abpi.empauta.com

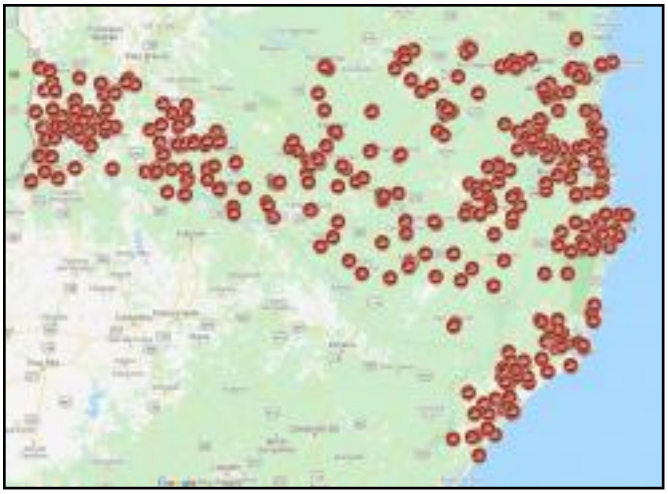
Associação Brasileira da Propriedade Intelectual
Clipping da imprensa

Brasília, 27 de janeiro de 2020 às 08h27
Seleção de Notícias

abpi.empauta.com

Operação combate comércio ilegal de cigarros e prende 24 pessoas em SC

SANTA CATARINA



Foram abordados e fiscalizados 693 bares e pequenos mercados em todo estado.

Fiscalização começou na tarde de quinta-feira e terminou na madrugada desta sexta - Foto: Polícia Militar/Divulgação

Cerca de 22 mil carteiras de cigarros ilegais foram apreendidas em uma operação realizada em bares e pequenos mercados de Santa Catarina nesta quinta (23) e sexta-feira (24). Conforme a Polícia Militar, 24 pessoas foram presas.

Estabelecimentos comerciais de todo o estado foram fiscalizados na ação realizada pela Polícia Militar. A operação, intitulada Varejo, começou na tarde de quinta, às 14h, e foi finalizada na madrugada desta sexta, às 2h.

Operação de combate à venda de cigarros contrabandeados foi realizada em todo estado - Foto: Polícia Militar de Santa Catarina/Divulgação

Foram fiscalizados 693 estabelecimentos comerciais e 1.727 veículos. Além dos cigarros, foram apreendidas também três armas de fogo, 40 veículos e 1.588 objetos ilegais envolvendo jogos de azar, **falsificações** e **pirataria.**

Um mapeamento da rede de varejo utilizada para a venda de cigarros ilegais será feito pela Receita Federal e a Secretaria da Fazenda a partir das informações reunidas durante a operação.

Veja outras notícias do estado no ***G1*** SC

EUA divulgam medidas para reprimir comércio eletrônico de produtos falsificados

Por David Shepardson

WASHINGTON (Reuters) - O governo Trump planeja divulgar nesta sexta-feira medidas para reprimir mercadorias falsificadas e piratas vendidas nos principais sites de ecommerce e pedir que empresas façam mais para fiscalizar vendedores terceirizados e aumentar os esforços de autopoliciamento.

O assessor do secretário interino de Segurança Interna, Chad Wolf, e o assessor da Casa Branca, Peter Navarro, estarão entre os funcionários em uma entrevista coletiva nesta sexta-feira para discutir a medida no Centro Nacional de Coordenação de Direitos de Propriedade Intelectual em Arlington, Virgínia, disseram autoridades do governo na quinta-feira.

Os vendedores estrangeiros enfrentam um risco pequeno de serem processados, disse um funcionário do governo à Reuters, de modo que uma forte ação do governo dos EUA "é necessária para realinhar fundamentalmente as estruturas de incentivo".

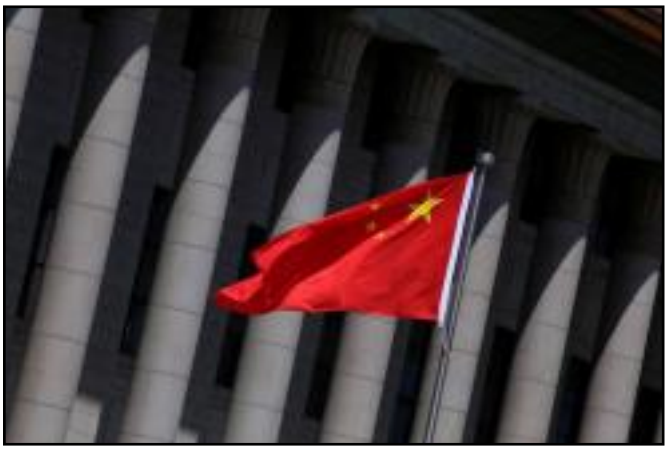
Agências policiais estão planejando "ações imediatas" para identificar mercadorias falsificadas e buscar "todas as autoridades estatutárias disponíveis para aplicar multas civis e outras penalidades contra essas entidades", de acordo com um relatório do DHS divulgado pelo Wall Street Journal na quinta-feira e confirmado por um oficial do governo.

