PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS PRÓ-REITORIA DE GRADUAÇÃO ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO CURSO DE GRADUAÇÃO EM DIREITO NÚCLEO DE PRÁTICA JURÍDICA COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

IMPLICAÇÕES LEGAIS DA COLABORAÇÃO ENTRE RED TEAMS E AUTORIDADES POLICIAIS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

JOÃO PEDRO DIAS AIRES
CLAUDIA LUIZ LOURENCO

GOIÂNIA – GO
2025

JOÃO PEDRO DIAS AIRES

IMPLICAÇÕES LEGAIS DA COLABORAÇÃO ENTRE RED TEAMS E AUTORIDADES POLICIAIS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

Monografia jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGOIÁS). Prof. (a) Orientador (a) - Dra. Claudia Luiz Lourenco

GOIÂNIA - GO
2025

RESUMO

Este trabalho analisa o papel dos Red Teams na prevenção e resposta a crimes cibernéticos, destacando a importância da colaboração entre os setores público e privado. A pesquisa aborda os conceitos e características dos crimes cibernéticos, explora a atuação dos Red Teams, examina o marco legal brasileiro e realiza uma análise comparativa internacional com países como Estados Unidos, União Europeia e Israel. A partir disso, são identificadas lacunas normativas, riscos jurídicos e impactos sobre os direitos fundamentais. O estudo propõe recomendações legislativas, diretrizes operacionais e políticas públicas para fortalecer a segurança cibernética no Brasil e promover ações eficazes no combate às ameaças digitais.

Palavras-chave: Crimes cibernéticos. Red Teams. Legislação. Segurança digital. Colaboração.

SUMÁRIO

INTRODUÇÃO

Este trabalho tem como foco a análise das implicações legais decorrentes da colaboração entre Red Teams — equipes especializadas em simular ataques cibernéticos — e autoridades policiais no contexto da investigação de crimes cibernéticos no Brasil. A pesquisa se concentra especificamente nos aspectos jurídicos e éticos que envolvem essa cooperação, considerando a atual ausência de um marco regulatório claro e específico no ordenamento jurídico brasileiro.

A delimitação abrange, ainda, a atuação dos Red Teams em ambientes controlados, com o consentimento das organizações alvo dos testes, e sua possível interação com órgãos de segurança pública na produção de provas, compartilhamento de informações ou apoio técnico em operações investigativas. Serão analisadas normas já existentes, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), além de experiências internacionais que possam servir de parâmetro para a realidade brasileira.

O problema de pesquisa que orienta este trabalho consiste em compreender quais são as implicações legais da colaboração entre Red Teams e autoridades policiais na investigação de crimes cibernéticos no Brasil, diante da inexistência de uma regulamentação específica que estabeleça os limites, responsabilidades e garantias jurídicas dessa interação. A ausência de um arcabouço normativo claro pode gerar insegurança jurídica para os profissionais envolvidos, comprometer a validade das provas obtidas e afetar direitos fundamentais, como a privacidade e a proteção de dados pessoais dos cidadãos, exigindo, portanto, uma análise crítica e propositiva sobre como essa colaboração pode ocorrer de forma legal, ética e eficaz.

A discussão sobre as implicações éticas e de privacidade é fundamental para assegurar que as ações realizadas no âmbito desta colaboração estejam alinhadas aos princípios de proporcionalidade e legalidade, prevenindo abusos e promovendo a confiança da sociedade nas instituições envolvidas.

Dessa forma, este trabalho busca preencher uma lacuna existente na literatura acadêmica e na prática jurídica brasileira, oferecendo uma base sólida tanto para futuras pesquisas quanto para a formulação de diretrizes claras e aplicáveis. A relevância do tema, somada à sua atualidade e ao impacto direto nas implicações legais da cooperação entre Red Teams e autoridades policiais na

investigação de crimes cibernéticos, torna essa discussão não apenas necessária, mas urgente.

A justificativa deste trabalho reside na necessidade de explorar e compreender as implicações legais dessa colaboração, dada a ausência de um arcabouço jurídico específico e claro no Brasil que regule essas interações. A falta de regulamentação pode gerar insegurança jurídica tanto para os Red Teams quanto para as autoridades policiais, além de potencialmente comprometer os direitos fundamentais dos cidadãos, como a privacidade e a proteção de dados pessoais.

Ademais, a análise de casos práticos e a comparação com experiências internacionais permitirão identificar boas práticas que podem ser adaptadas ao contexto brasileiro, promovendo uma maior eficácia nas investigações cibernéticas. A compreensão dos desafios e oportunidades dessa colaboração pode contribuir para a elaboração de políticas públicas e legislações que garantam uma atuação coordenada e eficiente no combate aos crimes cibernéticos, sem negligenciar a proteção dos direitos dos cidadãos.

A presente pesquisa tem como objetivo geral a análise das implicações legais da colaboração entre Red Teams e autoridades policiais na investigação de crimes cibernéticos, destacando os desafios, oportunidades e impactos dessa cooperação no contexto brasileiro e comparando com práticas internacionais. Quanto aos objetivos específicos, tem-se:

- Contextualizar os Crimes Cibernéticos: Apresentar uma visão abrangente sobre os crimes cibernéticos, suas principais características e impactos na sociedade, com foco especial no contexto brasileiro.
- Explorar o Papel dos Red Teams: Investigar as funções e metodologias dos Red Teams, incluindo suas técnicas de simulação de ataques cibernéticos e a importância dessas equipes na identificação de vulnerabilidades em sistemas de segurança.
- Analisar a Base Legal: Examinar a legislação brasileira vigente que permite ou regula a colaboração entre Red Teams e autoridades policiais, comparando-a com marcos regulatórios de outros países.
- Estudar Casos Práticos: Analisar casos práticos de colaboração entre Red Teams e autoridades policiais, identificando boas práticas, desafios enfrentados e resultados obtidos.

- Avaliar Implicações Éticas e de Privacidade: Discutir as implicações éticas e de privacidade envolvidas na colaboração entre Red Teams e autoridades policiais, propondo formas de equilibrar a eficácia na investigação de crimes cibernéticos com a proteção dos direitos fundamentais dos cidadãos.
- Propor Diretrizes para Colaboração: Desenvolver diretrizes e recomendações para uma colaboração eficaz e juridicamente segura entre Red Teams e autoridades policiais, visando aprimorar a investigação de crimes cibernéticos no Brasil.

A metodologia adotada nesta pesquisa foi de natureza qualitativa, com enfoque exploratório e descritivo, buscando compreender as implicações legais da colaboração entre Red Teams e autoridades policiais na investigação de crimes cibernéticos. A investigação foi conduzida por meio de revisão bibliográfica e documental, utilizando doutrinas jurídicas, artigos científicos, legislações nacionais e internacionais, além de relatórios técnicos e estudos de casos relacionados à atuação conjunta entre esses agentes.

Também foram analisadas experiências estrangeiras que pudessem servir como referência para o ordenamento jurídico brasileiro. Complementarmente, realizaram-se entrevistas semiestruturadas com especialistas em segurança cibernética e operadores do direito, com o objetivo de captar percepções práticas e identificar lacunas e oportunidades no atual cenário normativo. Essa abordagem permitiu uma análise crítica e fundamentada, capaz de embasar propostas de regulamentação e boas práticas para a atuação colaborativa nesse campo.

CAPÍTULO 1 - FUNDAMENTAÇÃO TEÓRICA

1.1 Crimes Cibernéticos

Os crimes cibernéticos configuram-se como condutas ilícitas cometidas por meio de recursos tecnológicos, especialmente com o uso da internet e sistemas informáticos, cujo propósito pode variar desde o acesso não autorizado a dados até a prática de fraudes complexas (CLOUGH, 2015).

De acordo com Clough (2015), crimes cibernéticos são "atos ilegais realizados através do uso de sistemas informáticos e redes de comunicação". Brenner (2010) complementa que esses crimes podem envolver tanto ataques diretos a sistemas de computação quanto a utilização de tecnologia digital para cometer crimes tradicionais.

