida a denúncia, o registro precisa ser efetuado respeitando a anonimização das informações, dos denunciante(s) e/ou denunciado(s), entre outros.

Com o registro das informações, a denúncia relatada deverá ser investigada por um grupo de pessoas competentes e habilitadas tecnicamente para apuração dos fatos com total imparcialidade, no intuito de realizar entrevistas, íntegras e transparentes, com o objetivo único de apuração/investigação do relatado, podendo ocorrer de forma exploratória ou confirmatória e, ao final da fase de investigação, o grupo técnico de profissionais deverá elaborar documento contendo uma conclusão acerca da investigação, bem como as medidas recomendadas para a situação fática.

Conclui-se que a necessidade de canais internos e externos de comunicação nas empresas ganhou gradativa importância ao longo dos anos, junto com a evolução das tecnologias e maiores opções de tratamento de dados, pois além de identificar possíveis irregularidades, a comunicação é o meio pelo qual as empresas conseguem agir a respeito de eventuais riscos operacionais e vulnerabilidades. O ponto mais relevante é a capacidade que uma empresa possui de demonstrar a adoção de medidas internas para a identificação de dados comprometidos, mitigação dos riscos e aprimoramento de ferramentas de *cyber security* em prol do cumprimento da Lei Geral de Proteção de Dados e dos direitos dos titulares que atuam na empresa.

Bibliografia

REFERÊNCIA BIBLIOGRÁFICA

LEAL JÚNIOR, João Carlos, et al. Monitoramento do correio eletrônico em ambiente de trabalho: o conflito entre o poder diretivo do empregador e o direito à intimidade de seu preposto in Semina: Ciências Sociais e Humanas, Londrina, v. 28, n.1, p. 69-80, jan./ jun. 2007

LEONARDI, Marcel. Tutela e privacidade na Internet. Editora Saraiva: São Paulo, 2012. Disponível em: ← http://leonardi.adv.br/wp-content/uploads/2012/01/mltpi.pdf→. Acesso em: 29 out 2018. https://www.dataprotection.ro/servlet/ViewDocument?id=1086

PINHEIRO, Patrícia Peck. Direito Digital. 6 ed. São Paulo: SaraivaJur, 2016, p. 243

NASCIMENTO, Amauri Mascaro. Iniciação ao Direito do Trabalho. 32 ed. São Paulo: LTr, 2006, p. 143.

SILVA, Leda Maria Messias da. Poder diretivo do empregador, emprego decente e direitos da personalidade. Revista Jurídica Cesumar, v. 6, n. 1, p. 277, 2006.

PINHEIRO, Patrícia Peck. Direito Digital. 6 ed. São Paulo: SaraivaJur, 2016, p. 244

PINHEIRO, Patrícia Peck. Direito Digital. 6 ed. São Paulo: SaraivaJur, 2016, p. 246
http://www.lecnews.com.br/blog/impactos-da-lgpd-em-due-diligence-de-terceiros/

RODOTÀ, Stefano. A vida na sociedade da vigilância (org. Maria Celina Bodin de Moraes).
Rio de Janeiro: Renovar, 2008.
https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf

LEI GERAL DE PROTEÇÃO DE DADOS E AS INVESTIGAÇÕES CORPORATIVAS

Fernanda Maia

Remilina Yun

Rafael Siqueira

Thiago Braga

Maria L. Gándara

Mariana Moura

IPRC
INSTITUTO DE PESQUISA DO RISCO COMPORTAMENTAL