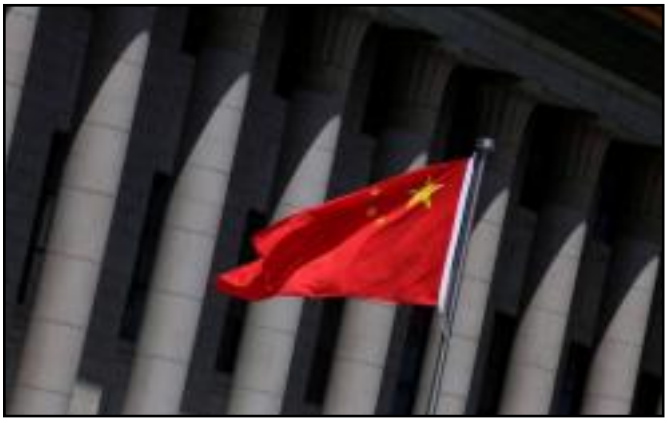
O governo Trump também está buscando autoridade legal "para permitir explicitamente que o governo busque medidas cautelares contra marketplaces de terceiros e outros intermediários que vendem mercadorias falsificadas", confirmou o funcionário.

Empresas como Amazon, eBay e Alibaba têm políticas que proíbem produtos falsificados e apontaram seus investimentos em programas para evitar **falsificações** em suas plataformas.

A Amazon disse no ano passado que "investe pesadamente em medidas proativas para impedir que produtos falsificados cheguem às nossas lojas. Somente em 2018, gastamos mais de 400 milhões de dólares no combate a **falsificações,** fraudes e outras formas de abuso". A Amazon não quis comentar antes do anúncio desta sexta-feira.

Empresas Chinesas têm histórico de acusações de roubos de dados





Â Por Cristiane Barbieri - O Estado de S. Paulo China foi acusada de 'roubar' US$ 100 bilhões por ano em propriedade intelectual

O desvio de informações estratégicas e roubo de propriedade intelectual de empresas norte-americanas por concorrentes chinesas estiveram entre os principais argumentos usados pelo presidente dos Estados Unidos, Donald Trump, para levar adiante a guerra comercial contra a China. Diferentes estatísticas e think tanks, como são chamados os centros de pesquisa independentes globais, identificaram essa tendência.

Em 2018, por exemplo, o diretor do conselho de assuntos econômicos da Casa Branca, Kevin Hassett, afirmou que a China 'roubava' US$ 100 bilhões por ano em propriedade intelectual. Já o representante comercial do país, Robert Lightizer, disse que o custo das empresas norte-americanas por esse uso indevido ficava entre US$ 225 bilhões a R$ 600 bilhões anuais. Uma pesquisa feita pela CNBC com diretores financeiros de empresas dos EUA que, somadas, têm US$ 5 trilhões em valor de mercado, concluiu que uma, de cada cinco delas, havia sofrido desvio de segredos corporativos por companhias chinesas, nos últimos dez anos. O think tank American Enterprise Institute, com sede em Washington, publicou vários estudos sobre o tema.

Depois de negar por anos a prática, o aumento da pressão fez com que, em dezembro de 2018, o governo chinês anunciasse 38 medidas punitivas impostas a empresas daquele país, envolvidas nesse tipo de conduta. Entre elas, o veto a financiamentos do governo e ter o nome exposto em bases de dados acessáveis por estrangeiros. Ao saber da iniciativa, especialistas se dividiram entre o ceticismo e o aplauso a uma iniciativa de tentar educar a população do país.

Há dezenas casos e notícias sobre processos envolvendo grupos globais contra empresas chinesas por desvios de dados e roubo de patentes. Abaixo, alguns deles:

Tesla - em março de 2019, a Tesla processou um ex-funcionário contratado pela fabricante de carros Xiaopeng Motors, alegando que havia levado informações estratégicas e valiosas para a concorrente. Em julho, durante julgamento, o funcionário admitiu que havia subido para sua própria nuvem no iCloud 300 mil arquivos do projeto de carro sem motorista, mas que teria deletado parte deles e saído da conta, antes de ir para a Xiaopeng.

Samsung - no fim de 2018, a Samsung acusou nove executivos, entre eles o presidente da fabricante chi-

Continuação: Empresas Chinesas têm histórico de acusações de roubos de dados

nesa de telas Toptec, de criar uma empresa fantasma para vender informações estratégicas sobre suas telas flexíveis. A Toptec, que era fornecedora da Samsung, negou, mas três executivos foram presos.

Apple - em julho de 2018, um ex-funcionário da Apple que havia feito o download do circuito de um carro sem motoristas e embarcado para a China, para trabalhar para a fabricante de carros Xiaopeng Motors, foi preso no aeroporto. Ele admitiu o download, mas negou o uso das informações na concorrente.

GE Aviação - em outubro de 2018, um oficial da inteligência chinesa foi preso e acusado de roubar segredos industriais e informações sensíveis de empresas áreas e aeroespaciais americanas, entre elas, a GE Aviação.

Velodyne - em agosto de 2019, a maior fabricante de sensores para carros sem motorista acusou duas empresas chinesas de vender produtos que usavam suas **patentes** sem respeitar a propriedade intelectual.

Invasão de hardwares - em outubro de 2018, a Bloomberg reportou que a Apple e a Amazon teriam descoberto que a Supermicro, uma das principais fornecedoras de servidores a empresas dos Estados Unidos, teria inserido microchips em placas-mãe para captar informações de empresas e governos. As empresas negaram.