São considerados crimes de alta complexidade, marcados por sua natureza técnica, pelo dinamismo das ferramentas envolvidas e pela abrangência territorial, que muitas vezes ultrapassa fronteiras nacionais. Essa característica transnacional dificulta a investigação e o enquadramento jurídico dos delitos, visto que os agentes criminosos podem atuar de qualquer lugar do mundo, explorando vulnerabilidades em sistemas alheios e ocultando suas identidades por meio de técnicas de anonimização (SILVA; RODER; SILVA, 2018).

Além disso, a volatilidade das provas digitais – que podem ser rapidamente apagadas, alteradas ou transferidas – impõe grandes desafios às autoridades encarregadas da persecução penal. Outro aspecto relevante é a constante evolução das técnicas e ferramentas utilizadas pelos cibercriminosos, o que exige atualização contínua dos profissionais da área de segurança da informação e das instituições responsáveis pela investigação criminal (CRUZ; RODRIGUES, 2018).

De acordo com Montel e de Paiva (2024), a tipologia dos crimes cibernéticos é ampla e abrange diferentes formas de conduta. Entre os principais tipos, destacam-se os crimes contra sistemas computacionais, como invasões de redes, disseminação de vírus, trojans e malwares, ataques de negação de serviço (DDoS), sequestro de dados (ransomware) e sabotagens digitais.

Há ainda os crimes que envolvem o uso da internet para a prática de delitos tradicionais, como fraudes bancárias, estelionato, comércio ilegal de produtos, pedofilia, assédio moral e sexual em ambientes virtuais, divulgação de conteúdo

íntimo sem consentimento, além de crimes contra a honra, como calúnia e difamação (MONTEL; DE PAIVA, 2024).

Os impactos sociais desses crimes são significativos e multifacetados. No plano individual, podem comprometer a privacidade, a integridade e o bem-estar psicológico das vítimas. No plano organizacional, afetam diretamente a reputação e a segurança de instituições públicas e privadas, podendo provocar perdas financeiras, interrupção de serviços e comprometimento de informações estratégicas (SILVA, 2022).

Já no âmbito social e estatal, os crimes cibernéticos representam um risco à ordem pública e à segurança nacional, especialmente quando envolvem infraestruturas críticas, como sistemas de energia, saúde e transportes. Assim, torna-se imprescindível o desenvolvimento de estratégias eficazes de prevenção e repressão, incluindo parcerias entre os setores público e privado, atualizações legislativas e investimento em capacitação técnica (SILVA, 2022).

1.2 Red Teams

Os Red Teams, ou times vermelhos, são equipes especializadas em simular ataques cibernéticos com o objetivo de testar e avaliar a eficácia das defesas de uma organização. Diferentemente de auditorias convencionais ou testes automatizados, essas equipes adotam uma abordagem ofensiva realista, semelhante àquela de agentes mal-intencionados, a fim de identificar vulnerabilidades que poderiam ser exploradas por criminosos virtuais (DIOGENES; OZKAYA, 2018).

Os Red Teams desempenham um papel crucial na segurança cibernética, atuando como grupos especializados na simulação de ataques cibernéticos para avaliar e aprimorar a proteção de sistemas e redes. Esses times são formados por profissionais com habilidades específicas para realizar testes de penetração e outras técnicas que imitam ações de cibercriminosos, proporcionando uma perspectiva realista das ameaças que as organizações enfrentam (DIOGENES; OZKAYA, 2018).

Conforme destacam Pereira e Silva (2018), os Red Teams utilizam técnicas avançadas de ataque e engenharia social para identificar vulnerabilidades em sistemas, oferecendo uma visão detalhada e precisa das fragilidades existentes (PEREIRA; SILVA, 2018, p. 45). Essa abordagem proativa é fundamental para

prevenir que essas vulnerabilidades sejam exploradas por cibercriminosos antes que possam causar danos significativos.

A principal função dos Red Teams é expor falhas de segurança, avaliar a resiliência de sistemas, redes e processos, além de testar a capacidade de resposta das equipes de defesa (frequentemente chamadas de Blue Teams). Seu trabalho não se limita ao aspecto técnico; também envolve o fator humano, investigando como pessoas e fluxos organizacionais podem ser explorados em um ataque bem planejado (DIOGENES; OZKAYA, 2018).

Entre as técnicas empregadas por Red Teams estão a exploração de falhas em sistemas operacionais, redes e aplicações, o uso de ferramentas de pentest (teste de penetração), e a realização de movimentações laterais dentro de ambientes comprometidos para obter acesso privilegiado. Um elemento central da atuação dessas equipes é a engenharia social, que consiste na manipulação psicológica de indivíduos para que revelem informações sensíveis ou executem ações que comprometam a segurança da organização (DIOGENES; OZKAYA, 2018).

Isso pode incluir o envio de e-mails fraudulentos (phishing), telefonemas disfarçados, ou até mesmo tentativas de acesso físico a ambientes restritos. A engenharia social é uma ferramenta poderosa porque explora uma das principais vulnerabilidades de qualquer sistema: o comportamento humano (DIOGENES; OZKAYA, 2018).

Em contextos reais, os Red Teams atuam geralmente em organizações de médio e grande porte, especialmente nos setores financeiro, governamental, industrial e de tecnologia, onde a proteção de dados sensíveis é crítica. Suas simulações são planejadas para ocorrer de forma controlada, sem causar danos permanentes, mas com realismo suficiente para testar todos os pontos frágeis da estrutura de segurança.

Os resultados dessas ações são documentados em relatórios detalhados que servem de base para a tomada de decisões estratégicas e o aprimoramento das defesas. Além disso, sua atuação contribui para o desenvolvimento de uma cultura organizacional voltada à segurança da informação, promovendo treinamentos, revisões de políticas internas e ajustes técnicos que aumentam a maturidade cibernética da instituição como um todo.

A legislação brasileira sobre crimes cibernéticos e a colaboração com Red Teams está em desenvolvimento, mas já conta com algumas normas importantes que regulam a atuação nesses contextos. Essa legislação é crucial para garantir que as práticas de segurança cibernética, como as realizadas pelos Red Teams, sejam realizadas dentro dos limites legais e com respeito às normas de proteção de dados e privacidade.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representa um marco significativo no combate aos crimes cibernéticos no Brasil. De acordo com Silva (2020), "a Lei nº 12.737/2012 é um ponto de inflexão na legislação brasileira, estabelecendo penalidades específicas para invasões de dispositivos eletrônicos e crimes relacionados" (SILVA, 2020, p. 102). Esta lei, nomeada em homenagem à atriz Carolina Dieckmann, que teve seus dados pessoais divulgados ilegalmente, introduziu artigos que criminalizam o acesso não autorizado a dispositivos de informática e a divulgação de dados obtidos por meios ilícitos. Ela é um passo importante para combater práticas como hacking e vazamento de informações pessoais.

Além da Lei Carolina Dieckmann, a Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, desempenha um papel crucial na regulamentação da proteção de dados pessoais no Brasil. A LGPD regula o tratamento de dados pessoais, afetando diretamente a forma como os Red Teams devem lidar com informações coletadas durante seus testes de segurança.

Como Freitas (2021) aponta, "a LGPD estabelece normas rigorosas para a coleta, armazenamento e tratamento de dados pessoais, impondo restrições significativas sobre como essas informações podem ser usadas, o que impacta diretamente a colaboração entre Red Teams e autoridades" (FREITAS, 2021, p. 54). Essa legislação visa proteger a privacidade dos indivíduos e garantir que os dados sejam manipulados de maneira segura e responsável, o que é essencial para a atuação dos Red Teams, que frequentemente lidam com dados sensíveis durante suas atividades de teste.

2.3 Marco Legal Brasileiro

No Brasil, o marco legal relacionado aos crimes cibernéticos e à segurança da informação é composto por diversas leis que têm como objetivo regulamentar o uso da tecnologia e a proteção dos dados pessoais. Entre essas normas, destacam-se a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que são fundamentais para compreender o contexto jurídico das atividades realizadas por Red Teams e autoridades policiais na investigação de crimes cibernéticos (MAURA; INÁCIO; SERVO, 2022; GARCIA *et al*., 2020).

