



CRIMES CIBERNÉTICOS E A NECESSIDADE DE ADOÇÃO DE PROGRAMAS DE INTEGRIDADE PELAS PLATAFORMAS DIGITAIS

Chaiene Meira de Oliveira¹

Com o presente trabalho objetiva-se investigar as possibilidades de responsabilização das plataformas digitais em face da ocorrência de crimes cibernéticos e a necessidade da adoção de uma cultura de integridade como forma de prevenção e identificação de ilícitos. A temática está relacionada com a necessidade da adoção de uma cultura de integridade e responsabilização das plataformas digitais e ocorrência de crimes cibernéticos estando delimitada ao contexto brasileiro.

Considerando a possibilidade de responsabilização das plataformas digitais na ocorrência de crimes cibernéticos, propõe-se o seguinte questionamento: de que forma a adoção de uma cultura de integridade pode contribuir para fins preventivos e sancionatórios?

Para responder ao problema de pesquisa, utilizou-se do método de abordagem dedutivo tendo em vista que partindo de uma contextualização ampla sobre o cenário vivenciado pelo aumento da ocorrência de crimes cibernéticos a nível nacional passa-se a análise específica sobre de que modo a adoção de programas de integridade, como o *compliance*, pode contribuir para evitar a ocorrência de ilícitos e, caso ocorram, na sua identificação. O método de pesquisa é o bibliográfico e, as técnicas de pesquisa resumem-se à consulta a livros, artigos, periódicos, teses, dissertações, legislação, notícias e dados veiculados oficialmente.

A justificativa, em termos teóricos, centra-se na necessidade de ampliar os estudos sobre a temática, a qual sofre constantes modificações não apenas em termos legislativos e doutrinários, mas no dia a dia dos usuários das plataformas digitais e seus responsáveis. Em termos práticos, justifica-se pela relevância do tema que afeta milhares de pessoas no mundo e mais especificamente no Brasil ocasionando em prejuízos para as vítimas de golpes e para as empresas.

A hipótese inicial é no sentido de que a adoção de instrumentos de integridade pode contribuir não apenas para prevenção da ocorrência de atos ilícitos internos nas empresas detentoras de plataformas digitais, como pode auxiliar na identificação dos autores e forma de atuação caso estes ocorram de modo a colaborar efetivamente com o Estado.

¹ Doutora em Direito. Universidade de Santa Cruz do Sul - UNISC. E-mail: chaiene@mx2.unisc.br.



Os objetivos específicos, em conformidade com a divisão dos tópicos, são em um primeiro momento objetiva-se contextualizar o cenário vivenciado pelo aumento da ocorrência de crimes cibernéticos a nível nacional; após visa-se apresentar as definições e previsão normativa dos programas de integridade no Brasil e por fim, verificar de que modo a adoção de programas de integridade, como o *compliance*, pode contribuir para evitar a ocorrência de ilícitos e, caso ocorram, na sua identificação.

Inicialmente, em relação ao primeiro tópico, é preciso apresentar uma breve contextualização sobre o cenário vivenciado no Brasil quanto à ocorrência de crimes cibernéticos; conforme divulgado pela Rádio Senado (2025), os crimes digitais subiram 45% no ano de 2024 totalizando cerca de 5 milhões de fraudes de acordo com a ADDP (Associação de Defesa de Dados Pessoais e do Consumidor).

Importante salientar que não se trata de um tipo penal único, mas sim, uma série de condutas ilícitas, de acordo com a definição apresentada pela Polícia Federal em seu site institucional, os crimes cibernéticos são infrações penais cometidas por meio da internet ou de sistemas digitais afetando pessoas, empresas e instituições públicas ou privadas. Por exemplo, as fraudes bancárias, os crimes de alta tecnologia, o abuso sexual infanto-juvenil online, e os crimes de ódio, quando cometidos por meio da Internet ou de sistemas digitais.

Segundo Leal (2023), diferente dos crimes tradicionais onde a identificação das vítimas é costumeiramente óbvia, no ambiente digital a detecção dos crimes cibernéticos, seus autores e vítimas é em muitos casos dificultada pelo mascaramento dos instrumentos e meios utilizados. Especificamente no âmbito do direito, é possível citar como exemplo o denominado “golpe do falso advogado” no qual golpistas se passando pelo advogado das vítimas, exigem o pagamento de quantias em dinheiro para a suposta liberação de valores de ações judiciais.

Recentemente foi sancionada a Lei 15.397/2026, a qual altera o Código Penal aumentando as penas para delitos como furto, roubo, estelionato e receptação, endurecendo o tratamento penal de crimes contra o patrimônio e contra serviços públicos essenciais, como energia e telecomunicações. No caso dos golpes ou fraudes bancárias, a pena é de reclusão de quatro a dez anos, e multa, se houver furto cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso.

Por sua vez, a conduta de utilizar “contas laranja” possui reclusão, de um a cinco anos, e multa, para quem ceder, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto. E, no



caso de fraudes eletrônicas, a pena é de reclusão de quatro a oito anos, e multa, para fraude cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento, duplicação de dispositivo eletrônico ou aplicação de internet.

No tocante ao segundo tópico, o termo deriva do verbo *to comply* que, em sentido literal, expressa o sentido de agir em conformidade com as regras. Importante salientar que embora seja majoritariamente ligado a ideia de conformidade e prevenção de práticas ilegais, como a corrupção, tais programas possuem um amplo rol de possibilidades como é o caso do *compliance* na esfera ambiental e antidiscriminatória, por exemplo.