Startup brasileira Vuxx processa chinesa Lalamove por desvio de dados

Lalamove

Com mais de 25 milhões de clientes em todo o mundo, a Lalamove é chamada de 'Uber da logística'

Além de se tornar uma ação indenizatória da Vuxx contra a Lalamove, o caso marca um movimento maior, o do crescimento do desvio de dados e uso indevido de propriedade intelectual no mundo das startups

Depois de quase quebrar em 2016, a startup Vuxx finalmente havia decolado. Espécie de shopping virtual para transporte de cargas pesadas, a empresa cresceu seis vezes em 2019, sobre o ano anterior. Tinha organizado uma nova rodada de captação para 2020 e a perspectiva era ganhar escala. Até que, em setembro, recebeu um alerta de que um funcionário havia baixado uma grande quantidade de dados estratégicos. Dois dias depois, ele pediu demissão. Nas semanas seguintes, a concorrente chinesa Lalamove passou a abordar seu clientes sabendo exatamente com quem falar, que preço cobrar e como concretizar a venda. Detalhe: o ex-funcionário havia enviado os dados e negociado sua própria contratação pela competidora nos computadores da Vuxx.

Além de se tornar uma ação indenizatória da Vuxx contra a Lalamove, o caso marca um movimento maior - o do crescimento do desvio de dados e uso indevido de propriedade intelectual no mundo das startups. Também, pela primeira vez, traz a indicação da participação de uma empresa chinesa nesse tipo de crime no País. A prática foi muito debatida após o início da guerra comercial entre Estados Unidos e China (

Com mais de 25 milhões de clientes em todo o mundo, a Lalamove é chamada de 'Uber da logística'

"A gente tinha uma vantagem competitiva grande, íamos surfar uma onda de crescimento e captar investimentos", diz Felipe Trevisan, fundador da Vuxx. "Vem então uma empresa altamente capitalizada, mas sem as informações estratégicas de mercado e, por meio de concorrência desleal, acaba com nossa vantagem competitiva."

Segundo ele, a estratégia da Lalamove era contar com a lentidão da Justiça brasileira para ganhar vantagem e fazer "o crime compensar". "Porém, eles não esperavam a qualidade das provas nem a agilidade e a qualidade da decisão liminar proferida", diz Gabriel Rocco, advogado do escritório Pereira Neto Macedo, que representa a Vuxx no processo.

Assim que percebeu o desvio da base de dados, a startup contratou uma equipe de peritos e um tabelião para entender o que havia acontecido. Percebeu que, ao se desligar da empresa, o ex-funcionário Adriano Misina não havia se deslogado do computador. Ou seja, todas suas conversas, inclusive as feitas via WhatsApp, estavam disponíveis na máquina. Havia diálogos nos quais contava à mulher o que havia feito - e ela o aconselha a ter cuidado em apagar rastros. Bem como conversas com Daniel Hsu, diretor de vendas da Lalamove e com quem havia trabalhado anteriormente em outra empresa. Nelas, ambos comemoram a obtenção das planilhas "com 6042 clientes filtrados por status, fase das negociações, emails de quem decide (...) que darão um p(...) faturamento" à empresa chinesa. "Bora botar pra dentro", responde Hsu.

Continuação: Startup brasileira Vuxx processa chinesa Lalamove por desvio de dados

Com as evidências em mãos, a Vuxx conseguiu liminarmente na Justiça que a Lalamove fosse impedida de contactar mais de 900 clientes ativos da base de dados. Na liminar concedida no fim de novembro, foi fixada multa de R$ 50 mil, em caso de descumprimento, para cada cliente acessado.

No recesso do judiciário, a Lalamove tentou derrubar a liminar. Entre seus argumentos, ela diz que os dados mencionados são públicos e facilmente encontrados no mercado e que a Vuxx tenta, na verdade, impedir a livre concorrência. Por ser uma grande multinacional e dona de uma base de dados gigantesca, não teria sentido desviar um pequeno arquivo da Vuxx. Também diz não estar envolvida institucionalmente, tendo a iniciativa partido exclusivamente de Misina, que foi desligado em seu período de experiência "por ser um dos piores vendedores". Há uma declaração dele, feita antes do processo, de que a Lalamove não foi a responsável por sua atitude. A chinesa diz ainda não ter usado a base de dados.

A Vuxx rebateu, dizendo que era pouco provável a empresa não estar envolvida, uma vez que a notificou dos fatos e Hsu permanece como diretor da empresa. O fato dele ter comemorado a obtenção do arquivo por WhatsApp com Misina denota a importância do arquivo desviado e o fato de não serem informações públicas. Além disso, tanto diretores da Vuxx quanto clientes cujos contatos pessoais estavam cadastrados apenas na base de dados desviada, receberam e-mails da Lalamove com ofertas de serviços. Seria uma prova de que as informações foram usadas. A liminar foi mantida tanto no plantão, quanto pelo relator definitivo.

Reparos

Além de impedir que a Lalamove acesse seus clientes, a Vuxx pediu uma indenização por danos emergentes. Startup de livro-texto, começou oferecendo um software a empresas de transporte e pivoteou - como é chamada no setor uma mudança de estratégia de negócios - para se tornar um market place, após pesquisar a área. Por três anos, 12 funcionários, munidos de ferramentas de inteligência artificial, mergulharam nos clientes para entendê-los até conseguir fazer um produto de sucesso. O resultado desse trabalho estava no arquivo desviado. Por esse custo, a Vuxx pede R$ 1 milhão em indenização.

