UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE JORNALISMO

NICOLLAS CÉSAR ALCÂNTARA

A INFLUÊNCIA DA SEGURANÇA DE DADOS NA PRÁTICA DO JORNALISMO: Proteção e integridade das informações

MARIANA
2025

NICOLLAS CÉSAR ALCÂNTARA

A INFLUÊNCIA DA SEGURANÇA DE DADOS NA PRÁTICA DO JORNALISMO: Proteção e integridade das informações

Monografia apresentada ao curso de Jornalismo da Universidade Federal de Ouro Preto, como requisito parcial para obtenção de título de Bacharel em Jornalismo.

Orientadora: Profª. Dra. Debora Cristina Lopez

MARIANA
2025

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

A347i Alcantara, Nicollas Cesar.
A influência da segurança de dados na prática do jornalismo [manuscrito]: proteção e integridade das informações. / Nicollas Cesar Alcantara. - 2025.
77 f.

Orientadora: Profa. Dra. Debora LOPEZ.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Instituto de Ciências Sociais Aplicadas. Graduação em Jornalismo .

1. Ética. 2. Jornalismo. 3. Proteção de dados. I. LOPEZ, Debora. II. Universidade Federal de Ouro Preto. III. Título.

CDU 070.11

Bibliotecário(a) Responsável: Essevalter de Sousa - CRB6/1407

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS SOCIAIS E APLICADAS
DEPARTAMENTO DE JORNALISMO

FOLHA DE APROVAÇÃO

Nicollas César Alcântara

A influência da segurança de dados na prática do jornalismo: Proteção e integridade das informações

Monografia apresentada ao Curso de Jornalismo da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel

Aprovada em 18 de agosto de 2025

Membros da banca

Dra. - Debora Cristina Lopez - Orientadora (Universidade Federal de Ouro Preto) Dr. - Marcelo Freire Pereira de Souza - (Universidade Federal de Ouro Preto) Mestranda - Sabrina Kelly Roza - (Universidade Federal de Ouro Preto)

Debora Cristina Lopez, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 25/09/2025

Documento assinado eletronicamente por **Debora Cristina Lopez**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 29/09/2025, às 09:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0985796** e o código CRC **0C13A27C**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3558-2275 - www.ufop.br

Para meus pais, que caminharam por noites escuras só para que eu visse o amanhecer.

AGRADECIMENTOS

A realização deste Trabalho de Conclusão de Curso representa não apenas a finalização de uma etapa acadêmica, mas também a materialização de um percurso construído com o apoio, incentivo e dedicação de muitas pessoas, às quais dedico minha mais sincera gratidão.

Agradeço, primeiramente, aos meus familiares, cujo apoio incondicional foi fundamental em todos os momentos desta caminhada. À minha mãe e ao meu pai, agradeço por acreditarem em meu potencial mesmo nos momentos mais desafiadores, oferecendo sempre palavras de encorajamento, paciência e amor.

Expresso minha profunda gratidão à minha orientadora, Profa. Debora Cristina Lopez, por sua orientação criteriosa, pelas contribuições técnicas e teóricas, e por sua disponibilidade e comprometimento durante todas as etapas desta pesquisa. Sua postura ética e excelência acadêmica foram fontes constantes de inspiração.

Agradeço também aos professores e professoras do curso de Jornalismo, cujas aulas e discussões enriqueceram minha formação intelectual e crítica. Cada disciplina contribuiu, de forma única, para a construção do conhecimento que aqui se apresenta.

Aos colegas de graduação, pela convivência, pelas trocas de experiências e pelos aprendizados coletivos ao longo desses anos. Compartilhar essa trajetória com vocês foi essencial para tornar essa jornada mais leve e significativa.

Por fim, agradeço a todas as pessoas que, direta ou indiretamente, colaboraram para a realização deste trabalho. A cada um e a cada uma, deixo o meu reconhecimento e apreço.

"Privacidade não é algo que você precise esconder.
É algo que você tem o direito de proteger."
(Edward Snowden)

RESUMO

Este trabalho analisa a influência da segurança de dados na prática jornalística, com ênfase na proteção e integridade das informações tratadas pelas redações. A pesquisa qualitativa investigou os desafios enfrentados por profissionais de comunicação da Rádio Itatiaia no manejo de dados sensíveis, a aplicação de políticas de segurança digital e o impacto de incidentes cibernéticos na rotina jornalística. Por meio de revisão bibliográfica, análise documental e entrevistas semiestruturadas, buscou-se compreender as estratégias adotadas para garantir a confidencialidade das fontes e a precisão das notícias. Os resultados apontam para a necessidade de aprimoramento contínuo das medidas de segurança e para o papel central da conscientização dos profissionais na proteção das informações, contribuindo para a credibilidade e transparência do jornalismo contemporâneo.

Palavras-chave: segurança de dados; jornalismo; proteção da informação; integridade da notícia; políticas de segurança digital.

ABSTRACT

This paper analyzes the influence of data security on journalistic practice, with emphasis on the protection and integrity of the information handled by newsrooms. The qualitative research investigated the challenges faced by journalists in managing sensitive data, the application of digital security policies, and the impact of cyber incidents on journalistic routines. Through literature review, document analysis, and semi-structured interviews, the study sought to understand the strategies adopted to ensure source confidentiality and the accuracy of news. The results highlight the need for continuous improvement of security measures and the central role of professionals' awareness in protecting information, contributing to the credibility and transparency of contemporary journalism.

Keywords: data security; journalism; information protection; news integrity; digital security policies.

SUMÁRIO

1. INTRODUÇÃO

Essa pesquisa tem como objetivo analisar de que forma a segurança de dados impacta a prática do jornalismo, com ênfase na proteção e integridade das informações. O estudo busca compreender os desafios enfrentados por jornalistas no tratamento de dados sensíveis e como as políticas de segurança são aplicadas na rotina jornalística. A questão de pesquisa que norteia este trabalho é: "Como a segurança de dados influencia a prática do jornalismo em relação à proteção e integridade das informações?". A relevância deste estudo reside na crescente importância da segurança de dados diante do aumento de ameaças cibernéticas e da necessidade de garantir a confidencialidade, a precisão e a transparência das informações jornalísticas. Ao investigar esse tema, procura-se oferecer subsídios teóricos que possam aprimorar as políticas de segurança no jornalismo de dados.

Para compreender de maneira aprofundada a influência da segurança digital na prática do jornalismo e os mecanismos de proteção e integridade das informações, a pesquisa é conduzida a partir de um procedimento metodológico estruturado em etapas inter-relacionadas, com abordagem qualitativa e exploratória. Essa abordagem permite não apenas descrever e analisar as práticas existentes, mas também identificar desafios, oportunidades e estratégias utilizadas na proteção de dados no ambiente jornalístico.

A primeira etapa consiste em uma revisão bibliográfica, cujo objetivo é fundamentar teoricamente a investigação, proporcionando uma visão crítica e contextualizada sobre os conceitos de segurança digital, proteção de dados e seu impacto na atividade jornalística. Para tanto, foram selecionados e analisados criticamente livros, artigos científicos, teses, dissertações, relatórios técnicos e documentos normativos relacionados à segurança da informação e às legislações pertinentes, como o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR) e a Lei Geral de Proteção de Dados (LGPD). Essa revisão permitiu identificar as principais práticas de segurança digital, as diretrizes normativas e as estratégias recomendadas para a proteção da informação jornalística, além de evidenciar lacunas teóricas e questões ainda não suficientemente exploradas na literatura.

Na segunda etapa, realiza-se uma análise documental, com foco em documentos institucionais, políticas de privacidade e diretrizes internas de proteção de dados. Essa fase tem como objetivo examinar, de maneira crítica, como as políticas de segurança digital são implementadas em ambientes jornalísticos, de que forma as legislações vigentes orientam

essas práticas e quais são as vulnerabilidades mais recorrentes no trato da informação sensível. A análise documental contribuiu para a compreensão de como as organizações jornalísticas estruturam suas políticas de proteção de dados e como tais diretrizes se traduzem em medidas concretas de segurança.

A terceira etapa do estudo envolveu a realização de entrevistas semiestruturadas com profissionais que atuam diretamente no campo da comunicação, como jornalistas e editores. As entrevistas aprofundaram a compreensão acerca das experiências práticas desses profissionais em relação aos desafios impostos pela segurança digital, investigando como percebiam e implementavam medidas protetivas no cotidiano das redações. Além disso, buscou-se compreender como incidentes de segurança impactavam a apuração, a produção e a divulgação de notícias, bem como a integridade e a confidencialidade das informações jornalísticas. As entrevistas foram conduzidas com base em um roteiro previamente elaborado, permitindo flexibilidade para explorar aspectos emergentes durante as conversas.

Por fim, os dados coletados ao longo das etapas anteriores são sistematizados e analisados por meio de técnicas de análise qualitativa, com ênfase na análise de conteúdo. Esse procedimento permite a identificação de padrões, convergências e divergências nas percepções e práticas de segurança digital no jornalismo. A análise de conteúdo é realizada a partir de categorias previamente definidas com base no referencial teórico e em categorias emergentes oriundas do próprio material empírico, permitindo uma interpretação densa e multifacetada do objeto de estudo.

A amostra é composta por entrevistas com quatro profissionais da área de comunicação, selecionados intencionalmente com base em sua experiência no manuseio de dados sensíveis e na adoção de práticas de segurança digital. No contexto da pesquisa, optou-se por entrevistar profissionais da Rádio Itatiaia, considerando seu papel de destaque no jornalismo radiofônico brasileiro e sua experiência no trato de informações sensíveis. A escolha da emissora justifica-se pela necessidade de compreender como um veículo de grande alcance e credibilidade lida com os desafios relacionados à segurança digital, especialmente no que se refere à proteção de fontes e à integridade das informações divulgadas.

Os resultados obtidos ao longo da investigação estão consolidados em um relatório de pesquisa detalhado, que sintetiza as principais conclusões e fornece recomendações práticas para o aprimoramento das políticas e práticas de segurança digital no contexto jornalístico. Espera-se que os achados desta pesquisa contribuam não apenas para o campo acadêmico, mas também para a atuação profissional, oferecendo subsídios para a implementação de medidas mais eficazes de proteção de dados e integridade da informação em ambientes de

produção jornalística.

2. METODOLOGIA

Para investigar a influência da segurança digital na prática do jornalismo e na proteção e integridade das informações, esta pesquisa foi desenvolvida por meio de um procedimento metodológico estruturado em quatro fases interligadas, com abordagem qualitativa e caráter exploratório.

Na primeira etapa, foi realizada uma revisão bibliográfica abrangente, com o objetivo de construir uma base teórica sólida sobre os principais conceitos envolvidos. Foram selecionados e analisados criticamente livros, artigos acadêmicos, relatórios técnicos e documentos relevantes sobre segurança digital, proteção de dados e suas implicações no campo jornalístico. Essa etapa permitiu compreender o estado atual do conhecimento, identificar lacunas na literatura e mapear as melhores práticas e estratégias recomendadas.

Em seguida, conduziu-se uma análise documental, que envolveu a coleta e o exame de documentos relacionados a incidentes de segurança que afetaram organizações jornalísticas, bem como a análise de normas, políticas e regulamentos sobre proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) e a Lei Geral de Proteção de Dados (LGPD). Essa etapa possibilitou compreender como tais políticas vêm sendo aplicadas no contexto jornalístico e quais medidas de segurança são sugeridas ou adotadas para garantir a integridade das informações.

Na terceira fase, foram realizadas entrevistas semiestruturadas com jornalistas, editores e outros profissionais da área de comunicação. As entrevistas buscaram compreender, a partir das experiências desses profissionais, como os desafios relacionados à segurança digital são enfrentados na prática do jornalismo, quais estratégias são utilizadas para proteger dados e de que forma os incidentes de segurança impactam o trabalho cotidiano das redações.

Por fim, os dados obtidos nas fases anteriores foram organizados e analisados por meio de análise de conteúdo e análise descritiva. Essa etapa permitiu identificar padrões, tendências, desafios e boas práticas emergentes no que se refere à segurança digital no jornalismo. Com base nos achados, foi elaborado um relatório final que sintetiza os resultados da pesquisa e apresenta recomendações práticas voltadas ao fortalecimento da proteção de dados e da integridade das informações no exercício jornalístico.

3. SEGURANÇA DE DADOS NO CAMPO JORNALÍSTICO

A segurança de dados é um campo multidisciplinar que abrange um conjunto de práticas, políticas, regulamentações e tecnologias voltadas à proteção da informação contra acessos não autorizados, vazamentos, alterações indevidas, perdas e danos. Em um mundo cada vez mais digitalizado, a circulação de informações ocorre em larga escala e em tempo real, sendo impulsionada pelo fenômeno do Big Data, que representa o imenso volume de dados gerados continuamente por indivíduos, organizações e sistemas interconectados. O termo Big Data "passou também a se referir ao grande volume de informações estruturadas e não estruturadas originadas de diversas fontes, com os quais as organizações deveriam fazer uso, visando à melhoria do processo decisório" (Maçada; Brinkhues; Freitas Júnior, 2015, p. 1). A sociedade contemporânea, fortemente dependente da tecnologia, enfrenta desafios complexos quanto à privacidade, transparência e controle de informação, tornando a segurança de dados um dos pilares fundamentais para garantir direitos individuais, a soberania digital e a confiabilidade das relações sociais e econômicas.

Além dos portais das principais redes de rádio e TV, jornais e revistas tradicionais, as redes sociais como Facebook e X (antigo Twitter) também permitem a rápida disseminação de informações. Como afirmam Marcon, Machado e Carvalho (2013, p. 15):

> Por estarem conectadas, todas as informações que os usuários visualizam (notícias, novidades, vídeos, leituras, links, entrevistas, entre outros) podem ser rapidamente compartilhadas, o que vem a caracterizar a participação do sujeito na rede, criando sua identidade no ciberespaço.

Diante do avanço das tecnologias da informação e da comunicação (TICs) e da ascensão da internet, a coleta, o armazenamento e o compartilhamento de dados transformaram-se significativamente, beneficiando o acesso à informação e a qualidade dos serviços digitais. Contudo, esse progresso também evidenciou vulnerabilidades exploráveis por agentes mal-intencionados, o que elevou a proteção dos dados a uma prioridade global.

No Brasil, os primeiros dispositivos legais que tratavam da proteção de dados estão presentes no Código de Defesa do Consumidor (Lei nº 8.078/1990), que já assegurava o direito dos consumidores de acessar e corrigir suas informações em cadastros e bancos de dados. Essa proteção foi reforçada pela Lei Federal nº 9.296/1996, que garantiu a inviolabilidade das comunicações, restringindo seu acesso a casos específicos mediante ordem judicial. Em seguida, o Marco Civil da Internet (Lei nº 12.965/2014) introduziu

princípios essenciais para a governança digital, como a privacidade e a neutralidade da rede, e o Decreto nº 7.962/2013 complementou essas diretrizes ao estabelecer normas sobre segurança da informação em transações eletrônicas (Distrito Federal, [20--]).

No cenário internacional, o interesse pela proteção dos dados tem raízes históricas na década de 1970, quando, na Alemanha, o avanço da computação e o impacto do regime nazista motivaram a criação das primeiras normas regulatórias, culminando em uma legislação formal em 1978 (Distrito Federal, [20--]). Em 1995, a União Europeia avançou ao instituir a Diretiva 95/46/CE, que posteriormente evoluiria para o Regulamento Geral sobre a Proteção de Dados (GDPR – *General Data Protection Regulation*) em 2018. Este regulamento impôs regras rigorosas para o tratamento de dados pessoais e obrigou grandes empresas, como Facebook e Google, a reformularem suas políticas de coleta e uso de informações, servindo de modelo para outras nações, inclusive o Brasil (Distrito Federal, [20--]).

A necessidade de alinhar a legislação brasileira às tendências globais culminou na criação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), sancionada em 2018 e em vigor desde setembro de 2020. Apesar da proteção de dados já estar embutida na Constituição Federal de 1988, que assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas (Brasil, 1988), a LGPD consolidou e ampliou esse arcabouço, estabelecendo princípios como finalidade, necessidade, adequação, transparência, livre acesso, segurança, prevenção e responsabilização. Entre suas inovações, destacam-se a exigência de consentimento explícito para o uso de dados, a criação da Autoridade Nacional de Proteção de Dados (ANPD) e a aplicação de penalidades rigorosas para o descumprimento das normas (Distrito Federal, [20--]).

Em paralelo, o crescente número de ciberataques — que, segundo dados da Forti Labs, registrou 103,16 bilhões de tentativas em 2022, representando um aumento de 16% em relação ao ano anterior — evidencia a necessidade urgente de estratégias de segurança mais eficazes e de um controle regulatório robusto para proteger os dados pessoais contra usos indevidos (Brasil sofreu [...], 2023).

Os impactos da LGPD foram amplos e abrangentes, afetando diversos setores da economia e exigindo uma reestruturação das políticas de governança de dados. Empresas e órgãos públicos precisaram investir na implementação de medidas de conformidade, incluindo a nomeação de um Encarregado de Proteção de Dados (DPO — *Data Protection Officer*), a adoção de políticas de segurança cibernética mais robustas e a realização de auditorias internas para garantir a conformidade com a lei.

Apesar dos avanços, a aplicação da LGPD ainda enfrenta desafios, especialmente em relação à fiscalização e ao cumprimento efetivo das normas. A Autoridade Nacional de Proteção de Dados (ANPD)[1], responsável pela regulamentação e aplicação da lei, tem desenvolvido diretrizes para orientar empresas e usuários sobre boas práticas na proteção de dados.

Nesse contexto, a proteção de dados não se limita apenas ao setor corporativo, mas também se estende a outras áreas críticas, como o jornalismo. A segurança da informação é um elemento essencial para a apuração e divulgação de notícias, garantindo que dados sensíveis e fontes confidenciais sejam resguardados contra acessos não autorizados, adulteração ou destruição. O jornalismo, especialmente o investigativo, lida frequentemente com denúncias e informações sigilosas, tornando indispensável a adoção de medidas rigorosas para evitar vazamentos, manipulações e possíveis represálias contra jornalistas e informantes. Como destaca o Código de Ética dos Jornalistas Brasileiros, é dever do profissional respeitar a privacidade, a honra e a imagem dos indivíduos ao divulgar informações (FENAJ, 1987). A ética, nesse contexto, não deve ser encarada apenas como um princípio subjetivo, mas como um compromisso fundamental do jornalista com a verdade e a responsabilidade social (Christofoletti, 2008).

A proteção de dados no jornalismo vai além de uma preocupação ética; ela é essencial para garantir a integridade do processo informativo e a segurança de jornalistas e fontes. O jornalismo investigativo, em especial, lida frequentemente com denúncias e informações sigilosas, exigindo medidas rigorosas contra vazamentos, manipulações e possíveis represálias. O Código de Ética dos Jornalistas Brasileiros destaca a importância de respeitar a privacidade, a honra e a imagem dos indivíduos ao divulgar informações (FENAJ, 1987), reforçando que a ética não deve ser apenas um princípio subjetivo, mas um compromisso com a verdade e a responsabilidade social (Christofoletti, 2008).

Contudo, o avanço tecnológico tornou esse equilíbrio ainda mais complexo. A instantaneidade da internet e a disseminação de conteúdos digitais enfraquecem as fronteiras entre o interesse público e a exposição indevida. A espetacularização da notícia, como no caso

[1] A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão federal brasileiro responsável por zelar pela proteção de dados pessoais e pela implementação e fiscalização do cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD). A ANPD foi criada pela Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853, de 8 de julho de 2019. A estruturação da ANPD teve início em 28 de dezembro de 2018, quando os artigos referentes à sua constituição entraram em vigor (Brasil, 2024).

da polêmica capa da Revista Veja sobre Cazuza[2], evidencia o dilema entre a liberdade de informação e o respeito à dignidade individual (Karam, 1997). Assim, a decisão de divulgar informações não pode se basear apenas no impacto da notícia, mas também na responsabilidade social do jornalista, que deve equilibrar a busca pela verdade com a proteção dos direitos individuais (Christofoletti, 2008).

Além da questão ética, a segurança da informação no jornalismo envolve também a preservação da integridade e da disponibilidade dos dados. No contexto atual, a manipulação de documentos e a alteração de informações têm o potencial de comprometer seriamente a credibilidade dos veículos de comunicação. Por isso, a adoção de protocolos rigorosos de segurança digital e ferramentas que detectem alterações indevidas se tornou essencial. Ataques cibernéticos, como ransomware[3], representam uma ameaça crescente, não apenas pela possibilidade de bloqueio de acesso aos dados, mas também pelo impacto significativo na continuidade do trabalho investigativo.

