QUESTÕES ÉTICAS RELACIONADAS AO MONITORAMENTO DE REDES DE DADOS

ETHICAL ISSUES RELATED TO MONITORING DATA NETWORKS

Filipe Lima
Faculdade de Tecnologia de Americana
filipe.lima9@fatec.sp.gov.br

Victor Henrique de Alvarenga
Faculdade de Tecnologia de Americana
victor.alvarenga01@fatec.sp.gov.br

Wagner José da Silva
Faculdade de Tecnologia de Americana
wagner.silva@fatec.sp.gov.br

Resumo

A tecnologia da informação é uma área em constante e rápida expansão, e junto com ela o monitoramento de redes de dados é uma prática cada vez mais crucial na era digital, mas que levanta preocupações sobre a privacidade, segurança e direitos individuais. Neste artigo são explorados os desafios éticos inerentes a essa prática profissional. Utilizando referenciais teóricos e estudo de campo são levantadas questões éticas, morais e o cuidado com cumprimento das legislações pertinentes à segurança de informações, com foco no exame das implicações do monitoramento de rede de dados em vários contextos. O objetivo é verificar o nível de conhecimento e comprometimento de profissionais e usuários sobre este tema.

Palavras-chave: Monitoramento de redes de dados, ética em redes de dados, ética em informática.

Abstract

Information technology is a field undergoing constant and rapid expansion, and along with it, data network monitoring has become an increasingly crucial practice in the digital age. However, it raises concerns about privacy, security, and individual rights. This article explores the inherent ethical challenges of this professional practice. By using theoretical frameworks and field studies, ethical and moral questions are raised, as well as the importance of complying with information security regulations, with a focus on examining the implications of data network monitoring in various contexts. The objective is to assess the level of knowledge and commitment of professionals and users regarding this topic.

Keywords*:* Monitoring, networks, security, professional, ethics.

1. Introdução

Atualmente, com a rápida e crescente expansão e evolução da tecnologia da informação em todas as áreas do conhecimento, os serviços de redes de dados e conectividade com a internet são essenciais tanto para uso pessoal quanto para uso corporativo, e neste segundo caso são, muitas vezes, considerados críticos para a continuidade dos negócios. Manter os serviços de redes de dados em pleno funcionamento depende de técnicas e ferramentas específicas, entre elas o monitoramento das atividades nas redes de dados para a prevenção e rápida detecção de problemas, bem como efetiva correção de falhas que possam comprometer a disponibilidade, integridade e confiabilidade dos serviços, já que, de acordo com Silva (2024) o tempo de atendimento e solução de problemas de redes é um fator crítico que pode prejudicar ou paralisar as operações da empresa, causando grandes prejuízos.

No entanto, Cordeiro et. al. (2023) relata que apesar de o monitoramento da rede de dados ser essencial para garantir o funcionamento das redes, coloca em conflito a necessidade de segurança e a preservação da privacidade e dos direitos individuais dos usuários, devido a inevitável coleta de informações sensíveis e ao armazenamento de dados que trafegam pela rede, já que para os autores “à medida que a tecnologia avança e as ameaças cibernéticas se tornam cada vez mais sofisticadas, encontrar um equilíbrio entre a busca pela segurança e a garantia dos princípios éticos e legais torna-se um desafio crucial, e em constante evolução” (Cordeiro, 2023 pag. 02).

Partindo desse pressuposto, este estudo exploratório busca elucidar, a partir de referencial teórico, de estudos de caso e de estudos empíricos, o nível de conhecimento da legislação e preceitos éticos tanto de profissionais de monitoramento de redes de dados quanto dos usuários destes sistemas, respondendo à seguinte pergunta de pesquisa: Profissionais de monitoramento de redes e usuários são éticos em sua atuação e seguem as leis sobre segurança da informação?

2. Referencial Teórico

Na era da digital em que vivemos, o crescimento dos ataques cibernéticos impulsionou a adoção generalizada do monitoramento de redes como um escudo essencial para empresas e organizações. O expressivo aumento de 95,9% nas detecções de ciberataques no Brasil a partir do primeiro semestre de 2018, comparado ao mesmo período em 2017, conforme apontado no relatório dfndr lab (PSafe, 2018), evidencia a vulnerabilidade das infraestruturas de tecnologia da

informação e a necessidade de medidas de segurança robustas. Nesse contexto, o monitoramento de redes surge como uma ferramenta vital para identificar e neutralizar ameaças, enquanto coleta dados para análises estratégicas que permitam a melhoria contínua dos mecanismos de segurança nas redes de dados.