Pede ainda lucros cessantes, cujo valor será calculado por um perito. O julgamento do mérito do processo é esperado para o fim do ano. Em 2019, a Vuxx faturou R$ 30 milhões e espera fazer uma rodada para captar R$ 30 milhões e expandir o serviço para outras capitais.

Com mais de 25 milhões de clientes em todo o mundo, a Lalamove é chamada de 'Uber da logística'. Foi fundada em 2013 por Shing Chow, ex-aluno da Universidade Stanford que conseguiu recursos para criar a empresa jogando pôquer profissionalmente. Em 2019, levantou US$ 300 milhões em uma rodada de investimentos liderada por Sequoia China e Hillhouse Capital.

Não há um levantamento sobre o desvio de dados ou roubo de **propriedade** intelectual das startups no Brasil. Porém, os especialistas dizem que é uma realidade relativamente comum, uma vez que segurança não está entre as primeiras prioridades de uma novata. "As empresas pensam que ter dados desviados é algo de Hollywood ou feito por um 007 da espionagem industrial, mas é muito comum quando é feita por um insider (funcionário) ou por meio de ataques cibernéticos", diz Leonardo Militelli, sócio da empresa de segurança cibernética Ibliss Digital Security, que tem um braço voltado a startups. "Como nas startups, as prioridades são a entrega do produto e o atendimento ao investidor, nem sempre o controle e a segurança é priorizada." Segundo ele, tem havido aumento na procura tanto nos quanto nos serviços de proteção, "mais por dor do que por tentar se prevenir do problema".

Procurada, a Lalamove não concedeu entrevista. Em

Continuação: Startup brasileira Vuxx processa chinesa Lalamove por desvio de dados

comunicado via assessoria de imprensa, porém, disse que "não usa nenhum tipo de informação confidencial de terceiros. (...) Nossa postura é a de entender e buscar a verdade por meio do diálogo e da transparência, reforçando a crença no livre mercado." Segundo a empresa, o departamento jurídico está trabalhando para esclarecer os fatos da melhor forma possível. "Ressaltamos nossa confiança na Justiça brasileira e vamos cooperar totalmente com as autoridades legais, acreditando na rápida resolução deste assunto." Procurado por meio da Lalamove, Hsu não falou. Adriano Misina também não quis ser entrevistado, limitando-se a dizer que "não podia prestar informações."

Primeira operação de combate a pirataria do ano apreende 154 réplicas de óculos na Capital

MATO GROSSO

A Delegacia Especializada do Consumidor (Decon), em parceria com o Procon Municipal e apoio de outras delegacias da região metropolitana, realizou nesta quinta-feira (23.01), a primeira operação de combate a **pirataria** do ano, na Capital. A operação intitulada **Pirataria** 1 apreendeu mais de 150 óculos réplicas de marcas famosas, que eram comercializados a preço muito abaixo ao de mercado.

O trabalho contou com apoio das equipes da Delegacia Especializada de Roubos e Furtos (DERF) de Cuiabá, Delegacia Especializada de Repressão a Roubos e Furtos de Veículos (DERRFVA), e Delegacia Especializada de Direitos da Criança e Adolescente (Deddica).

As investigações iniciaram após a Decon receber requerimento das marcas dos fabricantes de óculos e acessórios Okley e Ray-Ban sobre a comercialização de supostas réplicas de seus produtos. Os alvos de averiguações foram seis bancas de um comércio coletivo, localizado no Bairro Dom Aquino, em Cuiabá.

Em todas as bancas fiscalizadas foram apreendidos possíveis réplicas das marcas, totalizando 154 óculos, sendo 78 Ray-Ban e 76 Oakley. Os produtos recolhidos foram encaminhados a Perícia Oficial e Identificação Técnica (Politec)

Segundo o delegado, Antônio Carlos de Araújo, nas lojas foram localizadas réplicas de outras marcas, porém somente foram recolhidos os produtos dos fabricantes que registraram a reclamação. Pois somente as duas mandaram o modelo padrão dos seus produtos para confronto pela perícia, explicou o delegado.

Os seis Autos de Investigação Preliminar (AIP) foram transformados em inquérito policial e os responsáveis pelas lojas foram intimados a comparecer à Decon, em data marcada, para prestar esclarecimentos.

Os responsáveis pelos estabelecimentos poderão responder por crimes relativos a condutas praticadas no comércio de produtos falsificados ou pirateados, que estão tipificadas no artigo 190, inciso 1 da Lei 9.279/96, do Código de Propriedade Industrial, pena detenção de 3 meses a 1 ano; artigo 7, inciso 7, VII, da Lei 8.137/90 da lei contra as Relações de consumo, pena de 2 a 5 anos ou multa; por fraudes no comércio, previsto no artigo 175, inciso I do CPB, e ainda por infrações praticadas dentro do Código de Defesa do Consumidor (Lei 8.078/90 em seu artigo 67).

CenárioMT - Assessoria | PJC-MT

Melado paranaense conquista selo de qualidade geográfica

Geraldo Bubniak/AEN Geraldo Bubniak/AEN Geraldo Bubniak/AEN

Mais um produto tipicamente paranaense ganhou reconhecimento nacional. O **INPI** (Instituto Nacional da Propriedade Industrial) concedeu, em dezembro, a IG (**Indicação** Geográfica) para o melado produzido na cidade de Capanema, no Sudoeste do Estado. A partir de agora, o produto passa a ser comercializado com o selo ?Capanema?, único no mercado.