Um exemplo notório ocorreu em setembro de 2024, quando o jornal francês *La Croix* e outras publicações do Grupo Bayard sofreram um ataque de ransomware que paralisou suas operações. O incidente comprometeu servidores editoriais, ferramentas de diagramação, sistemas de impressão e até plataformas de comércio eletrônico do grupo, resultando na suspensão temporária da publicação impressa e digital do *La Croix* e de revistas associadas, como *Le Pèlerin* e *J'aime lire*. Durante dias, as equipes de jornalismo precisaram operar em regime emergencial, utilizando redes Wi-Fi e VPNs improvisadas para manter alguma continuidade editorial, enquanto avaliavam a extensão dos danos e buscavam restaurar os sistemas críticos (Le Monde, 2024; FranceTV Info, 2024). Dessa forma, proteger dados no jornalismo vai além de evitar distorções; trata-se de garantir a confiança, a acessibilidade e a responsabilidade social das informações transmitidas.

No Brasil, episódios semelhantes já ocorreram. Em 2022, a RecordTV foi alvo de um ransomware que criptografou arquivos internos, derrubou sistemas de e-mail e interrompeu transmissões ao vivo, obrigando a emissora a alterar sua grade de programação por dias enquanto trabalhava na recuperação dos dados (WeLiveSecurity, 2022). Além disso, dados pessoais de ex-funcionários foram expostos, configurando uma violação da Lei Geral de

[2] Em abril de 1989, a revista *Veja* publicou em sua edição n.º 1.077 a capa com a manchete "Cazuza - uma vítima da AIDS agoniza em praça pública", acompanhada de uma imagem do cantor visivelmente debilitado. A reportagem gerou intensa repercussão por expor sua condição de saúde de maneira considerada sensacionalista.

[3] Ransomware é um tipo de software malicioso projetado para bloquear ou criptografar o acesso aos dados de um sistema, exigindo um resgate para restaurar a normalidade. Ameaças como o ransomware têm se tornado um risco crescente para organizações de diversos setores, incluindo o jornalismo, comprometendo dados sensíveis e afetando a continuidade de operações essenciais, como reportagens investigativas.

Proteção de Dados (LGPD), que estabelece normas para a proteção de informações pessoais. Este incidente evidencia a necessidade de conformidade com o Art. 46 da LGPD, que determina que os agentes de tratamento adotem medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou divulgação (Lei nº 13.709/2018, Art. 46). A falta de políticas de segurança eficazes e de planos de resposta a incidentes expõe as organizações a sanções administrativas, como advertências, multas e até a suspensão de atividades de tratamento de dados (ANPD, 2022). Assim, além do impacto operacional e financeiro, ataques cibernéticos envolvendo dados pessoais trazem graves riscos jurídicos e reputacionais, reforçando a importância de medidas preventivas robustas e conformidade com a LGPD para proteger tanto os dados quanto a confiança do público.

A interação com o público também impõe desafios consideráveis em termos de segurança de dados. Muitos veículos de comunicação coletam informações sensíveis de leitores, como hábitos de leitura, preferências e dados financeiros relacionados a assinaturas. A proteção desses dados é crucial para assegurar que informações pessoais não sejam expostas, mal utilizadas ou vulneráveis a vazamentos. Isso exige o cumprimento de regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, que estabelecem diretrizes claras para o uso ético e seguro de informações pessoais. Assim, a segurança da informação no jornalismo deve se estender não apenas ao conteúdo produzido, mas também ao manejo responsável das informações coletadas dos usuários.

Outro aspecto crítico no contexto atual é a disseminação de desinformação e os ataques coordenados contra jornalistas, especialmente em plataformas digitais e redes sociais. A crescente polarização das opiniões públicas e a proliferação de fake news têm implicações diretas na qualidade e na confiança do jornalismo. A segurança de dados deve, portanto, incluir estratégias de verificação da autenticidade das informações compartilhadas, utilizando ferramentas avançadas de monitoramento e algoritmos para detectar conteúdos falsos. O combate a ataques digitais e a desinformação tornou-se uma prioridade para garantir que a liberdade de imprensa não seja corroída por campanhas orquestradas de manipulação de informações. A preocupação com a qualidade e veracidade da informação, que já era debatida no final do século XIX, permanece atual. Warren e Brandeis, ao discutirem os limites da liberdade de imprensa e a invasão da privacidade na era da comunicação massiva, alertaram para os perigos da utilização irresponsável da informação para fins sensacionalistas: “A fofoca não é mais um recurso do preguiçoso e do imoral, mas se tornou um negócio, que é

conduzido com diligência e descaramento" (Warren; Brandeis, 1890, p. 196). Esses desafios contemporâneos exigem uma abordagem estratégica para equilibrar a liberdade de expressão com a responsabilidade jornalística e a proteção dos dados.

Além dos riscos associados à desinformação e aos ataques coordenados, destaca-se a necessidade urgente de adoção de boas práticas de segurança digital por jornalistas, sobretudo os que atuam com reportagens investigativas ou coberturas sensíveis. A despeito da crescente percepção do risco, pesquisas apontam que muitos profissionais ainda não adotam sequer medidas básicas de proteção, como autenticação de dois fatores, uso de senhas fortes, criptografia de comunicações ou segregação de contas em dispositivos. Conforme destacado por especialistas como Robert Guerra (Digital Security, 2013), do Citizen Lab, e instituições como a Freedom of the Press Foundation[4], pequenas ações já podem reduzir significativamente a vulnerabilidade digital, protegendo não apenas o jornalista, mas também suas fontes. Ferramentas e guias como os oferecidos pela Repórteres Sem Fronteiras, Commitee to Protect Journalists (CPJ[5]) e Access Now desempenham um papel fundamental na disseminação de boas práticas, especialmente entre *freelancers* e jornalistas que não contam com uma estrutura institucional robusta. Essa realidade evidencia que a segurança da informação no jornalismo vai além da infraestrutura técnica: ela exige formação continuada, cultura organizacional e protocolos de resposta a incidentes, inserindo-se diretamente na discussão sobre liberdade de imprensa, proteção de dados e responsabilidade ética na era digital.

Diante desse cenário, a segurança de dados no jornalismo não é apenas uma necessidade técnica, mas um pilar essencial para garantir a credibilidade da imprensa e a segurança dos envolvidos no processo de apuração e divulgação de informações. O investimento em boas práticas de proteção digital, aliado ao uso de tecnologias avançadas e à conformidade com normas de privacidade e segurança, é indispensável para que o jornalismo continue exercendo sua função essencial de informar a sociedade, fiscalizar o poder e dar voz a quem precisa ser ouvido, sem colocar em risco aqueles que contribuem para a construção da verdade.

---

[4] A Freedom of the Press Foundation oferece treinamentos, ferramentas e recursos voltados à segurança digital no jornalismo, incluindo o uso de criptografia e boas práticas de proteção de fontes.

[5] O Committee to Protect Journalists (CPJ) é uma organização independente, sem fins lucrativos, sediada em Nova York, dedicada à promoção da liberdade de imprensa e à proteção de jornalistas em todo o mundo. A entidade fornece apoio a profissionais ameaçados, documenta ataques à liberdade de imprensa e atua em campanhas para responsabilização de governos e instituições.

4. PLATAFORMIZAÇÃO

A disseminação de informações em ambientes digitais tem sido influenciada por plataformas digitais que operam em mediação algorítmica como Facebook e Google. Essas, por sua vez, utilizam sistemas automatizados que filtram, organizam e recomendam conteúdos com base em dados e no comportamento dos usuários, modificando profundamente o modo como a informação é mediada. Esse processo, conhecido como governança algorítmica (Castro, 2018), implica a substituição parcial das decisões editoriais humanas por regras automatizadas que priorizam conteúdos segundo padrões definidos por algoritmos.

Esse fenômeno se insere no contexto do capitalismo de plataforma (Srnicek, 2017 *apud* Silva Neto, 2019), um modelo econômico no qual os dados são o principal ativo, e as plataformas buscam maximizar o engajamento e a retenção dos usuários para ampliar lucros. Nesse ambiente, diferentes tipos de conteúdo — desde notícias jornalísticas até postagens pessoais e publicidade — competem pela atenção em um mesmo espaço digital, sendo exibidos segundo critérios algorítmicos que nem sempre privilegiam a qualidade ou a veracidade.

A coexistência desses conteúdos variados dificulta a distinção entre informações verificadas e conteúdos potencialmente enganosos, o que contribui para a circulação de desinformação e notícias falsas — fenômenos que têm recebido crescente atenção acadêmica devido ao seu impacto social (Wardle; Derakhshan, 2017). Enquanto o jornalismo tradicional pauta-se por valores como precisão, relevância e rigor na verificação (Galtung; Ruge, 1965), as plataformas digitais operam com base em "valores-algoritmo" (Castro, 2019b), que refletem objetivos técnicos e comerciais, priorizando a personalização e a performance dos conteúdos para aumentar a interação dos usuários. Segundo Gillespie (2014), esses valores correspondem aos critérios embutidos nos algoritmos que determinam quais conteúdos são promovidos ou suprimidos nas plataformas digitais. Diferentemente dos valores jornalísticos, os valores-algoritmo privilegiam objetivos técnicos e comerciais, como a maximização do engajamento dos usuários, a personalização dos conteúdos e o aumento do tempo de permanência nas plataformas. Assim,

> os algoritmos não apenas classificam ou organizam o conteúdo, mas incorporam valores específicos que influenciam quais conteúdos são amplificados e quais são marginalizados, frequentemente priorizando o engajamento e interesses comerciais em detrimento da qualidade jornalística ou da precisão factual (Gillespie, 2014, p. 171).

É importante retomar as origens e transformações do conceito de plataforma. Antes da ascensão dos gigantes da tecnologia, no início dos anos 2000, empresas como Microsoft, Intel e Cisco já exemplificam plataformas como mercados de dois lados, conectando desenvolvedores e consumidores e gerando valor por meio dos efeitos de rede (Gawer; Cusumano, 2014; Rochet; Tirole, 2002). Essa perspectiva econômica influenciou profundamente os modelos de negócios digitais atuais.

No campo da comunicação, a noção de plataforma ganhou nova conotação com a Web 2.0, termo cunhado por Tim O'Reilly (2005) para descrever a internet como espaço de participação ativa dos usuários. Pesquisadores como Jenkins (2009) e Benkler (2006) destacaram o potencial das plataformas para fomentar culturas colaborativas e democratizar a produção de conteúdo. Porém, estudos posteriores apontam que esse discurso de participação muitas vezes esconde os interesses comerciais e o controle exercido pelas plataformas, que se baseiam na coleta massiva de dados pessoais para monetização (Van Dijck; Nieborg, 2009).

O conceito de plataformização é, portanto, fundamental para entender não só o avanço tecnológico, mas também as mudanças políticas, econômicas e culturais que as plataformas promovem. Plataformização refere-se ao processo pelo qual setores diversos da sociedade — como mídia, comércio e educação — estruturam suas atividades em torno de plataformas digitais dominadas por algoritmos e sistemas proprietários, que moldam a produção, distribuição e consumo de conteúdo.

Segundo Gillespie (2010), o termo "plataforma" é estratégica e deliberadamente ambíguo: embora sugira neutralidade e abertura, ele oculta relações de poder reais e decisões intencionais sobre moderação, priorização de conteúdo, coleta de dados e regras econômicas que afetam diretamente a visibilidade dos conteúdos e a remuneração de seus produtores. Nas obras *The Politics of 'Platforms'* (2010) e Custodians of the Internet (2019), Gillespie afirma que a metáfora da plataforma é utilizada pelas empresas para se apresentarem como meros canais "técnicos, econômicos e culturais" (Gillespie, 2010, p. 10), mas essas organizações simultaneamente "fazem escolhas sobre o que os usuários veem e dizem" (Gillespie, 2018, p. 360), minando a suposta imparcialidade.

Além disso, estudos computacionais e técnicos — como os de Montfort e Bogost (2009) e Helmond (2015) — contribuíram com uma abordagem que enfatiza a dimensão material e programável das plataformas digitais. Essa perspectiva entende as plataformas não apenas como espaços de interação ou modelos de negócio, mas como infraestruturas técnicas concretas, compostas por camadas de hardware (servidores, dispositivos, redes) e software

(códigos, APIs, algoritmos) que operam de maneira programável. Ou seja, são sistemas projetados para executar tarefas específicas, como a coleta, o processamento e a análise de grandes volumes de dados, muitas vezes de forma automatizada. Essa arquitetura técnica, altamente modular, viabiliza a criação de ecossistemas interconectados, nos quais diferentes serviços de terceiros operam sob regras definidas pelas plataformas. Com isso, as empresas responsáveis por essas infraestruturas mantêm o controle sobre os fluxos de informação, a integração de novos serviços e os mecanismos de monetização — elementos centrais para entender o funcionamento interno e o alcance dessas tecnologias na sociedade contemporânea.

Diante das múltiplas abordagens — econômicas, comunicacionais e computacionais —, a plataformização pode ser compreendida como um processo que transforma profundamente a organização das interações sociais, culturais e econômicas no ambiente digital. Nesse contexto, plataformas são entendidas como infraestruturas digitais programáveis, ou seja, sistemas técnicos compostos por camadas de hardware e software configuráveis, que permitem o desenvolvimento, a integração e o controle de serviços e funcionalidades por meio de códigos, interfaces de programação de aplicações (APIs) e algoritmos. Essas infraestruturas não são neutras porque, como afirmam Van Dijck, Nieborg e Poell, elas funcionam como "infraestruturas sociais onde hierarquias e dependências estão construídas em sua arquitetura" — ou seja, mesmo antes de qualquer uso, já impõem relações de poder, controle e visibilidade predefinidas (van Dijck, Nieborg & Poell, 2019, p. 1). Em outras palavras, decisões técnicas — como quais APIs serão disponibilizadas, como os algoritmos ranqueiam e recomendam conteúdo, e quais dados são coletados e para que fins — definem quem pode participar, quais informações são visíveis ou ocultas, e como os fluxos de comunicação e dados são controlados. Essa orientação técnica e institucional embutida nas plataformas molda o acesso e as possibilidades de monetização, mesmo que os códigos e estruturas pareçam neutros à primeira vista.

Anne Helmond (2015) observa que a plataformização envolve a expansão das plataformas de mídia social para o restante da web e o esforço contínuo dessas empresas para tornar os dados externos "prontos para a plataforma" (Helmond, 2015, p. 1). Nesse processo, as APIs desempenham um papel central ao transformar sites de redes sociais em plataformas de mídia social, descentralizando a produção de dados, mas recentralizando sua coleta e controle. Essa mediação ocorre principalmente por meio de algoritmos, que organizam e filtram as interações — como nos mecanismos de recomendação, ranqueamento de conteúdo e moderação automatizada — influenciando diretamente comportamentos, percepções e

decisões dos usuários.

É exatamente a partir dessa complexa articulação técnica e econômica que a análise se volta para a plataformização no jornalismo, com ênfase nas suas implicações para a segurança de dados. Ao operar em ambientes mediados por infraestruturas digitais proprietárias, o jornalismo se vê inserido em um ecossistema onde os modelos técnicos e econômicos das plataformas impactam diretamente a proteção das informações sensíveis. Isso inclui a integridade e confidencialidade das fontes jornalísticas, os dados produzidos pelas redações e os rastros informacionais deixados pelas audiências. Assim, a inserção do jornalismo nesse contexto amplia as camadas de risco relacionadas a vazamentos, rastreamento e uso indevido de dados, especialmente em um cenário marcado pela vigilância estatal, ataques cibernéticos e exploração comercial dessas informações.

Essa dinâmica de exposição a riscos também se relaciona com a forma como redações e veículos jornalísticos utilizam infraestruturas digitais operadas por grandes empresas de tecnologia, como Google e Meta. Ao adotarem essas plataformas para viabilizar a distribuição de conteúdo, engajamento de audiência e estratégias de monetização, os meios de comunicação passam a operar dentro de sistemas cujos parâmetros técnicos e lógicos são definidos externamente ao campo jornalístico. Como observa Rogério Christofoletti (2025), essa relação envolve condições assimétricas, nas quais os veículos de comunicação recorrem a ferramentas e serviços oferecidos por grandes empresas de tecnologia — como mecanismos de busca, redes sociais, sistemas de gerenciamento de conteúdo e ferramentas de análise de dados — para garantir que suas reportagens sejam encontradas, compartilhadas e acessadas pelo público. Isso significa, por exemplo, usar o Google Analytics para monitorar o tráfego no site, publicar conteúdos por meio do Facebook ou Instagram para alcançar mais leitores, ou adaptar formatos de notícia para atender aos critérios de ranqueamento dos buscadores. Tais escolhas tornam-se parte das estratégias de inserção e permanência desses veículos no ambiente digital, moldando a forma como produzem, distribuem e analisam o conteúdo jornalístico em um ecossistema regido por regras e infraestruturas que não são definidas pelo próprio campo da comunicação.

Essa dependência não se limita aos aspectos técnicos ou operacionais. Iniciativas como o Google News Initiative (GNI) e o Meta Journalism Project (MJP) consistem em programas voltados ao apoio e desenvolvimento do jornalismo digital, oferecendo treinamentos, ferramentas, financiamento e parcerias com redações. No entanto, esses programas são estruturados a partir das próprias plataformas dessas empresas, o que implica que, para participar das iniciativas, os veículos de mídia precisam operar dentro dos

ecossistemas tecnológicos oferecidos por Google e Meta. Isso inclui, por exemplo, o uso de ferramentas de analytics, hospedagem de conteúdo em formatos proprietários, integração com sistemas de recomendação, anúncios e monetização. Dessa forma, as práticas jornalísticas passam a ser, em parte, mediadas por soluções fornecidas por essas corporações, o que pode ter implicações tanto para o controle sobre os fluxos informacionais quanto para a gestão e segurança dos dados produzidos e armazenados nesse ambiente.

A lógica da plataformização envolve estruturas técnicas e econômicas que não são neutras. Grandes empresas de tecnologia, como Google e Meta, operam com modelos de negócios sustentados pela coleta, processamento e análise de grandes volumes de dados, prática central para a geração de valor econômico nessas plataformas (Gillespie, 2018; Srnicek, 2017 *apud* Silva Neto, 2019; OECD, 2020). Isso inclui, entre outros, os dados gerados por atividades jornalísticas. Informações como pautas, listas de fontes, documentos internos e investigações em andamento são frequentemente produzidas, armazenadas e compartilhadas por meio de ferramentas dessas empresas, inserindo-se em sistemas cujo controle não pertence às redações (Marwick; Lewis, 2017).

Ferramentas como Google Docs e Google Drive, por exemplo, são utilizadas para redação colaborativa e armazenamento de arquivos jornalísticos. Segundo os Termos de Serviço e a Política de Privacidade do Google, os dados armazenados nesses serviços podem ser analisados automaticamente para fins como manutenção e aprimoramento dos produtos. Embora a empresa afirme que não utiliza o conteúdo desses documentos para fins publicitários, ela realiza o processamento técnico dessas informações — o que inclui a coleta de metadados, como histórico de edição, autoria, além de informações sobre dispositivos e padrões de uso (Google, 2023; Google, [20--]a).

De forma semelhante, o Gmail processa automaticamente os dados das mensagens — mesmo aquelas criptografadas em trânsito — para prover funcionalidades como categorização e detecção de spam. Embora o conteúdo em si não seja utilizado para publicidade personalizada, os metadados de comunicação (remetente, destinatário, horário de envio, etc.) são coletados, armazenados e associados a outras atividades do usuário na conta Google.

O Facebook Creator Studio, da Meta, é uma plataforma usada para gerenciar e analisar publicações em redes sociais. Ao utilizá-la, jornalistas e organizações de mídia compartilham dados sobre o desempenho de postagens, horários de publicação, formatos de conteúdo e padrões de engajamento com a audiência. Esses dados são processados pela plataforma e alimentam os sistemas de recomendação e entrega de conteúdo da empresa, que, por sua vez, definem quais postagens têm maior alcance.

No caso do WhatsApp Business, também operado pela Meta, embora as mensagens sejam protegidas por criptografia de ponta a ponta, o aplicativo coleta e compartilha com o restante do ecossistema Meta dados como número de telefone, dados de uso, informações do dispositivo e horário de interação. Esses elementos são utilizados para fornecer serviços, prevenir abusos e integrar funcionalidades com outras plataformas da empresa, como Facebook e Instagram.

A utilização contínua dessas ferramentas por jornalistas insere as operações jornalísticas em infraestruturas tecnológicas que operam com lógicas próprias, nas quais o controle dos dados fica centralizado em plataformas externas (Marwick; Lewis, 2017; Gillespie, 2018). Esse processo envolve o armazenamento e o processamento de informações em servidores que não pertencem às organizações jornalísticas, o que pode representar desafios significativos para a proteção da confidencialidade das fontes, para o controle dos fluxos informacionais e para a integridade dos documentos sensíveis (Kaye, 2019; Google, 2023).

Além disso, a inserção das *big techs* no ecossistema jornalístico também ocorre por meio de aportes financeiros e parcerias institucionais estruturadas em programas específicos. Um exemplo é o Google News Initiative (GNI), lançado pelo Google em 2018, que oferece financiamento, treinamento e suporte técnico a organizações de mídia em diversos países, com o objetivo de fortalecer o jornalismo na era digital. A Meta, por sua vez, desenvolve iniciativas como o Meta Journalism Project, que inclui programas de aceleração, doações diretas e parcerias para o desenvolvimento de produtos com redações locais e internacionais.