A Lei nº 12.737/2012, popularmente chamada de Lei Carolina Dieckmann, foi sancionada em 2012 em resposta ao caso de divulgação não autorizada de fotos íntimas da atriz Carolina Dieckmann. Ela tipifica crimes de invasão de dispositivos eletrônicos, como computadores, smartphones e outros meios digitais, e estabelece penalidades para quem invadir sistemas e divulgar informações privadas de forma indevida.

Essa legislação foi um marco importante no combate aos crimes cibernéticos no Brasil, pois criou um dispositivo legal específico para as práticas de hacking, antes tratadas de forma genérica pelo Código Penal. A Lei Carolina Dieckmann também prevê punições para o acesso não autorizado a dados armazenados, bem como para a utilização desses dados para cometer fraudes ou outros crimes. Ela estabeleceu um importante precedente para a regulamentação dos crimes digitais, colocando o Brasil em sintonia com as normas internacionais que combatem as violações de segurança da informação.

Já a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representa um avanço significativo na proteção dos dados pessoais no Brasil, regulamentando a coleta, armazenamento, tratamento e compartilhamento de informações pessoais. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD tem como objetivo principal garantir os direitos dos cidadãos à privacidade e à proteção de seus dados, ao mesmo tempo em que estabelece obrigações para as organizações que lidam com essas informações.

Para os Red Teams, a LGPD apresenta uma série de desafios, pois suas atividades muitas vezes envolvem a coleta e análise de dados sensíveis durante os testes de segurança. A legislação exige que essas equipes adotem medidas

rigorosas para garantir que os dados tratados durante os testes sejam armazenados e compartilhados de maneira segura e em conformidade com as normas de proteção. Caso contrário, as organizações podem ser penalizadas com multas e sanções administrativas.

Além da Lei Carolina Dieckmann e da LGPD, o Brasil também conta com outras normas relevantes para a regulamentação das atividades no ciberespaço. Entre elas, destaca-se o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece direitos e deveres para os usuários e provedores de serviços da internet, regulamentando questões como a neutralidade da rede, a privacidade online e a responsabilidade por conteúdos publicados na rede.

O Marco Civil foi um dos primeiros passos para a criação de uma infraestrutura jurídica para a internet no Brasil, abordando questões essenciais como a proteção da privacidade, o acesso à internet e a responsabilidade de plataformas digitais. Outra norma importante é a Lei de Crimes de Informática (Lei nº 9.983/2000), que tipifica diversos crimes relacionados à tecnologia e à informática, incluindo fraudes, invasões de sistemas e crimes contra a propriedade intelectual no meio digital.

Essas e outras normas compõem o arcabouço legal brasileiro para a segurança cibernética, mas ainda há espaço para aprimoramentos, especialmente em relação à integração entre as diferentes legislações e à adaptação às rápidas mudanças tecnológicas que ocorrem na sociedade digital.

2.4 Colaboração Público-Privada na Segurança Cibernética

A colaboração público-privada na segurança cibernética tem ganhado destaque nos últimos anos como uma abordagem essencial para o combate aos crimes digitais e a proteção das infraestruturas críticas. Essa parceria envolve a cooperação entre órgãos governamentais e empresas do setor privado, com o objetivo de fortalecer a segurança das redes e sistemas, além de aprimorar as investigações de crimes cibernéticos. Essa colaboração é fundamental, pois os ataques cibernéticos não respeitam fronteiras e exigem uma resposta coordenada entre os setores público e privado para proteger tanto os interesses nacionais quanto os dados pessoais dos cidadãos (MOREIRA, 2019).

Os modelos de cooperação entre o setor público e privado na segurança cibernética variam conforme os objetivos e as necessidades de cada contexto, mas, em geral, incluem a troca de informações sobre ameaças, a colaboração em testes de segurança, a realização de treinamentos conjuntos e o desenvolvimento de políticas públicas para a segurança digital.

No Brasil, a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e a Lei Geral de Proteção de Dados (LGPD) criaram uma base para regulamentar a proteção de dados pessoais e a privacidade dos cidadãos, mas a colaboração público-privada pode ser vista como uma forma de superar as limitações da legislação existente. Além disso, a troca de informações entre as empresas que lidam com dados sensíveis e os órgãos de segurança pública pode acelerar a detecção e resposta a incidentes cibernéticos, ao mesmo tempo em que permite um aprendizado mútuo sobre as melhores práticas de segurança.

Entre os modelos de cooperação, destacam-se os programas de compartilhamento de inteligência cibernética, que envolvem a troca de dados sobre vulnerabilidades, incidentes e novas ameaças. Por exemplo, empresas de tecnologia podem fornecer ao governo informações sobre ataques cibernéticos em tempo real, enquanto o governo pode compartilhar dados sobre ameaças provenientes de grupos criminosos ou ataques de países adversários.

Outro modelo comum de cooperação é a criação de parcerias públicas e privadas para a realização de testes de segurança, como o envolvimento de Red Teams em simulações de ataques a sistemas governamentais e empresariais, com o objetivo de identificar falhas antes que cibercriminosos possam explorá-las. Essas

simulações podem fornecer informações valiosas para as autoridades policiais e para as organizações privadas, contribuindo para a melhoria das estratégias de segurança e prevenção.

No entanto, apesar dos muitos benefícios da colaboração público-privada, existem riscos associados a essa parceria, principalmente no que diz respeito à privacidade, à transparência e à responsabilidade. Um dos principais desafios é garantir que a troca de informações sobre incidentes cibernéticos não viole os direitos dos indivíduos, especialmente no que se refere à proteção de dados pessoais.

A coleta e o compartilhamento de dados entre o setor público e privado podem gerar preocupações sobre a segurança das informações e a possibilidade de abuso ou uso indevido. Além disso, a falta de clareza sobre as responsabilidades de cada parte envolvida na colaboração pode resultar em falhas na coordenação e na resposta a incidentes, prejudicando a eficácia das ações de segurança cibernética. Outro risco importante é o vazamento de informações confidenciais durante as investigações, o que pode comprometer não apenas a segurança da operação, mas também a confiança da sociedade nas instituições envolvidas.

Por outro lado, os benefícios da colaboração público-privada são evidentes, especialmente quando se trata de uma resposta mais rápida e eficiente aos ataques cibernéticos. A troca de informações pode ajudar na identificação precoce de ameaças e no desenvolvimento de soluções inovadoras para mitigar riscos. Além disso, a cooperação entre empresas e governos pode contribuir para a criação de um ambiente digital mais seguro e resiliente, protegendo os sistemas e dados essenciais para a economia e a sociedade. Em um contexto global de aumento dos ataques cibernéticos, a colaboração estreita entre o público e o privado é, sem dúvida, uma estratégia fundamental para garantir a segurança cibernética a longo prazo.

2.5 Implicações Éticas e Jurídicas da Colaboração

A colaboração entre Red Teams e autoridades policiais na investigação de crimes cibernéticos gera uma série de implicações éticas e jurídicas que devem ser cuidadosamente analisadas para garantir que as práticas de segurança cibernética respeitem os direitos dos indivíduos e o ordenamento jurídico vigente. A interação

entre o setor público e privado nesse contexto exige um equilíbrio entre a eficácia na investigação e a proteção dos direitos fundamentais dos cidadãos, como a privacidade e a proteção de dados pessoais. Essas questões são de extrema relevância, considerando o caráter sensível das informações manipuladas durante as investigações cibernéticas e os potenciais impactos negativos em caso de abusos ou falhas nas práticas adotadas.

Uma das principais preocupações éticas e jurídicas refere-se à privacidade e à proteção de dados. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece um rigoroso regime de proteção de dados pessoais, impondo restrições significativas sobre como essas informações podem ser coletadas, processadas e compartilhadas. A colaboração entre Red Teams e autoridades policiais, muitas vezes envolvendo a coleta de dados sensíveis durante as simulações de ataques ou a investigação de incidentes cibernéticos, precisa estar em conformidade com as disposições da LGPD.

A utilização de dados pessoais sem o consentimento adequado ou em desacordo com os princípios estabelecidos pela legislação pode acarretar em sanções tanto para as autoridades quanto para as empresas envolvidas. Além disso, a privacidade dos indivíduos deve ser resguardada em todas as etapas da investigação, o que implica que as práticas de coleta e uso de dados devem ser transparentes e justificadas, com a implementação de medidas de segurança para evitar vazamentos ou acessos não autorizados.