Com a indicação de procedência, o melado passa a ser mais valorizado, possibilitando a expansão do comércio dentro do Brasil e até mesmo no exterior. De acordo com a prefeitura do município, Capanema conta atualmente com oito agroindústrias e 16 produtores de cana de açúcar, base do melado batido da região.

A produção de melado na cidade, segundo a Secretaria de Estado da Agricultura e Abastecimento, é de 400 toneladas por ano. As cooperativas e nove indústrias de médio porte de Capanema garantem 200 empregos diretos.

A conquista do certificado já mobiliza os produtores locais. Eles falam em ampliar a produção para conseguir levar o produto a novos mercados. ?A expectativa é muito boa, pensamos em alcançar uma escala maior de vendas. É uma ótima oportunidade para trazer novas famílias para a produção da matéria-prima, gerando mais empregos?, disse Itamar Schuck.

Ele é diretor-presidente da Cooperfronteira (Cooperativa Agroindustrial Fronteira Iguaçu) que conta com 45 cooperados, entre agroindústrias, produtores de cana e pessoas com interesse em participar do processo produtivo. ?A conquista da IG era o que precisávamos para buscar mais inovações e tecnologia. Estamos na parte final da criação da nossa marca?, afirmou.

Norberto Ortigara, secretário de Estado da Agricultura e Abastecimento, também comemora a conquista estadual. ?São pequenas e médias propriedades que apostaram na cana de açúcar, especialmente na produção do melado e do açúcar mascavo. Se tornou uma grife do município?, afirmou. ?É um melado de muita qualidade, e isso permitiu ganhar essa diferenciação. É o reconhecimento desse esforço de décadas. Esse melado o consumidor só encontra aqui no Paraná?, acrescenta.

GEOGRAFIA

Outro produtor, Gilberto Hass revelou detalhes do processo que garantiram o selo de qualidade ao melado de Capanema. Segundo ele, o município conta com uma geografia favorável, que garante uma cana de açúcar diferenciada. Citou ainda o tipo de terreno para o cultivo, com muito pedregulho, e o clima quente da região. ?Com isso nossa cana tem mais sacarose, ficando mais doce?.

Ele também faz planos para aumentar a produção na empresa, que administra com a ajuda dos dois filhos. Espera mudar para a sede nova até julho, renovando maquinário e automatizando parte do processo produtivo.

Com isso, diz acreditar que pode saltar dos atuais 400 quilos de melado a cada dois dias prontos para a comercialização de 2.500 quilos no mesmo período. Hass intercala a produção de melado com a de açúcar mascavo.

No horizonte da família está a exportação da mercadoria. Hass contou que já iniciou conversas com dois países: Estados Unidos e Holanda. ?Estamos correndo atrás de tecnologia, passo importante para

Continuação: Melado paranaense conquista selo de qualidade geográfica

conseguirmos aumentar a produção?, afirmou.

Reforço que se dará em cadeia. Mais melado significa mais necessidade de cana. ?Vamos firmar parcerias com pequenos agricultores. Acho que podemos atingir até 100 famílias?.

Outro fator que influencia é a proximidade do Rio Iguaçu, que garante uma ótima qualidade no processo de irrigação. ?O que deu notoriedade ao produto foi a qualidade. Temos que nos preocupar em crescer, mas sempre mantendo essa característica?, ressaltou Rafael Morgenstern.

Agrônomo de formação, ele voltou para Capanema para ajudar a família, há 22 anos envolvida com a produção e venda de açúcar mascavo e melado. ?Tudo aqui é bem familiar?, contou. Os Morgenstern fabricam 1,5 mil quilos de cada produto por semana.

Há, contudo, outros segredos que vão além da qualidade da cana. Secretária municipal de Agricultura e Meio Ambiente, Raquel Belchior Szimanski diz que para o produto ficar tipicamente de Capanema depende da moagem da cana, do processo de decantação, da fervura em alta temperatura para a retirada de impurezas e, por fim, o processamento em um tacho acoplado a uma batedeira. ?A cor é mais escura, com uma cremosidade diferente e uma doçura especial?, destacou.

IGs PARANAENSES

O Paraná conta atualmente com oito produtos com **Indicação** Geográfica reconhecida. Além do melado de Capanema, cujo processo contou com a colaboração integral do Sebrae-PR, também receberam destaque do **INPI** a erva-mate de São Mateus do Sul; o café do Norte Pioneiro; a goiaba de Carlópolis, o queijo colonial de Witmarsun; as uvas finas de Marialva e o mel de Ortigueira.

E, ao que tudo indica, Capanema pode ganhar um novo selo de certificação nos próximos meses. O açúcar mascavo produzido na cidade está passando por detalhes para também ser reconhecido pelo **INPI.**

?Isso é mais renda para o produtor. A IG também ajuda a trazer mais gente ao nosso Sudoeste, mostrando que só aqui em Capanema tem esse produto?, afirmou Fernando Martini, presidente da Associação Doce Iguassu. A entidade foi responsável por dar entrada no processo que terminou com a conquista da **Indicação** Geográfica.