Ferramentas de monitoramento de redes, apesar de serem bastante eficientes na coleta, análise e visualização de dados que trafegam pela rede de dados, não são capazes de identificar informações ou situações que possam ser utilizadas de forma antiética. Silva (2024), por exemplo, diz que o Zabbix é uma plataforma de monitoramento utilizada em larga escala e ajuda as empresas a manterem o controle de seus ativos e sistemas, por exemplo. Mas depende da interação e senso crítico de humanos seja para interpretar as informações que dispõe, seja para iniciar uma ação a partir de um alerta ou ainda para configurar a ferramenta para que atenda deforma mais assertiva às necessidades da empresa.

No entanto, a coleta massiva de dados e a possibilidade de vigilância intrusiva inerentes ao monitoramento de redes levantam importantes questões éticas. Magrani (2019) explica que diante do contexto atual, onde o tratamento e compartilhamento de informações de forma online é cada vez mais comum e necessário, é crucial debater noções de privacidade e ética, visto a grande quantidade de informações acessadas e coletadas por sistemas informatizados das quais humanos podem ter acesso legal ou ilegalmente. O autor aponta que a privacidade é prevista na legislação brasileira, tanto da Constituição Federal de 1988 como em leis posteriores, como a Lei Geral de Proteção de Dados - LGPD – (Lei nº 13.709/2018) e outras.

Masiero (1994) define a ética profissional como um guia para a tomada de decisões corretas do ponto de vista da sociedade, num espaço de tempo determinado, sendo essencial para que uma profissão seja reconhecida e respeitada por essa sociedade.

Na realidade brasileira, não apenas o Marco Civil da Internet é relevante para a regulação do tratamento de informações pessoais e proteção da privacidade. Legislações como a Lei Geral de Proteção de Dados (LGPD) e a chamada Lei Carolina Dieckmann também desempenham uma função crucial nesse âmbito. Em um panorama global, o Regulamento Geral sobre a Proteção de Dados (GDPR) estabelecido pela União Europeia define padrões rigorosos no que diz respeito à salvaguarda dos dados pessoais, tendo repercussões mundiais para empresas onde ocorre coleta ou processamento desses dados por cidadãos europeus, por isso tornou-se referência mundial em

termos de legislação para segurança de dados.

As principais legislações brasileiras que contemplam ética na área de tecnologia da informação surgem a partir de problemas decorrentes de questões éticas, relacionadas a profissionais e usuários de tecnologia da informação. Segundo Silva (2024) a evolução das leis no Brasil refletiu a necessidade e enfrentamento de crimes digitais, como por exemplo a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, um passo fundamental no combate às condutas indevidas como invasão de dispositivos informáticos.

Outra importante lei brasileira relacionada a questões de tecnologia "foi o Marco Civil da Internet, instituído pela Lei nº 12.965/2014, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção de dados pessoais e a responsabilidade dos provedores de serviços" (Silva, 2024, p.146).

Mais recentemente, a Lei 14.155/2021 trouxe novas tipificações penais para crimes cibernéticos, como a invasão de dispositivo informáticos mediante fraude, furto e estelionato digital, e a Lei 14.132/2021 criminalizou o stalking, que é a prática de perseguição digital a outras pessoas, reforçando a proteção dos usuários no ambiente digital.

A associação ISACA - Information Systems Audit and Control Association disponibiliza um framework que se destaca por ser um guia abrangente para gerenciamento e governança de TI que contém um conjunto de práticas e princípios recomendados. Esse framework é o COBIT - Control Objectives for Information and Related Technology. Quando aplicado ao monitoramento de rede, esse framework promove os princípios essenciais da ética. No contexto do monitoramento de rede, o destaque do COBIT são os princípios de confidencialidade, proteção de dados, conformidade legal e transparência, porque é fundamental garantir a ética e a responsabilidade nessa prática.

