

SEGURANÇA DIGITAL E DIGNIDADE HUMANA: O PAPEL DAS TIC NA PREVENÇÃO DA EXPOSIÇÃO NÃO CONSENTIDA DE CONTEÚDOS ÍNTIMOS NAS REDES SOCIAIS

DIGITAL SECURITY AND HUMAN DIGNITY: THE ROLE OF ICT IN PREVENTING THE NON-CONSENSUAL EXPOSURE OF INTIMATE CONTENT ON SOCIAL MEDIA

Altino Dias Sacawe¹

RESUMO: O presente artigo analisa o papel das Tecnologias da Informação e Comunicação (TIC) na prevenção da exposição não consentida de conteúdos íntimos nas redes sociais, articulando a segurança digital com a proteção da dignidade humana no contexto da província de Luanda, Angola. A investigação baseia-se na análise de produções científicas, documentos institucionais, instrumentos jurídicos e materiais públicos relacionados com a divulgação indevida de imagens e vídeos íntimos. Metodologicamente, adota-se uma abordagem qualitativa, exploratória e descritiva, sustentada por pesquisa bibliográfica e análise documental. Os resultados evidenciam que a exposição não consentida constitui um fenómeno multidimensional, associado à interação entre vulnerabilidades individuais, práticas sociais, características das plataformas digitais e limitações institucionais. Verifica-se ainda que a literacia digital desempenha um papel relevante na prevenção, mas não substitui mecanismos de proteção, denúncia, resposta institucional e responsabilização dos agentes envolvidos. O estudo contribui para a reflexão sobre segurança e violência digital em Angola, oferecendo subsídios para políticas públicas, programas de literacia digital e estratégias integradas de proteção da dignidade humana no ambiente digital.

1

Palavras-chave: Segurança digital. Dignidade humana. Violência digital. Exposição não consentida de conteúdos íntimos. literacia digital.

ABSTRACT: This article analyzes the role of Information and Communication Technologies (ICTs) in preventing the non-consensual exposure of intimate content on social media, linking digital security with the protection of human dignity in the context of Luanda Province, Angola. The research is based on an analysis of scientific publications, institutional documents, legal instruments, and publicly available materials related to the improper dissemination of intimate images and videos. Methodologically, a qualitative, exploratory, and descriptive approach was adopted, supported by bibliographic research and documentary analysis. The results show that non-consensual exposure is a multidimensional phenomenon associated with the interaction between individual vulnerabilities, social practices, characteristics of digital platforms, and institutional limitations. The study also found that digital literacy plays an important role in prevention, but does not replace mechanisms for protection, reporting, institutional response, and accountability of the actors involved. The study contributes to the discussion on digital security and digital violence in Angola by providing insights that may support public policies, digital literacy programs, and integrated strategies for protecting human dignity in the digital environment.

Keywords: Digital security. Human dignity. Digital violence. Non-consensual exposure of intimate content. Digital literacy.

¹Mestre em Direção Estratégica em Engenharia de Software, Instituto Superior Politécnico Sol Nascente - A Escola do Huambo.

I. INTRODUÇÃO

A rápida evolução das Tecnologias da Informação e Comunicação (TIC) tem transformado as relações sociais, a construção das identidades e os processos de produção, circulação e consumo da informação. Embora as redes sociais ampliem as possibilidades de comunicação, participação e acesso à informação, as suas arquiteturas sociotécnicas e mecanismos algorítmicos também podem favorecer a circulação e amplificação de conteúdos associados a diferentes formas de violência digital (Castro, 2019; Lemos; Pastor, 2020).

Entre essas manifestações destaca-se a exposição não consentida de conteúdos íntimos, frequentemente associada à pornografia de vingança, que pode produzir consequências sociais, psicológicas e jurídicas e comprometer a dignidade, a privacidade, a reputação e o direito à imagem das vítimas (Deslandes et al., 2022). Esse fenómeno resulta da interação entre fatores individuais, tecnológicos, culturais, sociais e institucionais, sendo igualmente influenciado pela lógica da economia da atenção e pelos mecanismos de circulação das plataformas digitais (Castro, 2019; Bruno; Bentes; Faltay, 2019).

No contexto angolano, particularmente na província de Luanda, o fenómeno apresenta relevância social e institucional, embora permaneça insuficientemente explorado pela investigação científica nacional. Os materiais analisados evidenciam desafios relacionados com prevenção, denúncia, proteção das vítimas e responsabilização dos infratores. Congo (2023) destaca ainda limitações na tutela das vítimas perante as especificidades da divulgação não consentida de conteúdos íntimos no ambiente digital.

A problemática relaciona-se diretamente com a dignidade humana, a privacidade, a proteção dos dados pessoais e o controlo sobre a própria imagem, direitos que permanecem aplicáveis no ciberespaço (Sarlet, 2015). Crianças e adolescentes constituem um grupo particularmente vulnerável, reforçando a importância da literacia e da educação digital como instrumentos de prevenção e promoção de uma cidadania digital segura (UNESCO, 2019; UNICEF Brasil, 2019).