Ao se pensar em integridade, Zenkner (2020) menciona que há uma relação direta com os valores consolidados com base em conceitos de ética e moralidade; de uma forma direta, a integridade implica na correspondência entre os valores morais defendidos por determinada pessoa e sua concretização quando é colocada diante de situações problema no dia a dia. Em conclusão, integridade pressupõe uma consistência interna e externa de virtudes que impeçam a prática de atos incoerentes ou que conflitem com a postura explicitada.

Dessa forma, segundo Assi (2013), *compliance* se refere também aos sistemas de controles internos que permitem esclarecer e proporcionar maior segurança aos que utilizam da contabilidade para fins de análise tanto econômico-financeira quanto de gerenciamento operacional.

Nestes controles estão incluídos a prevenção às fraudes e operações ilegais que possam causar desfalques à própria instituição e a terceiros. Na mesma linha, defende Antonik (2016), que o objetivo principal do *compliance* é o combate à corrupção e, diferentemente da ética, a qual é assumida de forma espontânea, a adoção dos programas de *compliance* está relacionada à responsabilidade legal necessitando para tanto da formulação e estruturação de mecanismos específicos.

Por fim, é preciso pontuar que neste trabalho não vão ser discutidos eventuais aspectos penais relacionados à pessoa jurídica por não haver previsão legal e tal estudo demandar uma abordagem mais específica e aprofundada de modo que os exemplos trazidos não abrangem esta seara. Nesta linha, o Supremo Tribunal Federal (STF) definiu, no Tema 987 da repercussão geral, que é parcialmente inconstitucional a regra do artigo 19 do Marco Civil da Internet (MCI – Lei 12.965/2014). O dispositivo exige o descumprimento de ordem judicial específica para que os provedores de aplicações de internet sejam responsabilizados civilmente por danos causados por conteúdo publicado por terceiros.



Além disso, foi decidido que enquanto o Congresso Nacional não editar nova lei sobre o tema, a plataforma será responsabilizada civilmente pelos danos decorrentes de conteúdos gerados por terceiros em casos de crimes em geral ou atos ilícitos se, após receber um pedido de retirada, deixar de remover o conteúdo. A regra também vale para os casos de contas denunciadas como falsas.

Relacionando com a discussão proposta, ficou decidido também que os provedores deverão editar uma autorregulação abrangendo um sistema de notificações, devido processo, bem como relatórios anuais de transparência no que tange a notificações extrajudiciais, anúncios e impulsionamentos, bem como as plataformas deverão disponibilizar canais permanentes de atendimento, de preferência eletrônicos, acessíveis e amplamente divulgados.

É evidente que o cenário é novo, mas é preciso que o Estado e a iniciativa privada estejam preparados para lidar com os riscos e novas formas de criminalidade oriundas dos avanços tecnológicos. Nesta seara, um programa de integridade bem estruturado pode preservar a atividade da empresa bem como prepará-la para eventuais ocorrências sob o seu domínio. Para além de novas normas, sejam estas reguladoras ou incriminadoras, é preciso que haja uma colaboração conjunta entre todos os agentes envolvidos.

Diante do exposto, considerando o espaço para abordagem e o caráter inicial desta proposição de pesquisa, passa-se a responder ao problema de pesquisa o qual questionou: de que forma a adoção de uma cultura de integridade pode contribuir para fins preventivos e sancionatórios? Até o momento, resta confirmada a hipótese inicial no sentido de que a adoção de instrumentos de integridade pode contribuir não apenas para prevenção da ocorrência de atos ilícitos internos nas empresas detentoras de plataformas digitais, como pode auxiliar na identificação dos autores e forma de atuação caso estes ocorram de modo a colaborar efetivamente com o Estado.

Palavras-chave: *Compliance*. Crimes cibernéticos. Regulação. Tecnologia.

REFERÊNCIAS

ANTONIK, Luis Roberto. *Compliance*, ética, responsabilidade social e empresarial: uma visão prática. Rio de Janeiro, RJ: Alta Books, 2016.

ASSI, Marcos. *Gestão de compliance e seus desafios: como implementar controles internos, superar dificuldades e manter a eficiência dos negócios*. São Paulo: Saint Paul Editora, 2013.



BRASIL. Polícia Federal. **Combate a crimes cibernéticos**. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/combate-a-crimes-ciberneticos>. Acesso em: 04 maio 2026.

BRASIL. Senado Federal. **Crimes digitais sobem 45% e Senado tem propostas para frear sequestro de dados**. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2025/01/16/crimes-digitais-sobem-45-e-senado-tem-propostas-para-frear-sequestro-de-dados>. Acesso em: 04 maio 2026.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 04 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Brasília, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/>. Acesso em: 04 maio 2026.

LEAL, Rogério Gesta. Realidade virtual e criminalidade: tensões e desafios. **Revista de Direitos e Garantias Fundamentais**, v. 24, p. 107-135, 2023.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Tema 987 – Repercussão geral:** constitucionalidade do art. 19 da Lei nº 12.965/2014 (Marco Civil da Internet). Julgado em 27 jun. 2025. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987>. Acesso em: 05 maio 2026.

ZENKNER, Marcelo. **O papel do setor privado na promoção da integridade nos negócios**. In: *Compliance, gestão de riscos e combate à corrupção: integridade para o desenvolvimento*. Belo Horizonte: Fórum, 2020.