A proporcionalidade e a legalidade nas atividades desempenham um papel crucial na determinação dos limites éticos e jurídicos da colaboração entre Red Teams e autoridades policiais. A atuação das equipes de segurança deve ser pautada por princípios de necessidade e proporcionalidade, de modo que as medidas adotadas para investigar ou combater crimes cibernéticos não ultrapassem os limites do que é estritamente necessário para o alcance dos objetivos da investigação.

Isso significa que a coleta e o uso de dados pessoais, bem como as ações realizadas para testar sistemas de segurança, devem ser cuidadosamente ajustadas para não violar direitos fundamentais. Além disso, qualquer ação realizada deve estar dentro dos parâmetros da legalidade, ou seja, deve estar devidamente respaldada por normas jurídicas que regulam as práticas de segurança cibernética e a proteção dos dados.

A falta de regulamentação específica no Brasil para a atuação conjunta entre Red Teams e autoridades pode gerar insegurança jurídica e dificuldades para determinar a legalidade de determinadas práticas, o que torna essencial o desenvolvimento de um marco regulatório claro que oriente essas interações.

Outro ponto importante refere-se à responsabilidade civil e penal pelas ações tomadas durante a colaboração entre Red Teams e autoridades policiais. A responsabilidade civil envolve a obrigação de indenizar danos causados a terceiros em decorrência de práticas inadequadas ou ilegais. No contexto de segurança cibernética, se um Red Team ou uma autoridade policial causar danos a sistemas ou a dados de maneira inadequada, pode haver a necessidade de reparação dos prejuízos, especialmente se a segurança de sistemas ou a privacidade dos cidadãos for comprometida.

Já a responsabilidade penal trata das possíveis infrações cometidas no decorrer dessas atividades. Embora a colaboração entre Red Teams e autoridades tenha a finalidade de prevenir e combater crimes cibernéticos, a atuação ilegal de qualquer parte envolvida pode resultar em sanções penais, como em casos de invasões indevidas ou uso de técnicas proibidas para coleta de dados. Por isso, é fundamental que as atividades dessas equipes e das autoridades policiais estejam em consonância com as normas penais e civis, de forma a evitar que os envolvidos respondam por crimes relacionados a invasões, danos a sistemas e violações de privacidade.

Portanto, as implicações éticas e jurídicas da colaboração entre Red Teams e autoridades policiais exigem uma análise detalhada e cuidadosa, a fim de garantir que as práticas adotadas sejam compatíveis com os direitos e garantias constitucionais, a proteção da privacidade e os princípios da legalidade e proporcionalidade. A falta de regulamentação específica pode aumentar a complexidade dessa questão, tornando ainda mais importante a criação de um marco legal claro e robusto que permita a colaboração eficaz sem prejudicar os direitos dos cidadãos.

CAPÍTULO 2 - ANÁLISE COMPARATIVA INTERNACIONAL

Nos Estados Unidos, a abordagem à segurança cibernética é marcada por uma integração robusta entre setor público e privado, com ênfase na cooperação estratégica para enfrentar ameaças digitais em constante evolução. O país adota uma postura proativa na prevenção e resposta a crimes cibernéticos, com instituições consolidadas como o Federal Bureau of Investigation (FBI), o Departamento de Segurança Interna (DHS) e a Cybersecurity and Infrastructure Security Agency (CISA), que coordenam ações em conjunto com empresas privadas, universidades e centros de pesquisa. Essas parcerias são fundamentais para o compartilhamento ágil de informações sobre ameaças, vulnerabilidades e incidentes, possibilitando respostas mais rápidas e eficientes a ataques cibernéticos.

A atuação dos chamados Red Teams também é amplamente institucionalizada nos Estados Unidos, tanto em ambientes corporativos quanto no âmbito da defesa nacional. A utilização dessas equipes, especializadas em simular ataques reais para identificar falhas de segurança, é uma prática comum em setores críticos como financeiro, energético, aeroespacial e governamental.

Muitas dessas atividades são conduzidas em colaboração com agências federais e integram políticas nacionais de cibersegurança. Um exemplo notável é o “Cyber Red Teaming” conduzido pelas Forças Armadas dos EUA e suas agências de inteligência, que testam constantemente a resiliência das infraestruturas de defesa do país.

No plano legal, os Estados Unidos não possuem uma legislação unificada de proteção de dados como a LGPD brasileira, mas contam com leis setoriais específicas, como a Health Insurance Portability and Accountability Act (HIPAA) para dados de saúde e a Children's Online Privacy Protection Act (COPPA) para dados de menores.

Além disso, estados como a Califórnia implementaram legislações próprias, como o California Consumer Privacy Act (CCPA), que oferece direitos aos consumidores sobre o uso de seus dados pessoais. A legislação federal também prevê punições severas para crimes cibernéticos por meio de leis como o Computer Fraud and Abuse Act (CFAA), que criminaliza o acesso não autorizado a sistemas de informação.

A cultura de segurança cibernética nos Estados Unidos favorece a experimentação controlada, o incentivo à inovação tecnológica e o desenvolvimento constante de capacidades ofensivas e defensivas no ciberespaço. O modelo norte-americano destaca-se ainda pela transparência em incidentes cibernéticos relevantes, exigindo que empresas de setores regulados notifiquem violações de dados, o que contribui para uma maior responsabilização e amadurecimento do ecossistema de segurança digital. Essa abordagem fortalece a resiliência institucional e proporciona uma referência importante para outros países que buscam estruturar políticas eficazes de combate a crimes cibernéticos e fortalecer a atuação conjunta entre Estado e sociedade civil.

Na União Europeia, a segurança cibernética é tratada como uma prioridade estratégica coletiva, refletida em políticas públicas integradas e mecanismos de cooperação entre os Estados-membros. O bloco adota uma abordagem coordenada por meio de instituições como a Agência da União Europeia para a Cibersegurança (ENISA), que atua na promoção de normas comuns, na elaboração de diretrizes técnicas e no fortalecimento da capacidade cibernética dos países integrantes.

A cooperação entre governos, setor privado e sociedade civil é incentivada por meio de programas como o “EU Cybersecurity Act”, que estabelece um quadro de certificação europeu para produtos, serviços e processos de TIC, promovendo padrões de segurança confiáveis em todo o território da União.

A atuação de Red Teams também faz parte das práticas de segurança no contexto europeu, especialmente em setores críticos como telecomunicações, energia, transportes e finanças. Esses exercícios são frequentemente conduzidos em larga escala por instituições públicas em parceria com empresas privadas, com o objetivo de testar a resiliência de sistemas e preparar respostas a incidentes complexos.

Um exemplo significativo é o programa TIBER-EU (Threat Intelligence-Based Ethical Red Teaming), desenvolvido pelo Banco Central Europeu, que fornece uma estrutura padronizada para simulações de ataques cibernéticos realistas em instituições financeiras. Essa prática busca não apenas identificar vulnerabilidades técnicas, mas também avaliar a eficácia dos protocolos internos de defesa, resposta e recuperação.

No âmbito legal, a União Europeia se destaca pela criação do Regulamento Geral sobre a Proteção de Dados (GDPR), que entrou em vigor em 2018 e passou a

ser referência global na defesa da privacidade e dos direitos digitais dos cidadãos. O GDPR estabelece obrigações rigorosas para o tratamento de dados pessoais, impõe sanções elevadas para violações e reforça a transparência e o controle do usuário sobre suas informações.

Além disso, a Diretiva NIS (Diretiva sobre Segurança de Redes e Sistemas de Informação), revisada pela NIS2, estabelece medidas para melhorar o nível de segurança cibernética em setores essenciais, exigindo das empresas a implementação de controles técnicos e a notificação obrigatória de incidentes.

A cultura de segurança cibernética na União Europeia valoriza a ética, os direitos fundamentais e a proporcionalidade nas ações de monitoramento e resposta. Existe um esforço constante para equilibrar a proteção da infraestrutura digital com a preservação da privacidade e das liberdades individuais, promovendo debates públicos sobre os limites do uso de tecnologias intrusivas.