2. REFERENCIAL TEÓRICO

SEGURANÇA DIGITAL

O processo de transformação digital modificou profundamente as formas de comunicação, produção de conhecimento e organização da vida social, tornando as interações humanas cada vez mais dependentes de ambientes conectados em rede (Castells, 2009; OECD,

2019). Nesse contexto, a segurança digital assume um papel central, não apenas na proteção dos sistemas, mas também na preservação da privacidade, da confiança e da dignidade humana no ambiente virtual (ENISA, 2023).

Do ponto de vista conceptual, a segurança digital ultrapassa as dimensões da segurança da informação e da cibersegurança. Enquanto a segurança da informação se concentra na proteção de dados e sistemas, e a cibersegurança na defesa de redes e infraestruturas, a segurança digital incorpora também dimensões humanas, jurídicas, éticas e sociais, relacionadas com a proteção da identidade, reputação, intimidade e direitos fundamentais dos utilizadores (NIST, 2018; OECD, 2019; UNESCO, 2021).

Com a expansão dos serviços digitais, os riscos passaram a atingir diretamente os indivíduos, incluindo roubo de identidade, fraude eletrónica, invasão de contas, assédio online, manipulação de conteúdos e divulgação não consentida de informações íntimas (ENISA, 2023; ITU, 2023). Por isso, princípios como *confidencialidade*, *integridade*, *disponibilidade*, *autenticidade* e *responsabilização* constituem fundamentos essenciais para relações digitais seguras e confiáveis (NIST, 2018).

A segurança digital não depende apenas de soluções tecnológicas. O comportamento dos utilizadores, a literacia digital e a existência de políticas institucionais adequadas também são fundamentais (OECD, 2019; UNESCO, 2021). Assim, a segurança digital aproxima-se da cidadania digital, exigindo competências para reconhecer riscos, proteger dados, gerir a presença online e respeitar os direitos de terceiros. Mais do que uma resposta a ameaças externas, constitui uma prática social orientada para a prevenção, a convivência segura e a preservação da dignidade humana no espaço virtual. A partir dessa perspetiva multidimensional, torna-se necessário analisar o papel das TIC na transformação das relações sociais e na criação de novas condições de exposição e vulnerabilidade.

Tecnologias da Informação e Comunicação e a transformação da sociedade digital

As Tecnologias da Informação e Comunicação (TIC) constituem importantes vetores de transformação das sociedades contemporâneas, redefinindo as formas de comunicação, produção do conhecimento, organização económica e participação social. A expansão da Internet, dos dispositivos móveis, da computação em nuvem e das plataformas digitais consolidou uma sociedade interligada, marcada pela circulação instantânea da informação.

Castells (2009) caracteriza esse processo como *sociedade em rede*, na qual os fluxos de informação estruturam as relações sociais, económicas e culturais.

As TIC passaram, assim, de instrumentos operacionais a elementos estruturantes da vida quotidiana, estando presentes na educação, nos serviços públicos, nas atividades financeiras, nas relações laborais e na sociabilidade (Lemos; Pastor, 2020). Embora essa transformação tenha ampliado o acesso à informação, a colaboração, a inovação e a participação cidadã, também modificou a natureza dos riscos digitais.

A intensificação das interações nas redes sociais aumentou a exposição da vida privada e tornou imagens, vídeos e informações pessoais componentes da identidade digital. Paralelamente, a facilidade de reprodução e disseminação de conteúdos permite que informações partilhadas em contextos privados alcancem rapidamente ampla visibilidade, ampliando vulnerabilidades individuais (Lévy, 2010).

Nesse contexto, riscos como roubo de identidade, fraude eletrónica, ciberassédio, desinformação, discurso de ódio, violação da privacidade e divulgação não consentida de conteúdos íntimos demonstram que os impactos das TIC ultrapassam a dimensão tecnológica, envolvendo questões éticas, jurídicas e sociais. A UNESCO (2021) destaca, por isso, a importância da literacia digital, da proteção da privacidade e da cidadania digital.

4

Em Angola, a expansão da Internet e das redes sociais tem criado novas oportunidades de comunicação e acesso à informação, mas também evidencia desafios relacionados com literacia digital, proteção de dados e segurança online. Assim, a transformação digital deve ser acompanhada por mecanismos de proteção dos direitos fundamentais, tornando essencial compreender a relação entre *TIC, vulnerabilidades digitais e dignidade humana*, particularmente no estudo da exposição não consentida de conteúdos íntimos.

SEGURANÇA DIGITAL COMO MECANISMO DE PROTEÇÃO DA DIGNIDADE HUMANA

A consolidação da sociedade digital ampliou a importância da segurança digital como instrumento de proteção dos direitos fundamentais. Inicialmente associada à proteção de sistemas e infraestruturas tecnológicas, a segurança digital passou a abranger também a proteção da pessoa humana, especialmente da privacidade, identidade, imagem e dados pessoais, enquanto dimensões fundamentais da dignidade no ciberespaço.