Esses aportes ocorrem na forma de editais de inovação, subsídios para projetos de transformação digital e programas de capacitação técnica que envolvem o uso de produtos e serviços das próprias plataformas — como Google Analytics, Facebook Audience Network, entre outros. Embora esses programas sejam apresentados como iniciativas de apoio ao jornalismo, eles também criam vínculos duradouros entre as organizações jornalísticas e as infraestruturas técnicas e comerciais das *big techs*. Na prática, isso pode influenciar a autonomia editorial e estratégica das redações, ao condicionar parte de sua sustentabilidade financeira e operacional ao acesso a esses recursos. Como afirma Christofoletti, “injetar recursos nas organizações do setor acaba atraindo a simpatia de editores e eventualmente inibindo coberturas mais críticas e severas sobre os negócios e estratégias das big techs” (Christofoletti, 2025, p. 13). Esse tipo de influência compromete o papel fiscalizador da imprensa, ao enfraquecer sua capacidade de investigar criticamente justamente os atores que hoje concentram uma parcela significativa do poder informacional global. A função

fiscalizadora da mídia pressupõe independência editorial para questionar, denunciar e escrutinar os diversos centros de poder. No entanto, quando organizações jornalísticas passam a depender de recursos — financeiros, técnicos ou de capacitação — fornecidos por grandes plataformas digitais, cria-se uma relação assimétrica que pode afetar essa autonomia.

Um aspecto particularmente relevante nessa relação diz respeito ao direito autoral e à reprodução de conteúdo jornalístico. Na Espanha, por exemplo, o Google News foi desativado em 2014 após a aprovação de uma lei de "direitos conexos", que obrigava agregadores como o Google a pagar uma taxa fixa por reproduzir notícias — o chamado "ancillary copyright"(Eletronic Frontier Foundation, 2014). Posteriormente, com a transposição da Diretiva Europeia de Direito de Autor, que passou a permitir negociações diretas entre plataformas e veículos, o Google News pôde retornar ao país em 2021 (Euronews, 2021).

Outro caso importante ocorreu na Austrália. A partir de 2021, vigora o News Media Bargaining Code, que obriga plataformas como Google e Meta a negociar pagamentos justos com veículos de notícias locais ou enfrentar sanções — inclusive a designação compulsória por parte do Tesouro australiano. Isso levou o Facebook a bloquear notícias no país como forma de protesto, gerando forte impacto no ecossistema editorial até que concessões ao texto do código fossem acordadas. Mesmo assim, o governo australiano seguiu firme em sua política, agora considerando até impor um imposto sobre plataformas que não fecharem acordos — medida que pode entrar em vigor em 2025 (The Guardian, 2021).

Esses exemplos ilustram como a relação entre jornalismo, direito autoral e as grandes plataformas digitais é complexa, permeada por tensões entre modelos de negócio, regulação estatal e a preservação da independência editorial. A função fiscalizadora da mídia pressupõe autonomia para questionar, denunciar e escrutinar os diversos centros de poder — algo que pode ficar comprometido quando as próprias fontes de financiamento e infraestrutura técnica são as plataformas sob análise.

Nesse cenário, a segurança de dados não se restringe apenas à proteção técnica de informações sensíveis, mas adquire também uma dimensão ética e política. A proximidade entre redações e *big techs* pode gerar efeitos sutis e cumulativos, como censura indireta, autocensura e omissão editorial. Esses efeitos nem sempre são explícitos ou impostos, mas podem surgir como reflexo da dependência estrutural em relação a essas plataformas, comprometendo a capacidade da imprensa de cumprir seu papel público de maneira plena e crítica.

Esse cenário se torna ainda mais complexo com a entrada em vigor de iniciativas regulatórias como o Digital Markets Act (DMA) e o Digital Services Act (DSA), aprovados pela União Europeia e aplicados de forma plena a partir de 2024. Essas legislações representam uma tentativa inédita de impor limites concretos ao poder das grandes plataformas digitais, regulando sua atuação comercial e sua responsabilidade sobre conteúdos e dados. Embora sejam consideradas um avanço na proteção da concorrência e dos direitos digitais, as medidas foram recebidas com forte resistência pelas *big techs*, que alegam impacto negativo sobre a inovação, custos elevados de conformidade e riscos à privacidade e à segurança operacional.

No Brasil, o Projeto de Lei n.º 2.630/2020, conhecido como "PL das Fake News", visa ampliar a transparência das plataformas digitais em temas como moderação de conteúdo, publicidade e proteção de dados. No entanto, sua tramitação enfrentou forte resistência das próprias *big techs*, que chegaram a utilizar suas infraestruturas para veicular mensagens contra o projeto. Em 2023, empresas como Google e Spotify foram acusadas por órgãos públicos e pesquisadores de promover uma campanha de desinformação institucionalizada contra a proposta, usando espaços privilegiados — como a página inicial do Google Search — para divulgar conteúdos tendenciosos (Agência Estado, 2023; STF determina [...], 2023). "Google, Spotify e outras plataformas deixaram seus cômodos lugares para espalhar anúncios contrários ao projeto de lei em flagrante campanha de desinformação" (Christofoletti, 2025, p. 15), observa o autor, ressaltando o paradoxo de empresas que se apresentam como defensoras da informação confiável atuarem de maneira opaca e politicamente engajada.

A presença da inteligência artificial (IA) nas rotinas jornalísticas tem sido incorporada com o objetivo de automatizar tarefas, reduzir custos e aprimorar a produtividade. Ferramentas de IA são utilizadas para redigir textos, organizar grandes volumes de dados, classificar conteúdos e até sugerir pautas com base em métricas de engajamento. Paralelamente, essa tecnologia também pode ser empregada para gerar conteúdos sintéticos que imitam o estilo jornalístico, muitas vezes de forma automatizada e sem supervisão humana. Como observa Christofoletti, "a Inteligência Artificial pode contribuir para a geração de textos e dados, pode auxiliar a tomar decisões editoriais e pode, igualmente, produzir e espalhar desinformação em escalas inimagináveis" (Christofoletti, 2025, p. 15).

No contexto prático, o uso de IA no jornalismo apresenta riscos concretos. Em 2023, a CNET interrompeu a publicação de artigos gerados por IA após identificar erros factuais e indícios de plágio, mostrando a fragilidade de processos automatizados sem supervisão humana (WIRED, 2023). De forma semelhante, a Gannett suspendeu sua ferramenta de

resumos esportivos automatizados depois que textos gerados produziram conteúdos absurdos e imprecisos, evidenciando falhas estilísticas e de verificação (Washington Post, 2023). Além disso, há um crescimento acelerado de sites noticiosos criados por IA, com pouca ou nenhuma supervisão humana, que republicam boatos e conteúdos reciclados visando receita publicitária, criando vetores de desinformação institucionalizada (NewsGuard, 2024).

Nesse contexto, o uso da IA no jornalismo não levanta apenas questões técnicas, mas também exige atenção aos fundamentos que orientam a prática jornalística: como garantir que princípios como veracidade, acurácia, contextualização e responsabilidade editorial continuem sendo observados em processos mediados por algoritmos? A dificuldade de compreender e auditar o funcionamento dessas tecnologias coloca desafios para a manutenção dos critérios que tradicionalmente distinguem o jornalismo de outras formas de produção de informação.

Em suma, a plataformização do jornalismo implica uma série de dilemas para a segurança de dados e para a integridade da prática jornalística. A presença cada vez mais intensa das *big techs* nas redações não é neutra, tampouco benéfica em todos os aspectos. Se, por um lado, essas empresas oferecem ferramentas e recursos para a manutenção das atividades jornalísticas, por outro, condicionam o exercício profissional a infraestruturas tecnológicas que operam sob lógicas de mercado alheias ao interesse público. Como afirma Christofoletti, “o desafio para editores e jornalistas não é só evitar a extinção da sua atividade, mas também escolher e inventar sua sobrevida” (Christofoletti, 2025, p. 15). Essa sobrevida precisa necessariamente ser construída com soberania tecnológica, com políticas de proteção de dados robustas e com um posicionamento crítico diante das plataformas que moldam o presente e o futuro da informação. A relação com a segurança de dados se torna central nesse contexto, uma vez que dependência de plataformas externas e sistemas programáveis aumenta o risco de vazamentos, ataques cibernéticos, manipulação de conteúdo e comprometimento da confidencialidade das fontes. Garantir a proteção de arquivos, fluxos de informação e metadados é essencial não apenas para a continuidade operacional das redações, mas também para preservar a confiança do público e a integridade do processo informativo, prevenindo que a tecnologia se torne um vetor de vulnerabilidade em vez de suporte editorial.

5. INTERAÇÃO COM O PÚBLICO

O avanço do jornalismo digital tem promovido o aumento significativo da interação entre veículos de comunicação e o público, resultando na geração de grandes volumes de dados pessoais e informações sensíveis. Esses dados, provenientes de comentários, cadastros e outras formas de participação online, demandam uma gestão rigorosa para garantir a segurança da informação e a proteção da privacidade dos usuários (Solove, 2006). A implementação de normas e legislações específicas, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, tem estabelecido parâmetros para o tratamento ético e legal dessas informações (União Europeia, 2016). Situações semelhantes emergem em outras regiões do mundo: em países africanos, por exemplo, redações enfrentam não apenas os desafios da proteção de dados, mas também ataques cibernéticos e bloqueios governamentais que comprometem a privacidade dos usuários e a integridade do jornalismo digital (Quartz, 2021; RSF, 2020).

Nesse contexto, redações e organizações jornalísticas precisam adotar práticas e políticas adequadas para o manejo e a preservação dos dados coletados durante as interações digitais, a fim de assegurar a confiança dos públicos e cumprir com os requisitos legais vigentes. A gestão segura desses dados torna-se um componente essencial para a sustentabilidade da comunicação digital e para a proteção dos direitos dos indivíduos envolvidos (Hermida, 2010; Usher, 2014). A interação entre jornalistas e público passou por transformações ao longo das últimas décadas, acompanhando a evolução do jornalismo e a incorporação gradual das tecnologias digitais nas redações. A internet possibilitou o surgimento de novos canais de comunicação, como comentários online, redes sociais, enquetes e compartilhamentos, que ampliaram as formas pelas quais o público pode manifestar-se diretamente. Embora a comunicação entre veículos e audiência já ocorresse anteriormente por meio de cartas, telefonemas e outras modalidades, esses métodos apresentavam restrições relacionadas à abrangência, ao tempo de resposta e à simultaneidade das interações. As plataformas digitais, por sua vez, ampliaram o alcance, a diversidade e a velocidade dessas manifestações, alterando o contexto da comunicação jornalística.

Esse cuidado é ainda mais crítico em regiões onde redações são alvo frequente de campanhas de desinformação, ataques de negação de serviço (DDoS) e vigilância estatal, como relatado em países da África Subsaariana e do Norte da África (Dark Reading, 2024).

O que se observa é a permanência de uma cultura jornalística sustentada por rotinas

rígidas, por uma divisão assimétrica de papéis e pelo privilégio dado a determinadas vozes no processo de produção da notícia. Essa constatação é reforçada por Traquina em *Porque as notícias são como são* (2005) ao demonstrar que as notícias não são simples reflexos da realidade, mas sim construções narrativas moldadas por filtros institucionais, critérios de seleção e convenções do campo jornalístico. Segundo o autor, os jornalistas tendem a se guiar mais pelos acontecimentos visíveis — os chamados eventos noticiáveis — do que por problemáticas sociais de fundo, o que favorece a cobertura episódica e descontextualizada em detrimento de análises aprofundadas.

Esse modo de produção impacta diretamente a qualidade da interação com o público. Embora a audiência contemporânea esteja mais conectada e participativa, as práticas editoriais das redações digitais frequentemente utilizam as manifestações do público — como comentários, curtidas e compartilhamentos — principalmente como indicadores de engajamento ou métricas de audiência, sem que esses dados influenciem significativamente o processo editorial. Conforme Napoli, “as métricas digitais, apesar de sua importância para as estratégias comerciais e de engajamento, raramente traduzem-se em mudanças estruturais na agenda editorial” (Napoli, 2011, p. 58). Anderson também destaca que, mesmo com o aumento da interação digital, “a dinâmica interna das redações mantém o controle sobre a seleção e o enquadramento das pautas, limitando o impacto real da participação do público” (Anderson, 2013, p. 103).

No que diz respeito à comunicação entre jornalistas e público, os canais digitais — como redes sociais, formulários online e outras plataformas interativas — são cada vez mais usados para coletar informações e fomentar o diálogo. Hermida afirma que “o jornalismo digital tem expandido o conceito tradicional de audiência para uma rede ativa de participantes que geram e consomem informação simultaneamente” (Hermida, 2010, p. 299). No entanto, essa expansão traz desafios quanto ao manejo e à proteção dos dados pessoais, tema fundamental no jornalismo contemporâneo. Usher ressalta que “a coleta e o uso de dados digitais exigem uma atenção rigorosa às questões éticas e de segurança da informação, que ainda são pouco discutidas nas redações” (Usher, 2014, p. 45).

Castells (2010) observa que, mesmo com a ampliação dos canais digitais e a diversificação das plataformas de comunicação, a lógica dos meios de massa continua, em muitos casos, sendo mantida. A interatividade oferecida ao público limita-se, frequentemente, à resposta de consumo, ou seja, ao modo como a audiência reage em termos de cliques, tempo de permanência e viralização de conteúdos — e não à sua participação real no processo de construção do jornalismo. Isso gera uma tensão constante entre o ideal democrático que a

internet sugere e a realidade operacional das redações, ainda pautada por lógicas empresariais, critérios comerciais e estruturas hierárquicas.

Nesse contexto, o jornalismo contemporâneo enfrenta um duplo desafio: por um lado, precisa manter sua credibilidade e relevância em um cenário marcado por excesso de informações, fake news e disputas narrativas; por outro, deve desenvolver formas mais efetivas e democráticas de escutar, incluir e dialogar com sua audiência. A superação desse impasse passa por mudanças tanto nas rotinas de apuração quanto nos modelos de negócio e nas culturas organizacionais dos meios de comunicação. Trata-se de reconhecer o público não apenas como consumidor, mas como sujeito ativo e participante do ecossistema informativo.

Assim, a transformação da relação entre jornalistas e público depende de uma reconfiguração profunda das práticas jornalísticas, que incorpore a escuta ativa, a pluralidade de vozes e a transparência dos processos como elementos centrais. Segundo Deuze, o jornalismo participativo pressupõe um ambiente em que “a audiência não apenas consome, mas também contribui para a construção do conteúdo, ampliando a diversidade de perspectivas e fortalecendo o diálogo social” (Deuze, 2007, p. 272). Contudo, para que essa transformação seja efetiva, é necessário reconhecer que as interações digitais geram um volume significativo de dados — incluindo informações pessoais, comportamentais e contextuais — que exigem um manejo responsável e transparente (Usher, 2014; McStay, 2018).

Esses dados, produzidos por meio de comentários, compartilhamentos, cadastros e outras formas de participação online, têm implicações diretas na gestão da privacidade e na segurança da informação. Conforme aponta McStay, “a coleta massiva de dados digitais cria novos desafios éticos e técnicos para os meios de comunicação, que precisam equilibrar a participação do público com a proteção dos direitos individuais” (McStay, 2018, p. 44). Dessa forma, avançar no debate sobre a relação jornalística com o público implica também discutir as políticas e tecnologias aplicadas ao tratamento desses dados, para garantir um ambiente comunicacional que seja ao mesmo tempo inclusivo e seguro.

6. ANÁLISE QUALITATIVA

Fundada em 20 de janeiro de 1952 pelo jornalista e radialista Januário Laurindo Carneiro, a Rádio Itatiaia é considerada a principal emissora de Minas Gerais e uma das três mais influentes do Brasil. Com uma trajetória marcada pelo pioneirismo e pela credibilidade, a Itatiaia conquistou espaço e relevância no cenário nacional, sendo referência em jornalismo esportivo, político e de cidades. Desde a cobertura do Campeonato Sul-Americano de 1959, na Argentina, até sua presença constante em todas as Copas do Mundo desde 1966, a emissora construiu uma identidade comprometida com a informação, a independência editorial e o serviço à população mineira.

Segundo informações divulgadas no site oficial da Rádio Itatiaia, a emissora, parte do grupo empresarial liderado por Rubens Menin desde maio de 2021, opera com tecnologia de ponta e mantém uma estrutura robusta de transmissão que atinge boa parte do estado de Minas Gerais, incluindo a Região Metropolitana de Belo Horizonte e diversas áreas do interior, como Zona da Mata, Sul de Minas, Triângulo Mineiro e Alto Paranaíba, Norte de Minas, Vale do Mucuri, Campo das Vertentes, Jequitinhonha, Rio Doce e Oeste mineiro. Cidades como Juiz de Fora, Varginha, Montes Claros, Ouro Preto, Ipatinga, Uberlândia, Uberaba, Patos de Minas, Lavras, Alfenas, Itajubá, Passos, Poços de Caldas, Muriaé, Viçosa, Ubá e Ponte Nova estão entre as contempladas por sua ampla rede de afiliadas. A programação jornalística da rádio também é retransmitida por canais de TV por assinatura e está disponível globalmente via internet e aplicativos móveis, demonstrando sua capacidade de adaptação às transformações tecnológicas da comunicação moderna. A Rede Itatiaia é composta por cinco emissoras localizadas em Belo Horizonte, Juiz de Fora, Montes Claros, Ouro Preto e Varginha.

Com esse contexto histórico, estrutural e institucional da Rádio Itatiaia, esta análise qualitativa se propõe a discutir as práticas de segurança de dados no exercício do jornalismo contemporâneo, levando em conta os desafios enfrentados por uma emissora de grande porte e visibilidade.

Esta monografia conta com entrevistas realizadas com profissionais atuantes no jornalismo da rádio, dentre eles Maria Cláudia Santos (diretora de jornalismo da Rádio Itatiaia), João Felipe Lolli (jornalista) e Bruna Truocchio (gestora de comunicação) e que já passaram pela emissora, como Fernanda Rodrigues (jornalista, ex-integrante da Rádio Itatiaia e atual repórter da Record News). A análise desse material proporcionou uma visão acerca da

segurança de dados no exercício cotidiano da prática jornalística da Rádio Itatiaia, evidenciando tanto os desafios enfrentados quanto às estratégias desenvolvidas por diferentes perfis e estruturas organizacionais. As falas colhidas oferecem subsídios para compreender a atual maturidade da rádio Itatiaia frente às exigências da Lei Geral de Proteção de Dados (LGPD), assim como os níveis de consciência ética e técnica relativos ao tratamento das informações sensíveis, configurando um panorama que reflete as tensões e adaptações do jornalismo brasileiro na era digital.

Inicialmente, observa-se que existe uma conscientização crescente e transversal sobre a necessidade de proteção dos dados em ambientes jornalísticos. Essa consciência, todavia, apresenta variações significativas, refletindo o porte da organização, o perfil profissional e a posição hierárquica dos entrevistados. No caso da Rádio Itatiaia, conforme relato de sua diretora, Maria Cláudia Santos, a organização vivenciou uma transformação substancial em sua política de segurança da informação após sua incorporação por um grupo empresarial de maior porte em 13 de maio de 2021, quando foi adquirida pelo empresário Rubens Menin. Sobre esse processo, Santos afirma:

> Acho que o principal é entender que tem essa aproximação, ela aumentou a partir da venda da rádio, que durante mais de 70 anos ficou nas mãos da família do senhor Manoel Carneiro, do fundador Januário Carneiro. Mas há quatro anos e meio ela foi vendida para o grupo de negócios do empresário Rubens Menin. Isso tudo, primeiro, aumentou a nossa redação, o volume, a quantidade de pessoas lidando com dados e a quantidade de dados chegando.[6]

De acordo com Maria Cláudia, gestora da Rádio Itatiaia, em entrevista concedida no âmbito desta pesquisa, após a compra da emissora houve um esforço de maior estruturação nos processos internos e na adoção de práticas alinhadas à LGPD. Como ela relata: “a rádio contratou, à época, um escritório especializado em dados, LGPD e tudo mais, eles fizeram todo um inventário do tipo de dado que a gente lida, desde o jornalismo até o back office”[6], o que permitiu, posteriormente, a realização de treinamentos internos sobre o tratamento adequado das informações. Ainda segundo a gestora, esses treinamentos foram realizados *“*com vídeos instrutivos, palestras virtuais e encontros presenciais”[6], sendo seguidos por um processo de formalização: “todos os funcionários participaram de um preenchimento mesmo, de um formulário, [...] de entender a responsabilidade do dado que a gente está lidando”[6]. Além disso, medidas de segurança foram integradas aos fluxos de trabalho, como a restrição ao uso de planilhas ou arquivos pessoais e a adoção de sistemas específicos e internos, como

[6] Entrevista de pesquisa concedida em 11 de julho de 2025, via Google Meet.

o INews[7] e o CMS Brightspoit[8], para o gerenciamento de conteúdo. Essas ações, segundo Maria Cláudia, refletem o compromisso institucional com a privacidade, a proteção de fontes e a integridade das informações em um ambiente sensível como o jornalístico.