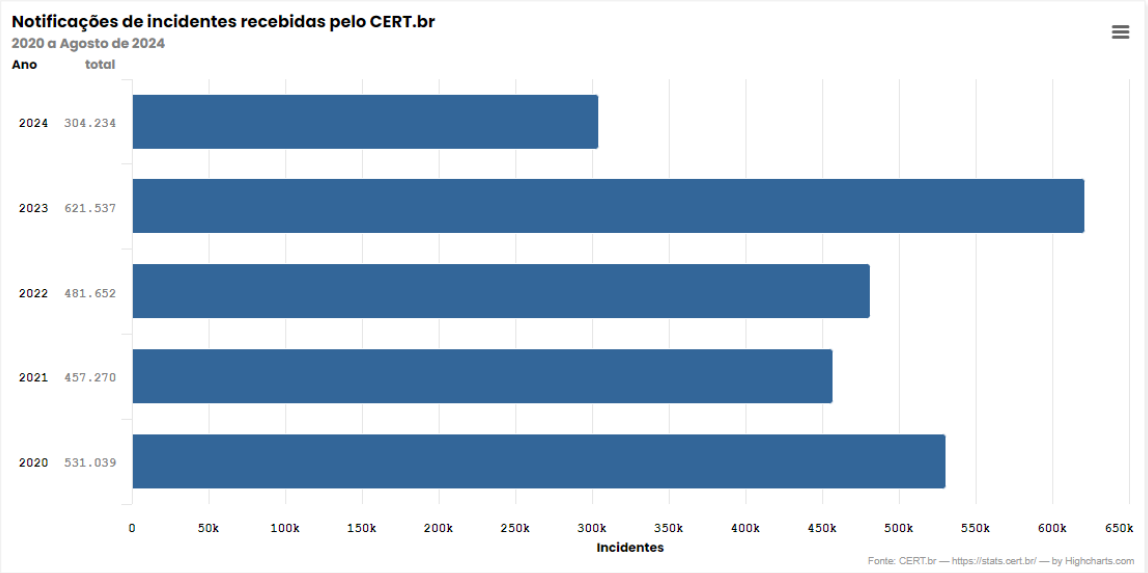
Outro ponto importante e extremamente atual a ser considerado é o uso de inteligência artificial, que está cada vez mais presente no cotidiano e não poderia ser diferente no monitoramento de redes de dados. De Lima (2024) explica que o uso de técnicas de inteligência artificial em segurança cibernética é um campo em crescimento, como a detecção e resposta automática a ameaças em tempo real. "a combinação de IA e análise de dados pode resultar em sistemas de defesa cibernética mais eficázes e adaptativos" (De Lima, 2024, p. 100).

De Lima (2024) utilizou a ferramenta CrowdStrike para detectar e atuar em tentativas de ataques contra sistema, sendo necessário para isso coletar e analisar uma grande quantidade de informações. Para o autor “explorar como proteger as informações pessoais dos usuários enquanto se obtêm insights úteis para a segurança é um desafio fundamental. Pesquisas podem se concentrar em métodos para garantir a anonimização dos dados, desenvolver políticas de privacidade robustas e abordar preocupações éticas relacionadas à coleta e uso de dados.” (De Lima, 2024, p. 101).

A norma ISO/IEC 27001, oferece diretrizes para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), também aborda questões éticas relacionadas ao monitoramento de redes. A ISO ressalta a importância de manter a confidencialidade, integridade e disponibilidade das informações, que abrangem dados coletados durante atividades de monitoramento. Além disso, o código de prática para controles de segurança da informação ISO/IEC 27002 expõe ainda a necessidade de controles para garantir a conformidade com os requisitos legais e regulatórios, incluindo leis de privacidade e proteção de dados. Adicionalmente, a norma destaca a importância da responsabilidade e do profissionalismo na condução do monitoramento, com a necessidade de treinamento adequado e autorização para acesso e manuseio de dados confidenciais.

De acordo com relatórios do Centro de Estudos, Resposta e Tratamento a Incidentes de Segurança no Brasil – Cert.br (2024), o cenário brasileiro evidencia a necessidade do monitoramento de redes, realizado de forma ética e que cumpra com a legislação vigente. O cert.br também mostra, em suas estatísticas evidenciadas pela Figura 01, um grande aumento de incidentes de segurança nos últimos anos, muitos deles relacionados a violação de privacidade e ao uso indevido de dados pessoais, visto que a terceira maior incidência de notificações de problemas de segurança nos últimos cinco anos estão relacionadas a fraudes, como mostra a Figura 02. Estes dados mostram a gravidade da desinformação que pode culminar em um crime cibernético e o potencial de monitoramento de rede para prevenir tais problemas.