A dignidade da pessoa humana constitui um princípio estruturante dos direitos fundamentais. Segundo Sarlet (2015), corresponde ao valor intrínseco e irrenunciável de cada

indivíduo, abrangendo a proteção da autonomia, personalidade e integridade física e moral. No ambiente digital, essa proteção estende-se aos direitos da personalidade, como honra, privacidade, intimidade, imagem e dados pessoais. Doneda (2021) destaca, nesse sentido, a necessidade de compatibilizar a circulação de dados com a proteção dos direitos fundamentais.

A segurança digital desempenha, portanto, uma função preventiva, através de mecanismos como autenticação, controlo de acesso, encriptação, configurações de privacidade e gestão da identidade digital. Contudo, a proteção efetiva não depende exclusivamente da tecnologia ou dos utilizadores, exigindo também políticas públicas, educação digital e responsabilização institucional. A UNESCO (2021) reforça a importância de competências digitais associadas à ética, responsabilidade e respeito pelos direitos humanos.

Nesse contexto, ameaças digitais podem comprometer diretamente a privacidade, a identidade, a imagem e a autonomia dos indivíduos. Entre elas destaca-se a *exposição não consentida de conteúdos íntimos*, cuja análise se torna particularmente relevante no contexto angolano, marcado pela expansão das redes sociais e pelos desafios de proteção das vítimas. Assim, a segurança digital deve ser compreendida como instrumento de concretização dos direitos fundamentais e de promoção da dignidade humana na sociedade digital.

A EXPOSIÇÃO NÃO CONSENTIDA DE CONTEÚDOS ÍNTIMOS COMO MANIFESTAÇÃO DA VIOLÊNCIA DIGITAL

5

A evolução exponencial da digitalização das relações sociais favoreceu o surgimento de novas formas de violência no ambiente virtual, entre as quais se destaca a *exposição não consentida de conteúdos íntimos*, pelos seus impactos sobre a privacidade, a identidade, a honra e a dignidade das vítimas (Deslandes, 2022). A facilidade de produção, armazenamento e partilha de conteúdos digitais, associada à rapidez de circulação nas plataformas, amplia significativamente o potencial de disseminação e a permanência dos danos.

Embora a expressão “*pornografia de vingança*” (*revenge porn*) tenha sido amplamente utilizada, a literatura contemporânea privilegia a designação *exposição não consentida de conteúdos íntimos*, por abranger situações motivadas não apenas por vingança, mas também por chantagem, sextorsão, assédio, vantagens económicas ou partilha irresponsável de conteúdos privados (Deslandes, 2022).

Do ponto de vista dos direitos fundamentais, essa prática viola direitos da personalidade, incluindo intimidade, vida privada, honra, imagem e autodeterminação informativa. A dignidade humana constitui, nesse sentido, fundamento da proteção desses direitos (Sarlet,

2015). Os impactos podem ultrapassar o ambiente digital, envolvendo sofrimento psicológico, isolamento social, dificuldades familiares, profissionais e educativas (Deslandes, 2022).

No contexto angolano, particularmente em Luanda, o fenómeno apresenta crescente relevância social. Segundo Congo (2023), embora existam mecanismos jurídicos gerais de proteção da honra, imagem e vida privada, persistem desafios relacionados com a resposta jurídica e institucional às especificidades da circulação digital desses conteúdos.

A prevenção exige, portanto, uma abordagem multidimensional que articule *segurança digital, literacia digital, proteção jurídica, responsabilização institucional e respeito pela dignidade humana*. Com base nessa compreensão, o estudo adota uma abordagem qualitativa, exploratória, descritiva e interdisciplinar, sustentada por pesquisa bibliográfica e análise documental, com particular atenção ao contexto angolano e à província de Luanda.

3. METODOLOGIA

A investigação foi desenvolvida a partir de uma abordagem qualitativa, de carácter exploratório e descritivo, com perspetiva interdisciplinar. O desenho metodológico foi definido em função do objetivo de compreender as relações entre segurança digital, dignidade humana e exposição não consentida de conteúdos íntimos no contexto angolano.

6

TIPO E NATUREZA DA PESQUISA

A presente investigação caracteriza-se como *qualitativa, exploratória e descritiva*, opção metodológica adequada à análise das relações entre segurança digital, dignidade humana e exposição não consentida de conteúdos íntimos nas redes sociais. Em vez de privilegiar a mensuração estatística, o estudo centra-se na interpretação crítica das informações, processos e relações identificados na literatura científica e nos documentos selecionados.

A abordagem qualitativa permite compreender fenómenos sociais complexos e interpretar os significados e relações que não podem ser plenamente apreendidos por indicadores quantitativos (Minayo, 2014). O carácter exploratório justifica-se pela necessidade de aprofundar a compreensão do fenómeno, particularmente no contexto angolano, onde a sua sistematização académica ainda é limitada (Gil, 2019). A dimensão descritiva permite identificar e sistematizar os principais fatores, mecanismos e riscos associados à produção e circulação não consentida de conteúdos íntimos, bem como as estratégias de prevenção relacionadas com a segurança digital, privacidade e dignidade humana.

