CODING RIGHTS
www.codingrights.org
contact@codingrights.org

Rio de Janeiro, 24 de março de 2021.

À Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados

Assunto: Regulamentação de notificação de incidentes de segurança (Tomada de Subsídios nº 2/2021 - reunião técnica)

O convite para contribuir com o trabalho da Coordenação-Geral de Normatização por meio da reunião técnica realizada no âmbito da tomada de subsídios nº 2/2021 teve como enfoque responder às seguintes perguntas:

a. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?
b. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?

Levando-se em conta o disposto no artigo 48 da Lei Geral de Proteção de dados (LGPD), que trata da obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados a ocorrência de incidentes de segurança que possam acarretar em risco ou dano, a Coding Rights faz as seguintes contribuições às duas perguntas acima.

Medidas preventivas de incidentes de segurança que possam acarretar em risco ou dano para o titular dos dados

A Lei Geral de Proteção de Dados (LGPD) prevê a implementação **de medidas técnicas e organizacionais para a segurança e sigilo do processamento de dados pessoais, levando-se em consideração a natureza das informações tratadas, o estado da tecnologia e as propriedades distintivas do processamento,** tais como **escala, contexto e objetivo** *(*Art 46 § 1º*)*. Em particular, estas **medidas devem proteger os dados pessoais** de acessos não-autorizados e **de incidentes de segurança tanto acidentais quanto propositais** capazes de **comprometer a confidencialidade, a integridade e a disponibilidade dos dados** *(*CNSSI 4009 Committee on National Security Systems (CNSS) Glossary).[1] As medidas técnicas

[1]https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

mencionadas a seguir são sugestões para assegurar a conformidade aos três pilares da segurança de dados.

(i) A **Confidencialidade** pode ser garantida por meio de:

(i.1) Pseudonimização para o tratamento de dados, que pode ser realizada através da modificação dos dados pessoais por códigos aleatórios.

(i.2) Política de controle de acesso, que garante que apenas pessoas autorizadas tenham acesso aos dados.

(i.3) Política de monitoração interna para garantir que agentes internos estejam em conformidade com as políticas de segurança.

(i.4) Descentralização do processamento dos dados para que o corrompimento de um sistema não comprometa integralmente os dados dos titulares.

(i.5) Encriptação de comunicação de dados sensíveis, de discos rígidos, de mídias de armazenamento e de dados confidenciais.

(ii) A **Integridade** pode ser garantida por meio de:

(ii.1) Segurança de transferência de dados, que pode ser garantida pela geração de certificados de "websites" e por conexões criptografadas.

(ii.2) Controle de entrada para garantir que todas as entradas feitas nos sistemas sejam registradas e para que os "logs" sejam arquivados.

(ii.3) Política de transparência e documentação do tratamento de dados.

(iii) A **Disponibilidade** pode ser garantida por meio de:

(iii.1) Instauração de mecanismos abrangentes e regulares de replicação de dados ("backups") para evitar a perda de dados.

(iii.2) Arquitetura de redes implementada de forma redundante.

(iii.3) Plano de continuidade para a rápida recuperação dos dados em casos de perda acidental ou de incidentes de segurança comprometedores.

Também é interessante o emprego regular de testes para avaliar a eficácia das medidas técnicas e institucionais adotadas, como testes de intrusão. Auditorias realizadas por autoridades externas também são aconselháveis.

É, portanto, de responsabilidade dos agentes de tratamento de dados **tomar medidas técnicas e organizacionais para PREVER e AVERIGUAR a ocorrência de incidentes de segurança envolvendo dados pessoais, REAGIR para mitigar danos e INFORMAR** rapidamente a Autoridade Nacional de Proteção de Dados e os titulares dos dados.

De acordo com posicionamento[2] do Article 29 Working Party[3], agentes de tratamento de dados devem também **ter uma avaliação preliminar de riscos de incidentes de segurança como parte da sua avaliação de impacto na proteção de dados antes de iniciadas as operações de processamento.** Este posicionamento, posteriormente incorporado na "Regulation(EU) 2018/1725" da União Europeia e esclarecido pelas diretrizes do "European Data Protection Supervisor", tem ressonância com o artigo 32 da Lei Geral de Proteção de Dados, que também deve ser regulamentado.

Obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados

O artigo 48 da LGPD assim dispõe: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares." Entendemos que **qualquer incidente de segurança que envolva comprometimento de confidencialidade, integridade ou disponibilidade de dados pessoais acarreta risco aos titulares e, como tal, a comunicação entre agentes de tratamento e a Autoridade Nacional de Proteção de Dados é imprescindível. Isso porque** é a partir da **comunicação entre agentes de tratamento e o governo brasileiro que serão traçadas estratégias efetivas de proteção de dados e que trabalhos preventivos** serão desenvolvidos para evitar novos riscos e incidentes de segurança.

A relação entre a **ocorrência de incidentes de segurança de informação e o desenvolvimento de mecanismos de defesa tanto jurídicos quanto técnicos que assegurem a proteção de informações é dialética,** isto é, a evolução de métodos capazes de assegurar a proteção de dados é o resultado do constante conflito entre forças contraditórias que podem ser classificadas em eventos sócio-digitais disruptivos e recursos defensivos. Portanto, a **notificação serve também para a capacitação adequada de profissionais de Segurança da Informação das esferas pública e privada e para o fortalecimento dos sistemas tecnológicos, responsáveis pela proteção de dados.**

Nesse sentido, **não deve haver exceções para a obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados sobre incidentes de segurança que envolvam dados**

[2] "Guidelines on Personal data breach notification under Regulation 2016/679", disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[3] O Article 29 Working Party, cuja denominação completa é "The Working Party na Proteção de Indivíduos no Processamento de Dados Pessoais", foi um conselho consultivo formado por representantes das autoridades de proteção de dados de cada estado membro da União Européia, da Supervisão Europeia de Proteção de Dados e da Comissão Europeia.

pessoais, seja visando a **coleta de informações sobre a evolução do ecossistema de segurança da informação no país,** seja para que agentes de tratamento de dados sejam orientados para a melhor forma de atuar em coerência com a proteção de dados dos titulares. **Não deve ficar apenas a cargo do agente de tratamento de dados pessoais a avaliação sobre se o incidente de segurança causou risco ou dano ao titular do dado, pois ele é o principal interessado em negar riscos ou danos.** Normalmente incorre, portanto, em conflito de interesse nesse tipo de avaliação. **Tal avaliação deve caber à ANPD.**

Qualquer argumentação contra a notificação mandatória de qualquer tipo de incidente que seja pautada pelo argumento de um possível excesso de notificações deve ser comprovada com dados que comprovem tal temor. Aqui, cabe relembrar o **caráter educativo da ANPD, nos termos do artigo 55-J da LGPD.**

Necessidade da ANPD estabelecer uma matriz de classificação de riscos de incidentes de segurança que envolvem dados pessoais

Com base nos incidentes relatados[4], acreditamos que a ANPD deva estabelecer uma **matriz de classificação de risco de incidentes de segurança** para que esta possa estabelecer melhores diretrizes de atuação e mitigação e para deliberar pela obrigatoriedade de relatório de impacto à proteção de dados pessoais para determinados tipos de tratamento de dados, nos termos do artigo 32 da LGPD.

De acordo com sugestão do WP29:

"The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests ***categories of data subjects*** *to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others,* ***children and other vulnerable groups, people with disabilities, employees or customers.*** *Similarly,* ***categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.***
Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. ***Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories.*** *In this way, it is linked to the requirement of describing the likely consequences of the breach."*[5]

[4] E em proximidade com as medições do CERT.br: https://www.cert.br/stats/incidentes/
[5] Article 29 Data Protection Working Party. "Guidelines on Personal data breach notification under Regulation 2016/679", disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Em conformidade com essa visão, as diretrizes[6] que interpretam o artigo 34 da Regulation(EU)2018/1725 da União Europeia determinam que os riscos identificados previamente no estudo de impacto à proteção de dados (DPIA) podem servir de ponto de partida para classificação de riscos de incidentes.

Obrigatoriedade de notificar o titular de dados

Consideramos que **qualquer incidente de segurança que envolva dados pessoais pode acarretar em risco ou dano para o titular do dado**. Portanto, o titular deve ser notificado sempre, mesmo que medidas técnicas e organizacionais preventivas tenham sido adotadas pelo agente de tratamento. Desta forma, o titular se torna ciente dos riscos envolvidos no manuseio de seus dados e poderá buscar amparo legal, inclusive para avaliar pedidos de indenização por danos, quando cabível, bem como terá mais informações para avaliar se o agente de tratamento tem sido capaz de resolver incidentes e ser digno de alguma confiança. Visando respaldar a privacidade e evitar maior dano, o aviso de incidentes deve ser feito em comunicação direcionada para o titular do dado sempre que possível.