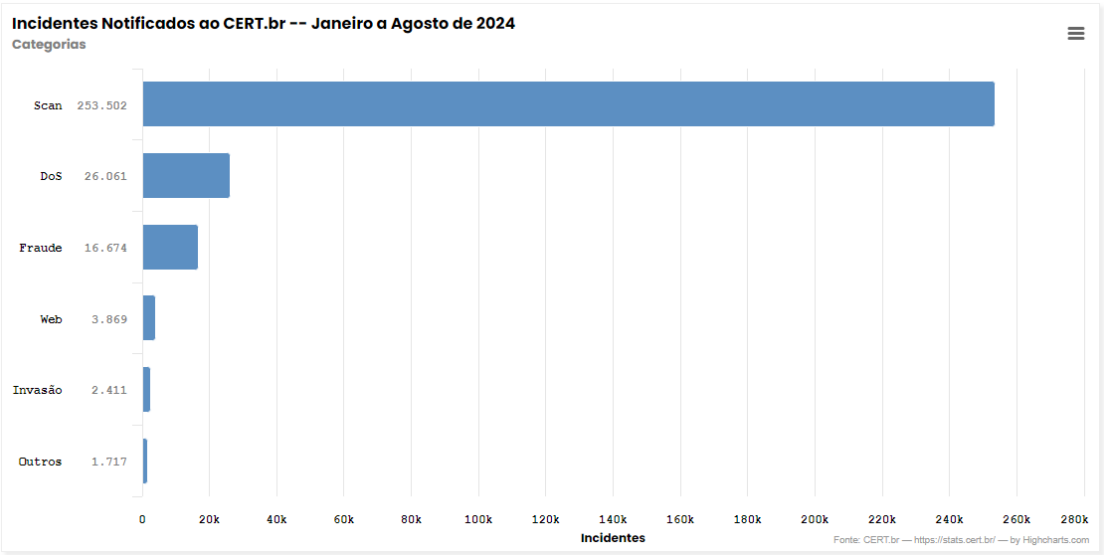
Figura 01 – Gráfico de notificações recebidas pelo cert.br.



Fonte: cert.br (2024)

A figura 01 mostra a incidência de notificações de incidentes de segurança da informação relatados nos últimos cinco anos ao cert.br, onde é possível notar o aumento gradativo na quantidade de incidentes ano a ano, com aumento mais expressivo entre 2022 e 2023 com cerca de 22,5% de casos a mais.

Figura 02 – Tipos de incidentes registrados pelo cert.br de acordo com o tipo.



Fonte: cert.br (2024)

Na Figura 02 é possível observar a comparação entre os tipos de incidentes reportados ao cert.br. No primeiro caso está o tipo Scan, com maior incidência por ser o tipo de ataque comumente utilizado para encontrar brechas nos sistemas de informação que proporcionem ataques de outros tipos, seguido de ataques DoS, que objetivam tirar do ar sites, servidores ou sistemas por diferentes motivos e, em terceira colocação o tipo Fraude, que comumente são cometidos em decorrência da obtenção ilícita de dados sigilosos, como o caso marcante do vazamento de dados da Serasa Experian em 2020, por exemplo.

Outro caso de destaque envolvendo fraude de sistemas digitais ocorreu em 2014, quando, segundo Casemiro (2014) a operadora de telefonia Oi foi multada por violação ao direito à privacidade e intimidade, e por publicidade enganosa. O que mostra recorrência nos casos de fraudes utilizando os sistemas computacionais.

3. Materiais e Métodos

A realização deste trabalho contou com as seguintes etapas: de investigação na bibliografia existente para compreender como as questões éticas influenciam e são importantes para os profissionais que atuam nas redes de dados e, portanto, têm acesso aos dados que por ela circulam, bem como por usuários que, por terem acesso constante aos sistemas informatizados, são considerados um importante elo na garantia da segurança dos sistemas, principalmente quando se trata de redes corporativas de dados.

Complementarmente foram aplicados dois questionários eletrônicos, um destinado exclusivamente à profissionais atuantes em redes de dados e outo destinado a usuários comuns de sistemas informatizados, especialmente sistemas corporativos. Os questionários têm o objetivo de elucidar o nível de conhecimento e comprometimento com as questões éticas envolvendo a rede de dados da qual participa do gerenciamento ou é usuário. Os questionários foram aplicados em diferentes organizações empresariais de ramos distintos, sem que se identificasse o participante e sua respectiva empresa.

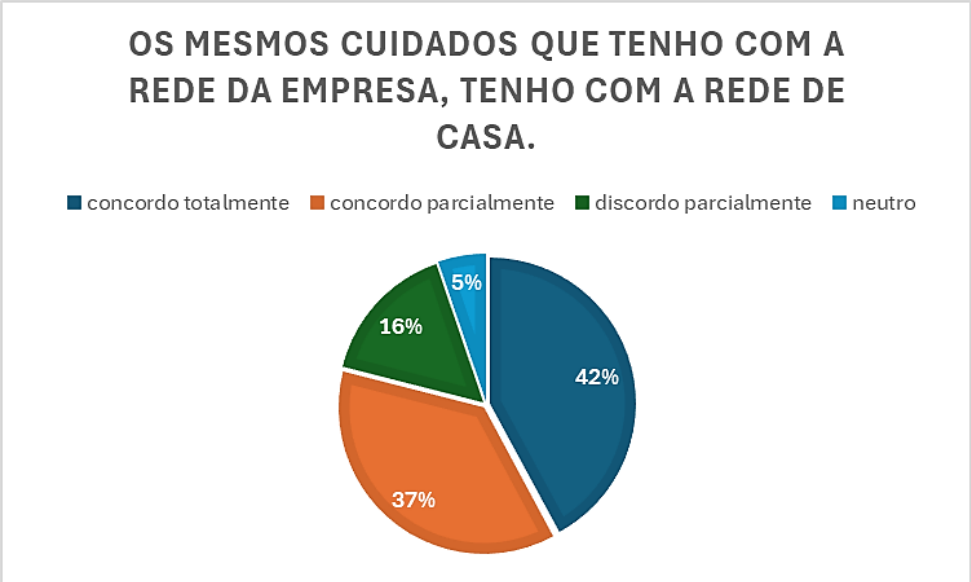
Por meio de questionário eletrônico foram consultados 20 profissionais de tecnologia da informação atuantes em redes de dados e 20 usuários de sistemas informatizados de organizações empresariais. Esta pesquisa teve como objetivo entender o nível de compreensão da importância das ações para a promoção da segurança das informações que