A investigação assume ainda uma perspectiva interdisciplinar, articulando contributos da segurança digital, do direito, da comunicação, da sociologia e dos estudos sobre cidadania digital. Essa abordagem permite compreender o fenómeno nas suas dimensões tecnológica, jurídica, social e cultural, relacionando condições de ocorrência, impactos e possibilidades de prevenção.

Com base nesse desenho metodológico, foram adotados como principais procedimentos a pesquisa bibliográfica e a análise documental, utilizadas para fundamentar o enquadramento teórico e contextualizar o fenómeno no cenário angolano, particularmente na província de Luanda.

3.1. PROCEDIMENTOS METODOLÓGICOS

Em conformidade com a natureza qualitativa, exploratória, descritiva e interdisciplinar da investigação, foram adotados dois procedimentos metodológicos complementares: a pesquisa bibliográfica e a análise documental. A articulação entre esses procedimentos permitiu, por um lado, construir o enquadramento teórico e conceptual do estudo e, por outro, contextualizar a problemática da exposição não consentida de conteúdos íntimos no ambiente digital, com particular atenção à realidade angolana e à província de Luanda.

Pesquisa bibliográfica

A pesquisa bibliográfica constituiu um dos principais procedimentos de sustentação teórica e conceptual da investigação, permitindo o levantamento e a análise crítica de conhecimentos previamente produzidos sobre o fenómeno estudado. Segundo Marconi e Lakatos (2021), esse procedimento possibilita o contacto com produções científicas já publicadas e contribui para a construção de interpretações fundamentadas.

Foram selecionados livros, artigos científicos, dissertações, relatórios e outros materiais académicos e institucionais em língua portuguesa, considerando a sua pertinência para os objetivos e categorias analíticas do estudo. A seleção privilegiou trabalhos relacionados com segurança digital, direitos da personalidade, violência digital, literacia digital, exposição não consentida de conteúdos íntimos e proteção de crianças e adolescentes no ambiente digital.

O levantamento recorreu a bases de dados e repositórios como SciELO, Google Académico e outras fontes científicas e institucionais relevantes, incluindo materiais da UNESCO, UNICEF Brasil e produções jurídicas e institucionais angolanas. A análise dessas fontes permitiu identificar conceitos, perspetivas teóricas e categorias analíticas que fundamentaram o referencial teórico e orientaram a interpretação dos documentos selecionados.

Análise documental

A análise documental foi utilizada de forma complementar à pesquisa bibliográfica, com o objetivo de contextualizar a exposição não consentida de conteúdos íntimos na realidade angolana, particularmente na província de Luanda. Segundo Gil (2019), a pesquisa documental permite utilizar materiais relevantes para a investigação, submetendo-os a processos de seleção, organização e interpretação de acordo com os objetivos do estudo.

Foram analisados documentos jurídicos, notícias de órgãos de comunicação angolanos, campanhas de sensibilização, pronunciamentos institucionais e materiais relacionados com a proteção de crianças e adolescentes no ambiente digital. A seleção considerou a relevância dos documentos para as dimensões sociais, jurídicas e institucionais do fenómeno.

A análise procurou identificar formas de abordagem pública, desafios de prevenção, limitações institucionais e representações sociais da violência digital, sem pretender quantificar a frequência dos casos. Os elementos encontrados foram articulados com os contributos da pesquisa bibliográfica, permitindo construir uma interpretação contextualizada do fenómeno.

Assim, a pesquisa bibliográfica sustentou a delimitação conceptual e teórica, enquanto a análise documental contribuiu para a contextualização do problema no cenário angolano. A articulação entre ambas constituiu o corpus de informações utilizado na etapa posterior de

CRITÉRIOS DE SELEÇÃO E DELIMITAÇÃO DAS FONTES

A seleção e delimitação das fontes foram orientadas por critérios de *pertinência, credibilidade, relevância temática e relação direta com o problema e os objetivos da investigação*. Na pesquisa bibliográfica, foram privilegiados livros, artigos, dissertações e outras produções académicas sobre segurança digital, dignidade humana, privacidade, violência digital, exposição não consentida de conteúdos íntimos, literacia digital, cidadania digital e proteção de crianças e adolescentes, com preferência por fontes em língua portuguesa e atenção ao contexto angolano.

Na análise documental, foram considerados *instrumentos jurídicos, documentos institucionais, notícias e materiais de sensibilização* relacionados com segurança digital, cibercrime, privacidade, proteção da imagem e violência digital, dando especial atenção à realidade de Angola e da província de Luanda. Foram excluídos materiais repetidos, sem autoria ou origem identificável, sem relação direta com o objeto de estudo ou sem adequada sustentação científica ou documental.

As notícias e demais documentos públicos foram utilizados para contextualizar o fenômeno e identificar acontecimentos, discursos e respostas institucionais, não para determinar a sua incidência ou frequência estatística. Após a seleção, as fontes foram organizadas segundo a sua natureza e os principais eixos temáticos, constituindo um corpus bibliográfico e documental coerente com os objetivos da investigação e posteriormente submetido à análise temática.