Outras produções no Estado também estão em processo de certificação: a bala de banana de Antonina, a cachaça de Morretes, e o barreado e a farinha de mandioca, tradicionais no Litoral do Paraná.

O que é **Indicação** Geográfica?

A IG nada mais é do que a identificação que dá origem a um produto ou serviço. Após conquistado, somente os produtores e prestadores de serviços da região (em geral, organizados em entidades representativas) podem utilizar o selo.

As indicações são divididas em dois tipos: as de **denominação** de origem reconhecem o nome de um país, cidade ou região cujo produto ou serviço tem certas características específicas graças a seu meio geográfico, incluídos fatores naturais e humanos.

Já a indicação de procedência se refere ao nome de um país, cidade ou região conhecido como centro de extração, produção ou fabricação de determinado produto ou de prestação de determinado serviço.

A Lei Geral de Proteção de Dados (LGPD) aplicada à saúde: cinco pontos importantes sobre a proteção de dados do paciente

No âmbito da saúde, a coleta de dados do paciente é condição imprescindível ao exercício da atividade. Todo o histórico de saúde, bem como as condutas adotadas pelo profissional, são registradas por meio de prontuário, um documento definido pelo Conselho Federal de Medicina (CFM) como ***um*** conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membro da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo (Resolução 1.6038/02).

Ocorre que, de acordo com a lei 13.709/18 (LGPD), que deverá entrar em vigor em agosto de 2020, as informações referentes à saúde são "dados pessoais sensíveis", e seu tratamento deve atender aos princípios estipulados por essa lei. Desse modo, hospitais e clínicas devem estar atentos às novas regras.

1) Por que é necessário falar em proteção dos dados sensíveis do paciente?

O direito ao sigilo, à privacidade, à autonomia e à dignidade são garantias constitucionais. A Lei Geral de Proteção de Dados (LGPD) vem para reforçar a proteção a bens que são extremamente caros a todo ser humano.

Quando se fala em saúde, essa proteção se torna ainda mais importante, uma vez que cuida de informações que são bastante íntimas do paciente, mas ao mesmo tempo essenciais para o tratamento médico.

Outro ponto importante da lei é a vedação ao uso dos dados sensíveis dos pacientes pelas operadoras de planos de saúde para contratação ou exclusão de beneficiários.

2) Como o tratamento dos dados influencia na relação médico-paciente?

A anamnese é um procedimento essencial para que o médico possa compreender os sintomas do paciente e chegar a um diagnóstico, e, para que seja realizada de modo satisfatório, é essencial que exista uma relação de confiança do paciente para com o profissional.

O paciente jamais se sentirá á vontade para falar sobre fatos íntimos se não tiver a segurança de que seus dados serão adequadamente preservados. Além disso, determinados diagnósticos resultam em estigma social, e o eventual vazamento da informação pode causar danos irreparáveis.

3) Quais as normas atuais para tratamento de dados sensíveis do paciente?

A iminência da entrada em vigor da LGPD tem sido motivo de inquietação para médicos e gestores da área de saúde, em especial devido às sanções administrativas descritas na lei. Contudo, o tema da proteção dos dados dos pacientes já é normatizado pela Constituição, leis e resoluções e essas regras devem

ser observadas desde já. São exemplos:

Constituição Federal: além de garantir a dignidade da pessoa humana, determina que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Código Civil: os **direitos** da personalidade são irrenunciáveis, sendo possível ao seu titular exigir que cesse a ameaça, ou a lesão, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Código Penal: tipifica o crime de violação de segredo profissional (artigo 154). Código de Ética Médica: elenca os deveres de sigilo e respeito à autonomia do paciente. Resolução CFM 1.605/00: o médico não pode, sem o consentimento do paciente, revelar o conteúdo do prontuário ou ficha médica. Resoluções CFM 1.821/07 e 2.218/18: Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Obs.: As resoluções são hierarquicamente inferiores às leis, de modo que, havendo incompatibilidade entre uma Resolução do CFM e a LGPD, prevalece a regra da lei.

4) Como evitar falhas na proteção dos dados sensíveis do paciente?

A LGPD determina que sejam utilizadas 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 e difusão desses dados.

A mera adoção de barreiras tecnológicas não é suficiente para a proteção jurídica dos agentes de tratamento de dados. Isso porque a maioria das falhas na segurança resulta de ação humana (basta lembrar dos casos de pacientes famosos que tiveram sua imagem compartilhada por profissionais dos hospitais).

É necessário que haja treinamento e conscientização de todos aqueles que trabalham na unidade e que possam ter acesso aos dados dos pacientes. A LGPD destaca a importância da adoção de práticas de governança e políticas internas que demonstrem o compromisso com a segurança dos dados.

5) Como médicos, clínicas e hospitais podem ser responsabilizados por falhas na proteção de dados dos pacientes?

A LGPD elenca sanções administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), e variam desde uma advertência até multa de 2% sobre o faturamento da pessoa jurídica. Essas sanções, é preciso lembrar, não excluem as responsabilidades cíveis e penais resultantes da falha na segurança dos dados.