circulam pelos sistemas informatizados.

4. Resultados e Discussões

Apesar de ser uma amostra pequena, o estudo revelou com base nas respostas coletas, que os profissionais da área de redes mostram-se confortáveis em relação as leis que devem seguir e aplicar. A Figura 03 retrata a parcela de profissionais que tem pouca discordância ou que se diz neutro em relação aos cuidados, somados representam 21% dos respondentes, o que leva a crer que hoje, o profissional possui consciência sobre seu papel profissional dentro e fora da empresa.

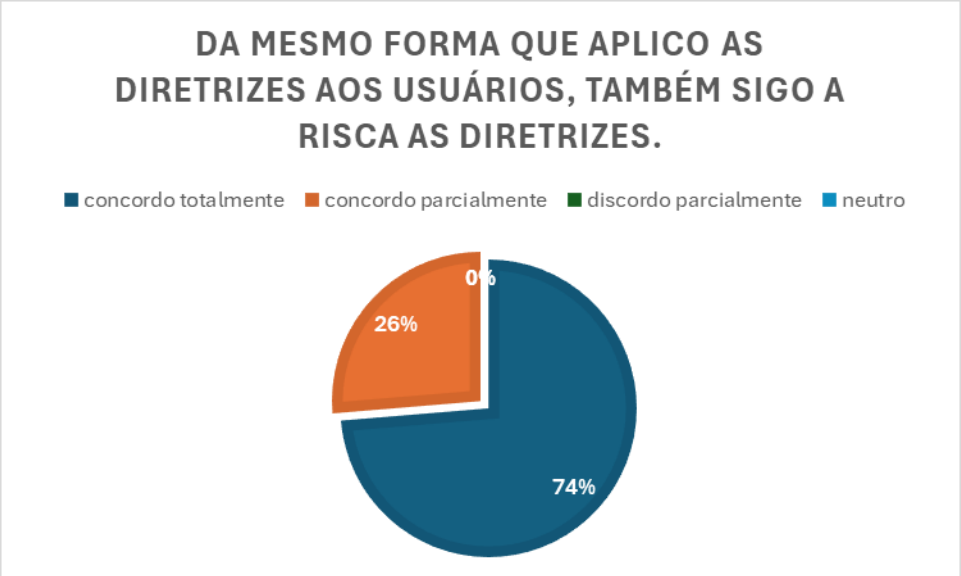
Figura 03 – Pesquisa de campo com profissionais da área



Fonte: própria (2024)

A Figura 04 por sua vez, mostra que 100% dos profissionais concordam quanto a necessidade e aplicação de compliance, ou seja, regras de conduta em relação as normas que devemos seguir. Da amostra coletada, observa-se que 26% concordam parcialmente com as normas, e os demais concordam plenamente.