De acordo com The Working Party on the Protection of Individuals with regard to the Processing of Personal Data": *Communicating a breach to individuals* ***allows the controller to provide information on the risks*** *presented as a result of the breach and the* ***steps those individuals can take to protect themselves from its potential consequences.*** *The focus of any breach response plan should be on protecting individuals and their personal data. Consequently,* ***breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.***[7]

Diferença nos tipos de notificações enviadas para a ANPD e o titular de dados

Entendemos que, por motivos de segurança, podem existir situações extraordinárias em que a ANPD deva ser comunicada antes do titular de dados sobre incidentes de segurança que estão em andamento, inclusive para orientar o controlador sobre medidas de mitigação.

Nesse sentido, novamente, o **desenvolvimento por parte da ANPD de uma classificação de risco dos diferentes incidentes de segurança que envolvem dados pessoais** pode ser **importante também para estabelecer o fluxo e formato de comunicação de incidentes para titulares de dados.** Tal classificação seria importante inclusive para evitar um fluxo excessivo de comunicações de incidentes com os titulares de dados. Com efeito, incidentes resolvidos e que incorreram baixo risco podem ser notificados de maneira agregada, apenas a título de

[6] European Data Protection Supervisor. "Guidelines on personal data breach notification For the European Union Institutions and Bodies", disponível em: https://edps.europa.eu/sites/default/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf
[7] Article 29WP Guidelines, conforme mencionado acima.

informação, por exemplo, em relatórios periódicos, enquanto incidentes graves, nos quais titulares também podem tomar medidas de mitigação, devem ter notificação em formato mais alarmante.

Portanto, entendemos que, ainda que o artigo 48 da LGPD não estabeleça diferenças entre a notificação da ANPD e do titular, em conformidade com o modelo europeu, é necessário regulamentar possível considerar dois tipos de notificação de acordo com o notificado (ANPD ou titular), cabendo, portanto, à ANPD estabelecer as diretrizes e formato de ambas.

Estímulo à denúncias (whistle blowers) em caso de incidentes não notificados

Além das notificações por parte dos agentes de tratamento de dados, em conformidade também com sugestões do Article 29 WP, acreditamos que a ANPD deva criar canais para permitir denúncias anônimas sobre incidentes de segurança que envolvam dados pessoais. Desta forma, empregados, clientes e jornalistas investigativos poderão notificar a ANPD sobre possíveis vazamentos subnotificados ou irregularidades cometidas por agentes de tratamentos de dados. Nesse caso, caberá à ANPD iniciar investigações de conformidade.

Agradecemos a oportunidade de contribuir com as duas questões propostas na tomada de subsídios nº 2/2021. Seguimos à disposição para mais contribuições e esclarecimentos.

Contribuição por

Joana Varon
Diretora executiva da Coding Rights, Fellow de Direitos Humanos e Tecnologia do Carr Center for Human Rights Policy da Harvard Kennedy School. Afiliada ao Berkman Klein Center for Internet and Society at Harvard University. Advogada, com experiência em direitos humanos e segurança digital, opera em fóruns técnicos na intersecção de debates legais e de desenvolvimento de códigos para a proteção de direitos, entre eles, iniciou o grupo de trabalho sobre Considerações de Direitos Humanos para Standards e Protocolos no Internet Engineering Task Force (IETF).

Rafaella Nunes
Estudante de Ciência da Computação da Universidade de São Paulo e consultora em cibersegurança para a Coding Rights. Realizou intercâmbio acadêmico focado em

Cybersecurity na Far Eastern Federal University (Vladivostok, Rússia) e, atualmente, é estudante de “Game Theory and Operations Research (Master program)” na Saint Petersburg State University (São Petersburgo, Rússia).

OUTROS LINKS DE REFERÊNCIA

(i) Classificação de incidentes

European Union Agency for Cybersecurity:
https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

European Commission:
https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

(ii) Notificações e definição de incidente de segurança

NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NIST: https://csrc.nist.gov/glossary/term/security_categorization
CERT.br: https://www.cert.br/docs/whitepapers/notificacoes/

(iii) “Confidentiality, integrity, availability”

O NIST utiliza, explicitamente, a terminologia adotada pelo documento abaixo:

CNSSI 4009 Committee on National Security Systems (CNSS) Glossary - https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

"COMPUTER SECURITY: Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer."

(iv) Estatísticas do CERT.br

https://www.cert.br/stats/incidentes/