Os sistemas tecnológicos empregados pela Rádio Itatiaia, como o iNews e o CMS Brightspot, são mencionados pela diretora Maria Cláudia como instrumentos essenciais para garantir a integridade e a rastreabilidade das informações. O iNews organiza as etapas de apuração, redação e edição por meio de um sistema de login com permissões definidas para cada colaborador, o que impede acessos indevidos e garante que todas as ações realizadas fiquem registradas e possam ser auditadas. Já o CMS Brightspot atua no gerenciamento e publicação do conteúdo, utilizando controle de versões, rastreamento de alterações e fluxos de aprovação antes da veiculação de qualquer material. Essas medidas permitem identificar quem criou, editou ou aprovou cada item, assegurando a integridade, autenticidade e rastreabilidade das informações.

Assim, a Itatiaia evita práticas menos seguras, como o uso de planilhas eletrônicas e documentos compartilhados sem controle, promovendo uma cultura de responsabilidade e proteção de dados no ambiente jornalístico. A presença de mecanismos de rastreamento de acessos dos usuários internos, como jornalistas, editores e produtores, o controle rigoroso de licenças e a centralização das informações em ambientes digitais monitorados configuram uma arquitetura de segurança alinhada com as melhores práticas do setor, em conformidade com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que se refere à segurança, à prevenção e à responsabilização. Essas medidas não apenas reforçam a proteção de dados pessoais, mas também fomentam uma cultura organizacional baseada no comportamento ético e consciente dos profissionais envolvidos.

Segundo Bruna Truocchio, João Felipe Lolli e Fernanda Rodrigues, a incorporação desses sistemas mudou significativamente a rotina de produção. Por exemplo, todo o conteúdo sensível, como denúncias anônimas, relatos de violência ou casos envolvendo menores de idade, é tratado com protocolos de sigilo e responsabilidade que incluem a anonimização das informações, a restrição de acesso apenas a profissionais autorizados, a não divulgação de nomes ou qualquer dado que possa identificar vítimas ou denunciantes,

[7] O iNews (Avid iNEWS) é um sistema de computador de redação (Newsroom Computer System – NRCS), amplamente utilizado em emissoras de rádio e televisão. Permite planejamento, colaboração e automação da produção jornalística — incluindo roteiros, escaletas e distribuição de conteúdo para múltiplas plataformas (TV, web, rádio e mobile) em tempo real.

[8] O Brightspot é um CMS corporativo (Content Management System) focado em organizações de mídia e publicadoras. Ele oferece modelos flexíveis de conteúdo, fluxos de trabalho colaborativos, multi-canal de publicação e gestão integrada de ativos digitais, além de escalabilidade e segurança em ambientes de alto tráfego.

conforme previsto no artigo 13 do Estatuto da Criança e do Adolescente (ECA) e nos princípios da LGPD, como a necessidade e a minimização de dados. Estes protocolos visam garantir a proteção da identidade dos envolvidos e preservar a integridade das apurações jornalísticas.

Os profissionais também são orientados a não registrar nomes ou dados identificáveis em rascunhos ou documentos abertos, preservando a identidade de fontes e vítimas desde o início da apuração. No dia a dia, especialmente durante a apuração externa, é comum que jornalistas utilizem aplicativos de mensagens como o WhatsApp para se comunicar com a redação, de forma rápida e prática. Já dentro da redação, o conteúdo é processado por meio de plataformas específicas como o iNews (para gestão de notícias e pauta) e o CMS Brightspot, que concentram as informações de maneira mais estruturada e controlada.

Além disso, o uso de plataformas com controle de acesso permite que apenas pessoas autorizadas tenham contato com determinados materiais, reduzindo o risco de vazamentos internos. Essas práticas estão conectadas com os princípios discutidos anteriormente nesta monografia, como a minimização de dados, o princípio do acesso restrito e a responsabilização individual na cadeia de produção jornalística. A implementação desses elementos de segurança e controle na rotina da Itatiaia reflete a adaptação da emissora às demandas atuais de proteção de dados e ética jornalística.

A escolha de sistemas como iNews e CMS Brightspot permite um fluxo de trabalho estruturado, garantindo rastreabilidade e acesso restrito, enquanto o uso do WhatsApp em campo equilibra agilidade e praticidade. No entanto, essas ferramentas envolvem riscos potenciais relacionados à segurança da informação. Apesar de o WhatsApp oferecer criptografia de ponta a ponta, mensagens armazenadas em dispositivos ou backups em nuvem podem ser vulneráveis a acessos não autorizados em caso de perda, roubo ou falhas de configuração. O iNews, usado para roteiros e produção de conteúdo, depende da segurança de servidores centrais e de permissões de usuário; portanto, há o risco de exposição de informações sensíveis caso ocorram problemas de gerenciamento ou ataques direcionados. Já o CMS Brightspot, eficiente para publicação e gestão de conteúdos digitais, pode implicar riscos ligados à publicação de conteúdos ou controle de acessos caso haja falhas humanas ou lacunas nos procedimentos de segurança.

Essa combinação de facilidades e riscos evidencia que, embora a rádio conjugue tecnologia e responsabilidade para manter a confiança do público e a integridade das informações, é necessário adotar políticas de proteção de dados robustas, auditorias

constantes e conscientização das equipes, garantindo que as normas legais e protocolos de segurança sejam efetivamente aplicados no cotidiano da redação.

Ademais, a política de restrição ao uso de dispositivos pessoais para acesso às redes internas é rigorosamente aplicada na Rádio Itatiaia como uma medida estratégica de proteção contra vazamentos e ataques cibernéticos. Os jornalistas e demais colaboradores não podem utilizar seus próprios laptops ou dispositivos móveis conectados à rede da empresa, mesmo que prefiram por questões de comodidade. Em vez disso, a emissora fornece equipamentos corporativos configurados com sistemas de segurança específicos, permitindo o monitoramento remoto e a aplicação de políticas centralizadas de controle de acesso, autenticação e atualização.

Antes da implementação formal dessa política, o uso de dispositivos pessoais para acesso às redes internas era menos controlado, o que representava riscos potenciais à segurança da informação. Contudo, observa-se que os jornalistas e colaboradores da Rádio Itatiaia têm ciência de que tais medidas visam à mitigação de riscos cibernéticos e à proteção das informações sensíveis. A política de restrição ao uso de dispositivos pessoais passou a ser adotada de forma mais ampla após sua formalização, e a utilização dos equipamentos corporativos fornecidos pela emissora tornou-se parte do cotidiano de trabalho. Tal prática reflete um movimento institucional voltado ao alinhamento com as melhores práticas de segurança da informação e *compliance*, contribuindo para a integridade dos dados e a continuidade das operações jornalísticas.

Essa política visa minimizar os riscos associados ao uso de máquinas sem a devida blindagem, especialmente diante do crescimento de ameaças como ransomwares[3] e invasões a sistemas corporativos[9]. Segundo a entrevistada Maria Cláudia, os computadores fornecidos pela rádio possuem permissões diferenciadas para funcionários, visitantes e prestadores de serviço, e são conectados a ambientes de rede separados, o que dificulta o deslocamento lateral de um eventual invasor. Embora os entrevistados não tenham se manifestado diretamente sobre essa medida, sua adoção é compreendida no contexto de práticas corporativas voltadas à proteção dos dados e da operação jornalística, sendo integrada à rotina sem aparentes resistências ou impactos negativos relatados.

Assim, a Itatiaia adota uma postura preventiva e alinhada com os princípios de segurança por design e de Zero Trust[10], buscando antecipar e conter riscos antes que

[9] Casos como o ataque sofrido pela Record TV em outubro de 2022, que interrompeu operações jornalísticas e afetou a infraestrutura da emissora, ilustram a gravidade desse tipo de ameaça (RECORD TV sofre [...], 2022).

[10] "Segurança por design" refere-se à prática de incorporar medidas de proteção desde a concepção dos sistemas, enquanto o modelo "Zero Trust" parte do princípio de que nenhum acesso — interno ou externo — deve ser

comprometam dados sensíveis ou a operação jornalística. Essas abordagens impactam positivamente ao reduzir a exposição a falhas humanas e técnicas, garantindo que informações sensíveis, como pautas em apuração, denúncias anônimas ou dados de fontes, permaneçam protegidas sem comprometer a agilidade da redação.

Além da infraestrutura tecnológica, destaca-se o compromisso da organização em manter a adaptação contínua às inovações tecnológicas e aos novos vetores de ameaça. A inserção da inteligência artificial (IA) na rotina da empresa é tratada com cautela, limitando seu uso à transcrição automática dos conteúdos radiofônicos e vetando sua aplicação em processos de produção jornalística que envolvam dados sensíveis ou sigilosos. Este veto é uma regra formal, fundamentada no risco de que ferramentas baseadas em inteligência artificial possam coletar, armazenar ou expor inadvertidamente informações sensíveis, podendo comprometer a confidencialidade das fontes e do conteúdo jornalístico. Essa postura demonstra um alinhamento entre a adoção de tecnologias emergentes e a preservação da confidencialidade, reconhecendo que o avanço tecnológico, especialmente com o uso crescente de ferramentas de inteligência artificial, pode ser simultaneamente um facilitador e um risco à segurança dos dados.

Nesse cenário, torna-se essencial discutir a regulação do uso da inteligência artificial, uma vez que algoritmos podem ser utilizados tanto para proteger informações (por meio de detecção de ameaças e automação de respostas), quanto para comprometer a privacidade, por exemplo, com a identificação indevida de fontes, perfis ou padrões de comportamento a partir de dados sensíveis. Portanto, o uso responsável e transparente dessas tecnologias deve ser orientado por normas éticas e legais, que garantam não apenas eficiência operacional, mas também a integridade e o respeito aos direitos fundamentais envolvidos no exercício jornalístico.

Complementarmente, o jornalista João Felipe Lolli traz uma perspectiva prática sobre segurança de dados, baseada em sua atuação diária com fontes diversas e, por vezes, sensíveis. Ele adota práticas como o uso de softwares atualizados, o armazenamento de conteúdos em servidores protegidos e o acesso restrito a computadores institucionais. Também evita abrir arquivos sem identificação clara e busca gravar entrevistas em ambientes controlados, frequentemente com o Wi-Fi desligado, para reduzir riscos de interceptação. Essas ações, embora simples, fazem parte de uma rotina orientada por boas práticas de segurança, ainda que informais, repassadas pela equipe de tecnologia da rádio. Lolli relatou

confiado por padrão, exigindo verificação contínua.

que já enfrentou situações de exposição digital, especialmente em contextos de maior sensibilidade pública. Em um caso específico, após uma matéria sobre o uso irregular de pistas exclusivas de ônibus em Belo Horizonte, foi alvo de críticas por parte de taxistas, que chegaram a circular montagens com sua imagem acompanhada da legenda “inimigo dos taxistas” nas redes sociais e em grupos de aplicativos. Esse episódio o levou a redobrar os cuidados com sua atuação digital e a adotar uma postura mais cautelosa ao lidar com informações sensíveis e com sua própria presença nas plataformas online.

No âmbito da gestão da comunicação, Bruna Truocchio, gestora da Rádio Itatiaia, contribui para o debate ao relatar aspectos práticos do manuseio cotidiano de informações sensíveis, tanto no campo editorial quanto na gestão interna da equipe. Segundo ela, há uma atenção especial com dados como nome completo e referências de localização que possam identificar indivíduos: “Às vezes a gente pode falar o bairro, né? Aconteceu em tal cidade, tal bairro, mas sem nenhum endereço que remeta à pessoa, por exemplo, como o nome da rua, referência de prédios, postos de gasolina, etc.”[11]

Bruna também menciona que, além da apuração jornalística, lida frequentemente com informações sensíveis no âmbito da gestão de pessoas: “Eu recebo denúncias de profissionais, de ciclano que não gostou do que fulano fez, e isso é o tempo inteiro, né?”[11]. Tais relatos reforçam que, mesmo em contextos organizacionais onde não há uma estrutura tecnológica robusta ou protocolos rígidos de segurança da informação, existe uma percepção concreta sobre a importância de proteger determinados tipos de dados.

Para mitigar esses riscos, a emissora adota alternativas viáveis dentro de sua realidade. As principais ferramentas utilizadas na comunicação com fontes e no recebimento de denúncias são o WhatsApp corporativo, que conta com criptografia de ponta a ponta, e os e-mails institucionais, utilizados por cada profissional. A gestão também orienta que as denúncias sejam canalizadas preferencialmente para o WhatsApp do jornalismo, um canal oficial criado para organizar o fluxo de informações sensíveis. Além disso, há uma separação deliberada entre os canais de participação pública (como Instagram, Facebook e o site da rádio) e os canais destinados a denúncias, a fim de manter o controle e a confidencialidade dos dados recebidos. Embora nem todas essas ferramentas estejam integradas a uma política automatizada de segurança, a gestão demonstra um comprometimento contínuo com a melhoria desses processos, reforçando a ideia de que a segurança da informação é uma responsabilidade compartilhada, que envolve todos os níveis da organização.

Por sua vez, a entrevista com Fernanda Rodrigues, jornalista atuante em contextos

[11] Entrevista de pesquisa concedida em 1 de julho de 2025, via Google Meet.

organizacionais menos estruturados do ponto de vista tecnológico, reflete a realidade de grande parte dos profissionais brasileiros, que convivem com limitações de infraestrutura, ausência de políticas formais e dificuldades de acesso a ferramentas seguras. Embora possua postura ética sólida e compromisso explícito com a proteção das fontes e das apurações, Fernanda relata o uso de canais de comunicação criptografados, como WhatsApp e e-mail, além de documentos abertos para coleta e armazenamento de dados. Essas práticas, embora funcionais e adaptadas às condições locais, expõem a fragilidade da proteção das informações, ressaltando a necessidade urgente de padronização, capacitação e investimento em soluções tecnológicas acessíveis que garantam a confidencialidade e a integridade dos dados jornalísticos.

Em todas as entrevistas, ressalta-se a preocupação constante com a responsabilidade ética e técnica na guarda e no uso dos dados, com ênfase especial na proteção das fontes, um princípio fundamental do jornalismo responsável. Essa preocupação, no entanto, não se limita mais às práticas tradicionais de sigilo e reserva. Atualmente, além de vazamentos internos ou falhas humanas, Maria Cláudia Santos chama atenção para um ponto sensível: o uso indiscriminado de sistemas gratuitos de inteligência artificial generativa por parte de profissionais pode resultar na exposição involuntária de dados sensíveis. Ferramentas aparentemente inofensivas, como assistentes de texto ou plataformas de transcrição baseadas em IA, operam sob lógicas de aprendizado de máquina, que muitas vezes envolvem a coleta e armazenamento dos dados inseridos para treinar os algoritmos. Isso implica que trechos de denúncias, nomes de fontes, ou até mesmo documentos internos, se forem processados por esses sistemas sem os devidos cuidados, podem alimentar bancos de dados externos, fora do controle da empresa, gerando implicações legais, éticas e reputacionais para o veículo.

Esses novos desafios exigem uma reformulação da mentalidade institucional, onde a gestão da segurança da informação não seja tratada apenas como uma responsabilidade da equipe técnica, mas como uma prática transversal e contínua, incorporada à rotina da redação. Isso envolve o reconhecimento de que cada escolha de ferramenta, cada procedimento de apuração ou cada rotina de edição pode ser um ponto vulnerável — e, por isso, precisa ser reavaliado sob a ótica da ética digital e da proteção de dados. Trata-se, portanto, de um campo em expansão que exige preparo técnico, reflexividade ética e atualização constante frente às transformações tecnológicas em curso.

Diante desse cenário, a análise qualitativa permite concluir que a segurança de dados na prática jornalística brasileira está em um estágio de transição e adaptação, em que grandes veículos já implementaram políticas robustas de conformidade e mitigação de riscos,

enquanto veículos menores e profissionais autônomos ainda dependem da autonomia individual, do comprometimento ético e da criatividade para proteger informações em ambientes menos seguros. Tal constatação evidencia uma disparidade que pode comprometer a integridade jornalística e a segurança dos profissionais, e aponta para a necessidade premente de desenvolvimento de soluções escaláveis, acessíveis e customizadas para os diferentes contextos do jornalismo nacional.

Nesse sentido, medidas como a elaboração e disseminação de cartilhas de boas práticas, a capacitação contínua em segurança da informação, a adoção de ferramentas seguras de comunicação e armazenamento de dados, bem como a implementação de políticas institucionais claras — acompanhadas por suporte jurídico e orientação técnica — são fundamentais para o fortalecimento da proteção dos dados jornalísticos. Embora o foco deste trabalho esteja na realidade da Rádio Itatiaia, os desafios enfrentados pela emissora se mostram ressonantes com discussões mais amplas na literatura científica recente. Estudos como o de Venier e Rodilla (2024) evidenciam que a aplicação de tecnologias de inteligência artificial generativa no jornalismo sonoro, como locução automática, edição inteligente de áudio, roteirização automatizada e produção de conteúdo em larga escala, vem promovendo mudanças significativas na prática profissional em diversos países. Ao mesmo tempo, tais inovações carregam implicações éticas, jurídicas e culturais, sobretudo no que diz respeito à preservação da identidade das fontes, à confiabilidade editorial e à privacidade dos dados tratados.

Esses estudos reforçam que o avanço tecnológico, especialmente no campo da inteligência artificial, não pode ser tratado apenas como um ganho operacional, mas deve ser acompanhado de marcos regulatórios, critérios de transparência e políticas internas robustas que garantam a integridade do trabalho jornalístico. No caso analisado, observa-se que a Rádio Itatiaia tem buscado incorporar tais preocupações de forma concreta, limitando formalmente o uso da inteligência artificial a tarefas automatizadas de apoio, como a transcrição de conteúdos, e vedando sua aplicação em atividades que envolvam dados sensíveis. Essa decisão revela uma compreensão crítica por parte da gestão e dos profissionais da emissora sobre os riscos envolvidos, mesmo em um cenário de recursos limitados.

Assim, este trabalho, ao compilar e analisar as práticas adotadas no contexto empírico, contribui para o debate crítico sobre o uso de tecnologia no jornalismo, oferecendo subsídios para a formulação de políticas e condutas que equilibrem inovação, ética profissional e responsabilidade na gestão da informação.

7. CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo analisar de que forma a segurança de dados impacta a prática do jornalismo, com ênfase na proteção e integridade das informações. A questão de pesquisa — "Como a segurança de dados influencia a prática do jornalismo em relação à proteção e integridade das informações?" — guiou a investigação em direção à compreensão dos desafios enfrentados por profissionais da comunicação no tratamento de dados sensíveis, assim como das políticas e práticas adotadas por organizações jornalísticas no ambiente digital.

O estudo partiu de uma abordagem qualitativa e exploratória, fundamentada em uma revisão teórica sobre segurança digital, proteção de dados e jornalismo, mobilizando conceitos relacionados à confidencialidade, integridade, transparência e responsabilidade ética no uso da informação. Foram consideradas também diretrizes normativas como a LGPD e o GDPR, além de estudos que discutem a mediação entre tecnologia e práticas jornalísticas. A análise documental e as entrevistas com profissionais da Rádio Itatiaia contribuíram para a compreensão prática de como as diretrizes institucionais e o contexto organizacional moldam a segurança da informação nas redações.

Com base nos dados coletados e analisados, pode-se afirmar que os objetivos da pesquisa foram plenamente atingidos. A análise qualitativa realizada indicou que a segurança de dados no jornalismo está em processo de mudança, influenciada por demandas legais, tecnológicas e éticas do ambiente digital atual. O estudo da Rádio Itatiaia mostrou como uma organização focada no setor de comunicação pode implementar políticas e práticas que combinam tecnologia, legislação e processos internos para garantir a proteção, integridade e confidencialidade das informações.

A incorporação da emissora por um grupo empresarial maior marcou o início da formalização das práticas de segurança da informação, demonstrando que fatores institucionais são determinantes para a organização dessas práticas. A adoção de sistemas de gerenciamento de conteúdo, restrições ao uso de dispositivos pessoais e treinamentos internos indicam que a segurança de dados envolve aspectos técnicos e operacionais, além de questões organizacionais.

No entanto, o estudo também apontou que a aplicação dessas práticas varia no campo jornalístico, especialmente em veículos menores que enfrentam limitações de infraestrutura e ausência de políticas formais. Nesses casos, a proteção dos dados depende principalmente do

compromisso individual dos profissionais, o que pode não ser suficiente diante das ameaças digitais. Essa situação destaca a necessidade de soluções acessíveis, formação e orientação técnica para fortalecer a segurança de dados em diferentes contextos.