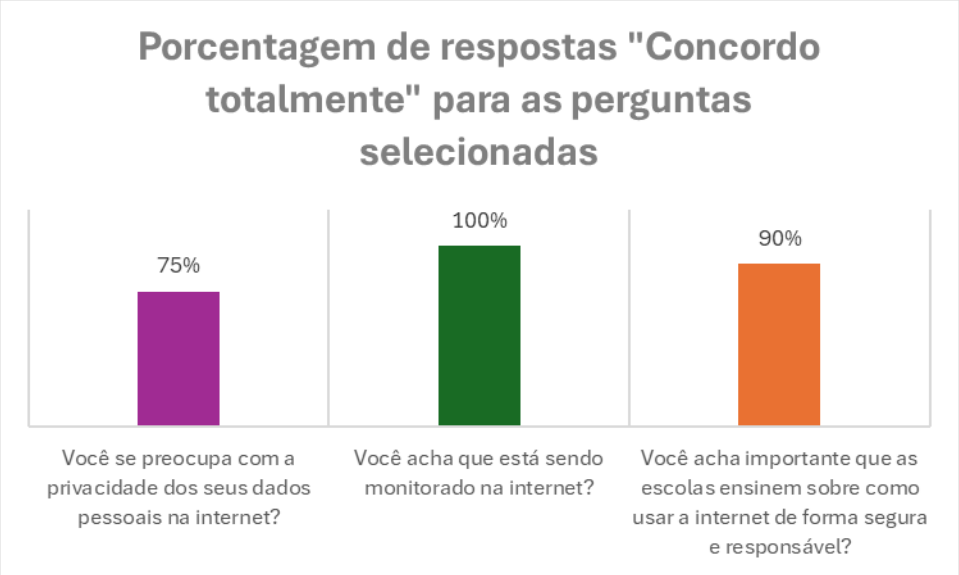
Figura 04 – Pesquisa de campo com profissionais da área



Fonte: própria (2024)

Já os usuários revelaram por meio da pesquisa, como pode ser verificado na Figura 05, que apenas 75% dos participantes demonstram preocupação com a segurança de seus dados em sistemas computacionais, como a internet. concordaram totalmente com essa afirmação, apesar de os 100% dos entrevistados acreditarem estar sendo monitorados na internet. Além disso, 90% dos participantes expressaram total concordância sobre a necessidade de instituições educacionais instruírem os alunos sobre o uso seguro e responsável da internet, ressaltando o papel crítico que a educação desempenha nesse contexto.

Figura 05 – Pesquisa de campo com usuários



Fonte: própria (2024)

Figura 06 – Pesquisa de campo com usuários

Fonte: própria (2024)

Seguramente é possível afirmar com base nos autores consultados que é extremamente importante e relevante a promoção do monitoramento da rede de dados com foco na promoção da segurança das informações, bem como que preceitos éticos e legais estão intrinsicamente ligados a essa tarefa.

O caso da Serasa Experian ilustrado anteriormente destaca a importância do uso de ferramentas como o monitoramento responsável e ético de redes de dados para a segurança das informações. Nesse incidente, informações pessoais de mais de 220 milhões de brasileiros foram expostas e comercializadas ilegalmente na internet; entre os dados divulgados estavam CPFs, nomes completos, datas de nascimento, endereços e até mesmo a foto das pessoas, dados esses que muito provavelmente causaram prejuízos e constrangimento a inúmeras pessoas. Este exemplo ressalta ainda mais a gravidade de falhas na segurança de dados e o impacto devastador que pode causar na vida das pessoas.

Um outro exemplo marcante é o vazamento de dados da rede social Facebook, que afetou aproximadamente 533 milhões de usuários em 2021. Informações pessoais, como nomes, números de telefone, endereços de e-mail e até mesmo detalhes sobre localização foram expostas e disponibilizadas em fóruns na internet. Esse incidente não apenas comprometeu a segurança dos dados de milhões de pessoas, mas também levantou sérias questões sobre a responsabilidade das empresas em proteger as informações de seus usuários e a necessidade de um monitoramento adequado para prevenir tais falhas.

Com a pesquisa realizada, foi possível identificar que as pessoas envolvidas com as redes de dados, sejam usuários ou profissionais que mantêm os serviços disponíveis, conhecem e estão em grande parte comprometidos com o uso consciente dos recursos que acessam. A pesquisa revelou que todos os profissionais concordam de alguma forma com a aplicação de regras e normas para o correto uso das informações que trafegam pelos serviços que monitoram, e revelaram cumprir todas as regras que eles devem fazer valer por conta de suas funções, com um ponto de atenção aos usuários dos sistemas, visto que 25% revelam não estarem preocupados com a segurança de seus dados na internet, e alarmantes 40% revelaram não ter o hábito de trocar suas senhas de segurança com frequência. Esses dados revelam a necessidade de divulgações de informações sobre segurança da informação principalmente aos usuários dos sistemas de informação.

Em que pese as implicações éticas sobre o monitoramento de redes de dados, vale ressaltar os seguintes pontos:

Garantir a não invasão de privacidade, ou seja, do ato de coletar e/ou analisar, sem o consentimento do proprietário, dados ou tráfego de rede que possam expor informações

sensíveis ou comunicação, por exemplo. Como forma de proteger a privacidade de usuários, diversos países elaboraram legislações para governar o uso de dados pessoais, tais como, a General Data Protection Regulation (GDPR) na União Europeia e Lei Geral de Proteção de Dados (LGPD) no Brasil (ALVES, 2021, p.2).