ESTRATÉGIAS DE ANÁLISE DAS INFORMAÇÕES

As informações reunidas por meio da pesquisa bibliográfica e da análise documental foram examinadas com base na técnica de análise de conteúdo, com ênfase na abordagem temática proposta por Bardin (2016). A escolha dessa estratégia decorre da necessidade de organizar e interpretar sistematicamente conteúdos provenientes de diferentes fontes, identificando categorias, recorrências, relações e significados relevantes para a compreensão do fenômeno investigado.

A análise de conteúdo mostrou-se adequada aos objetivos da investigação, uma vez que possibilitou ultrapassar a simples descrição das fontes consultadas e desenvolver uma interpretação crítica das informações relacionadas à exposição não consentida de conteúdos íntimos, à segurança digital e à proteção da dignidade humana. Nesse sentido, a análise procurou estabelecer relações entre os contributos identificados na literatura científica e os elementos presentes nos documentos selecionados, particularmente aqueles relacionados com o contexto angolano.

O processo analítico foi desenvolvido em três etapas articuladas. A primeira correspondeu à pré-análise e à organização do material, fase em que as fontes selecionadas foram submetidas a leitura exploratória e posterior sistematização, considerando a sua pertinência em relação aos objetivos e ao problema de investigação. Essa etapa permitiu delimitar o corpus de análise e identificar os conteúdos mais relevantes para o desenvolvimento do estudo.

Na segunda etapa, procedeu-se à categorização temática das informações. Os conteúdos identificados nas fontes bibliográficas e documentais foram organizados em eixos analíticos relacionados com as principais dimensões do fenômeno investigado, incluindo a segurança digital, a exposição não consentida de conteúdos íntimos, a literacia digital, a proteção da privacidade e da dignidade humana, a responsabilidade das plataformas digitais e os mecanismos institucionais de prevenção e proteção.

Por fim, realizou-se a interpretação crítica das informações organizadas, estabelecendo relações entre as categorias identificadas e o referencial teórico que sustenta a investigação. Essa etapa permitiu analisar convergências, especificidades e limitações presentes nas fontes examinadas, bem como compreender de que forma os diferentes fatores sociais, tecnológicos e jurídicos se articulam na ocorrência e na prevenção da violência digital.

Assim, a análise de conteúdo temática constituiu o principal procedimento de interpretação das informações, permitindo transformar o conjunto de fontes selecionadas em categorias analíticas coerentes com os objetivos da investigação. A sua utilização contribuiu, desse modo, para uma abordagem sistemática e interpretativa do fenómeno, sem reduzir a análise à simples descrição dos materiais consultados.

PREVENÇÃO, PROTEÇÃO DA DIGNIDADE HUMANA E DESAFIOS INSTITUCIONAIS NO CONTEXTO ANGOLANO

A identificação desses limites conduz ao quarto eixo, dedicado às condições institucionais e às formas de prevenção, proteção e responsabilização.

Conforme Flick (2009), a utilização articulada de diferentes fontes pode contribuir para ampliar a compreensão de um fenómeno, desde que essas fontes sejam analisadas de forma complementar e em consonância com os objetivos da investigação. No presente estudo, essa articulação não corresponde à triangulação de técnicas de recolha junto de participantes, mas à confrontação e complementaridade entre informações provenientes da produção científica e dos documentos selecionados.

Do ponto de vista ético, a investigação observou princípios relacionados com o rigor na utilização das fontes, o respeito pelos direitos de autor e a adequada referenciação das obras e documentos consultados, em conformidade com as normas da American Psychological Association (APA, 7.^a edição). Considerando a sensibilidade da temática, procurou-se ainda evitar a reprodução ou divulgação desnecessária de conteúdos íntimos, imagens ou informações que pudessem contribuir para a revitimização das pessoas envolvidas nos casos analisados.

Assim, o desenho metodológico manteve correspondência entre problema de investigação, objetivos, corpus documental e estratégia de análise, estabelecendo a base para a apresentação e interpretação dos resultados.

RESULTADOS

O presente capítulo apresenta os resultados obtidos a partir da análise das fontes bibliográficas e documentais selecionadas para a investigação. A organização das informações seguiu os critérios metodológicos definidos anteriormente, permitindo identificar convergências, especificidades e desafios relacionados à exposição não consentida de conteúdos íntimos nas redes sociais, com particular atenção ao contexto angolano e à realidade da província de Luanda.

A análise evidenciou que o fenómeno não pode ser compreendido exclusivamente como consequência de decisões individuais ou do uso inadequado das Tecnologias da Informação e Comunicação (TIC). Pelo contrário, as fontes examinadas apontam para a articulação entre fatores sociais, culturais, tecnológicos e institucionais que contribuem tanto para a ocorrência quanto para a disseminação e a persistência dessa forma de violência no ambiente digital.

Com base na análise temática do corpus bibliográfico e documental, os resultados foram organizados em quatro eixos principais: (i) a exposição não consentida de conteúdos íntimos como forma de violência e violação da dignidade humana; (ii) a literacia digital e as vulnerabilidades associadas ao uso das TIC; (iii) o papel das plataformas digitais e dos mecanismos tecnológicos na circulação dos conteúdos; e (iv) os desafios de prevenção, proteção e responsabilização no contexto angolano.