Além disso, a UE investe em capacitação técnica, pesquisa e inovação por meio de programas como o Horizon Europe, incentivando o desenvolvimento de soluções avançadas para prevenir e mitigar ataques cibernéticos. A integração entre os países-membros e a padronização de normas e práticas tornam o modelo europeu um exemplo de governança colaborativa em segurança digital, com foco tanto na eficiência operacional quanto na proteção dos direitos dos cidadãos.

Israel é amplamente reconhecido como uma das nações líderes mundiais em segurança cibernética, tanto no setor público quanto no privado. A cibersegurança é considerada uma questão de segurança nacional, o que levou o país a investir massivamente em pesquisa, inovação e capacitação profissional desde a década de 1990.

A experiência acumulada pelas Forças de Defesa de Israel, especialmente através da Unidade 8200 — uma divisão de inteligência especializada em guerra cibernética — influenciou diretamente o desenvolvimento de um ecossistema robusto de empresas de tecnologia, startups e centros de excelência em cibersegurança.

A atuação de Red Teams em Israel é fortemente integrada ao cotidiano de organizações públicas e privadas. Esses grupos, compostos por especialistas treinados em técnicas ofensivas, são usados para testar continuamente a resiliência de infraestruturas críticas, como energia, telecomunicações, setor financeiro e saúde. Israel adota a filosofia de “security by design”, onde a simulação de ameaças

é parte do processo desde o desenvolvimento de sistemas e softwares, garantindo uma postura proativa e preventiva. Além disso, a colaboração entre militares e civis permite que conhecimentos adquiridos em operações reais sejam rapidamente transferidos para o setor empresarial.

No campo jurídico, Israel possui uma legislação específica voltada à cibersegurança, com foco em proteção de infraestrutura crítica, combate ao cibercrime e regulação de privacidade. Embora não possua um equivalente direto ao GDPR europeu, o país implementa a Lei de Proteção da Privacidade de 1981, atualizada para atender às novas demandas digitais.

A Autoridade de Proteção da Privacidade é o órgão responsável pela fiscalização do uso de dados pessoais, e empresas que operam internacionalmente tendem a seguir padrões compatíveis com as exigências de outros mercados, como Europa e EUA, por questões de conformidade comercial.

A política cibernética israelense também é marcada por uma forte colaboração público-privada. O National Cyber Directorate atua como órgão centralizador das políticas de segurança digital e coordena ações com empresas de tecnologia, universidades e agências governamentais. O modelo israelense de cooperação é baseado na confiança mútua e na troca contínua de informações sobre ameaças, vulnerabilidades e respostas, criando um ambiente de vigilância constante e aprendizado coletivo.

Israel também se destaca por seu posicionamento ético e estratégico diante dos desafios da cibersegurança. Embora haja críticas relacionadas ao uso de tecnologias de vigilância em contextos de conflito, como nos territórios palestinos, o país procura justificar tais ações com base na segurança nacional. Ainda assim, a comunidade internacional acompanha de perto o equilíbrio entre segurança e direitos civis, o que tem motivado discussões sobre a necessidade de maior transparência e regulação em alguns setores.

Com forte presença internacional, Israel exporta tecnologia de segurança cibernética para diversos países, consolidando-se como um polo global de inovação na área. Sua experiência em contextos reais de ameaças, combinada à integração entre academia, governo e setor privado, torna o modelo israelense um dos mais avançados e influentes do mundo na gestão de riscos cibernéticos.

O Brasil pode extrair diversas lições e boas práticas a partir da análise dos modelos internacionais de segurança cibernética, especialmente dos casos de

Israel, Estados Unidos e União Europeia. Esses países demonstram que a cibersegurança eficaz exige investimentos contínuos em tecnologia, capacitação profissional, legislação atualizada e, sobretudo, integração entre atores públicos e privados. Uma das principais lições é a necessidade de tratar a segurança cibernética como uma prioridade estratégica nacional, o que implica na criação de políticas públicas robustas, centros de resposta a incidentes e fortalecimento das capacidades de defesa digital.

A experiência de Israel destaca a importância da formação de talentos por meio da educação especializada e de programas de treinamento militar, o que poderia inspirar o Brasil a ampliar parcerias entre universidades, centros de pesquisa e órgãos governamentais. O país também se beneficia de uma estreita colaboração entre governo e setor privado, com mecanismos eficientes de compartilhamento de informações sobre ameaças cibernéticas em tempo real — prática ainda incipiente no contexto brasileiro.

Nos Estados Unidos, o uso de Red Teams como parte de uma estratégia constante de testes e simulações de ataques oferece uma boa prática replicável. A criação de estruturas semelhantes no Brasil poderia aumentar a resiliência de sistemas críticos e promover uma cultura de segurança preventiva. Além disso, os americanos apostam em regulamentações claras e em estruturas jurídicas específicas para tratar incidentes cibernéticos, o que reforça a importância de o Brasil continuar evoluindo seu marco regulatório, garantindo maior segurança jurídica e incentivando o cumprimento das normas.

A União Europeia, por sua vez, é um exemplo de abordagem orientada à proteção de dados e aos direitos fundamentais dos usuários, por meio da GDPR. O Brasil, com sua LGPD, já deu um passo importante nesse sentido, mas ainda enfrenta desafios na implementação e fiscalização. Assim, pode aprender com os europeus sobre mecanismos de conformidade, educação digital da população e empoderamento dos titulares de dados.

De forma geral, o Brasil precisa fortalecer sua governança cibernética, promovendo maior integração entre ministérios, agências reguladoras, setor produtivo, sociedade civil e comunidades técnicas. Também é necessário fomentar a cultura de segurança nas empresas e entre os cidadãos, tornando o ambiente digital mais confiável e resiliente. A adoção dessas boas práticas internacionais contribuiria

significativamente para a proteção das infraestruturas críticas nacionais, o combate ao cibercrime e a promoção de um ecossistema digital mais seguro e inovador.

CAPÍTULO 3 - ANÁLISE CRÍTICA DAS IMPLICAÇÕES LEGAIS

3.1 Lacunas na Legislação Brasileira

Apesar dos avanços no marco legal brasileiro voltado à segurança cibernética, como a promulgação da Lei nº 12.737/2012 (Lei Carolina Dieckmann) e da Lei Geral de Proteção de Dados (LGPD), ainda existem lacunas significativas que dificultam uma atuação mais eficaz no enfrentamento dos crimes cibernéticos. A legislação atual não consegue acompanhar, com a mesma velocidade, o ritmo de inovação tecnológica e a complexidade das novas ameaças digitais. Muitos tipos de ataques, especialmente os mais sofisticados, não são devidamente tipificados no Código Penal, o que gera insegurança jurídica e limita a responsabilização dos criminosos.

Outro ponto crítico é a ausência de uma lei geral sobre cibersegurança que unifique diretrizes, estabeleça competências claras entre os entes federativos e defina padrões mínimos de proteção para órgãos públicos e privados. Essa ausência dificulta a articulação nacional em casos de incidentes de grande escala, como ataques a infraestruturas críticas. Além disso, falta regulamentação específica para o uso de ferramentas ofensivas por agentes autorizados, como no caso de Red Teams vinculados a órgãos de segurança pública ou defesa, o que levanta questões éticas e jurídicas sobre os limites dessas atuações.

A legislação brasileira também apresenta falhas na definição de responsabilidades civis e penais em contextos de compartilhamento de dados entre instituições, especialmente quando há colaboração público-privada. As regras sobre transparência, consentimento e prestação de contas nem sempre são claras, o que pode afetar direitos fundamentais dos cidadãos. Adicionalmente, a LGPD ainda carece de maior efetividade na sua aplicação, com desafios como a capacitação de agentes fiscalizadores, o desenvolvimento de uma cultura organizacional voltada à proteção de dados e a ausência de jurisprudência consolidada.