Não permitir a violação de segurança de dados. Quando não implementado ou gerenciado corretamente, o monitoramento de redes pode resultar em vulnerabilidades que expõem organizações a ataques cibernéticos e vazamento de dados, por isso a segurança dos durante o monitoramento de redes devem adotar medidas robustas de proteção, como criptografia, autenticação forte e políticas de acesso restrito, para garantir a confidencialidade e a integridade das informações.

Atenção ao monitoramento de funcionários, já que a confiabilidade nas atividades desenvolvidas por funcionários com acesso a dados sensíveis, embora justificável em alguns casos para garantir a produtividade, levanta preocupações éticas sobre a privacidade no local de trabalho, além de poder criar um clima de desconfiança e ansiedade entre os funcionários, por isso a importância de manter registro de todas as operações e monitoramento por imagens que devem ser acessados somente quando estritamente necessário.

Cuidar da relação de confiança, pois a falta de transparência e a vigilância indiscriminada podem minar a confiança entre pessoas, empresas e até nações. A sensação constante de estar sendo observado pode gerar autopreservação, limitando tanto a liberdade de expressão quanto a criatividade e produtividade dos colaboradores.

Uso de dados sensíveis para disseminar notícias falsas objetivando benefício próprio ou de terceiros. As chamadas fakes news são cada vez mais comuns e não raro partem de vazamentos de dados que, divulgados de forma distorcida pode ter diferentes conotações. Para isso é importante manter a comunidade informada e consciente sobre os riscos da propagação de notícias falsas.

5. Considerações Finais

Os resultados deste estudo mostram que o monitoramento de redes de dados é essencial no combate a crimes cibernéticos, mas sua eficácia depende também do respeito aos preceitos éticos e legais. Casos como os vazamentos do Facebook e da Serasa Experian evidenciam os

riscos de falhas na segurança que, entre outras coisas, prejudicam a confiança na empresa, causam prejuízos pessoais e coletivos, com o potencial de deixar uma grande quantidade de usuários vulneráveis. A pesquisa conclui que políticas claras e a correta divulgação de informações sobre segurança da informação são cruciais para garantir o monitoramento responsável, promovendo um ambiente digital seguro e confiável.

É possível concluir ainda que existe o compromisso e responsabilidade dos profissionais de tecnologia da informação responsáveis pelo monitoramento de redes com o cumprimento da legislação e de boas práticas para o exercício de suas funções. Enquanto, em relação aos usuários, um aspecto significativo é a necessidade de alcançar um equilíbrio entre segurança e privacidade no ambiente online, especialmente com a promoção de ações de disseminação de informação e conscientização sobre os riscos, aspectos legais e aspectos éticos relacionados às informações nos meios digitais.

Com isso, entende-se que as iniciativas destinadas a conscientizar e fornecer educação sobre segurança da informação estão se tornando cada vez mais essenciais para garantir a proteção de dados e a privacidade dos usuários da internet.

Por fim, foi possível identificar ainda por meio desse estudo que, apesar de existirem muitas publicações a respeito, há um vasto campo a ser explorado para explorar as questões éticas relacionadas ao exercício da profissão em tecnologia da informação, como por exemplo a análise das diferentes ferramentas de monitoramento e sua conformidade com os preceitos éticos e legais ou a investigação se as legislações afetam de alguma forma as atividades de monitoramento de redes de dados, entre outras.

Referências

ALVES, Carina; NEVES, Moisés. Especificação de Requisitos de Privacidade em Conformidade com a LGPD: Resultados de um Estudo de Caso. In: WER. 2021. Disponível em: https://www.inf.puc-rio.br/wer/WERpapers/artigos/artigos_WER21/WER_2021_paper_31.pdf. Acesso em 26 set 2024.

Business Insider. Facebook data leak: 533 million users' phone numbers and personal data leaked online. Business Insider, 7 de abril de 2021. Disponível em: https://www.businessinsider.com/facebook-data-leak-533-million-users-2021-4. Acesso em: 30 set de 2024.

CARVALHO, Luiz Paulo; OLIVEIRA, Jonice; SANTORO, Flávia Maria. A presença de conteúdos sobre ética computacional na literacia em computação institucional brasileira. Encontro Virtual ABCiber - UNIFAE. São João da Boa Vista/SP, 2021. Disponível em: https://www.researchgate.net/profile/Luiz-Paulo Carvalho/publication/353979542_COMPUTACAO_LITERACIA_E_ETICA_COMPUTACIONAL_UM_ESTUDO_EXPLORATORIO_PELO_CIBERESPACO_BRASILEIRO/links/611d18a71e95fe241adc69b4/COMPUTACAO-LITERACIA-E-ETICA-COMPUTACIONAL-UM-ESTUDO-EXPLORATORIO-PELO-CIBERESPACO-BRASILEIRO.pdf. Acesso em 21 set 2024.