11

EXPOSIÇÃO NÃO CONSENTIDA DE CONTEÚDOS ÍNTIMOS COMO FORMA DE VIOLÊNCIA E VIOLAÇÃO DA DIGNIDADE HUMANA

A análise das fontes bibliográficas e documentais permitiu identificar a exposição não consentida de conteúdos íntimos como uma manifestação de violência digital que ultrapassa os limites do ambiente virtual. A divulgação não autorizada de imagens e vídeos de carácter íntimo compromete a privacidade, a imagem, a autonomia e a integridade moral das pessoas expostas, podendo produzir consequências duradouras nas suas relações sociais e na sua participação no espaço público.

A discussão retoma os quatro eixos dos resultados, mas desloca o foco da descrição para a interpretação. Procura-se, assim, explicar o significado dos achados, confrontá-los com a literatura mobilizada e delimitar as implicações que podem ser sustentadas pelo corpus analisado no contexto angolano.

No contexto angolano, particularmente a partir dos documentos e casos divulgados no espaço público, verificou-se que a problemática tem adquirido maior visibilidade social. Contudo, a natureza qualitativa e bibliográfico-documental do estudo não permite estabelecer a incidência estatística do fenómeno nem afirmar, de forma conclusiva, a sua evolução quantitativa. O que as fontes permitem evidenciar é a existência de situações e debates que revelam a relevância social da exposição não consentida de conteúdos íntimos e os desafios relacionados com a sua prevenção.

Os resultados sustentam a interpretação da exposição não consentida de conteúdos íntimos como uma forma de violência digital cujos efeitos ultrapassam a publicação inicial. A reprodução, o reenvio e a circulação continuada prolongam a violação e ajudam a explicar por que a remoção de um conteúdo de uma plataforma não significa, necessariamente, a recuperação da privacidade anteriormente perdida.

A compreensão dessas vulnerabilidades conduz ao segundo eixo dos resultados, centrado no papel da literacia digital como instrumento de prevenção, sem, contudo, transferir para os utilizadores ou para as potenciais vítimas a responsabilidade exclusiva pela ocorrência da violência.

LITERACIA DIGITAL E VULNERABILIDADES ASSOCIADAS AO USO DAS TIC

12

O segundo eixo evidencia a importância da literacia digital para a compreensão e a prevenção dos riscos associados à utilização das TIC. A análise das fontes demonstra que o acesso às tecnologias e às redes sociais não significa, necessariamente, a existência de competências suficientes para a proteção da privacidade, dos dados pessoais e da segurança individual no ambiente digital.

A literacia digital, nesse sentido, ultrapassa o domínio técnico das ferramentas. Ela envolve a capacidade de compreender os mecanismos de funcionamento das plataformas, reconhecer situações de risco, avaliar as consequências da divulgação de informações pessoais e agir de forma ética e responsável nas interações digitais. Essa perspetiva aproxima-se das orientações da UNESCO (2019), que destaca a necessidade de desenvolver competências críticas para uma participação mais consciente no ambiente informacional e tecnológico.

Os materiais analisados também evidenciam a particular vulnerabilidade de crianças, adolescentes e jovens diante das dinâmicas de exposição presentes nas redes sociais. A busca por reconhecimento, visibilidade e integração social pode favorecer práticas de partilha que não

consideram plenamente os riscos relacionados à permanência, reprodução e circulação dos conteúdos digitais. Contudo, essa constatação não deve ser interpretada como responsabilização das vítimas, pois a divulgação não consentida constitui uma violação praticada por quem compartilha ou reproduz o conteúdo sem autorização.

No contexto angolano, as fontes consultadas sugerem desafios relacionados com a consolidação de programas sistemáticos de educação e sensibilização para a segurança digital. A insuficiência de iniciativas contínuas de formação pode contribuir para o desconhecimento sobre mecanismos de proteção, privacidade, denúncia e prevenção. Por conseguinte, o fortalecimento da literacia digital apresenta-se como uma dimensão relevante da prevenção, especialmente quando articulado com a atuação das instituições educativas, das famílias, das organizações sociais e dos organismos públicos.

Todavia, embora a educação digital possa reduzir determinadas vulnerabilidades, ela não é suficiente para impedir, isoladamente, a circulação não consentida de conteúdos íntimos. A persistência e a velocidade da disseminação dependem igualmente das características técnicas e económicas das plataformas digitais, o que conduz ao terceiro eixo de análise.

PLATAFORMAS DIGITAIS, CIRCULAÇÃO DE CONTEÚDOS E DESAFIOS DA SEGURANÇA DIGITAL

13

O terceiro eixo dos resultados evidencia que a exposição não consentida de conteúdos íntimos está diretamente relacionada com as condições técnicas que permitem a rápida reprodução, armazenamento, reenvio e republicação de informações no ambiente digital. Uma vez inserido em circulação, um conteúdo pode ser copiado e redistribuído por diferentes utilizadores e plataformas, tornando a contenção dos danos particularmente complexa.