_____

*Ana Helena de Miranda Guimarães é advogada, inscrita na OAB/GO sob o número 43.660. Formada em Direito pela PUC-GO. Pós-Graduada em Direito Público pela Faculdade Damásio. Cursando Pós-Graduação em Direito Médico e da Saúde pela Faculdade Legale. Atuante nas áreas de Direito Civil, Direito do Consumidor e Direito Médico e da Saúde. Membro da Comissão de Direito médico, Sanitário e Defesa da Saúde da OAB/GO. Membro do Comitê de Ética em pesquisa Humana do Hospital da Clinicas de Goiânia.

Ana Helena Guimarães

A violação de dados pessoais e seus impactos sob a égide do Regulamento Europeu de Proteção de Dados (GDPR)

Em novembro de 2018, uma das autoridades supervisoras da Alemanha (LfDI- ***Landesbeauftragte*** für den Datenschutz und die Informationsfreiheit, autoridade responsável pela proteção de dados e liberdade de informação em Baden-Württemberg) multou o aplicativo de mensagens Knuddels em 20 mil euros após uma violação que comprometeu os dados pessoais de aproximadamente 300 mil usuários. A causa foi a não utilização pela empresa de criptografia nos dados pessoais dos usuários, o que facilitou a violação.1 Mais recentemente -- em janeiro de 2020 --, a autoridade pública em matéria de proteção de dados do Reino Unido (Information Commissioner's Office) impôs uma multa de 500 mil libras em razão de um ataque cibernético que afetou, ao menos, dados de 14 milhões de pessoas, incluindo nomes, CEPs e endereços de e-mail.2

Episódios como esses e o comportamento das empresas em relação aos dados pessoais dos indivíduos geram uma preocupação maior sobre o tema, inclusive sobre a violação -- ou vazamento -- de dados. Neste contexto, novas legislações foram elaboradas e aperfeiçoadas com o objetivo de proteger a privacidade e os dados pessoais.

No Brasil, ainda aguardamos o início da vigência da Lei Geral de Proteção de Dados (LGPD, que entrará em vigor em agosto de 2020, podendo tal data ainda ser prorrogada para agosto de 2022, caso seja aprovado o projeto de lei 5762/19), de forma que ainda não há uma lei estruturada para regular a proteção de dados pessoais, inclusive no contexto de violação. Por outro lado, na União Europeia, o Regulamento Geral sobre a Proteção de Dados (mais conhecido pela sigla ***GDPR,*** do inglês ***General*** Data Protection Regulation) está em vigor desde 25 de maio de 2018 e possui um conjunto de direitos, obrigações e sanções para o caso de descumprimento de seus preceitos -- o que inclui a violação de dados.

Dessa forma, na seara do GDPR, como é tratado um caso de quebra de dados pessoais? O que pode o indivíduo afetado fazer? E, principalmente, como deve a pessoa jurídica responsável agir?

O que é violação de dados pessoais?

De acordo com o artigo 4(12) do GDPR, a violação de dados pessoais (ou ***personal*** data breach) consiste em uma infração da segurança que tenha por efeito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, seja de modo acidental, seja de modo ilícito.

Por consequência, tanto o acesso não autorizado, quanto a divulgação não autorizada de dados como nome, endereço, e-mail, números de identificação pessoal e fiscal, informações bancárias, ***login,*** senha, identidade do usuário, informações relacionadas à saúde, preferência religiosa, política, além de outros dados sensíveis e não-sensíveis, podem ser enquadrados como violação de dados pessoais. Convém frisar que violação de dados é um gênero, enquanto que a divulgação e o acesso não autorizados

são algumas de suas espécies.

Quais são os personagens envolvidos na violação de dados pessoais?

De modo geral, os sujeitos presentes no contexto de uma violação de dados pessoais, para o GDPR, são os seguintes:

indivíduo ou indivíduos afetados, os quais necessariamente devem ser pessoas naturais; responsável pelo tratamento (***data*** controller), ou seja, aquele que define o propósito e como os dados pessoais serão tratados; subcontratante (***data*** processor), o qual realiza o processamento de dados em nome do responsável pelo tratamento; encarregado da proteção de dados (***data*** protection officer), o qual, em determinadas circunstâncias, deve ser contratado e que possui uma série de funções relacionadas à proteção de dados pessoais; autoridade supervisora, que deve fiscalizar a aplicação do regulamento europeu e que possui um conjunto de atribuições e poderes.

Conforme o direito europeu, tanto os responsáveis pelo tratamento quanto os subcontratantes possuem a obrigação de implementar medidas técnicas e organizacionais visando garantir um nível de segurança adequado ao risco relacionado à proteção de dados pessoais. Dentre essas medidas, podem ser destacadas as seguintes: (i) pseudonimização e criptografia de dados pessoais; (ii) capacidade de manter a confidencialidade, a integridade, a disponibilidade e a resiliência dos sistemas e serviços de tratamento de dados; (iii) restabelecimento da disponibilidade e acesso aos dados pessoais em caso de um incidente técnico ou físico; (iv) realização regular de testes e avaliações em relação à efetividade das medidas técnicas e organizacionais para garantir a segurança do tratamento dos dados.

Houve uma violação de dados pessoais, e agora?

No caso de uma violação de dados pessoais, o responsável pelo tratamento pode detectar tal falha por conta própria ou pode ser informado pelo indivíduo afetado pelo evento ou por outra fonte. De qualquer forma, como se verá adiante, o ***controller*** possui um tempo significativamente reduzido para agir.