CASEMIRO, Luciana; XAVIER, Luiza. Oi é multada em R$ 3,5 milhões por invasão de privacidade feita por Velox: Segundo Ministério da Justiça, serviço de banda larga monitorava navegação de usuários e vendia perfil a anunciantes. Jornal Eletrônico O Globo, 2014. Disponível em: http://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505. Acesso em: 21 set 2024.

DE LIMA, Leonardo Bruscagini. Detecção de anomalias em tempo de resposta de servidores web: Uma abordagem automatizada para aprimorar a segurança e a eficiência. 2023. Tese de Doutorado. Dissertação de Engenharia Elétrica e de Computação 2023. Tese de Doutorado. Campinas/SP. Disponível em: https://repositorio.unicamp.br/Busca/Download?codigoArquivo=562437&tipoMidia=0 . Acesso em: 10 nov 2024.

GIAMPAOLLI, Ricardo Zoldan; TESTA, Maurício Gregianin; LUCIANO, Edimara Mezzomo. Contribuições do Modelo COBIT para a Governança Corporativa e de Tecnologia da Informação: Desafios, Problemas e Benefícios na Percepção de Especializas e CIOs. Análise (PUCRS), 2011. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/10329/2/Contribuicoes_do_Modelo_COBIT_para_a_Governanca_Corporativa_e_de_Tecnologia_da_Informacao_Desafios_Problemas_e.pdf. Acesso em set 2024.

ISO. International Standarts Organization - ISO/IEC 27001, 27001:2022. Disponível em: https://www.iso.org/standard/27001. Acesso em: 09 nov. 2024.

ISO. International Standarts Organization - ISO/IEC 27002, 27002:2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 09 nov. 2024.

ISACA. A COBIT 5 Overview. Information Systems Audit and Control Association. Disponível em: https://www.isaca.org/resources/cobit/cobit-5. Acesso em 21 set. 2024.

MAGRANI, Eduardo. Entre dados e robôs. Ética e Privacidade na Era da Hiperconectividade. 2a. Ed. Porto Alegre/RS. Editora Arquipélago, 2019. Disponível em: http://eduardomagrani.com/wp-content/uploads/2019/07/Entre-dados-e-robo%CC%82s-Pallotti-13062019.pdf. Acesso em 20 set 2024.

MASIERO. P. C. Ética para Profissionais em Computação. 12ª Ed. São Carlos/SP. Rev. Notas Didáticas. Instituto de Ciências Matemáticas de São Carlos. 1994. Disponível em: https://repositorio.usp.br/directbitstream/5c0f3a6c-615f-448a-b4d2-c2fff6c83a8a/872884.pdf. Acesso em 20 set 2024.

PSAFE.DFNDR LAB. Relatório da Segurança Digital no Brasil: Segundo trimestre - 2018. PSafe Security. 2018. Disponível em: https://dfndrlab.com/assets/pdf/dfndr-lab-segundo-trimestre-2018.pdf. Acesso em: 08 Set 2024.

SANTOS, G. M.; OLIVEIRA, H.; CORDEIRO, F. da S.; SILVA, W. J. O MONITORAMENTO DE ATAQUE LOIC UTILIZANDO O WIRESHARK. FatecSeg - Congresso de Segurança da Informação, [S. l.], 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/140. Acesso em: 14 set. 2024.

SILVA, Ari Venâncio da; FRAILE, Fernando Ferro; SILVA, Nilce Delha Oliveira da. UMA ANÁLISE SOBRE CRIMES CIBERNÉTICOS: Contexto, Tipologia e Implicações Jurídicas no Brasil. Judicare, [S.l.], v. 21, n. 2, p. 143-153, jun. 2024. ISSN 2237-8588. Disponível em: http://revista.fadaf.com.br/revistacientifica/index.php/judicare/article/view/285. Acesso em: 21 set. 2024.

SILVA, Roger Assunção da; SILVA, Wagner José da. IMPLEMENTAÇÃO DE MONITORAMENTO DE REDE DE DADOS COM ZABBIX E GRAFANA: um estudo de caso. P2P E INOVAÇÃO, Rio de Janeiro, RJ, v. 10, n. 2, p. e-6904, 2024. DOI: 10.21728/p2p.2024v10n2e-6904. Disponível em:. Acesso em: 14 set. 2024.https://revista.ibict.br/p2p/article/view/6904. Acesso em: 14 set. 2024.