ARTIGO

CIBERSEGURANÇA, SOCIEDADE E FUTURO

POR
Patricia Peck Garrido Pinheiro
patriciapeck@peckadv.com.br

Desde 1990, com a aceleração da digitalização da sociedade, em que bens corpóreos foram sendo substituídos por bens digitais, e o modelo de riqueza passou a estar mais centrado nos dados, houve uma maior necessidade de se investir em cibersegurança. Afinal, assim como as instituições passaram a ter uma maior necessidade de gestão de ativos intangíveis, também aumentou a preocupação com as ameaças e ataques a este patrimônio incorpóreo. Por esta razão, a demanda por soluções de cibersegurança e de equipes especializadas trouxe para pauta prioritária de Conselhos de Empresas o indicador de conformidade em segurança cibernética, que passou a estar mais presente também nos relatórios anuais das companhias (*anual reports*).

Contudo, devido à dinâmica da própria tecnologia e seus impactos sobre cultura e comportamento, se por um lado há um grande mercado em expansão, que carece de mais profissionais qualificados, por outro lado, os criminosos cibernéticos também evoluíram e sofisticaram a técnica, exigindo um ritmo de atualização constante.

Hoje, a Internet tem um alcance muito amplo, se fazendo presente em todas as camadas sociais e setores econômicos. Tendo sido tratada como direito essencial

na legislação do Marco Civil da Internet em 2014, ela se mostrou ainda mais relevante recentemente para o enfrentamento de pandemias. Mas, apesar de toda adesão à transformação digital, ainda há desafios em três níveis a serem tratados pela cibersegurança: 1) no nível técnico; 2) no nível da governança; 3) no nível das pessoas.

Além da necessidade de adoção de ferramentas protetivas, passou a ser um requisito essencial ter regras claras para legitimidade e viabilidade legal da proteção de patrimônio e reputação, que saltou do monitoramento padrão para uso de recursos com maior capacidade de detenção e resposta em qualquer lugar e a qualquer momento.

Ou seja, onde houver maior aplicação de protocolos de segurança, sempre há que se adequar ao uso transparente, com avisos de ciência prévios, respeitando questões relacionadas à privacidade e proteção de dados pessoais. Este equilíbrio tem envolvido equipes multidisciplinares, que também atuam sob o prisma de gestão de riscos e realização de campanhas educativas.

A relação de tempo real com o uso dos recursos e das informações e a ocorrência de incidentes, que podem ocasionar uma grande exposição, passaram a exigir uma cibersegurança mais holística e preventiva, além da necessidade de resposta rápida, neutralização de eventos e reação imediata para contenção de ataques, que podem vir de qualquer lugar, por acesso interno ou externo, ultrapassando barreiras territoriais.

No contexto da economia global digital, a segurança pressupõe estado de alerta permanente e treinamento, que deve alcançar das equipes especializadas até o usuário comum.

A chegada da inteligência artificial novamente provocou um certo desequilíbrio no ambiente de cibersegurança, na medida em que os infratores passaram a usar recursos como *deep fake* para burlar os sistemas de autenticação. Uma das premissas mais importantes no âmbito da segurança cibernética é a validação e checagem de identidades confiáveis. Qualquer vulnerabilidade neste mecanismo coloca em risco toda a proteção.

Portanto, o debate dos padrões mínimos de cibersegurança, que passaram a ser tratados por regulamentações mais recentes, como a Lei de Proteção de Dados Pessoais (LGPD), até exigências específicas e setorizadas, como ocorre no setor Financeiro, de Energia, de Saúde, tudo isso, passou a provocar o nascimento de um ecossistema da cibersegurança, culminando na recente criação da Comissão Nacional de Cibersegurança (CNCiber).

Como evitar situações como ataque de *data poisoning* (envenenamento de dados), que podem provocar grandes estragos? Passamos a conviver com todo tipo de golpe, que vai do uso de vírus ao *ransomware*, chegando até o uso de IAs maliciosas.

Todos esses assuntos são necessários na abordagem educativa da cibersegurança, pois não há como estabelecer uma estrutura forte e abrangente

de segurança cibernética sem entender os dilemas técnicos, sociais e culturais envolvidos. Isto porque precisamos alinhar a necessidade de medidas de segurança robustas para as pessoas e organizações com a salvaguarda dos direitos fundamentais e respeito aos princípios nacionais e internacionais. Além dos custos relacionados, a conformidade desempenha um papel crucial no gerenciamento de segurança, para garantia de controles de segurança apropriados, o que só é possível quando alinhado com a legislação pertinente e regulamentação setorial aplicável.

No contexto da cibersegurança, enquanto matéria que vive em contínua atuação e readequação, alinhada com o processamento massivo de dados, faz-se essencial promover uma cultura de cibersegurança mais responsiva e proativa, em vez de meramente reativa, absorvendo princípios como o *ethics by design*[1] *e o privacy by design*[2].

Outro desafio é responder ao crime cibernético com maior efetividade, conseguindo "desarmar" e "desfazer" as quadrilhas que inclusive compartilham na deep web suas abordagens, ferramentas, metodologias e ainda comercializam os resultados do crime. Novamente, somente trazendo uma ação em rede, com integração de inteligência e contrainteligência, será possível ganhar esta verdadeira guerra contra o crime organizado digital.

