LGPD E INTELIGÊNCIA: OS LIMITES NO TRATAMENTO DE DADOS PESSOAIS COLETADOS EM FONTES ABERTAS

Lilian Coutinho *

Resumo

Os serviços de Inteligência conduzem um trabalho vital para a salvaguarda da sociedade e do Estado. Os avanços tecnológicos trouxeram novos contornos e maiores desafios à sua atuação, com ameaças cada vez mais complexas em campos como o terrorismo, ataques cibernéticos e redes criminais. Esse cenário exige maior desenvolvimento e técnicas que possibilitem o cumprimento de sua missão institucional com eficiência. Por outro lado, se mal conduzido ou administrado, o trabalho para identificação e contraposição às ameaças também pode, potencialmente, atingir direitos fundamentais, especialmente à privacidade e à proteção de dados. Nos últimos anos, mudanças legislativas têm buscado regular, controlar e garantir transparência no tratamento de dados acessíveis, tanto por pessoas jurídicas de direito privado, quanto por aquelas de direito público. No Brasil, exemplo disso é a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Essa delimita que o tratamento de dados pessoais, quando realizado para fins exclusivos de segurança do Estado, será regido por legislação específica. Contudo, na ausência desse normativo, o contexto permanece complexo e impreciso. Este artigo visa demonstrar a importância do equilíbrio entre o tratamento e a proteção de dados pessoais na futura legislação específica. Para tanto, apresentará alguns dos desafios no uso das novas tecnologias que utilizam dados obtidos em fontes abertas, discutirá os impactos que o uso indevido desses dados pode gerar e demonstrará como leis adequadas são necessárias para a proteção tanto dos direitos e garantias fundamentais, quanto do próprio profissional de Inteligência e da Atividade, permitindo que o Serviço de Inteligência brasileiro cumpra com excelência a sua missão.

Palavras-chaves: LGPD. Inteligência. Osint. Dados pessoais. Fontes abertas.

LGPD AND INTELLIGENCE: THE LIMITS IN THE TREATMENT OF PERSONAL DATA GATHERED FROM OPEN SOURCES

Abstract

Intelligence services leads a vital work for the safeguard of both the society and the State. The technological progress has brought new aspects and greater challenges to its activities, with increasingly complex threats in fields as terrorism, cyber attacks and criminal networks. This scenario requires further development and new techniques which enable the achievement of its institutional mission efficiently. Conversely, if misadministrated, the work of identifying and addressing these threats may potencially impact fundamental rights, specially privacy and data protection. In recent years, changes in law have sought to regulate, control and guarantee transparency in the treatment of accessible data, both to legal entities of private and public law. In Brazil, an example is the Law nº 13.709/2019,

* Oficial Técnica de Inteligência da Agência Brasileira de Inteligência, graduada em Direito pelo Centro Universitário de Brasília (UniCEUB).

known as Lei Geral de Proteção de Dados Pessoais (LGPD). This law states that the processing of personal data, when performed for the exclusive purposes of State security, will be governed by specific legislation. This paper aims to present the importance of the balance between personal data processing and protection in this future specific legislation. To this extend, it will present some of the challenges in the use of new technologies that utilize data from open sources, discuss the impacts that the improper use of these data can generate and demonstrate how adequate laws are necessary to protect both fundamental rights and guarantees, as well as the Intelligence professional and the Activity, allowing the brazilian Intelligence Service to fulfill its mission with excellence.