Outro aspecto identificado foi a influência das tecnologias emergentes, especialmente a inteligência artificial. A Rádio Itatiaia adotou uma postura cautelosa, limitando o uso da IA a funções específicas e evitando sua aplicação em processos que envolvam dados sensíveis. No entanto, essa estratégia preventiva pode gerar uma falsa sensação de controle. Mesmo quando a utilização de IA é restrita, algoritmos e sistemas automatizados frequentemente operam em segundo plano, integrados a ferramentas de análise de dados, fluxos de produção e plataformas de monitoramento, o que dificulta a visibilidade total sobre suas ações. Além disso, a complexidade e opacidade dessas tecnologias — muitas vezes tratadas como "caixas-pretas" — tornam desafiador avaliar se decisões automatizadas podem, de fato, impactar dados sensíveis ou alterar processos editoriais.

A falsa sensação de controle também se manifesta no aspecto humano: gestores podem acreditar que ao definir restrições pontuais já garantem a segurança e a integridade editorial, quando, na prática, vazamentos, erros de classificação, viés algorítmico e automações inesperadas ainda podem ocorrer. Esse cenário evidencia que a limitação isolada do uso da IA não é suficiente para assegurar proteção completa, nem para evitar impactos indiretos na confiabilidade das notícias.

Portanto, torna-se essencial que a regulamentação e a governança da IA no jornalismo não se limitem a vetos ou proibições superficiais. É necessário implementar protocolos de auditoria contínua, monitoramento de fluxos algorítmicos, transparência na utilização de sistemas automatizados e treinamento crítico das equipes. Somente dessa forma é possível transformar a cautela em controle real, preservando a segurança dos dados, a integridade editorial e a confiança do público frente a tecnologias cada vez mais presentes nas redações.

A pesquisa também mostrou que a segurança de dados vai além do aspecto técnico, envolvendo a preservação da confiança pública, a transparência e a responsabilidade do veículo jornalístico. A proteção das fontes e a gestão de informações sensíveis influenciam diretamente a credibilidade do jornalismo, o que reforça a importância de políticas claras e da formação dos profissionais.

Para enfrentar os desafios identificados, recomenda-se a elaboração e disseminação de orientações práticas de segurança para veículos jornalísticos de diferentes portes, com foco na capacitação contínua dos profissionais. A implementação de sistemas acessíveis de gestão segura de dados, associados a políticas institucionais claras, pode contribuir para a proteção

eficiente das informações. Além disso, é fundamental que os veículos adotem processos de auditoria e monitoramento constantes para garantir a conformidade e mitigar falhas de processos.

A regulamentação específica para o uso de tecnologias emergentes, especialmente inteligência artificial, deve ser fortalecida, garantindo transparência e segurança no tratamento de dados sensíveis. A articulação entre órgãos reguladores, veículos de comunicação e profissionais é essencial para estabelecer padrões e boas práticas que possam ser amplamente adotadas.

Este estudo busca contribuir com a compreensão das práticas de segurança de dados em um veículo jornalístico brasileiro, destacando avanços, desafios e possíveis caminhos para outras organizações e para o debate sobre segurança da informação no jornalismo contemporâneo.

REFERÊNCIAS

AGÊNCIA ESTADO. PL das Fake News: Google pagou R$ 670 mil à Meta em contrapropaganda. **UOL Notícias**, São Paulo, 2023. Disponível em: https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2023/05/10/pl-das-fake-news-go og le-pagou-mais-de-meio-milhao-a-meta-em-contrapropaganda.htm. Acesso em: 12 jul. 2025.

ANDERSON, C. W. Rebuilding the News: Metropolitan Journalism in the Digital Age. **Journalism Studies**, *[S. l.]*, v. 14, n. 5, p. 1-217, 2013. Disponível em: https://www.researchgate.net/publication/289858953_Rebuilding_the_News_Metropolitan_J o urnalism_in_the_Digital_Age. Acesso em: 28 maio 2025.

AVILÉS RODILLA, C.; VENIER, E. Rádio e inteligência artificial: uma sistematização e caracterização das aplicações e dos desempenhos. **Revista Latinoamericana de Ciencias de la Comunicación**, *[S.l.]*, v. 22, n. 44, 2024. Disponível em: https://revista.pubalaic.org/index.php/alaic/article/view/1042/964. Acesso em: 17 jul. 2025.

BASTOS, E. A. V.; PANTOJA, T. L. S.; SANTOS, S. H. C. S. Os impactos das novas tecnologias da informação e comunicação no direito fundamental à privacidade. **Brazilian Journal of Development**, Curitiba, v.7, n.3, p. 29247-29267, mar. 2021. Disponível em: https://www.brazilianjournals.com/index.php/BRJD/article/view/26840/21237. Acesso em: 30 maio 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jun. 2021.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: DATA

BRASIL. Constituição da República Federativa do Brasil de 1988. **Art. 5º, incisos X e XII**. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 jun. 2025.

BRASIL. Quando a LGPD entrou em vigor? **Gov.Br**, Brasília, DF, 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequen te s/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd. Acesso em: 20 jul. 2025.

BRASIL. **Projeto de Lei n.º 2630, de 2020**: institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (Lei das Fake News). Senado Federal, Brasília, DF, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 20 jul. 2025.

BRASIL SOFREU 103,16 bilhões de tentativas de ataques cibernéticos em 2022. **Security Leaders**, *[S. l]*, 2023. Disponível em: https://securityleaders.com.br/brasil-sofreu-10316-bilhoes-de-tentativas-de-ataques-cibernetic os-em-2022/. Acesso em: 21 jul. 2025.

BENKLER, Y. **The wealth of networks**: how social production transforms markets and freedom. New Haven; Londres: Yale University Press, 2006. Disponível em: https://www.benkler.org/Benkler_Wealth_Of_Networks.pdf. Acesso em: 09 jul. 2025.

CASTELLS, M. **The Rise of the Network Society**: Volume I of The Information Age: Economy, Society and Culture. 2. ed. Oxford: Wiley-Blackwell, 2010. Disponível em: https://memotef.web.uniroma1.it/sites/default/files/file%20lezioni/Manuel%20Castells%20-%20The%20Rise%20of%20the%20Network%20Society%2C%20With%20a%20New%20Prefa ce_%20Volume%20I_%20The%20Information%20Age_%20Economy%2C%20Society%2C %20and%20Culture%20%28Information%20Age%20Series%29%20%282010%2C%20Wile y-Blackwell%29%20-%20libgen.lc_.pdf. Acesso em: 1º de agosto de 2025.

CALDAS, M. S.; SILVA, E. C. C. Fundamentos e aplicação do Big Data: como tratar informações em uma sociedade de yottabytes. **Bibliotecas Universitárias: pesquisas, experiências e perspectivas,** Belo Horizonte, v. 3, n. 1, p. 65-83, 2016. Disponível em: https://periodicos.ufmg.br/index.php/revistarbu/article/view/3086/1886. Acesso em: DATA

CASTRO, J. C. L. de. Plataformas algorítmicas: interpelação, perfilamento e performatividade. **Revista Famecos**, *[S. l.]*, v. 26, n. 3, p. 1-24, 2019a. Disponível em: https://revistaseletronicas.pucrs.br/revistafamecos/article/view/33723/19366. Acesso em: 15 jul. 2025.

CASTRO, J. C. L. de. Das massas às redes: comunicação e mobilização política. *In:* JESUS, E.; TRINDADE, E.; JANOTTI, J.; ROXO, M. (org.). **Reinvenção comunicacional da política: modos de habitar e desabitar o século XXI**. Salvador, BA, EDUFBA/Brasília, DF: Compós, p. 149-166, 2016a. Disponível em: https://hal.science/hal-03226020v1/file/Julio_Cesar_Lemes_de_Castro_-_Das_massas_as_red es.pdf. Acesso em: 14 jul. 2025.

CASTRO, J. C. L. de. Máquinas de guerra híbrida em plataformas algorítmicas. **E-Compós**, *[S. l.]*, v. 23, p. 1-29, 2020a. Disponível em: https://www.e-compos.org.br/e-compos/article/view/1929/1983. Acesso em: 14 jul. 2025.

CASTRO, J. C. L. de. Neoliberalismo, guerra híbrida e a campanha presidencial de 2018. **Comunicação & Sociedade**, *[S. l.]*, v. 42, n. 1, p. 261-291, 2020b. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688549. Acesso em: 15 jul. 2025.

CASTRO, J. C. L. de. Da lógica editorial à lógica algorítmica da notícia. **Conexão – Comunicação e Cultura**, *[S. l.]*, v. 18, n. 36, p. 36-56, 2019b. Disponível em: https://sou.ucs.br/etc/revistas/index.php/conexao/article/view/9481/4447. Acesso em: 14 jul. 2025.

CASTRO, J. C. L. de. Redes sociais como modelo de governança algorítmica. **Matrizes**, *[S.*

l.], v. 12, n. 2, p. 165-191, 2018. Disponível em: https://revistas.usp.br/matrizes/article/view/140890/147048. Acesso em: 15 jul. 2025.

CASTRO, J. C. L. de. Social networks as dispositives of neoliberal governmentality. **Journal of Media Critiques**, *[S. l.]*, v. 2, n. 7, p. 85-102, 2016b. Disponível em: https://www.researchgate.net/publication/309438785_Social_networks_as_dispositives_of_ne oliberal_governmentality. Acesso em: 17 jul. 2025.

CHRISTOFOLETTI, R. **Ética no Jornalismo**. São Paulo: Editora Contexto, 2008.

CHRISTOFOLETTI, R. Ameaças das plataformas digitais ao jornalismo: contributos para a regulação. **Estudos Avançados**, São Paulo, ano 39, n. 113, 2025. Disponível em: https://www.scielo.br/j/ea/a/8hHNLM7tdB5HBvYQr5tNd3L/. Acesso em: 10 jul. 2025.

COMISSÃO EUROPEIA. **Digital Markets Act:** rules for digital gatekeepers to ensure open markets enter into force. Bruxelas, 2022. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423. Acesso em: 23 jul. 2025.

DEUZE, M. **Media Work**. Cambridge; Malden: Polity Press, 2007. Disponível em: https://www.academia.edu/182097/Media_Work. Acesso em: 10 jul. 2025.

DIGITAL SECURITY. **GIJN Resource Center**, *[S. l.]*, 2013. Disponível em: https://gijn.org/resource/digital-security/. Acesso em: 10 jul. 2025.

DISTRITO FEDERAL. LGPD – Histórico. **Portal LGPD DF**, Brasília, [20--]. Disponível em: https://lgpd.df.gov.br/historico/. Acesso em: 25 jul. 2025.

DUARTE, R. Entrevistas em pesquisas qualitativas. **Educar em Revista**, Curitiba, v. 20, n. 24, p. p. 213-225, 2004. Disponível em: https://www.scielo.br/j/er/a/QPr8CLhy4XhdJsChj7YW7jh/?format=pdf&lang=pt. Acesso em: 12 jul. 2025.

FENAJ. **Código de Ética**. Espírito Santo, ES, 2007. Disponível em: https://fenaj.org.br/wp-content/uploads/2014/06/04-codigo_de_etica_dos_jornalistas_brasileir os.pdf. Acesso em: 25 maio 2025.

FERREIRA, D. A. A.; PINHEIRO, M. M. K.; MARQUES, R. M. Privacidade e proteção de dados pessoais: perspectiva histórica**. InCID: Revista de Ciência da Informação e Documentação**, Ribeirão Preto, Brasil, v. 12, n. 2, p. 151–172, 2021. Disponível em: https://revistas.usp.br/incid/article/view/179778/177597. Acesso em: 13 jul. 2025.

GALTUNG, J; RUGE, M. H. The structure of foreign news: the presentation of the Congo, Cuba and Cyprus crises in four Norwegian newspapers. **Journal of Peace Research**, *[S. l.]*, v. 2, n. 1, p. 64-90, 1965. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/002234336500200104?download=true. Acesso em: 04 jul. 2025.

GAWER, A.; CUSUMANO, M. A. Industry Platforms and Ecosystem Innovation. **Journal of Product Innovation Management**, *[S. l.]*, v. 31, n. 3, p. 417-433, 2014. Disponível em: https://www.researchgate.net/publication/261330796_Industry_Platforms_and_Ecosystem_In novation. Acesso em: 05 jul. 2025.

GILLESPIE, T. **Custodians of the Internet**: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Londres: Yale University Press, 2018.

Disponível em: https://www.scirp.org/reference/referencespapers?referenceid=2935670. Acesso em: 28 maio 2025.

GILLESPIE, T. The relevance of algorithms. *In:* GILLESPIE, T.; BOCZKOWSKI, P. J.; FOOT, K. A. (ed.). **Media technologies**: essays on communication, materiality, and society. Cambridge: MIT Press, 2014. p. 167-194. Disponível em: https://www.researchgate.net/publication/281562384_The_Relevance_of_Algorithms. Acesso em: 29 maio 2025.

GILLESPIE, T. The politics of 'platforms'. **New Media & Society**, *[S. l.]*, v. 12, n. 3, p. 347-364, 2010. Disponível em: https://journals.sagepub.com/doi/10.1177/1461444809342738. Acesso em: 28 maio 2025.

GILLESPIE, T. **Custodians of the Internet**: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. New Haven: Yale University Press, 2018.

GOOGLE. Terms of Service. **Google**, *[S. l.]*, [20--]a. Disponível em: https://policies.google.com/terms?hl=en-US. Acesso em: 22 jul. 2025.

GOOGLE. Privacy Policy. **Google**, *[S. l.]*, [20--]b. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 22 jul. 2025.

GOOGLE. Política de Privacidade Arquivada. **Google**, *[S. l.]*, 2023. Disponível em: https://policies.google.com/privacy/archive/20231004-20231115. Acesso em: 22 jul. 2025.

GOOGLE NEWS INITIATIVE. Todos os treinamentos. **Google**, *[S. l.]*, [20--]. Disponível em: https://newsinitiative.withgoogle.com/pt-br/resources/trainings/. Acesso em: 20 jul. 2025.

HAVES, R.; KLEIM, L.; MEIRA, M.; OLIVEIRA, L.; ROSSI, A.; SALIBA, P.; TOLEDO, L.
F.; VERGILI, G.; ZAHAR, C.; ZANATTA, R.. **Jornalismo e proteção de dados pessoais**: a liberdade de expressão, informação e comunicação como fundamentos da LGPD. São Paulo: Abraji, 2022.

HELMOND, A. The Platformization of the Web: Making Web Data Platform Ready. **Social Media & Society**, *[S. l.]*, v. 1, n. 2, p. 1–11, set. 2015. Disponível em: https://www.researchgate.net/publication/282445359_The_Platformization_of_the_Web_Mak ing_Web_Data_Platform_Ready. Acesso em: 10 jul. 2025.

HERMIDA, A. Twittering the News: The Emergence of Ambient Journalism. **Journalism Practice**, *[S. l.]*, v. 4, 2010. Disponível em: https://www.researchgate.net/publication/228194206_Twittering_the_News_The_Emergenc e
_of_Ambient_Journalism. Acesso em: 16 jul. 2025.

JENKINS, H. **Cultura da convergênci**a. São Paulo: Aleph, 2009.

KAYE, D. **Speech Police:** The Global Struggle to Govern the Internet. Nova Iorque: Columbia Global Reports, 2019.

KARAM, F. J. C. **Jornalismo, ética e liberdade**. São Paulo: Editora Summus, 1997.

KOCH, I. V. Entrevista como procedimento metodológico: um espaço de construção de sentidos. **Revista Linhas**, *[S. l.]*, v. 20, n. 44, 2019.

LELOUP, D.; LAEMLE, B.; UNTERSINGER, M.; DASSONVILLE, A. Le journal « La Croix » et le groupe Bayard victimes d'une cyberattaque par rançongiciel. **Le Monde**, Paris, 2024. Disponível em: https://www.lemonde.fr/actualite-medias/article/2024/09/10/le-journal-la-croix-et-le-groupe-b ayard-victimes-d-une-cyberattaque-par-rancongiciel_6311493_3236.html. Acesso em: 21 jul. 2025.

CARMUÇA, F. **We Live Security.** Rede Record sofre ataque cibernético e tem programação afetada. Disponível em: https://www.welivesecurity.com/br/2022/10/10/rede-record-sofre-ataque-cibernetico-e-tem-pr ogramacao-afetada/. Acesso em: 24 ago. 2025.

MARCON, K.; MACHADO, J. B.; CARVALHO, M. J. S. Arquiteturas Pedagógicas e Redes Sociais: uma experiência no Facebook. **Revista de Informática Aplicada**, *[S. l.]*, v. 9, n. 2, 2013. Disponível em: https://seer.uscs.edu.br/index.php/revista_informatica_aplicada/article/view/6860/2958.

MARTINS, G. de A. **Metodologia da investigação científica para ciências sociais aplicadas**. São Paulo: Editora Atlas, 2009.

MARWICK, A. E.; LEWIS, R. **Media Manipulation and Disinfo Online**. Nova Iorque: Data & Society Research Institute, 2017. Disponível em: https://datasociety.net/wp-content/uploads/2024/04/Manipulacao-da-midia-e-desinformacao-o nline.pdf. Acesso em: 21 jul. 2025.

MAÇADA, A. C. G.; BRINKHUES, R. A.; FREITAS JÚNIOR, J. C. Big data e as capacidades de gestão da informação. **Com Ciência**, São Paulo, 2015. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/271604/000999738.pdf?sequence=1. Acesso em: 15 maio 2025.

MCSTAY, A. **Emotional AI**: The Rise of Empathic Media. London: SAGE Publications Ltd, 2018. Disponível em: https://www.researchgate.net/publication/326294717_Emotional_AI_The_Rise_of_Empathi c
_Media. Acesso em: 12 jul. 2025.

MELLO, P. C. Google lança ofensiva contra PL das Fake News, mostram emails e relatório. **Folha de São Paulo**, São Paulo, 2023. Disponível em: https://www1.folha.uol.com.br/poder/2023/05/google-lanca-ofensiva-contra-pl-das-fake-ne ws
-mostram-emails-e-relatorio.shtml#:~:text=O%20Google%20lan%C3%A7ou%20uma%20o fe nsiva,Rio%20de%20Janeiro%20(UFRJ). Acesso em: 14 jul. 2025.

MONTFORT, N.; BOGOST, I. **Racing the Beam:** The Atari Video Computer System. Cambridge (MA); London: MIT Press, 2009. Disponível em: https://theswissbay.ch/pdf/Gentoomen%20Library/Computer%20History/Racing_the_Beam_-
_The_Atari_Video_Computer_System.pdf. Acesso em: 22 jul. 2025.

MUNIZ, M.; GULLINO, D. Moraes manda PF ouvir diretores do Google, Meta e Spotify sobre publicidade contra PL das Fake News. **O Globo**, Brasília, 2023. Disponível em: https://oglobo.globo.com/politica/noticia/2023/05/moraes-manda-policia-federal-ouvir-diretor
-do-google-no-brasil.ghtml. Acesso em: 15 jul. 2025.

NAPOLI, P. M. **Toward a Model of Audience Evolution**: New Technologies and the Transformation of Media Audiences. *[S. l.]*, 2008. Disponível em: https://research.library.fordham.edu/mcgannon_working_papers/15/. Acesso em: 08 jul. 2025.

OECD. **OECD Digital Economy Outlook 2020**. Paris: OECD Publishing, 2020. Disponível em:
https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/11/oecd-digital-econom y-outlook-2020_3f7b7e58/bb167041-en.pdf. Acesso em: 15 jul. 2025.

O'CARROLL, L. This article is more than 1 year old EU unveils 'revolutionary' laws to curb big tech firms' power. **The Guardian**, Bruxelas, 2023. Disponível em: https://www.theguardian.com/world/2023/sep/06/eu-unveils-package-laws-curb-power-big-te ch-giants. Acesso em: 19 jul. 2025.

O'REILLY, T. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. **O'Reilly Network**, *[S. l.]*, 2005. Disponível em: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html. Acesso em: 10 jul. 2025.

RÁDIO ITATIAIA. **Quem somos.** *[S. l.]*, [20--]. Disponível em: https://www.itatiaia.com.br/quem-somos. Acesso em: 18 maio 2025.

RECORD TV sofre ataque hacker com pedido de resgate. **Meio & Mensagem**, *[S. l.]*, 2022. Disponível em: https://www.meioemensagem.com.br/midia/record-tv-ataque-hacker. Acesso em: 11 jul. 2025.

ROCHET, J.-C.; TIROLE, J. **Platform Competition in Two-Sided Markets**. *[S. l.]*, 2002. Disponível em: https://idei.fr/sites/default/files/medias/doc/wp/2002/platform.pdf. Acesso em: 13 jul. 2025.

SILVA, M. da. **O profissional de comunicação e a Lei Geral de Proteção de Dados: de que forma a notícia poderá ser impactada**. 2025. Trabalho de Conclusão de Curso (Graduação em Comunicação Social) – Centro Universitário SATC, Criciúma, 2025. Disponível em: https://repositorio.satc.edu.br/handle/satc/627. Acesso em: 20 jul. 2025.

SILVA NETO, V. J. da. Platform capitalism. **Revista Brasileira de Inovação**, Campinas, v. 18, n. 2, p. 449-454, 2019. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rbi/article/view/8654960/21737. Acesso em: 13 jul. 2025.