Devido à natureza transfronteiriça do ciberespaço, a cibersegurança de fato se tornou uma pauta internacional e multiterritorial. A colaboração entre todos os atores envolvidos passou a ser crucial para garantir maior proteção dos ativos e segurança dos indivíduos.

No Brasil, como já mencionado, neste sentido, avançamos tanto com a Convenção de Budapeste, como com a criação do Comitê Nacional de Cibersegurança (CNCiber), parte da Política Nacional de Cibersegurança (PNCiber), que tem o objetivo de contribuir para a orientação da atividade de cibersegurança no país, envolvendo diretrizes, ações, incremento da matéria de segurança e métodos de governança.

Mas, ainda é preciso melhorar muito a capacidade de identificação de autoria inequívoca no ambiente digital, com compromisso ação coordenada e célere daqueles que são responsáveis pelas por-

1 EUROPEAN COMMISSION. The aim of Ethics by Design is to incorporate ethical principles into the development process allowing that ethical issues are addressed as early as possible and followed up closely during research activities. It explicitly identifies concrete tasks which can be taken and can be applied to any development methodology (e.g. AGILE, V-Method or CRISP-DM). However, the advised approach should be tailored to the type of research being proposed keeping also in mind that ethics risks can be different during the research phase and the deployment or implementation phase. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, 25 November 2021. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Acesso em 10.Abr.2024. Tradução livre: Comissão Europeia. Ética por Design e Ética de Uso Abordagens para Inteligência Artificial. O objetivo do Ethics by Design é incorporar princípios éticos no processo de desenvolvimento, permitindo que as questões éticas sejam abordadas o mais cedo possível e acompanhadas de perto durante as atividades de pesquisa. Identifica explicitamente tarefas concretas que podem ser tomadas e aplicadas a qualquer metodologia de desenvolvimento (por exemplo, AGILE, V-Method ou CRISP-DM). No entanto, a abordagem recomendada deve ser adaptada ao tipo de pesquisa que está sendo proposta, tendo também em mente que os riscos éticos podem ser diferentes durante a fase de pesquisa e a fase de implantação ou implementação.

2 PINHEIRO, Patricia Peck. Privacy by design é um conceito criado pela canadense Ann Cavoukian, que estabelece que é necessário adotar medidas preventivas desde a concepção de cada projeto, para evitar que resultados indesejáveis ocorram. Disponível em: https://www.linkedin.com/pulse/patr%C3%AD-

tas de entrada, seja da Internet ou das aplicações. Isso sim irá permitir pegar literalmente o "bandido com a mão na máquina", além da necessidade de políticas públicas para se evitar reincidência. Além disso, um dos principais pontos que também merecem atenção e aperfeiçoamento está relacionado com a questão "quem vigia o vigia", ou seja, como tomar cuidado com aqueles que têm maior acesso e conhecimento e evitar desvios éticos desta função tão relevante.

Novamente, toda esta realidade demonstra a necessidade de um aprofundamento no ensino da segurança cibernética que prepare cuidadosamente as pessoas, tanto para a ação quanto para a reação, com foco de estudo em pormenores técnicos, instruções práticas, abordagens das escolas de pensamento, dilemas éticos, influência de questões climáticas, riscos e mitigação, para que possamos enfrentar as certezas e incertezas do futuro da sociedade digital e robótica e torná-la mais segura para todos.

cia=-peck-news-patricia-peck-pinheiro-phd1-f?trk-public_post. Acesso em 10.Abr.2024.

Referências:

1. EUROPEAN COMMISSION. Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, Version 1.0, 25 November 2021. Disponível em: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Acesso em 10.Abr.2024.
2. GOODMAN, Marc. Future Crimes. Ed. HSM. 2014. Pg 19, pg 253.
3. PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva. 7ª. edição. 2021.
4. PINHEIRO, Patricia Peck. Segurança Digital. Ed. GEN. 2020.
5. PINHEIRO, Patricia Peck. Patricia Peck News. Disponível em: https://www.linkedin.com/pulse/patr%C3%ADcia-peck-news-patricia-peck-pinheiro-phd-1f?trk=public_post. Acesso em 10.Abr. 2024.

PATRICIA PECK GARRIDO PINHEIRO é CEO e sócia-fundadora do escritório Peck Advogados. Advogada especialista em Direito Digital, Propriedade Intelectual, Proteção de Dados e Cibersegurança. Graduada e Doutorada pela Universidade de São Paulo, PhD em Direito Internacional com tese defendida sobre Propriedade Intelectual da Inteligência Artificial. Nomeada como Membro Titular para o Comitê Nacional de Cibersegurança (CNCiber). Conselheira titular nomeada para o Conselho Nacional de Proteção de Dados (CNPD). Autora/coautora de 46 livros de Direito Digital. Presidente do Instituto Peck de Cidadania Digital. Programadora desde os 13 anos. Certificada em Privacy e Data Protection EXIN.