Keywords: *LGPD. Intelligence. Osint. Personal data. Open source.*

LGPD E INTELIGENCIA: LOS LÍMITES EN EL TRATAMIENTO DE DATOS PERSONALES RECOLECTADOS EN FUENTES ABIERTAS

Resumen

Los servicios de inteligencia realizan un trabajo vital para salvaguardar la sociedad y el Estado. Los avances tecnológicos han traído nuevos contornos y mayores desafíos a su desempeño, con amenazas cada vez más complejas en campos como el terrorismo, los ciberataques y las redes criminales. Este escenario requiere un mayor desarrollo y técnicas que permitan el cumplimiento eficiente de su misión institucional. Por otro lado, si se realiza o administra de manera deficiente, el trabajo para identificar y contrarrestar las amenazas también puede potencialmente lograr los derechos fundamentales, especialmente la privacidad y la protección de datos. En los últimos años, los cambios legislativos han buscado regular, controlar y asegurar la transparencia en el tratamiento de los datos accesibles, tanto por las personas jurídicas de derecho privado como por las de derecho público. En Brasil, un ejemplo de esto es la Ley n° 13.709/2018, conocida como as Lei Geral de Proteção de Dados Pessoais (LGPD). Esto delimita que el tratamiento de datos personales, cuando se realice con fines exclusivos de seguridad del Estado, se regirá por la legislación específica. Sin embargo, en ausencia de esta regla, el contexto sigue siendo complejo e impreciso. Este artículo tiene como objetivo demostrar la importancia de equilibrar el tratamiento y la protección de los datos personales en la futura legislación específica. Para tanto, presentará algunos de los desafíos en el uso de nuevas tecnologías que utilizan datos obtenidos de fuentes abiertas, discutirá los impactos que el mal uso de estos datos puede generar y demostrará cómo son necesarias leyes adecuadas para proteger tanto los derechos y garantías fundamentales, como la propia Inteligencia y Actividad profesional, permitiendo que el Servicio de Inteligencia brasileño cumpla su misión con excelencia.

Palabras clave: *LGPD. Inteligencia. Osint. Datos personales. Fuentes abiertas.*

Introdução

A atividade de Inteligência é o exercício permanente de ações especializadas voltadas à produção de conhecimentos e à proteção da sociedade e do Estado, visando assessorar o mais alto nível decisório do país. Segundo a Doutrina Nacional da Atividade de Inteligência (2016), tal assessoramento abrange a identificação de oportunidades e de ameaças à consecução das políticas de governo, o planejamento e a execução de ações, a segurança de conhecimentos e dados sensíveis e das pessoas, áreas, instalações e meios que os guardam ou veiculam e, ainda, a prevenção, detecção, obstrução e neutralização de ações de Inteligência adversa.

Obter dados oportunos, adequados, dignos de confiança e abrangentes sempre foi um desafio. Com o desenvolvimento do espaço cibernético ou "ciberespaço", os trabalhos se tornaram ainda mais amplos e complexos, e os procedimentos da atividade de Inteligência executados na realidade física se estenderam à realidade virtual. Esse cenário exige um contínuo esforço de atualização e aperfeiçoamento.

Se o ciberespaço trouxe novas ameaças, também trouxe novas oportunidades. Sim, pois esse também funciona como campo no qual informações estratégicas são armazenadas, manipuladas e transmitidas — sendo, assim, repositório de dados, objeto de análise e ambiente operacional — e como espaço passível de monitoramento e estudos, haja vista os múltiplos atores que nele se fazem presentes com as mais diversas motivações (BRASIL, 2016).

Nesse mesmo contexto, atentos à necessidade de estabelecimento de limites nas operações que utilizam dados pessoais, vários países editaram legislações com vistas à proteção das pessoas naturais quanto ao processamento de seus dados. Exemplo disso é a *General Data Protection Regulation (GDPR)*, com aplicação nos países que integram a União Europeia e uma das regulações mais fortes em termos de privacidade e segurança de dados no mundo.

No caso do Brasil, foi editada a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Como veremos, a Lei, que entrou em vigor no dia 18 de setembro de 2020, delimita hipóteses nas quais não será aplicada integralmente, indicando a necessidade de edição de normas específicas.

Nesse artigo, buscaremos demonstrar a importância do equilíbrio entre o processamento e a proteção de dados pessoais na legislação específica que regulará o tratamento[1] de dados pessoais realizado para fins exclusivos de segurança do Estado. Para tanto, apresentaremos a *Open Source Intelligence*[2] (Osint) — e alguns dos desafios no uso das novas tecnologias que utilizam dados obtidos em fontes abertas. Discutiremos os impactos que o uso indevido desses dados pode gerar e demonstraremos como leis adequadas

1 Segundo o art. 5º, inciso X, da LGPD, "tratamento" deve ser compreendido como toda operação realizada com dados pessoais, como as que se referem a coleta, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, modificação etc.

2 Inteligência em Fontes Abertas.

são necessárias para a proteção tanto dos direitos e garantias fundamentais, quanto do próprio profissional de Inteligência e da Atividade.