SILVEIRA, M. A. Aplicação da LGPD ao conteúdo jornalístico. **SERT/SC**, Florianópolis, 2024. Disponível em: https://sertsc.org.br/site/aplicacao-da-lgpd-ao-conteudo-jornalistico/. Acesso em: 21 jul. 2025.

SOLOVE, D. J. A Taxonomy of Privacy. **University of Pennsylvania Law Review**, *[S. l.]*, v. 154, n. 3, p. 477-564, 2006. Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/. Acesso em: 15 jul. 2025.

STF DETERMINA remoção de anúncios com ataques ao PL das Fake News. **Notícias STF**, *[S. l.]*, 2023. Disponível em: https://noticias.stf.jus.br/postsnoticias/stf-determina-remocao-de-anuncios-com-ataques-ao-pl- das-fake-news/. Acesso em: 20 jul. 2025.

TRAQUINA, N. **Teorias do jornalismo**. A tribo jornalística — uma comunidade interpretativa transnacional. Florianópolis: Editora Insular, 2005.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022**. Regulamento relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Lei dos Serviços Digitais – Digital Services Act). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065. Acesso em: 22 jul. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Regulamento Geral sobre a Proteção de Dados (GDPR). GDPR, 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 22 jul. 2025.

USHER, N. **Making News at The New York Times**. Ann Arbor: University of Michigan Press, 2014. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1376&context=penn_law_review. Acesso em: 19 jul. 2025.

VAN DIJCK, J. Ver a floresta por suas árvores: visualizando plataformização e sua governança. **MATRIZes**, *[S. l.]*, v. 16, n. 2, p. 21-44, 2022. Disponível em: https://revistas.usp.br/matrizes/article/view/201591/185913. Acesso em: 15 jul. 2025.

VAN DIJCK, J; NIEBORG, D. Wikinomics and its discontents: a critical analysis of Web 2.0 business manifestos. **New Media & Society**, *[S. l.]*, v. 11, n. 5, p. 855-874, 2009. Disponível em: https://www.researchgate.net/publication/242156864_Wikinomics_and_its_discontents_A_cri tical_analysis_of_Web_20_business_manifestos. Acesso em: 15 jul. 2025.

VAN DIJCK, J.; Nieborg, D.; Poell, T. (2019). *Reframing platform power*. *Internet Policy Review*, 8(2). **DOI:** 10.14763/2019.2.1414. Acessado em: https://policyreview.info/pdf/policyreview-2019-2-1414.pdf . Acesso em: 24 ago. 2025.

VERNER, A. F. Valores-Notícia e Critérios de Noticiabilidade na Web: a "presença" da audiência e a necessidade de uma (re)discussão teórica. *In:* **I Seminário de Iniciação Científica para Publicações em Jornalismo** (PubliJor 2019: de 14 a 16 de maio de 2019). Ponta Grossa: Unisecal, 2019. Disponível em: https://institucional.unisecal.edu.br/wp-content/uploads/2019/08/PubliJor_Afonso_Verner.pdf. Acesso em: 20 jul. 2025.

WARDLE, C; DERAKHSHAN, H. **Information disorder: toward an interdisciplinary framework for research and policy making**. Strasbourg: Council of Europe, 2017. Disponível em: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-frame

wo rk-for-research-and-policy-making.html. Acesso em: 16 jul. 2025.

WARREN, S. D.; BRANDEIS, L. The right to privacy. **Harvard Law Review**, *[S. l.]*, v. 4, n. 5, p. 193-220, 1890. Disponível em: http://www.jstor.org/stable/1321160. Acesso em: 16 jul.
2025.

WEISS, H. C. A perspectiva infraestrutural na análise do trabalho por plataformas: a contribuição de José van Dijck. **Revista Contraponto**, *[S. l.]*, v. 8, n. 3, 2022. https://seer.ufrgs.br/index.php/contraponto/article/view/117994/84586. Acesso em: 16 jul. 2025.

WIRED. *CNET stops publishing AI-generated stories after staff pushback*, 2023. Disponível em:
https://www.wired.com/story/cnet-published-ai-generated-stories-then-its-staff-pushed-back/. Acesso em: 24 ago. 2025.

WU, Daniel. Gannett halts AI-written sports recaps after readers mocked the stories. **The Washington Post**, 31 ago. 2023. Disponível em:
https://www.washingtonpost.com/nation/2023/08/31/gannett-ai-written-stories-high-school-sp orts/. Acesso em: 24 ago. 2025.

Sadeghi, McKenzie; Dimitriadis, Dimitris; Arvanitis, Lorenzo; Padovese, Virginia; Pozzi, Giulia; Badilini, Sara; Vercellone, Chiara; Wang, Macrina; Huet, Natalie; Fishman, Zack; Pfaller, Leonie; Adams, Natalie; Wollen, Miranda. Tracking AI-enabled Misinformation: Over 1.200 'Unreliable AI-Generated News' Websites (and Counting), Plus the Top False Narratives Generated by Artificial Intelligence Tools. **NewsGuard**, 5 maio 2025. Disponível em: https://www.newsguardtech.com/special-reports/ai-tracking-center/. Acesso em: 24 ago. 2025.

VIJAYAN, Jai. *DDoS Attacks Surge as Africa Expands Its Digital Footprint*. **Dark Reading,** 26 dez. 2024. Disponível em:
https://www.darkreading.com/cloud-security/ddos-attacks-surge-africa-digital-footprin t. Acesso em: 27 ago. 2025.

REPORTERS WITHOUT BORDERS (RSF)**.** *How Internet shutdowns undermine journalism in sub-Saharan Africa*. **RSF**, 28 set. 2023. Disponível em:
https://rsf.org/en/how-internet-shutdowns-undermine-journalism-sub-saharan-africa. Acesso em: 27 ago. 2025.

LUMINATE; SEMBRAMEDIA. Despite challenges, digital news media is flourishing in Africa. Here's how. **Quartz,** s.d. Disponível em:
https://qz.com/2093836/despite-challenges-digital-media-in-africa-is-flourishing. Acesso em: 27 ago. 2025.

THE GUARDIAN**. Facebook asks Australia to let it make content deals with news outlets before being hit with media code**. 21 jan. 2021. Disponível em:
https://www.theguardian.com/technology/2021/jan/21/facebook-asks-australia-to-let-it-mak e- content-deals-with-news-outlets-before-being-hit-with-media-code. Acesso em: 27 ago. 2025.

EURONEWS. **Google News returns to Spain after the country adopts new EU copyright law.** 4 nov. 2021. Disponível em:

https://www.euronews.com/next/2021/11/04/google-news-returns-to-spain-after-the-country-a dopts-new-eu-copyright-law. Acesso em: 27 ago. 2025.

ELECTRONIC FRONTIER FOUNDATION (EFF). **Google News shuts shop in Spain thanks to ancillary copyright law.** 10 dez. 2014. Disponível em: https://www.eff.org/deeplinks/2014/12/google-news-shuts-shop-spain-thanks-ancillary-copyri ght-law. Acesso em: 27 ago. 2025.

APÊNDICE A — QUESTIONÁRIO

1. Qual é o seu nome e veículo de atuação?

2. Há quanto tempo você atua como jornalista?

3. Em quais áreas ou editorias costuma trabalhar (política, investigativa, cultura, etc.)?

4. A segurança de dados é um tema discutido na redação em que você atua? De que maneira?

5. Você já recebeu algum tipo de treinamento em segurança digital? Poderia contar como foi e quem ofereceu?

6. E em relação às leis que regulamentam a segurança e proteção de dados, como a LGPD, por exemplo — você conhece ou já teve contato com elas? O que considera mais importante nessas leis para a prática jornalística?

7. Quais são, na sua experiência, os dados que exigem maior cuidado no trabalho jornalístico?

8. Você costuma lidar com informações confidenciais ou sensíveis em seu trabalho?

9. Quais as recomendações da empresa jornalística em que você atua sobre esse armazenamento?

10. Quais os canais de comunicação oficiais da empresa em que você atua com os ouvintes? Além dos canais de interação, há ações, como promoções, que coletem dados da audiência através de formulários ou cadastros de acesso?

11. Já escolheu algum por considerá-lo mais seguro?

12. Quais são as estratégias utilizadas por você para garantir a segurança ou o não vazamento de dados sensíveis armazenados online?

14. Sua organização jornalística oferece algum suporte técnico ou diretrizes para proteção de dados?

15. Já teve alguma situação em que se sentiu desprotegida ou vulnerável em termos digitais?

16. Existe alguém na redação responsável por orientar jornalistas sobre como se proteger digitalmente?

17. Já sofreu ou conhece alguém que tenha sofrido invasão de contas, vazamento de dados ou ameaças digitais por conta de reportagens?

18. Em sua visão, quais são os maiores riscos atuais para jornalistas em termos de

segurança digital?

19. Você acredita que os jornalistas em geral conhecem os riscos e cuidados com segurança de dados?

20. Como você caracteriza a existência de uma cultura de segurança digital nas redações em que atua ou atuou?

21. Que conselhos você daria para jornalistas iniciantes no que diz respeito à proteção de suas informações e de suas fontes?

23. Há alguma experiência marcante que gostaria de compartilhar relacionada à segurança digital no seu trabalho?

APÊNDICE B — ENTREVISTA BRUNA TRUOCCHIO, GESTORA DA RÁDIO ITATIAIA

Nicollas: Qual é o seu nome e veículo de atuação?
Bruna: Meu nome é Bruna Truocchio.

Nicollas: Há quanto tempo você atua na Rádio?
Bruna: Eu trabalhei aqui como repórter. Agora sou gestora, e coordeno a área de jornalismo tem 4 anos, vai fazer 4 anos. Eu estou aqui na rádio Itatiaia Ouro Preto, que é uma filial de Belo Horizonte.

Nicollas: Em quais áreas ou editorias costuma trabalhar (política, investigativa, cultura, etc.)?
Bruna: Então, como é uma filial do interior, a gente trabalha com todas as editorias que surgem, né? Desde cultura, cidades, polícia, porque quando se trata de uma rádio maior, a gente conseguir dividir por editorias, mas no caso aqui, o que surge a gente fala, então é toda notícia que surgir, seja ela de cultura, polícia, de qualquer segmento a gente tem que apurar.

Nicollas: A segurança de dados é um tema discutido na redação em que você atua? De que maneira?
Bruna: Então assim, aqui a gente preza muito pela fonte. É a fonte. Quando a fonte é em off, quando é uma denúncia, a gente tem o custo de levar as denúncias, então a gente tem muito cuidado na apuração para que essa pessoa não sofra retaliação. Então assim, a gente chega no nosso WhatsApp profissional e aí a gente vai apurar com muito cuidado para não colocar nenhuma informação pessoal da pessoa, né, que está fazendo a denúncia.
Na nossa solicitação de informações, por exemplo, vamos supor que se trata de uma prefeitura, vou tentar o máximo no meu texto ali, no que eu estou digitando e solicitando para eles, não colocar nenhum detalhe que possa identificar essa pessoa, né? Para que ela não sofra nenhuma retaliação e aí por diante.
Inclusive em algumas fontes em off também. A gente tem que ter esse cuidado, por exemplo, dentro da polícia. A gente tem fontes dentro do corpo de bombeiro, dentro da própria prefeitura. Então são fontes confiáveis, né? Que a gente tem uma índole ali que tá querendo ajudar socialmente a cidade, vamos dizer assim, e que a gente não pode de forma alguma deixar que ela tenham uma referência das nossas solicitações, entendeu?

Nicollas: Então essas fontes são anônimas, certo?
Bruna: Sim.

Nicollas: Legal. Então, por conta dessas denúncias, você conhece sobre a LGPD ou já teve contato com ela?
Bruna: Então, com a lei sim, a gente faz treinamento. Na verdade, aqui na Itatiaia é uma rede, né? Então ela geralmente faz treinamento com todas as filiais, com todos os profissionais que trabalham para ela. A gente tem o treinamento aí, com as atualizações que a lei sofre ou a cada vez que entram pessoas novas, eles vão fazendo o treinamento em relação à proteção de dados.

Nicollas: E esse treinamento é basicamente uma conscientização pelo jornalismo profissional?
Bruna: Sim.

Nicollas: Então como é esse treinamento? Através de alguma plataforma online, por exemplo?
Bruna: A gente faz online, igual estamos fazendo vídeo chamada aqui. São ferramentas assim, e às vezes é num local onde tem gente presencialmente, já que algumas pessoas trabalham remotamente, porque são cidades e unidades separadas, né? Como são 5 cidades, então todos participam, mas alguns são remotos, alguns participam de forma remota.

Nicollas: Legal. Então, o que você considera mais importante nessas leis para a prática jornalística, na sua opinião?
Bruna: Olha, a lei, ela garante até a nossa ética, né? A gente tem que ter uma ética, temos aí o nosso código de ética, mas tem uma coisa que reforça esse código que a gente tem que seguir, que a gente não pode é delatar uma fonte. Em uma denúncia, a pessoa está tendo fé no seu trabalho e na sua profissão, então você não pode de forma alguma ir contra isso. A lei garante que você siga isso, então é muito importante.

Nicollas: Quais dados você tem maior cuidado durante o trabalho do jornalista?
Bruna: O nome completo da pessoa, referência dos endereços, né? Às vezes a gente pode falar o bairro, né? Aconteceu em tal cidade, tal bairro, mas sem nenhum endereço que remeta

à pessoa, por exemplo, como o nome da rua, referência de prédios, postos de gasolina, etc. São dados assim bem importantes, e eu falo dentro do jornalismo, né? Que em outras áreas vem CPF, vem outros dados que a gente não utiliza. Mas de acordo com o que a gente utiliza, eu creio que o nome completo e o endereço.

Nicollas: Você, como gestora, costuma lidar com informações confidenciais ou sensíveis em seu trabalho, além das denúncias?
Bruna: Sim, o tempo todo. Eu, por exemplo, faço gestão de pessoas, então eu recebo denúncias de profissionais, de ciclano que não gostou do que fulano fez e isso é o tempo inteiro, né?

Nicollas: Sim, isso é bem comum em ambientes corporativos, né?
Bruna: Sim.

Nicollas: Quais ferramentas vocês utilizam para se comunicar com as fontes?
Bruna: Apenas WhatsApp. O WhatsApp já tem a criptografia deles, né? Já tem essa função, então a gente utiliza a inteligência artificial do mecanismo que a gente utiliza de contato com a pessoa. Então é o WhatsApp.

Nicollas: Tem outras ferramentas que vocês utilizam para entrar em contato com as fontes?
Bruna: Agora aqui a gente tem os e-mails, né? O de contato geral, o e-mail de jornalismo, o e-mail de cada profissional. A gente tem também o canal do jornalismo do WhatsApp. O canal dos ouvintes a gente separa um pouco, apesar de que eles se confundem às vezes, mas sempre enfatizamos que o WhatsApp é para denúncia, é para participar dos programas, e a gente tem também o telefone fixo, o contato pessoal — que muita gente vem até a rádio para poder falar alguma coisa. E o Instagram, Facebook, o YouTube — a gente tem um, que tem pouca movimentação — mas o Instagram e o Facebook têm bastante. E tem o nosso site também, que tem como comentar nas notícias. O que a gente fala, a gente preza aqui é que nesses canais, quando alguém for denunciar alguma coisa, direcionar para o WhatsApp do jornalismo. Aí a gente continua a conversa, né? Através do canal oficial de denúncia.

Nicollas: E vocês têm algum formulário em que o ouvinte possa utilizar para entrar em contato com a empresa?
Bruna: Não. Não tem nada assim... oficial, né? Não tem um formulário predefinido. A gente

tem a orientação de perguntar se é anônimo ou não e perguntar os dados da pessoa, mas assim, só para título de informação. Porque, por exemplo, você vê que a pessoa denuncia algo que não é dela, então ela não quer falar o nome, não precisa falar. Então temos de ter esse cuidado, mas é porque o nosso contato não é muito mecânico, é uma conversa. Você pergunta e a pessoa responde, então não tem uma conversa. Para a gente poder fazer, tem que ter um pouco de bom senso do que a gente pergunta para saber as informações.

Nicollas: Ah, entendi. Então é uma conversa mais humana, né?
Bruna: Isso, conversa humana.

Nicollas: Quais as estratégias que vocês usam para garantir a segurança e que não aconteça um vazamento de dados, por exemplo?
Bruna: Todo profissional que entra, ele assina um termo de compromisso, que ele vai ter total sigilo com as informações que aqui chegam, né? Isso já é uma forma de blindar que aconteça esse tipo de situação contrária do que a gente quer. A gente também vigia, né? A gente fica o tempo todo ali vendo o que está acontecendo. As coisas estão sendo discutidas em reunião fechada, e os demais departamentos não têm acesso ao que o jornalismo tem. Então a gente tenta blindar dessa forma para não acontecer.

Nicollas: Já teve alguma situação em que se sentiu desprotegida ou vulnerável em termos digitais? Por exemplo, algum tipo de perseguição?
Bruna: Já, já sim. De pessoas, por exemplo, eu denunciei alguns crimes, então acontece que a gente fica com um pouquinho de medo, especialmente que a cidade é pequena e as pessoas acabam sabendo quem é quem, né? Então a gente tenta, quando vai publicar, não publicar no meu nome, publico como Rádio Itatiaia ou qualquer outro profissional que passa a matéria. A gente não coloca o nome, mas mesmo assim eles sabem quem são, vindo de cidade pequena, então dá para saber.
Mas a gente tenta fazer dessa forma ou, quando é um caso muito grave, ao invés da gente apurar aqui em Ouro Preto, a gente direciona a pauta para Belo Horizonte, para que eles apurem de lá. Aqui a gente só transmite a informação, não somos nós quem estamos construindo. E aí a gente consegue ficar um pouco blindado disso, sabe?

Nicollas: Existe alguém na redação responsável por orientar jornalistas sobre como se proteger digitalmente?

Bruna: Não. A gente conversa sobre tudo, orienta sobre tudo, mas não tem essa pessoa específica. E assim, a gente tem um departamento digital em Belo Horizonte, que eles dão um treinamento de como a gente alimenta as redes sociais e coloca o padrão que tem que seguir, mas nada relacionado à proteção, sabe?

Nicollas: Já sofreu ou conhece alguém que tenha sofrido invasão de contas, vazamento de dados ou ameaças digitais por conta de reportagens?
Bruna: Conheço, um repórter dentro da própria Itatiaia, que já passou por situações complicadas.

Nicollas: Em sua visão, quais são os maiores riscos atuais para jornalistas em termos de segurança digital?
Bruna: Ah, os que acontecem quando têm contas invadidas, e a pessoa utiliza seu nome. E no seu e-mail, suas formas de ter contato com essas fontes, se passar por você para poder colher informação. Eu acho que o maior risco seria esse.

Nicollas: Em sua opinião, você acredita que os jornalistas, em geral, conhecem os riscos e cuidados com segurança de dados?
Bruna: Eu acho um tema novo. Então ainda não foi tão bem estruturada uma forma de direcionar, um treinamento para a pessoa se autoproteger, do profissional se proteger ou até a própria empresa. Então tem que ser uma coisa bem desenvolvida. Tem que começar a falar sobre o assunto, buscar alternativas. A gente tem tanta tecnologia que possa melhorar, melhorar e proteger. Então tem que usar para isso.

Nicollas: E como você caracteriza a existência de uma cultura de segurança digital nas redações em que atua ou atuou?
Bruna: É um assunto que tá nascendo, né? Nessa cultura a gente não tem muita... como é que eu digo? A gente está começando, então acredito que futuramente a gente vai ter uma coisa mais consolidada, mas por enquanto é um assunto nascendo.

Nicollas: O assunto é bem novo, está surgindo agora?
Bruna: Isso, está surgindo agora, por conta das inteligências artificiais, muitas redes sociais, né? A gente tem para tudo — inteligência artificial, rede social que você tem contato com as pessoas. E de relacionamento profissional, a gente tem o LinkedIn. Então assim, pensando na

proteção, eu acho que se pensa muito em evoluir, em crescer essas tecnologias e essas redes, e esquecem um pouco de como se proteger.

Nicollas: Que conselhos você daria para jornalistas iniciantes no que diz respeito à proteção de suas informações e de suas fontes?
Bruna: Eu acho que o importante é que você tenha muita organização no seu cadastro de fontes. E que você não se esqueça do caderno, porque anotar é importante, é uma coisa que fica mais protegida fisicamente, né? Se você guardar com jeitinho, você sempre vai ter aquilo ali. Então é questão de você anotar suas fontes e, claro, pode usar recursos digitais, mas não se esqueça de anotar, porque é importante também.

Nicollas: Há alguma experiência marcante que gostaria de compartilhar relacionada à segurança digital no seu trabalho?
Bruna: Olha, por exemplo, eu tive uma experiência uma vez de uma denúncia. Foi em uma escola, e uma aluna estava denunciando que tinha bicho na comida da escola. E aí que eu não sei se houve alguma situação lá em que ela também reclamou e, como a denúncia veio à tona, eles acabaram descobrindo que era ela. E ela sofreu retaliação da diretora.
Então a diretora achou meu número pessoal, me ligou, fez um barraco pelo telefone, como se eu tivesse falado uma coisa absurda. E, na verdade, foi apurado que realmente tinha um bicho. A gente falou com a secretaria daquela escola, né? A gente procurou um órgão maior, e eles responderam falando que realmente tinha um bicho — eram de cereais — que não tinha nada prejudicial à saúde e tal. Então a diretora se sentiu ofendida com a notícia e com a denúncia, e começou a fazer esse tipo de retaliação. Foi isso.