A análise das fontes indica, portanto, que as plataformas digitais não devem ser compreendidas apenas como instrumentos neutros de comunicação. As suas arquiteturas técnicas, mecanismos de recomendação, sistemas de interação e modelos de visibilidade podem influenciar a forma como determinados conteúdos circulam e alcançam diferentes públicos. Essa perspetiva aproxima-se das discussões desenvolvidas no campo dos estudos sobre cultura digital e sociedade em rede, segundo as quais a tecnologia participa ativamente da organização das relações sociais e dos fluxos de informação.

No caso dos conteúdos íntimos divulgados sem consentimento, a possibilidade de reprodução sucessiva amplia os efeitos da violação inicial. Mesmo quando determinado material é removido de uma plataforma, podem persistir cópias armazenadas ou redistribuídas em outros

espaços digitais. Dessa forma, a segurança digital não pode ser reduzida apenas à proteção técnica das contas ou dispositivos, devendo também contemplar mecanismos de prevenção, detecção, denúncia e resposta à circulação de conteúdos que violem direitos fundamentais.

No contexto angolano, os documentos analisados apontam para desafios adicionais relacionados com o acesso à informação sobre procedimentos de denúncia e com a interação entre os utilizadores, as instituições nacionais e as plataformas digitais de alcance internacional. Essas dificuldades demonstram que a prevenção exige capacidades que ultrapassem a atuação individual, envolvendo responsabilidades institucionais e mecanismos técnicos mais eficientes.

Assim, o papel das plataformas constitui um elemento indispensável para compreender a persistência do fenómeno. Entretanto, a identificação dos riscos tecnológicos precisa ser acompanhada pela análise das respostas disponíveis para prevenir a violência, proteger as vítimas e responsabilizar os agentes envolvidos.

PREVENÇÃO, PROTEÇÃO DA DIGNIDADE HUMANA E DESAFIOS INSTITUCIONAIS NO CONTEXTO ANGOLANO

O quarto eixo reúne os resultados relacionados com os mecanismos de prevenção, proteção e responsabilização diante da exposição não consentida de conteúdos íntimos. A análise bibliográfica e documental evidencia que o enfrentamento do fenómeno exige uma abordagem integrada, uma vez que respostas exclusivamente jurídicas, tecnológicas ou educativas tendem a apresentar limitações quando utilizadas de forma isolada.

14

No plano jurídico e institucional, as fontes analisadas apontam para a importância da proteção dos direitos da personalidade, da privacidade, da imagem e da dignidade humana. As discussões relacionadas com o contexto angolano, incluindo as análises de Congo (2023), evidenciam os desafios de aplicação e adaptação dos mecanismos jurídicos existentes às particularidades das práticas realizadas no ambiente digital.

Entretanto, os resultados indicam que a existência de instrumentos normativos, por si só, não assegura a proteção efetiva das vítimas. A prevenção e a resposta institucional dependem também do conhecimento dos mecanismos disponíveis, da capacidade de acolhimento e orientação, da preparação técnica das instituições e da existência de procedimentos acessíveis de denúncia e encaminhamento.

Nesse sentido, a segurança digital deve ser compreendida como uma estratégia de proteção da dignidade humana. Isso implica desenvolver ações educativas voltadas para a literacia digital, fortalecer mecanismos institucionais de prevenção e apoio, aperfeiçoar os

procedimentos de denúncia e resposta e incentivar maior responsabilidade das plataformas na gestão de conteúdos que violem a intimidade e os direitos das pessoas.

A análise evidencia, portanto, que a prevenção da exposição não consentida de conteúdos íntimos exige uma responsabilidade partilhada. Os utilizadores devem ser capacitados para reconhecer riscos e exercer práticas digitais responsáveis; as instituições educativas e familiares devem contribuir para a formação e orientação; o Estado deve fortalecer mecanismos de proteção e responsabilização; e as plataformas devem aperfeiçoar instrumentos de segurança, denúncia e resposta.

SÍNTESE DOS RESULTADOS

A análise organizada nos quatro eixos demonstra que a exposição não consentida de conteúdos íntimos constitui um fenómeno multidimensional, produzido e ampliado pela interação entre práticas sociais, vulnerabilidades digitais, características das plataformas e fragilidades institucionais.

O primeiro eixo evidenciou que a divulgação não autorizada de conteúdos íntimos representa uma forma de violência digital com potencial para comprometer direitos fundamentais e a dignidade humana. O segundo demonstrou que a literacia digital constitui um importante mecanismo preventivo, embora não possa ser utilizada para transferir às vítimas a responsabilidade pela violência sofrida.

O terceiro eixo revelou que as características técnicas das plataformas favorecem a reprodução e a persistência dos conteúdos, tornando a interrupção da circulação uma tarefa complexa. Por sua vez, o quarto eixo demonstrou que a proteção efetiva exige respostas integradas, articulando educação digital, mecanismos de segurança, proteção jurídica, apoio institucional e responsabilidade das plataformas.