Open Source Intelligence (OSINT)

Tradicionalmente, a Inteligência em Fontes Abertas ou *Open Source Intelligence* (Osint) consiste na técnica de coleta de dados através de fontes como jornais, programas de televisão, estações de rádio, pronunciamentos, documentos oficiais, artigos acadêmicos, estudos etc. Esse tipo de coleta continua existindo, mas, com o advento da *internet* e dos grandes repositórios de dados, a Osint ganhou novos traços. Com o início e crescimento das mídias sociais, principalmente a partir dos anos 2000, os dados passaram a ser armazenados, processados e analisados em níveis nunca antes vistos. Hoje, é possível extrair conhecimento de vídeos, mensagens, *sites*, *blogs*, imagens, redes sociais, enfim, de uma série de novos meios. Nessa nova era digital, os desafios são enormes. Segundo Christl e Spiekermann (2016), para além do volume, ou seja, da impressionante e sempre crescente quantidade de dados, chama a atenção a velocidade — qual seja, o curto espaço de tempo no qual são produzidos e transmitidos os dados, e a variedade — consistente nos diferentes formatos e representações empregadas.

Nesse contexto, hoje, em muitos casos, a dificuldade não é a falta de informação, mas, sim, o excesso dela. É enorme o desafio de encontrar os dados úteis e oportunos em meio a todo esse volume, velocidade e variedade.

Tendo em vista o volume dos dados, bem como a velocidade e a facilidade com que esses são acessados, algumas preocupações começam a surgir. Isso porque não basta que as novas tecnologias permitam que uma quantidade inimaginável de dados sejam coletados e processados em um curto espaço de tempo. Conforme Pastor-Galindo et al. (2020), é necessário, também, que se desenvolvam recursos e mecanismos que garantam que os dados sejam compreendidos corretamente, não sendo retirados de seu contexto ou correlacionados de maneira inadequada. É igualmente importante que sejam utilizadas fontes seguras e razoavelmente confiáveis, pois as informações geradas não devem se basear em subjetivismos, desinformação ou dados imprecisos.

Para além das preocupações que advêm de questões técnicas, há aquelas que resultam de considerações éticas e legais. Há desafios envolvidos em todas as operações de tratamento de dados, e decisões equivocadas podem gerar malefícios individuais e coletivos, como manipulação, discriminação, fraude, quebra de segurança ou de confidencialidade, chantagem, redução da confiança no Estado e mudanças comportamentais. Podem ocorrer, ainda, danos irreparáveis a vários direitos, como à privacidade, à proteção aos dados pessoais, às liberdades de expressão e de ir e vir.

Todas essas questões surgem mesmo quando estamos falando de Inteligência de fontes abertas. São preocupações e desafios que não envolvem o acesso a dados controlados ou o uso de meios invasivos de obtenção de informações.

Como veremos, agregando dados pessoais que, *a priori*, pouco significam, podemos gerar perfis completos de um indivíduo, de um grupo e até mesmo de uma sociedade inteira.

O uso de dados pessoais

Como bem observa Bruno Bioni (2020), com o aprimoramento das tecnologias da informação e da comunicação e a possibilidade de processar e organizar um enorme volume de dados em um curto período de tempo, a economia foi redimensionada e os dados pessoais dos cidadãos se tornaram um ativo econômico valioso e um fator vital para o crescimento e o desenvolvimento dos negócios. Dados que antes eram considerados insignificantes ou sem valor agora servem de base para a construção de modelos, perfis e até mesmo previsões. Nesse contexto, hoje há empresas que trabalham especificamente com a venda de dados pessoais ou de informações derivadas desses dados para outras companhias[3]. Por essas razões, diz-se que, se o que você está consumindo *online* é de graça, então o produto é você (FURNAS, 2012).

Se, por um lado, toda essa informação pode ser usada para nos oferecer produtos e entregar serviços — sejam eles úteis ou não, também pode gerar consequências potencialmente danosas para a nossa privacidade, para a nossa autonomia e para a sociedade como um todo.

As preocupações não se limitam ao nome, *e-mail* ou telefone que o usuário voluntariamente inseriu em sua rede social; trata-se de dados como suas opiniões, crenças, hábitos, desejos, sentimentos, aspirações e outras questões sensíveis. De fato, quando uma empresa detém todos esses dados, ela pode não apenas prever os seus próximos passos, como também moldá-los. Pode gerar modelos preditivos não apenas sobre você, mas sobre pessoas com características semelhantes.