APÊNDICE C — ENTREVISTA FERNANDA RODRIGUES, EX-REPÓRTER DA RÁDIO ITATIAIA

Nicollas: Qual é o seu nome e veículo de atuação?
Fernanda: Meu nome é Fernanda Rodrigues e atualmente estou trabalhando na TV Record.

Nicollas: Há quanto tempo você atua na Rádio?
Fernanda: Na Record, eu era estagiária lá em 2022 e 2023. Saí e fui para a Itatiaia, né? Depois fui contratada na Itatiaia, fiquei trabalhando lá quase 2 anos e agora mudei para a Record tem um mês e meio, é bem recente.

Nicollas: Em quais áreas ou editorias costuma trabalhar (política, investigativa, cultura, etc.?
Fernanda: Na Itatiaia, que era onde eu trabalhei por mais tempo e onde eu estava até então, eu trabalhava cobrindo cidades. Que são gerais, e a gente considerava tudo que era de BH e do interior. Interior de Minas, também fazia cobertura do Brasil, em alguns casos mais nacionais e de maior repercussão, e também um pouquinho de alguns assuntos internacionais. Então lá eu trabalhava com essas 3 editorias, principalmente. E aqui na Record é mais cidades. Assim, como é local, né, a gente não faz um jornalismo que abrange mais lugares, é mais regional. Então eu faço cobrindo só cidades. Hoje eu sou produtora, apuradora e produtora. Na Itatiaia, eu era repórter multimídia de sites.

Nicollas: Quando você era da Rádio Itatiaia, a segurança de dados era um tema discutido por lá? De que maneira?
Fernanda: Então, eu vou ser sincera assim com você, Nicollas, eu acho que a gente entende a necessidade da proteção de dados. Por exemplo, tem algumas coisas que a gente não consegue ter acesso, principalmente quando a gente pede.
Te dou um exemplo: aqui tem o hospital João XXIII, que é um dos principais hospitais de acidentados. Muita gente é socorrida pelo SAMU aqui da região central de Belo Horizonte e é levada para lá. O hospital João XXIII, por exemplo, não passa nenhum tipo de dado de paciente. Não passa nada, nem estado de saúde. Então, se a gente quiser saber alguma coisa, tem que ser com o familiar do paciente.
A gente encontra alguns entraves. E em relação ao tratamento dos dados, eu acho que é mais no bom senso. Não existe uma coisa tipo: “nossa, tem que ter essa ferramenta ou isso não

pode compartilhar". A gente tem acesso… vamos supor, né, se eu tenho acesso a alguma informação sua, é mais no cuidado de não veicular o que não pode ser veiculado. Informações sensíveis, né?

Eu não posso dar nome ou mostrar o rosto de uma criança, de um menor de idade, vítima de algum tipo de violência. Isso é absolutamente proibido. Nem os pais da criança, nada que dê para identificar quem ele é. Por mais que a gente saiba quem são os pais, o nome da vítima, a gente tem que ter o cuidado para não expor isso.

Mas internamente, entre o jornalismo, acaba sendo compartilhado. Porque o trabalho não acaba em você. Muitas vezes, você troca de turno, a pessoa está rendendo o seu assunto. E a gente tem que ficar naquele contato. A informação sensível tem que ser tratada com cuidado e sem compartilhar indevidamente. Todo mundo sabe ali das regras, inclusive judiciais.

Na Itatiaia e na Record não tinha uma regra tão definida assim. Na Record, quando eu era estagiária, tentaram instruir a gente a não discutir as coisas via WhatsApp, que é a principal ferramenta de trabalho. Tentaram fazer com que só documentos com senha fossem compartilhados. Mas ficou contraprodutivo, porque o jornal exige rapidez.

Então é um tema sensível em todas as redações. As pessoas ainda patinam nesse quesito de segurança da informação. Acho que ainda tinha que ser um pouco melhor orientado, mais estruturado, mas sem atrapalhar o ofício jornalístico. Porque todas as tentativas acabam enterrando o trabalho. Não achamos um meio-termo ainda. Fica mais no bom senso e na ética.

Nicollas: Você acha que o jornalista tem alguma noção sobre a Lei Geral de Proteção de Dados?

Fernanda: Eu acho que tem pouca. Por mais que tenha alguns treinamentos. A gente assina algumas coisas também. Eu lembro que na Record, nessa época, tentaram cumprir a LGPD. A gente recebeu uma cartilha sobre a lei e teve alguns treinamentos. Mas eu ainda acho que é aquém. As pessoas têm noção do que é, o que pode ou não ser compartilhado. Mas ainda fica muito na esfera do "ah, eu sei o que é", e não numa coisa mais concreta.

Nicollas: No seu dia a dia, você costuma lidar com informações confidenciais?

Fernanda: Acho que sim. Dependendo da pauta, como eu falei, às vezes você tem uma informação de um crime mais sensível. Como eu cubro mais cidades, tem muita coisa criminal. Nome de menor de idade, vítima de violência sexual, por exemplo… esses processos estão em sigilo por lei.

A gente consulta muito o sistema judiciário, mas não tem acesso a tudo. Quando conversamos com a vítima ou temos acesso a boletim de ocorrência, há dados sensíveis: nome completo, nome da mãe, CPF, telefone pessoal. Então sim, lidamos com informações confidenciais.

Nicollas: Quais canais de comunicação você costuma usar com fontes? Além do WhatsApp?
Fernanda: Basicamente por ligação, já que temos os contatos das fontes ou assessores, ou por e-mail, para formalizar. Tudo com assessoria é por e-mail. Para deixar registrado que você pediu, quem respondeu.
Mas você conversa com essa pessoa por fora. Fala com a assessoria: "ó, preciso de uma nota", aí eles falam "beleza, manda um e-mail formalizando que eu já vou correr atrás". Então enquanto você está mandando o e-mail, eles já estão resolvendo.
Eu acho que deveria ser um WhatsApp corporativo. Na Record, por exemplo, temos celulares da empresa, mas ficam na empresa. Quando você vai para casa, usa o pessoal. Então seu número se espalha. É ruim, mas também é bom, porque pode ser daí que nasce uma fonte. Mas mistura tudo — pessoal e trabalho. É uma confusão, mas é a principal ferramenta.
Ferramentas como Teams ou Slack só em outras áreas. Em jornalismo, nunca usei. Na Itatiaia ou Record, é WhatsApp. Tudo é compartilhado lá. Desde pauta até BOs. Informações sensíveis circulam por lá.

Nicollas: Então teria alguma ferramenta específica para evitar vazamentos?
Fernanda: Não sei qual o nível de confiabilidade do WhatsApp. Hoje em dia tem criptografia, mas não sei se vazaria. Colocar senha em documentos mais sensíveis pode ser bom. Já tentaram isso, mas não deu certo.
Talvez documentos com informações sensíveis tivessem que ser protegidos, sim. Mas colocar senha em tudo também não funciona. Às vezes a pessoa não consegue acessar na hora de ir ao ar. Fica inviável. Mas para algumas coisas, acho que funcionaria.

Nicollas: Você já se sentiu desprotegida ou sofreu ameaça digital por causa de alguma reportagem?
Fernanda: Não, ainda bem. Já tive questionamentos de assessorias que não gostaram da matéria, mas nada no sentido de perseguição ou ameaça concreta, graças a Deus.
É um grande problema da profissão, especialmente para quem cobre policial e investigativo. Mas eu estou há pouco tempo formada, e graças a Deus não aconteceu comigo ainda.

Na Itatiaia, por exemplo, ano passado teve uma repórter política que publicou uma coisa, a pessoa não gostou e ameaçou ligar na chefia para demitir ela. Teve assédio mesmo, pressão. Então acontece, mas comigo, não.

Nicollas: Na Rádio Itatiaia, há alguém responsável por orientar sobre proteção digital?
Fernanda: Quem cuida normalmente dessa parte é o pessoal da TI. Tanto da Itatiaia quanto da Record. Eles entregavam cartilhas e davam orientações sobre proteção de dados. Era sempre a equipe de tecnologia que fazia isso.

Nicollas: Quais os maiores riscos para um jornalista em termos de segurança digital?
Fernanda: Acho que o risco é que, do mesmo jeito que temos acesso aos dados dos outros, os outros têm acesso aos nossos. Por exemplo, se eu tenho seu nome completo, consigo puxar sua ficha inteira. E eles também conseguem fazer isso conosco.
A profissão nos expõe. As pessoas podem descobrir seu endereço, telefone, onde trabalha, que horas trabalha… informações que não deveriam estar em qualquer lugar. E isso é um prato cheio para ameaças.

Nicollas: Vocês costumam usar fontes abertas para procurar pessoas?
Fernanda: Sim. Posso pesquisar seu nome completo em bancos abertos como o TJE (Tribunal de Justiça) e ver seus processos, desde que não estejam em sigilo.
Mas tem dados que só conseguimos com fontes. Por exemplo, BOs dentro do sistema da polícia. A assessoria pode passar o histórico da ocorrência, mas nunca o nome. Só que, se você tiver uma fonte lá dentro, ela pode conseguir.
Muitas informações vêm de bancos de dados públicos: dados epidemiológicos, estatísticas, etc. Mas algumas coisas são por fontes internas mesmo.

Nicollas: Com o avanço da tecnologia, você acredita que os jornalistas têm se preocupado mais com segurança de dados?
Fernanda: Acredito que sim. Acho que tem esse cuidado, sim. Pelo menos, é o que percebo.

Nicollas: Como você caracteriza a cultura de segurança de dados onde trabalha?
Fernanda: Ainda peca em muitos fatores, nas duas empresas em que trabalhei. É uma preocupação que existe, e o jurídico se preocupa com isso. Há cartilhas, termos,

treinamentos… Mas ainda é pouco falado no dia a dia.
Ações pontuais existem. Mas no dia a dia, o ritmo engole tudo. Compartilhamos muita coisa no WhatsApp, até pelo Instagram às vezes. Precisamos de mais cuidado. É um assunto novo. Há zonas cinzentas do que pode e do que não pode.

Nicollas: Que conselho você daria para jornalistas iniciantes?
Fernanda: Existem fontes que você tem que tomar cuidado para não compartilhá-las.

APÊNDICE D — ENTREVISTA JOÃO FELIPE LOLLI, REPÓRTER DA RÁDIO ITATIAIA

Nicollas: Qual o seu nome e veículo de atuação?
João: João Felipe Lolli e Silva atua há nove anos na rádio.

Nicollas: Tempo de atuação como jornalista?
João: Possuo ampla experiência no jornalismo, com quase uma década de atuação.

Nicollas: E quais áreas e editorias em que trabalha?
João: Sou jornalista e mestre pela UFOP, e trabalho com reportagens gerais. Costumo cobrir pautas de cidades, economia, política e outras áreas.

Nicollas: O tema da segurança de dados é discutido na redação?
João: Sim. A proteção das informações recebidas é considerada importante. A rádio Itatiaia utiliza computadores e smartphones, como iPhone, todos conectados à internet e protegidos por softwares de segurança atualizados, gerenciados pela equipe de tecnologia.

Nicollas: Já recebeu algum tipo de treinamento em segurança digital?
João: Já, sim. Já recebi orientações informais oferecidas pela equipe de tecnologia da empresa. Essas orientações não aconteceram por meio de palestras formais, mas por instruções contínuas sobre práticas seguras no uso de softwares, gravações, edições e armazenamento de conteúdo. Há o incentivo ao uso de softwares de proteção atualizados e a evitar utilizar arquivos ou materiais que não tenham identificação clara como conteúdo jornalístico.

Nicollas: Já teve algum contato com legislações como a LGPD?
João: Sim. Já, inclusive, abordei a LGPD em reportagens durante o período de debate e implementação da lei. Reconheço a importância da legislação para garantir direitos relacionados à proteção de dados pessoais, principalmente diante da crescente exposição de informações.

Nicollas: Na sua opinião, qual o aspecto mais relevante da LGPD para o jornalismo?
João: Penso que a legislação oferece uma proteção que antes não existia, assegurando direitos fundamentais dos indivíduos e estabelecendo punições em caso de uso indevido de dados.

Nicollas: Quais dados que exigem maior cuidado no jornalismo, no seu dia-a-dia no trabalho?
João: Informações sobre vítimas de crimes, ainda não comprovados judicialmente, como nome, endereço, local de trabalho, escola (no caso de menores), ou qualquer dado que possa identificá-las. Casos de violência e informações de crianças ou adolescentes também demandam atenção especial.

Nicollas: Você lida com informações confidenciais ou sensíveis com frequência?
João: A maioria das entrevistas não possui caráter sigiloso. No entanto, em algumas situações mais delicadas, como entrevistas com advogados sobre leis tributárias, existe sim o cuidado com o sigilo e a segurança das informações.

Nicollas: E quais as regras para armazenamento de dados sensíveis na rádio Itatiaia?
João: As reportagens geralmente são armazenadas em servidores seguros e em programas pagos que oferecem maior proteção. Os computadores utilizados para esse fim são previamente cadastrados, e o acesso se dá por e-mails institucionais autorizados.

Nicollas: E quais os canais de comunicação com ouvintes para coleta de dados que vocês utilizam?
João: A principal ferramenta de entrevista é o WhatsApp, utilizado em cerca de 95% dos casos, inclusive para recebimento de áudios de fontes como médicos, advogados ou assessorias de órgãos públicos. As entrevistas são feitas tanto presencialmente quanto a distância. Para garantir a qualidade da gravação, geralmente é utilizado um ambiente silencioso, com o Wi-Fi desconectado.

Nicollas: Existe uma preferência por plataformas mais seguras?
João: Não sei dizer. Apesar do uso frequente do WhatsApp, há um cuidado para que o ambiente de entrevista seja controlado e seguro.

Nicollas: Quais as estratégias pessoais para proteger dados online que a Rádio Itatiaia adota?
João: Pelo que sei, utiliza-se softwares atualizados, e evitamos o armazenamento em locais públicos ou não autorizados, seguindo as orientações da equipe de tecnologia da rádio.

Nicollas: E a empresa oferece suporte técnico para esses casos?
João: Sim, a rádio oferece suporte completo, com uma equipe altamente capacitada composta por engenheiros, técnicos de áudio e profissionais de ciência da computação. Essa equipe funciona em regime de plantão e está sempre disponível para ajudar, inclusive em fins de semana e feriados, comuns no jornalismo.

Nicollas: E você, em algum momento do ofício de sua profissão, já se sentiu vulnerável digitalmente?
João: Sim. Já recebi críticas e mensagens em redes sociais e aplicativos após algumas reportagens. Em um caso específico, ao fazer uma matéria sobre o uso irregular de pistas exclusivas de ônibus em BH, fui alvo de críticas de taxistas, que chegaram a montar uma imagem minha com a legenda de "inimigo dos taxistas". Mas nada que me ameaçasse fisicamente.

Nicollas: Há alguém na redação responsável por orientar sobre proteção digital?
João: Sim. A equipe de tecnologia orienta os jornalistas regularmente quanto à segurança digital.

Nicollas: Já sofreu ou conhece alguém que tenha sofrido invasões ou ameaças digitais?
João: Conheço colegas de trabalho que já passaram por situações delicadas, especialmente os que atuam em pautas policiais ou tratam de temas sensíveis, que são mais propensos a receber ameaças.

Nicollas: Quais os maiores riscos atuais para jornalistas, em sua opinião?
João: Penso que… a exposição de dados pessoais como número de telefone, redes sociais e e-mail, que muitas vezes são acessíveis a diversas fontes (vereadores, assessores, profissionais da saúde e do direito). Embora isso facilite o trabalho na maioria das vezes, torna-se um problema quando o contato se torna invasivo. Ainda assim, nunca enfrentou situações mais graves.

Nicollas: Você acha que os jornalistas têm consciência dos riscos?
João: Olha, essa é uma pergunta difícil. Porque eu não posso generalizar assim, né? Mas falando de forma… individual, acredito que há, sim, um cuidado constante por parte dos jornalistas em preservar os dados das fontes, evitando qualquer tipo de vazamento.

Nicollas: Já teve alguma experiência marcante relacionada à segurança digital?
João: Não. Apenas aquele que já mencionei, sobre a matéria sobre o uso irregular da faixa de ônibus em BH resultou em um ataque pessoal, em que fizeram uma montagem com minha imagem, que circulou entre grupos de taxistas como se eu fosse um "inimigo dos taxistas”.

APÊNDICE E — ENTREVISTA MARIA CLÁUDIA SANTOS, DIRETORA DA RÁDIO ITATIAIA

Nicollas: Então, queria começar me apresentando também. Meu nome é Nicollas, eu estou graduando em jornalismo pela Universidade Federal de Ouro Preto. E o tema do meu TCC é a segurança de dados na prática jornalística, né? Então, queria começar a entrevista para entender quem é você, qual que é o seu nome e qual que é o veículo que atua.
Maria Cláudia: Bom, meu nome é Maria Cláudia Santos, eu sou diretora de jornalismo da Rádio Itatiaia, que é uma rádio que atualmente atua numa plataforma 360, com um portal de rádio News e canais YouTube também.

Nicollas: Legal. E quanto tempo você atua dentro da Rádio Itatiaia?
Maria Cláudia: Eu estou na Rádio há 25 anos. Eu entrei aqui como... Eu era estagiária e eu era atendente de telefone no estúdio de ouvintes. E aí eu construí uma carreira aqui, fiz muitas coisas assim, em paralelo, mas eu nunca saí da Rádio. E aí eu agora sou diretora. Sou diretora há quase dez anos, há nove anos.

Nicollas: Você é diretora, mas tem alguma editoria específica que você atua?
Maria Cláudia: Eu sou diretora de todo o jornalismo. Eu só não comando a parte esportiva, porque a Rádio tem um diretor de esportes. Então, tudo de jornalismo que não seja esportes é comigo.