Por fim, há um déficit de normas específicas que tratem de temas emergentes, como a cibersegurança em ambientes de inteligência artificial, internet das coisas, computação em nuvem e criptomoedas. Essas tecnologias ampliam os vetores de ataque e requerem uma abordagem regulatória proativa, com foco preventivo e orientado à inovação. Assim, as lacunas na legislação brasileira não

apenas dificultam a repressão efetiva aos crimes cibernéticos, como também comprometem a construção de um ecossistema digital mais seguro, resiliente e confiável.

3.2 Necessidade de Atualização Normativa

A constante evolução tecnológica e a crescente sofisticação das ameaças digitais evidenciam a necessidade urgente de atualização normativa no Brasil. O ordenamento jurídico atual, embora contenha importantes avanços como a Lei nº 12.737/2012 e a Lei Geral de Proteção de Dados (LGPD), não é suficientemente abrangente ou dinâmico para lidar com os desafios impostos pela transformação digital.

As novas modalidades de crimes cibernéticos, que envolvem inteligência artificial, ataques automatizados, deepfakes, ransomware, fraudes em blockchain e espionagem cibernética, demandam uma legislação mais específica, técnica e alinhada às práticas internacionais.

A atualização normativa deve contemplar não apenas a tipificação penal de condutas ainda não previstas, mas também a regulamentação das atividades de cibersegurança em setores estratégicos, a atuação de profissionais especializados como os Red Teams e os limites éticos e legais da cooperação entre entes públicos e privados. A ausência de uma estrutura legal clara sobre a ciberdefesa nacional, por exemplo, cria um vácuo regulatório que compromete a capacidade do Estado de prevenir e reagir a ameaças contra a soberania e a infraestrutura crítica do país.

Além disso, a legislação precisa acompanhar os parâmetros estabelecidos por tratados e convenções internacionais, favorecendo a cooperação jurídica entre países e o intercâmbio de informações em investigações transnacionais. Nesse sentido, aderir a instrumentos como a Convenção de Budapeste pode fortalecer a capacidade do Brasil de atuar de forma coordenada no combate ao cibercrime global.

A atualização normativa deve ainda incorporar princípios fundamentais como transparência, proporcionalidade, proteção de dados pessoais e respeito aos direitos humanos, garantindo que as medidas de segurança não comprometam as liberdades civis. A criação de uma política nacional de cibersegurança integrada, com diretrizes claras, definição de competências e mecanismos de fiscalização,

também é essencial para promover segurança jurídica, prevenir abusos e incentivar a adoção de boas práticas em todos os setores.

Portanto, atualizar e modernizar o arcabouço legal brasileiro é não apenas uma medida de proteção, mas uma exigência estratégica para garantir a resiliência digital do país frente a um cenário de riscos complexos, interconectados e em constante mutação.

3.3 Riscos Jurídicos na Atuação Conjunta

A atuação conjunta entre entes públicos e privados no campo da segurança cibernética, embora essencial para enfrentar ameaças digitais de forma eficiente, implica diversos riscos jurídicos que precisam ser cuidadosamente avaliados. Um dos principais desafios é a definição clara das responsabilidades de cada parte envolvida. Em operações conjuntas, especialmente aquelas que envolvem Red Teams ou testes de intrusão realizados com o consentimento de empresas privadas, há o risco de ultrapassagem de limites legais, como a invasão indevida de sistemas, a coleta e o tratamento inadequado de dados pessoais ou a violação de direitos de terceiros (MOREIRA, 2019).

Outro aspecto relevante diz respeito à ausência de regulamentação específica para parcerias público-privadas no campo da cibersegurança. A inexistência de normas claras sobre os deveres, os limites de atuação, os protocolos de sigilo e as formas de compartilhamento de informações pode gerar conflitos jurídicos, inclusive no âmbito da responsabilidade civil e penal. Por exemplo, se uma empresa privada, em cooperação com um órgão público, realizar uma ação que resulte em dano a um cidadão ou a outro ente, poderá haver dificuldade em apurar quem deve responder judicialmente, ou como essa responsabilização deve ser processada (MOREIRA, 2019).

Adicionalmente, a atuação conjunta pode comprometer princípios constitucionais como a legalidade, a privacidade e o devido processo legal, especialmente quando ações são executadas sem base legal específica, autorização judicial ou adequada supervisão. Isso pode resultar em contestações judiciais, ações indenizatórias e questionamentos sobre a validade das provas obtidas, além de comprometer a reputação das instituições envolvidas.

Tais riscos tornam evidente a necessidade de um marco regulatório robusto e específico para guiar a cooperação público-privada na cibersegurança. Esse marco deve definir com clareza os limites da atuação conjunta, os direitos e deveres de cada agente, os mecanismos de fiscalização e prestação de contas, bem como prever medidas corretivas para eventuais excessos. Sem isso, a atuação conjunta, por mais bem-intencionada que seja, continuará operando em uma zona cinzenta do direito, sujeita a inseguranças e conflitos que podem enfraquecer os esforços de proteção digital em vez de fortalecê-los.

3.4 Impactos na Garantia de Direitos Fundamentais

A atuação conjunta entre entes públicos e privados na área da segurança cibernética pode gerar impactos significativos na garantia de direitos fundamentais, exigindo uma análise criteriosa sobre os limites e os princípios que devem orientar essas práticas. A privacidade é um dos direitos mais sensíveis nesse contexto, pois ações envolvendo testes de vulnerabilidade, monitoramento de redes ou coleta de dados podem facilmente resultar na exposição indevida de informações pessoais, especialmente quando não há consentimento claro ou quando os dados são compartilhados sem transparência. Esse risco se agrava diante de estruturas jurídicas ainda pouco consolidadas para reger tais parcerias, o que dificulta o controle e a responsabilização em caso de abusos.

Outro direito fundamental afetado é a liberdade de expressão, particularmente quando medidas de segurança cibernética resultam em bloqueios de conteúdo, vigilância de comunicações ou restrições ao uso de plataformas digitais. Sem uma regulação clara, práticas voltadas à proteção de sistemas podem acabar por violar esse direito, mesmo que de forma não intencional, gerando um efeito inibidor sobre o debate público e a atuação de grupos sociais diversos.

A presunção de inocência e o devido processo legal também podem ser comprometidos quando informações obtidas em ações conjuntas são utilizadas para fins judiciais sem os devidos cuidados legais. A cooperação entre entes públicos e privados não pode ocorrer à margem das garantias processuais, sob risco de legitimar práticas que enfraquecem o Estado de Direito.

Dessa forma, os impactos na garantia de direitos fundamentais exigem que qualquer atuação conjunta esteja subordinada a princípios como legalidade,

necessidade, proporcionalidade e transparência. É fundamental que as ações de segurança cibernética contem com salvaguardas normativas robustas, controle institucional adequado e mecanismos de correção, assegurando que a proteção digital não ocorra à custa das liberdades individuais, mas sim em consonância com elas.

CAPÍTULO 4 - PROPOSTAS E DIRETRIZES PARA UMA COLABORAÇÃO JURIDICAMENTE SEGURA

Diante dos desafios identificados no cenário da segurança cibernética e das lacunas observadas na legislação brasileira, torna-se essencial propor recomendações normativas e legislativas que visem fortalecer a atuação conjunta entre setor público e privado, sem comprometer os direitos fundamentais. Primeiramente, é recomendável a criação de um marco legal específico para regulamentar a colaboração entre agentes públicos e privados em operações de cibersegurança, com diretrizes claras sobre limites de atuação, procedimentos autorizados e responsabilidades civis e penais de cada parte envolvida.

Além disso, é necessário atualizar a legislação existente para abarcar práticas modernas de defesa digital, como os exercícios conduzidos por Red Teams, a utilização de técnicas de engenharia social e as simulações de ataques cibernéticos, estabelecendo critérios legais que diferenciem ações lícitas de condutas criminosas. Tais atualizações devem ser acompanhadas de dispositivos que garantam a transparência e o controle social, como a obrigatoriedade de relatórios públicos, auditorias independentes e a atuação de órgãos reguladores com competência técnica.

Também se recomenda o fortalecimento da Lei Geral de Proteção de Dados, com ênfase na proteção de informações sensíveis em ambientes de testes e operações conjuntas. Devem ser previstos mecanismos específicos para assegurar o consentimento do titular dos dados, a anonimização de informações quando possível, e a responsabilização objetiva em caso de incidentes decorrentes de falhas na proteção.