O responsável deve informar a quebra à autoridade supervisora em até 72 (setenta e duas) horas após tomar conhecimento sobre a ocorrência. Tal notificação deve conter, ao menos, os seguintes elementos: descrição da natureza da violação, da categoria e do número de indivíduos e dados afetados; o contato do encarregado de proteção de dados ou da pessoa designada para lidar com o evento; as consequências prováveis da violação e as medidas adotadas ou propostas para conduzir o caso, o que pode incluir medidas para mitigar os possíveis efeitos adversos da violação dos dados pessoais.

Convém pontuar que o responsável pelo tratamento deve fornecer o máximo de informações possível dentro do referido prazo. Se isso não for viável, ele deve, em tempo razoável, notificar a violação à autoridade competente, incluindo os motivos que ocasionaram o atraso. Além disso, a empresa/organização deve registrar os fatos relativos aos incidentes de segurança, seus efeitos e as medidas adotadas.

É importante esclarecer que o dever de notificar está atrelado ao responsável pelo tratamento dos dados. Todavia, o subcontratante deve notificá-lo de forma rápida, assim que souber da ocorrência da violação.

O GDPR oferece uma exceção ao dever de notificação: caso o responsável pelo tratamento consiga demonstrar que os riscos aos direitos e liberdades dos indivíduos são improváveis, não haverá a necessidade de notificar a autoridade supervisora sobre a quebra.

Ademais, o GDPR também contém normas relacionadas à comunicação com os indivíduos afetados. Entretanto, esse dever não se aplica a todos os casos de violação, mas apenas aos que possam re-

sultar em um alto risco aos direitos e liberdades das pessoas naturais. Mesmo nesses casos, a comunicação pode deixar de ser obrigatória em determinadas circunstâncias.

Se o responsável deixar de cumprir o dever de notificar ou o princípio da integridade e confidencialidade, o indivíduo pode apresentar uma reclamação diretamente à autoridade supervisora. Além disso, ele ainda pode optar pela via judicial, seja contra o responsável pelo tratamento ou o subcontratante, seja contra a autoridade supervisora, caso ela não informe o indivíduo sobre o acompanhamento ou resultado da reclamação no prazo de três meses ou ela não promova o andamento do procedimento.

E o que a autoridade supervisora pode fazer diante de uma violação dos dados pessoais?

Caso haja violação de dados pessoais, a depender das circunstâncias relacionadas ao evento e conforme as infrações dos preceitos do GDPR, a autoridade supervisora pode aplicar sanções, inclusive a imposição de multas, as quais devem, em cada caso, ser efetivas, proporcionais e dissuasivas. Essas penalidades são mensuradas de acordo com vários critérios, tais como o grau da infração e seus impactos; as medidas adotadas para a mitigação dos danos sofridos pelos indivíduos; a conduta e o grau de responsabilidade do ***controller*** e processor diante das circunstâncias.

É importante destacar que as multas relacionadas à violação de dados pessoais podem alcançar o importe de 10 milhões de euros ou 2% do volume de negócios anual, o que for maior.

Considerações finais

A violação de dados pessoais é um incidente preocupante e que pode trazer consequências graves ao direito fundamental à proteção de dados pessoais, tais como uso indevido dos dados, fraude, danos materiais e comprometimento da reputação dos indivíduos.

Considerando que o GDPR possui efeito extraterritorial - isto é, ele também pode alcançar empresas que não estejam estabelecidas na União Europeia e no Espaço Econômico Europeu,3 é de fundamental importância que as figuras envolvidas no tratamento de dados - seja como subcontratante, seja como responsável pelo tratamento - tenham agilidade e observem o GDPR em caso de violação de dados pessoais. Como explicado anteriormente, a autoridade supervisora deve ser informada o quanto antes e deve receber o maior número de informações possível sobre o ocorrido.

Portanto, é fundamental que os responsáveis e os subcontratantes, mesmo que não estabelecidos na Europa, realizem um diagnóstico para verificar se o GDPR é aplicável ao processamento de dados. Em caso positivo, eles devem observar atentamente e respeitar suas normas, princípios e padrões - inclusive os referentes à segurança dos dados -, adotar controles e medidas eficazes relacionados à proteção de informações pessoais e cumprir com o dever de notificar e comunicar em caso de violação dos dados pessoais.

_____

1 Irwin (2018).

2 "National retailer fined half a million pounds for failing to secure information of at least 14 million people" (2020)

3 "GDPR-Extraterritorial applicability | Deloitte Switzerland" (2017).

Clique aqui.

Clique aqui.

Clique aqui.

Clique aqui.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. Handbook on European data protection law: 2018 edition. Publications Office Of The European Union, 2018. 397 p.

_____

*Mateus Mello Garrute é advogado especialista em proteção de dados pessoais, mestre em direito processual pela UFES, LL.M. em direito europeu e transnacional da **propriedade** intelectual e da informação tecnológica pela Universidade de Göttingen (Alemanha), certificado pela International Association of Privacy Professionals (CIPP/E) e membro da European Association of Data Protection Professionals (EADPP).

*Estela Schmidt é advogada, LL.M. em direito europeu e transnacional da propriedade intelectual e da informação tecnológica pela Universidade de Göttingen (Alemanha) e bacharel em Direito pela Universidade Presbiteriana Mackenzie.

Mateus Mello Garrute e Estela Schmidt

Índice remissivo de assuntos