Nicollas: Ah, perfeito. Então, onde você costuma trabalhar, a segurança de dados é um tema discutido?
Maria Cláudia: Sim, a segurança de dados nós discutimos ela há alguns anos, estou tentando lembrar da data exata, e eu ia até te falar, Nicollas, que depois, na hora que eu entender melhor a sua demanda, eu posso verificar algum dado mais preciso que possa te ajudar aí para o trabalho ficar bem completo. Mas nós temos, a rádio contratou, a época, um escritório especializado em dados LGPD e tudo mais, eles fizeram todo um inventário do tipo de dado que a gente lida, desde o COO, que é o jornalismo, até o back office, e ali nesse depois desse inventário todo, depois desse inventário com gestores, depois desse inventário todo, criou-se alguns treinamentos, né, da importância, do cuidado, o que pode, o que não pode, o armazenamento, etc. Repassou isso para todo mundo, a gente tem todo esse material salvo,

assim, né, em arquivo aqui, e as pessoas tiveram que depois de entender tudo, todos os funcionários participar de um preenchimento mesmo, de um formulário, em que ele, depois dessas palestras, que foram online, no Shopping, etc., de entender a responsabilidade do dato, que a gente está lidando, etc., enfim, com todas as dicas e tudo mais. A gente vê esse processo no dia a dia, o nosso departamento jurídico aqui trata com muito cuidado várias coisas assim né. Eu vou tentar responder sempre em relação ao jornalismo. da sua... do seu trabalho, né? Então é muito comum chegar no jurídico, por exemplo, pedidos de escritório, de divulgado, de não sei o que, por exemplo, às vezes, dado de fontes de matérias nossas, alegando que muitas vezes não é para denúncia. Não é por prejudicar a pessoa, é porque a pessoa pode ajudar num caso tal, tal, tal. Então, nada disso nunca pode ser liberado, a gente não libera. A gente tem políticas, por exemplo, aqui na Rádio, a gente não pode preencher dados, sobretudo de ouvintes ou de apuração em tabelas como Excel, etc. A gente tem que fazer em sistemas internos. que são sistemas que só tem acesso aqui dentro, e que são protegidos, e não podem ser usados externamente. No jornalismo, a gente usa o INews. Então, a agenda fica dentro dele, todos esses detalhes ficam dentro dele, que você não consegue... Ninguém consegue, bom, invadir, né? É pegar uma planilha de Excel, uma pessoa mandar uma planilha de Excel com vários dados para o outro, né? Não consegue mais, e todo esse cuidado. No caso do digital, tudo é trabalhado dentro de um CMS, então as pessoas, os dados não são tratados mais assim. Cada um tem seu arquivo de Word. Não tem. Nenhum Word as pessoas têm. Tem outros. Em arquivos de textos, certas pessoas podem elaborar seus textos, seus rascunhos, etc. Mas, de fato, o material arquivado fica dentro de plataformas internas, nossas específicas. O CMS é uma plataforma... Norte-Americana, nosso CMS, o Brightspot, é quem é o CMS de gerencia do New York Times, etc, etc, etc. Rádio é importante, é importante o jeito de comunicação também nas Américas, e um dos pilares é que a gente tem tudo ali de forma segura, né, e não é acessado por qualquer um. A gente tem a política de dados, de distorção de voz, né? A gente já tem a política de dados que a gente já tem que simular, por exemplo, menores ou qualquer pessoa que, se identificada, pode fazer alguém encontrar um menor X. Então, também, se a gente obedece leis, normas do Ministério Público, etc., de distorção de voz, de impedir que a pessoa seja identificada por aquele ponto ali. Nós temos que nos assegurar também, até para não sermos forçados a liberar dados. A lei que protege fonte, etc. e mais, a gente se baseia nela. O contato de ouvinte. Nisso, a gente tem uma central, por exemplo, aqui de apuração. Muitos ouvintes ligam. querendo fazer uma denúncia, querendo fazer alguma coisa. Isso é tratado dentro de um processo específico, não fica a verba para rádio todo. Então, a central, que a gente chama de CIA, a central de apuração, quando recebe

isso, vai para um único movimento de processo de caminho, que é para uma produção para averiguar. Muitas vezes, muitos casos, a gente deixa de fazer no ar. Porque a gente verifica um alto risco de vazamento de dados daquela pessoa, né? Porque dados não é só endereço, não sei o que. O que ela diz também ali pode ser prejudicial, né? E a gente não faz, às vezes a gente resolve as questões sem torná-las matéria, ajuda a pessoa, encaminha, etc., sem torná-las matéria. Por causa dessa preocupação, a gente não passa para... Outros veículos, um personagem, um dado, uma pessoa, só é passada para um outro veículo. Quando a gente percebe que talvez a pessoa possa se interessar, por causa dela ter mais repercussão. O que é feito? A gente liga para a pessoa, ou entra em contato com a pessoa e fala o que ela quer. Né? Se ela quer, a gente... Normalmente, às vezes, a gente não passa. A gente passa do repórter que está procurando para ela, para ela entrar em contato. Então, a gente tem todo esse cuidado, tem uma consciência jornalística também, que eu percebo, inclusive dos mais novos, de muita preocupação com a exposição de dados, porque a gente sabe o que isso pode gerar, né? Então, tem todo um trabalho nisso aí, que é mais, hein? Bom, enfim, acho que o principal é entender que tem essa aproximação, ela aumentou a partir da venda da rádio, que a rádio durante mais de 70 anos ficou nas mãos de muita família, que era do senhor Manoel Carneiro, enfim, do fundador, Januário Carneiro, mas há quatro anos e meio ela foi comprada, vendida para o grupo do grupo de negócios do empresário Rubens Menin, isso tudo primeiro que aumentou a nossa redação, o volume, quantidade de pessoas lidando com dados e quantidade de dados chegando. Paralelo a isso, esse processo pós-venda profissionalizou extremamente vários processos que existiu na rádio, e uma das primeiras para a ação foi com isso, com essa questão dos dados, todas as formas, os contratos, os contratos têm regras muito exigentes, específicas de tudo, de LGPD, de dados não passados, você não tem nada de funcionário que hoje é no RH, por exemplo, em planilhas simples de Excel. Muito de sistemas que garantem uma certa proteção. Era isso que você estava querendo, Nicollas?

Nicollas: Sim, eu estava querendo saber, se era um tema discutido, né? E pelo que você falou, falou de uma forma bem completa, né? Mas eu tenho algumas dúvidas também, em relação ao treinamento, principalmente. Você falou que eles fazem palestras, workshops, ou é um treinamento mais interno, né? Tipo, alguma videoaula, por exemplo.

Maria Cláudia: É, nós tivemos, nesse processo que teve aí, ele durou alguns meses, inclusive, de inventário, treinamento, etc. Então, nós entramos em vídeo, Porque o escritório, eu acho que nem é só de Minas Gerais, a gente entrou em vídeo com os especialistas, nos de live mesmo, assim, fazendo. E eles foram passando ponto a ponto, né? Do que pode, o que

não pode, os dados, a legislação etc. Inclusive, com adequações LGPD, né? Nós tivemos muita discussão aqui sobre o WhatsApp, enfim. Usos de whatsapp, etc. Então a gente teve isso. E essas, digamos, lives explicativas, que a gente podia tirar dúvida. Eu me lembro que era uma média de mais de duas horas de live, ficava conversando. Teve todo um... Uma promoção aí.

Nicollas: Legal. E você também falou que não costuma tratar dados em relação à denúncia também, né? Então, qual que é o meio que vocês usam? É o WhatsApp mesmo ou tem algum outro?

Maria Cláudia: Chega pelo WhatsApp, porque hoje em dia não adianta a gente querer. Hoje em dia tá ouvinte no mando e-mail. Não manda, né? E as pessoas não são nem de ligar. Mas ligam ainda. Mas às vezes elas contactam a gente mais pelo WhatsApp. Principalmente quando os programas estão lá. Que eles mandam, né? Então a gente tem um único WhatsApp. que é gerido pelas pessoas específicas. E a partir do momento que a gente vai tratar aquele assunto, a gente trata tudo sobre ele, as anotações, dentro do sistema iNews. Porque o sistema iNews, ele tem tudo. Ele tem local de apuração, texto, pautas, agendas. Então, o sistema pelo qual a gente paga, né? Sistema fechado, ele tem quantidade de licenças que podem acessar, tem todo um, né? um cuidado de nossas seguranças. Então a gente trabalha dentro do sistema INews. No caso do digital, da parte mais digital, é dentro do CMS da Brightspot. São sistemas que tem um ambiente para tudo. E já é mais fácil também, porque aquela procuração. Se ela seguir, e se ela for virar uma matéria, ela já vira ali dentro, né? Aí já vai fazendo todo o processo até chegar na edição de um jornal, por exemplo, e ela já vai estar no espelho, né? Tem todo o que a gente fala retranca, mas que vai sendo continuada

Nicollas: Então, você falou do CMS também, né? Ele é basicamente um site ou é uma plataforma que faz essa gestão dos dados?

Maria Cláudia: Ele é uma plataforma de gestão, publicação e acompanhamento de conteúdo.

Nicollas: Ah, tá. Entendi.

Maria Cláudia: Tá? Gestão, produção e publicação. Tudo é publicado por meio dele. É um sistema realmente muito lento.

Nicollas: Ah, tá. Entendi. Então, é... Na rádio Itatiaia, você acha que... Que a LGPD, ela é bem aplicada?

Maria Cláudia: Eu acho que sim, é óbvio que nós estamos falando em termos de legislação, uma legislação nova. Acho que o jornalismo, pelo fato de ter esse cuidado sempre com preservar a fonte, já tem um pouco essa cultura interjectada, né, que não pode ficar, né, mas tem dados que não são tão sensíveis que às vezes não se atentava para ter tanto cuidado. Acho que sim, é claro que eu sei que a gente luta cada dia, nós estamos falando de humanos, de equipes grandes, né, equipes que misturam muito às vezes pessoas realmente jovens, que principalmente digital, que estão acabando de chegar no mercado de trabalho. Então, tem todo um processo adaptativo, e aí não tem como. Eu não acho que tem do mundo falar hoje em dia que as informações trazadas naquele ambiente são 100% seguras. Asseguradas 100%. O que eu acho é que a gente está tendo um movimento importante nesse sentido, por essa questão da LGPD.

Nicollas: Legal. Então, quais são as estratégias que vocês tomam? Para garantir que a segurança aconteça e que não tenha algum tipo de vazamento de dados.

Maria Cláudia: Assim, graças a Deus, eu tô tentando pensar aqui, eu não me recordo de a gente ter tido algum problema de vazamento de dados. Realmente, eu não lembro. Bom, eu acho que a primeira coisa... Quando nós estamos em sistemas fechados, internos, Todo mundo só acessa aquele sistema, só está naquele sistema, mas não tem uma senha, né? Ele tem que ter uma licença. E, normalmente, tudo que é feito no sistema tem um registro de PCs. Isso facilita muito as pessoas entenderem que tem que ser cuidadosa, porque vão ter que sair dela, né? que tem todo um rastreio. Então, acho que uma estratégia, essa estratégia de assegurar o uso de ambientes internos que são privados, que a gente consegue rastrear o movimento do dado e da informação, Então acho que isso ajuda numa política de consequências, que a pessoa saiba que tem consequências. Fica claro pra ela que existe consequência nesse dado aí, nessa coisa do cuidado de dado. Acho que essa questão de ser acompanhada por tratamento jurídico como estratégia boa, que estão sempre alertando, pra alguma coisa. Então, assim, você nunca vê a gente oferecer lista de nada aqui pra ninguém. Nada disso. É totalmente proibido. Acho que com essa questão jurídica e estando mais acompanhado, todos os contratos, tudo o que você faz, as pessoas têm que assinar aqui na Rádio aditivos. Eles assinaram aditivos de Consciência e da Lei, de respeitar. Todo mundo assina. A primeira estratégia é a responsabilização. Eu acho que todo mundo tem que ser responsável, senão a gente não consegue, né? Manter isso. A responsabilização não se dá por meio de processos organizados. Você está responsabilizado por isso, você está ciente, não fazendo, não pode, né?

Você pode ter consequências. Já tem uma preocupação bem natural mesmo, porque o jornalista sabe do perigo que é, né? O que que é a gente... deixar uma informação vazar. No que diz respeito a menores, é tudo bem cercado, é uma série de coisas que se acontece algum tipo de situação menor a gente precisa chamar rapidamente. Então, todo mundo tem essa consciência, principalmente quem cobre essas áreas mais de crime, enfim, dessas coisas todas. Então, tem todo um processo. A gente tem meio que um um código, uma conduta, uma diretriz. Se é um carro altamente complexo, com alto risco de vida, por exemplo, e tem uma denúncia, essa denúncia ela não fica dentro dessa cadeia natural, essa denúncia normalmente quando é assim, ela chega com exclusividade para alguém, para algum repórter, e o nosso comportamento é manter no nível coordenação para cima. Então aí o repórter começa a trabalhar direto com a coordenação, aí a coordenação normalmente sabe quem é o escravo, etc., mas a gente não sai Isso aí não fica acessível para mais duas, mais três pessoas, não. A gente tem que ter um cuidado muito grande, porque o vazamento a gente é uma realidade, né?

Nicollas: Bastante, né? Ainda mais com o aumento de ataques e essas coisas, né? E você, como diretora da Itatiaia, você já... Já sofreu algum tipo de vazamento de dados? Ou já se sentiu desprotegido em relação a termos digitais?
Maria Cláudia: Não, é isso que eu estava falando que você estava tentando lembrar. Eu acho que nunca teve um caso assim de... de ter tido um vazamento de dado e ouvinte. A única coisa que acontece em redação de jornalismo é o que vaza. Às vezes os dados são fofocas sobre ambientes internos, né? Quem tá saindo, quem tá entrando, é isso aí, né? Às vezes até me chateia, porque às vezes as pessoas colocam coisas absurdas, né? Fulano de tal, fulano de mentira de chai, porque não tava bom nisso. Não era, né? Era outra coisa. Mas isso aí já foge a nossa... E a gente sabe que com certeza é alguém de dentro, né? Mas isso aí foge a nossa... Isso aí foge a qualquer tipo de controle segurança de dados. Isso aí não é nem isso. Isso aí é... É outras coisas. Mas mesmo assim, nós vamos, inclusive, começar, acho que no ano que vem, um trabalho aqui, dentro da política de consequências, de conscientização sobre a responsabilização, a responsabilidade de ter, ao falar qualquer coisa sobre um colega, sobre o outro, dentro de redação, ou falar fora, ou falar que foi demitido por isso, entregar um pouco, gostar de trabalhar.

Nicollas: É tipo um termo, né? Pra... É um termo de compromisso, digamos assim, né?
Maria Cláudia: É, tem sim.

Nicollas: E na sua opinião, quais são os maiores riscos atuais para um profissional de comunicação em termos de segurança?
Maria Cláudia: Dados?

Nicollas: Isso, de dados.
Maria Cláudia: Segurança de dados, profissional de comunicação... Ah, não sei, assim... Ô Nicollas, eu acho que o maior risco é esse grande desenvolvimento tecnológico, né? Que é usado por bem e é usado por mal, né? Então, assim, tem... Como é que fala? Eu já invadir o meu celular pelo menos duas vezes, assumiram o número e a imagem de um parente meu, E conversou comigo, e eu fiz pics, eu, né? Quer dizer assim, custei entender de tão bem feito que o negócio estava, que se tratava de uma invasão. Aí o que eu penso? Se uma pessoa consegue entrar e fazer isso... Nós temos que saber que ele é um hacker e ele vem de todo lado. Então, eu acho que o hacker, essa coisa de hackear os outros, isso aí todo mundo tá vulnerável na comunicação mais ainda. Porque a gente mexe muito e lida muito com os sistemas, né? Então, a rádio tenta proteger de uma forma, tem outra coisa que eu falei que eu não... Nenhum funcionário pode trabalhar com computador próprio, fazer computador aqui dentro e usar rede. Não pode. Ele não consegue usar a rede, não consegue copiar. Para usar a rede, o meu computador é o da rádio. Aí, a minha coordenadora, agora, está podendo usar laptop, levar para casa e voltar. Mas é da rádio. Porque tem uma configuração da segurança da rádio. Para evitar também essa invasão do sistema. Então, tem todo mundo, né? Tem os universos de... as taxas de senhas aqui de dentro, quem pode usar quem pode, separado o ambiente online de quem é visitante. justamente pra evitar esse vazamento de dados. E nem é só vazar, sabe? A gente tem histórias de grandes redes, tendo todo o conteúdo sequestrado pelo exterior, e as pessoas exigindo altas resgates, altas verbas. Há pouco tempo teve em Belo Horizonte o caso de uma instituição de saúde, um negócio bem grave, E é algo muito grande, né? Então, assim, eu acho que o maior risco que a gente está não é esse risco do... do pequeno, de um funcionário, deixar vazar uma coisa, não ter cuidado com o trem, não ter cuidado com o dado, como denúncia. Eu acho que esse macro, essa macro-ambiência, essa macro-ameaça de invasão aos sistemas, né? Que aí, né, tá todo mundo sujeito, a gente tenta fazer os seguros, tenta, né, coibir. Aqui tem muito funcionário que fica muito chateado por não usar o próprio laptop. Porque gosta do próprio, mas não pode. Porque não dá. Não tem como usar, porque a gente precisa de um ambiente de segurança, tá todo mundo trafegando aqui, tudo em ambientes diferentes, tá usando um ambiente de risco. E esse, o nosso

computador, ele pode ser acessado remotamente pela rádio em qualquer lugar, desde que eu dê lá a autorização. Então é mais fácil de detectar ameaças, de ver problemas, porque normalmente invasor usa o ponto mais pra trás pra detectar, né, esses sistemas.

Nicollas: Então a rádio Itatiaia tem uma rede interna, né? Porque os funcionários usam o laptop da empresa pra isso, né?
Maria Claudia: É, funcionários não usam o laptop particular aqui não. Pra trabalho não.

Nicollas: Bem legal saber dessa medida de segurança, né? Então, tem alguma experiência marcante que você gostaria de compartilhar em relação à segurança digital? Acho que não, né?
Maria Cláudia: É, não tem uma. Se eu lembrar, eu te mando depois, que agora que eu escutei todos os questionamentos, se eu lembrar de mais pontos, eu mando no... Eu te chamo no e-mail, escrevo no e-mail, te mando algum depoimento que eu possa acrescentar, né? Porque às vezes tem alguma coisa que pode ser acrescentada.

Nicollas: Então, se você quiser, se você puder também, né? Tem algum documento que possa mostrar como é que é o procedimento de segurança? Tipo assim, pode ser uma cartilha, por exemplo.
Maria Cláudia: Isso aí, eu tenho que ver com jurídico, tá, Nicollas? Se tem alguma coisa. Eu não tenho autorização de liberar nenhum material. Era muito comum antes, os alunos vinham aqui, as sociedades, e aí a gente dava modelo de programa, modelo de jornal, a gente não faz mais isso.

Nicollas: Entendo. No mais, eu não tenho mais dúvidas, né? Porque você me passou uma visão bem completa de como funciona. E se você tiver alguma dúvida em relação ao meu trabalho, pode perguntar, fica à vontade.
Maria Cláudia: Eu acho o trabalho pertinente, né? A gente tem que discutir isso mesmo, e eu acho que o tempo todo vão nascer novas formas de gerar insegurança dos dados. Então, se a gente não tiver esse discurso de discutir como é que tá, o que tá fazendo, o que vai fazer, a gente perde totalmente. Uma coisa que eu tenho me preocupado e me atenado pra isso demais é a questão da inteligência social, que a inteligência artificial, por exemplo, se eu carregar lá um relatório meu, com várias questões aqui para eu me ajudar na organização, ela vai ser perfeita. Tenho certeza disso. Só que esse relatório vai ficar para o mundo. Está no mundo aí.

Então, eu acho que a Inteligência Especial também, ela é uma segurança. Porque a gente tem que entender que o que você compartilha ali, o que você alimenta, o que você vai alimentar ali, então é com esse tema aí que só Deus sabe como é que as pessoas podem acessar. Então, eu tenho muita preocupação com isso.

Nicollas: Eu acho que esse tema de inteligência social, ela é um tema que muita gente se preocupa, né? Porque você tá dando os seus dados todos para a inteligência artificial, né?
Maria Cláudia: É isso que me preocupa, que a gente fornece, e aí vai ficando cada vez melhor uma devolutiva dela pra gente, só que os dados estão lá, né?

Nicollas: Sim. Então, por exemplo, você que preocupa com a questão do jornalista, por exemplo, ele usar a inteligência artificial pra fazer uma, sei lá, uma redação, por exemplo, e acabar acidentalmente colocando dados de alguém lá? Uma preocupação, né?
Maria Cláudia: Sim, é uma preocupação. Aqui eu fingi muito que aqui não tem liberação para uso de inteligência especial na produção de nada. A inteligência especial hoje é usada na Itatiaia para transcrever o conteúdo do rádio. Então tá lá passando rádio simultaneamente, ela tá transcrevendo e ela já transcreve melhor que outros temas o material. Por quê? Porque aí a gente muitas vezes corta uma coisa do rádio e publica em texto. Aí alguém vai e revisa. Então assim, a Inteligência Social tá só transcrevendo aquilo que a gente já tá no ar, né? Ponto e isso. Na área de produção de conteúdo, é bem nesse sentido mesmo. Só, só. Não tem outras coisas. A gente não usa. A Rádio está se estudando a inteligência social. A gente já está estudando. Já está não, né? Hoje em dia, uma coisa que ainda está, já está atrasada. No sistema de inteligência social interno nosso, seguro. É exemplo, sei lá, eu tava conversando com uma advogada e ela falando que ela paga um sistema de inteligência artificial privada, todo um cercado de medidas de segurança e o sistema ajuda ela a fazer as peças. Você imagina a quantidade de dados que vai numa peça de um advogado, né?

Nicollas: Pois é.
Maria Cláudia: E eu sei que já é uma prática aí, que tá certificada, legalizada, autorizada em muitos ambientes aí. Então assim, mas é um trem que é... É um sistema que você adapta a ideia da inteligência social dentro de um processo que fica aberto pro mundo, né? Mas mesmo assim eu tenho medo. Quando ela falou isso eu pensei, não, não vou não ser nunca. Tô com medo disso. Né? Fazer uma peste no sistema. Isso porque ela me mandou uma mensagem. Eu mandei pra ela um dado, uma coisa de um problema meu. Ela me mandou uma mensagem

assim, por favor, responda a pessoa assim. Quando eu li que ela mandou essa mensagem em um segundo quase, a mensagem toda detalhada, com os negócios, eu pensei, nossa, só uma dúvida, porque eu sei que eu sou rápida, mas nunca vi eu entender isso. Como é que você consegue fazer isso aí, não sei o que? Ela falou que é um sistema de inteligência artificial desenvolvido para o meu escritório. Mas muito pessoal, entendeu? Já estava tudo adaptado, meus dados, minhas coisas lá. Não tinha dado pessoal, mas a minha... A questão que eu tinha que analisar e responder para a pessoa estava toda adaptada na lei. Toda já ajeitada. Então, enfim, eu acho que aí, Nícolas, acho que a gente pode falar que o avanço tecnológico inclui a IA. Sempre vai ser algo muito bom. que vai melhorar muitas práticas, pode dar mil possibilidades, mas sempre vai ser uma ameaça.

Nicollas: Sim, eu concordo com isso, né? Porque a tecnologia, ela pode ter influência para o bem, mas também pode acabar sendo uma ameaça também, né?
Maria Cláudia: E como ela lida com muitos dados, ameaça em dados, é natural que aconteça.

Nicollas: É bem isso. É, no mais é isso que eu tenho pra perguntar. Muito obrigado pelo seu tempo. E eu posso fazer uma pergunta pra qualquer dúvida. Seja por aqui mesmo ou por e-mail.
Maria Cláudia: Tá bom.