Por fim, é fundamental incorporar à legislação normas que promovam a capacitação continuada de agentes públicos e privados, bem como incentivos à pesquisa e desenvolvimento em segurança digital, fomentando uma cultura jurídica e técnica de prevenção. A legislação deve acompanhar a velocidade da inovação tecnológica, promovendo um equilíbrio entre a proteção cibernética, a liberdade individual e a segurança jurídica.

As diretrizes operacionais para Red Teams visam estabelecer práticas e procedimentos que garantam a eficácia de suas atividades no contexto da segurança cibernética, ao mesmo tempo em que asseguram o cumprimento das

normas legais e a proteção dos direitos fundamentais. Considerando o caráter sensível das operações realizadas por esses grupos, é essencial que suas ações sejam conduzidas com transparência, ética e responsabilidade. A seguir, destacam-se algumas diretrizes operacionais fundamentais para o funcionamento dos Red Teams:

Primeiramente, é crucial que a atuação de um Red Team seja sempre pautada pela autorização expressa e formal de todas as partes envolvidas. As operações de testes de penetração, simulações de ataques cibernéticos ou qualquer atividade que envolva a exploração de sistemas e redes devem ser previamente acordadas, com a definição clara do escopo das ações a serem realizadas, evitando que ultrapassem os limites acordados ou que invadam a privacidade de usuários ou sistemas não relacionados.

Uma segunda diretriz fundamental diz respeito à proteção de dados pessoais. Durante a realização de testes de segurança, os Red Teams devem adotar práticas rigorosas de anonimização e criptografia dos dados acessados, garantindo que informações sensíveis não sejam divulgadas ou mal utilizadas. O tratamento de dados pessoais deve estar em conformidade com a Lei Geral de Proteção de Dados (LGPD), assegurando o respeito ao consentimento dos titulares e a minimização dos riscos de vazamentos ou abusos.

Além disso, as atividades dos Red Teams devem ser sempre realizadas com foco na identificação de vulnerabilidades, e não na exploração ou criação de danos. Em todas as etapas de sua atuação, os membros dos Red Teams devem assegurar que suas ações visem unicamente aprimorar a segurança e não comprometer a integridade dos sistemas ou dados. O uso de técnicas de engenharia social, por exemplo, deve ser restrito a contextos que sejam explicitamente permitidos, com a plena conscientização das consequências de suas ações para a organização testada.

A transparência nas comunicações também é uma diretriz essencial. Após a realização dos testes, os Red Teams devem fornecer relatórios detalhados sobre os métodos utilizados, as vulnerabilidades encontradas e as recomendações para mitigação dos riscos identificados. Estes relatórios devem ser claros, objetivos e acessíveis, permitindo que as organizações ou autoridades envolvidas compreendam plenamente os resultados e possam tomar as ações corretivas necessárias.

Por fim, uma diretriz importante é a constante capacitação e atualização das equipes, visto que o cenário cibernético está em constante evolução. Os Red Teams devem ser treinados para lidar com novas ameaças, técnicas de ataque e, principalmente, com o panorama jurídico e ético envolvido em suas atividades. A capacitação contínua deve ser promovida tanto no aspecto técnico quanto nas questões relacionadas à legislação, ética e privacidade, garantindo que suas ações estejam sempre alinhadas às boas práticas e à legislação vigente.

Essas diretrizes operacionais são essenciais para assegurar que os Red Teams atuem de maneira responsável e eficiente, promovendo a segurança cibernética sem comprometer os direitos dos indivíduos ou a integridade dos sistemas analisados.

As boas práticas para as autoridades policiais na colaboração com Red Teams são essenciais para garantir uma investigação cibernética eficaz, enquanto asseguram o cumprimento das normas legais e o respeito aos direitos fundamentais dos cidadãos. Diante do crescente desafio dos crimes cibernéticos, é crucial que a atuação das autoridades policiais seja bem estruturada, coordenada e fundamentada em princípios éticos e jurídicos. A seguir, destacam-se algumas boas práticas que devem ser seguidas pelas autoridades policiais ao trabalhar em conjunto com os Red Teams:

A primeira boa prática é a formalização da colaboração. As autoridades policiais devem sempre estabelecer acordos claros e documentados com os Red Teams antes de qualquer operação. Esses acordos devem definir de maneira precisa o escopo das atividades, os objetivos da colaboração, as responsabilidades de cada parte, e as limitações quanto à coleta e ao uso de dados. A formalização ajuda a garantir a legalidade das ações e protege tanto os Red Teams quanto as autoridades de potenciais problemas jurídicos.

Além disso, as autoridades policiais devem garantir que as operações dos Red Teams estejam sempre alinhadas com a legislação vigente. A colaboração deve ser conduzida dentro dos limites da lei, em particular no que diz respeito à proteção de dados pessoais, conforme exigido pela Lei Geral de Proteção de Dados (LGPD) e outras normativas relacionadas. As autoridades precisam assegurar que todas as ações do Red Team que envolvam o acesso a sistemas e dados sejam autorizadas e realizadas de forma transparente, evitando a violação dos direitos fundamentais dos cidadãos.

Outra boa prática importante é o envolvimento de profissionais qualificados na supervisão das atividades dos Red Teams. A colaboração entre Red Teams e policiais deve ser acompanhada por especialistas em segurança cibernética dentro das forças policiais, garantindo que as ações dos Red Teams sejam compreendidas e monitoradas. Esses profissionais devem ter conhecimento tanto sobre as técnicas utilizadas pelos Red Teams quanto sobre as implicações legais envolvidas, para que possam orientar a operação de forma eficaz e jurídica.

A transparência e a comunicação contínua também são essenciais. Durante a colaboração, deve haver um fluxo constante de informações entre as autoridades policiais e os Red Teams, permitindo que ambos os lados compartilhem descobertas, atualizações e resultados. Relatórios claros e detalhados sobre as vulnerabilidades encontradas e as recomendações para mitigação devem ser elaborados pelos Red Teams e analisados pelas autoridades policiais, para que possam ser tomadas as medidas necessárias em resposta aos riscos identificados.

Uma boa prática adicional é garantir que a colaboração entre os Red Teams e as autoridades policiais respeite princípios éticos. As autoridades devem assegurar que as operações não resultem em danos desnecessários aos sistemas ou aos dados das organizações testadas. O respeito à privacidade das vítimas e a integridade das evidências são fundamentais para que a colaboração seja legítima e eficaz. Além disso, qualquer envolvimento do Red Team em investigações relacionadas a crimes deve ser conduzido de maneira cuidadosa, para evitar a utilização indevida de informações ou a criação de novos riscos cibernéticos.

Por fim, as autoridades policiais devem estar atentas ao aprimoramento contínuo de seus processos e à capacitação de suas equipes. Dada a rápida evolução das ameaças cibernéticas e das técnicas de ataque, é fundamental que as autoridades policiais mantenham-se atualizadas quanto às novas práticas de segurança cibernética e às implicações jurídicas que envolvem a colaboração com os Red Teams. A educação contínua, tanto no campo técnico quanto nas questões legais, garante que as autoridades possam atuar de forma eficiente e dentro dos padrões exigidos pela lei.

Essas boas práticas são fundamentais para a construção de uma colaboração eficiente, segura e juridicamente sólida entre os Red Teams e as autoridades policiais, permitindo uma atuação mais eficaz no combate aos crimes cibernéticos,

sem comprometer os direitos dos indivíduos ou a integridade dos sistemas analisados.

As sugestões para políticas públicas no contexto da segurança cibernética e da colaboração entre Red Teams e autoridades policiais são fundamentais para melhorar a eficácia das investigações e proteger a sociedade contra crimes cibernéticos. A implementação de políticas públicas bem estruturadas pode fortalecer a segurança digital, promover a inovação na área de segurança cibernética e assegurar que a colaboração entre diferentes atores envolva práticas éticas e jurídicas. A seguir, são apresentadas algumas sugestões que podem contribuir para a construção de políticas públicas robustas nessa área.