Atualmente, mesmo quando buscamos proteger nossa privacidade nas redes, verificar quais atores recebem os nossos dados é uma tarefa quase impossível. De acordo com Kaldestad (2020), para analisar um aplicativo de *smartphone* é necessário ler toda a política de privacidade, realizar uma análise técnica quanto ao tráfego de dados do aplicativo e identificar os terceiros que recebem os dados (o que nem sempre é possível, já que, geralmente, esses atores são tratados por termos genéricos). Feito isso, o próximo passo é ler a política de cada um desses terceiros — que, por sua vez, também disponibilizam os dados recebidos a outros atores e assim por diante. Perceba, portanto, que parece um caminho sem fim — e estamos falando apenas de um único aplicativo. O mesmo ocorre com *sites* na internet.

Isoladamente, talvez os dados de um único indivíduo não signifiquem muito para ele, ou para uma empresa. Mas o grande problema é que, ao serem agregados, esses dados tornam-se poderosos, e estamos entregando às empresas muito mais do que

3 São os chamados data *brokers* que, basicamente, coletam dados em inúmeras fontes *online* e *offline*, processam e agregam os dados obtidos, classificam os usuários em grupos e segmentos a partir de características comuns e, posteriormente, vendem o material gerado a outras empresas.

imaginávamos: não apenas informações sensíveis sobre nós mesmos, mas, também, informações que podem ser usadas contra outras pessoas (por exemplo, na criação de modelos preditivos e no direcionamento do comportamento de indivíduos com características semelhantes). Assim, é possível que os dados sejam utilizados de modo a gerar danos individuais, mas também é possível que ocorram danos coletivos, como a negação de determinado serviço a um grupo, ou o oferecimento de um produto a preços mais elevados, o não recebimento de uma oferta em razão da cor da pele, etc.

Como bem demonstrou o escândalo da Cambridge Analytica em 2016, os riscos não se limitam ao âmbito comercial ou publicitário. Com efeito, a empresa coletou um enorme volume de dados de toda a sociedade, principalmente através de aplicativos do *Facebook*, visando a construção de perfis psicológicos e o direcionamento de mensagens e anúncios que alterassem o comportamento dos indivíduos[4]. O objetivo final era influenciar o resultado das eleições em vários países. Se os usuários aceitaram a coleta de dados pelo *Facebook* para uma suposta melhoria de experiência, é bastante improvável que soubessem e concordassem com o compartilhamento com empresas que manipulassem suas emoções ou influenciassem seu voto ou os rumos políticos do seu país.

As preocupações são maiores ao constatarmos que o uso de dados pessoais não se dá apenas por empresas. De fato, os governos de vários países têm cada vez mais se engajado no uso de *softwares* e tecnologias de vigilância com base em dados pessoais.

O uso de dados por governos

O debate em regimes democráticos quanto à violação da privacidade por programas governamentais não é atual. No entanto, o tema ganhou notoriedade após os vazamentos de documentos classificados por Edward Snowden[5] em 2013. Os arquivos demonstravam que o programa PRISM da Agência de Segurança Nacional americana (NSA), originalmente criado para o rastreamento de terroristas, havia se transformado em uma vigilância eletrônica em massa, em parceria com gigantes da tecnologia, como *Microsoft, Google e Facebook*[6].

Esse tipo de discussão tem ganhado cada vez mais espaço e relevância na medida em que o direito à privacidade não é mais visto apenas como um direito ao sigilo, mas como um direito de controlar suas próprias informações, decidindo quem, como, quando e para que são usados os

4 As informações foram concedidas em entrevista do delator Christopher Wylie ao jornal The Guardian.

5 Edward Snowden é um ex-contratado da NSA e ex-administrador de sistemas da Agência Central de Inteligência americana (CIA), que se tornou mundialmente famoso ao tornar público detalhes de programas de vigilância da NSA.

6 No caso do Brasil, tornou-se público não apenas que os dados de milhões de brasileiros haviam sido coletados, mas que houve espionagem da empresa Petrobrás e até mesmo a interceptação da comunicação entre a então presidente Dilma Rousseff com seus principais assessores (ESTADÃO, 2014), levantando sérias preocupações em termos de segurança nacional e interferência externa.