Uma das principais sugestões é a criação de um marco normativo específico para a segurança cibernética, que estabeleça diretrizes claras sobre a atuação dos Red Teams, a colaboração com as autoridades policiais e as responsabilidades das partes envolvidas. Esse marco deve garantir que as práticas adotadas respeitem os direitos fundamentais dos cidadãos, como a privacidade e a proteção de dados pessoais. Além disso, deve ser dada atenção especial à definição de regras sobre a coleta e o uso de dados, prevenindo abusos e assegurando que as atividades de monitoramento ou teste de sistemas cibernéticos sejam realizadas de maneira legal e transparente.

Outro aspecto importante é a implementação de programas de capacitação contínua para profissionais de segurança cibernética, incluindo tanto membros das autoridades policiais quanto profissionais de Red Teams. Esses programas devem abranger tanto aspectos técnicos quanto jurídicos, promovendo a atualização constante sobre as novas ameaças cibernéticas, as técnicas de ataque, e as normativas legais relacionadas à segurança digital. Além disso, é essencial que essas capacitações enfoquem o fortalecimento da ética profissional, garantindo que todos os envolvidos na segurança cibernética compreendam as implicações de suas ações e respeitem os direitos dos cidadãos.

Além disso, as políticas públicas podem ser voltadas para a criação de plataformas de colaboração entre o setor público, o setor privado e a academia. Essas plataformas podem facilitar a troca de informações e boas práticas no combate aos crimes cibernéticos e promover o desenvolvimento de soluções inovadoras para a proteção de dados e sistemas. A cooperação entre diferentes setores pode proporcionar uma abordagem mais abrangente e eficiente na

identificação e mitigação de riscos cibernéticos, além de incentivar a inovação na segurança digital.

Outra sugestão importante é a definição de incentivos fiscais e financeiros para empresas que investem em segurança cibernética. Isso pode incluir desde a adoção de tecnologias avançadas de proteção de dados até a promoção de práticas de segurança cibernética em suas operações. Tais incentivos não apenas contribuirão para o fortalecimento da infraestrutura cibernética do país, mas também aumentarão a conscientização das empresas sobre a importância da proteção de dados e da segurança digital.

A criação de um sistema nacional de resposta a incidentes cibernéticos também é uma medida essencial. Esse sistema permitiria que as autoridades policiais e os Red Teams atuassem de forma coordenada e eficaz durante um incidente de segurança cibernética, como ataques a sistemas críticos ou vazamentos de dados em larga escala. A implementação de protocolos claros e processos estabelecidos para a comunicação e ação durante esses incidentes pode garantir uma resposta mais rápida e eficiente, minimizando os danos e restaurando a segurança o mais rápido possível.

Além disso, é fundamental que as políticas públicas incentivem a pesquisa e o desenvolvimento de novas ferramentas de segurança cibernética, apoiando a inovação em tecnologias de proteção, como sistemas de criptografia, inteligência artificial e análise preditiva de ameaças. O financiamento público para a pesquisa acadêmica e o desenvolvimento de novas tecnologias pode acelerar o avanço das soluções de segurança, além de proporcionar ao país uma vantagem competitiva no campo da segurança cibernética global.

Por fim, é importante que as políticas públicas considerem o papel da sociedade na segurança cibernética. Programas de conscientização pública, com foco em boas práticas de segurança digital, são essenciais para capacitar os cidadãos a protegerem suas informações e a evitar se tornarem vítimas de crimes cibernéticos. Iniciativas educativas nas escolas, universidades e empresas podem criar uma cultura de segurança cibernética que envolva todos os níveis da sociedade e contribua para a proteção coletiva.

Essas sugestões para políticas públicas são essenciais para a criação de um ambiente seguro e protegido no ciberespaço, onde a colaboração entre Red Teams, autoridades policiais e outros atores envolvidos contribua efetivamente para a

prevenção e combate aos crimes cibernéticos, respeitando sempre os direitos e a privacidade dos cidadãos.

CONSIDERAÇÕES FINAIS

Nas considerações finais deste trabalho, observa-se que a crescente complexidade dos crimes cibernéticos exige uma resposta coordenada e eficaz entre os diversos atores envolvidos na segurança digital, como Red Teams, autoridades policiais, empresas e organizações governamentais. A colaboração entre esses grupos é essencial para enfrentar as ameaças cibernéticas de forma mais eficiente e para garantir a proteção dos direitos fundamentais dos cidadãos, como a privacidade e a segurança de dados pessoais.

No entanto, ainda existem lacunas significativas na legislação brasileira que dificultam a implementação de medidas eficazes contra crimes cibernéticos e a regulamentação da atuação de Red Teams. A falta de um marco normativo claro e atualizado é uma das principais barreiras que precisam ser superadas para criar um ambiente mais seguro no ciberespaço.

As análises comparativas com outros países, como os Estados Unidos, a União Europeia e Israel, evidenciam boas práticas e lições que podem ser aplicadas no contexto brasileiro, ajudando a fortalecer a infraestrutura de segurança cibernética e a promover uma colaboração mais eficiente entre o setor público e privado.

É fundamental que o Brasil invista na atualização das suas normas e regulamentos, acompanhando as evoluções tecnológicas e as novas formas de ataque cibernético. A criação de políticas públicas que incentivem a colaboração entre os setores, a capacitação profissional contínua e a adoção de novas tecnologias de segurança são passos imprescindíveis para garantir a proteção das infraestruturas críticas e dos dados pessoais dos cidadãos. Além disso, é importante que as autoridades policiais estejam preparadas para atuar de forma legal e ética, respeitando os direitos fundamentais e utilizando as melhores práticas em suas investigações.

Por fim, as recomendações apresentadas ao longo deste trabalho visam fornecer um caminho para o aprimoramento da segurança cibernética no Brasil, com ênfase na construção de um marco normativo robusto, no fortalecimento da colaboração público-privada, na capacitação de profissionais e no desenvolvimento de novas tecnologias.

O fortalecimento da segurança cibernética não é apenas uma questão de proteção contra ataques, mas também de garantir a confiança da sociedade nas instituições e sistemas digitais, promovendo um ambiente mais seguro e resiliente para todos.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 30 nov. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 07 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 abr. 2025.

BRENNER, Susan W. **Cybercrime: criminal threats from cyberspace**. Bloomsbury Publishing USA, 2010.

CLOUGH, Jonathan. **Principles of cybercrime**. Cambridge University Press, 2015.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, 2018.

DIOGENES, Yuri; OZKAYA, Erdal. **Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics**. Packt Publishing Ltd, 2018.

FREITAS, Leonardo. **Lei Geral de Proteção de Dados e Segurança Cibernética**. Rio de Janeiro: Editora Proteção, 2021.

GARCIA, Lara Rocha *et al.* **Lei Geral de Proteção de Dados (LGPD): guia de implantação**. Editora Blucher, 2020.

MAURA, Isabelli Victoria Menezes; INÁCIO, Lucinda Esteves Campos; SERVO, Marina Calanca. A LEI N° 12.737/2012: UMA ANÁLISE HISTÓRICO-EVOLUTIVA DIANTE DA NECESSIDADE SOCIAL. **In: Anais do UNIC-Congresso Regional de Práticas Investigativas**. 2022. p. 36-36.

MONTEL, Izadora Fonseca; DE PAIVA, Jaqueline de Kassia Ribeiro. Crimes cibernéticos: panorama legislativo. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 11, p. 4495-4523, 2024.

MOREIRA, Maria Cristina de Castro. A parceria público-privada na ciberestratégia norte-americana: uma análise comparativa entre as ações dos governos Bush e Obama (2001-2017). 2019.

PEREIRA, Ana; SILVA, Bruno. **Red Teams: Desafios e Práticas**. Belo Horizonte: Editora Defesa, 2018.

SILVA, Ângelo Roberto Ilha da; RODER, Priscila Costa Schreiner; SILVA, Helder Magno da. Crimes cibernéticos. **Porto Alegre, Livraria do Advogado**, 2018.

SILVA, Amanda Cardoso da. Crimes cibernéticos breves considerações. 2022.

SILVA, Patrícia. **Legislação Brasileira sobre Crimes Cibernéticos**. Brasília: Editora Direito Digital, 2020.