Em conjunto, os resultados reforçam que a utilização racional das TIC não depende exclusivamente do comportamento individual dos utilizadores. A construção de um ambiente digital mais seguro exige uma atuação coordenada entre cidadãos, instituições educativas, Estado, sociedade civil e empresas responsáveis pelas plataformas digitais. É a partir dessa articulação que a segurança digital pode ser compreendida não apenas como uma questão técnica, mas como uma condição necessária para a proteção da dignidade humana no ciberespaço.

DISCUSSÃO DOS RESULTADOS

Os resultados devem ser interpretados à luz do referencial teórico e dos limites do corpus analisado. Em vez de repetir a descrição apresentada no capítulo anterior, esta discussão procura explicar o significado dos achados, identificar convergências com a literatura e explicitar as implicações para a prevenção no contexto angolano.

EXPOSIÇÃO NÃO CONSENTIDA DE CONTEÚDOS ÍNTIMOS E VIOLAÇÃO DA DIGNIDADE HUMANA

Os resultados sustentam a interpretação da exposição não consentida de conteúdos íntimos como uma forma de violência digital com efeitos que ultrapassam a publicação inicial. A reprodução, o reenvio e a circulação continuada prolongam a violação e ajudam a explicar por que a remoção de um conteúdo de uma plataforma não significa, necessariamente, a recuperação da privacidade anteriormente perdida.

Essa leitura converge com Deslandes (2022), para quem o vazamento de conteúdos íntimos deve ser analisado para além de uma perspectiva moralizante, considerando os efeitos sociais e a dimensão de violência de género. No corpus analisado, a associação de determinados episódios à curiosidade, ao entretenimento ou à espetacularização também sugere que a violência pode ser socialmente reproduzida por quem visualiza, comenta, partilha ou republica o material.

16

A implicação central é que a proteção da dignidade humana exige deslocar a análise de uma responsabilidade exclusivamente individual para uma abordagem que considere, simultaneamente, condutas dos agentes, práticas sociais e condições técnicas de circulação. Esta conclusão conduz à questão de como as competências dos utilizadores podem contribuir para reduzir vulnerabilidades sem transformar a vítima em responsável pela agressão.

LITERACIA DIGITAL E VULNERABILIDADES NO AMBIENTE DIGITAL

Os resultados confirmam a relevância da literacia digital como componente preventiva, mas também mostram os seus limites. O simples acesso frequente às redes sociais não garante conhecimento suficiente sobre privacidade, permanência dos conteúdos, proteção de dados e mecanismos de denúncia.

A convergência com UNESCO (2019) e UNICEF Brasil (2018) está na compreensão de que a educação digital deve desenvolver competências críticas, e não apenas domínio

operacional das tecnologias. No entanto, essa dimensão preventiva deve ser cuidadosamente delimitada: ensinar práticas seguras pode reduzir determinados riscos, mas não elimina a responsabilidade de quem divulga ou reproduz conteúdos sem consentimento.

No contexto angolano, a literatura e os documentos analisados apontam para a necessidade de consolidar ações sistemáticas de educação para a segurança e cidadania digital. A oportunidade, portanto, não está apenas em aumentar o acesso às tecnologias, mas em acompanhar esse acesso com competências de proteção, pensamento crítico e conhecimento dos mecanismos de apoio disponíveis.

PLATAFORMAS DIGITAIS, VIRALIZAÇÃO E DESAFIOS DA SEGURANÇA DIGITAL

A persistência dos conteúdos revela um limite importante das estratégias centradas exclusivamente no comportamento do utilizador. Uma vez reproduzido, o conteúdo pode ser armazenado, copiado e transferido para diferentes ambientes, o que dificulta a contenção dos danos.

As discussões de Bruno, Bentes, Faltay (2019) ; Castro (2019) ajudam a interpretar essa dinâmica ao evidenciarem que as plataformas digitais possuem mecanismos de visibilidade, perfilamento e interação que participam na organização dos fluxos informacionais. No presente estudo, contudo, não foi realizada uma auditoria técnica dos algoritmos; por isso, os resultados sustentam uma interpretação sobre as condições sociotécnicas de circulação, e não uma demonstração causal sobre o funcionamento de um algoritmo específico.

Essa distinção é importante para evitar um argumento excessivo. O problema não decorre apenas dos algoritmos, mas da combinação entre arquitetura das plataformas, práticas dos utilizadores, mecanismos de denúncia, possibilidade de cópia e capacidade institucional de resposta. A prevenção exige, por isso, mecanismos de deteção, denúncia e remoção articulados com ações que reduzam a redistribuição secundária dos conteúdos.

PREVENÇÃO, PROTEÇÃO INSTITUCIONAL E RESPONSABILIZAÇÃO

Os resultados sugerem que a existência de normas jurídicas constitui uma condição necessária, mas não suficiente, para uma resposta efetiva. A análise de Congo (2023) evidencia desafios de enquadramento jurídico da divulgação não consentida de conteúdos íntimos no ordenamento angolano; os documentos analisados acrescentam dificuldades relacionadas com

conhecimento dos direitos, acesso à denúncia e capacidade institucional de acolhimento e encaminhamento.

A discussão permite, portanto, distinguir três níveis de resposta que precisam de funcionar de forma articulada: prevenção, por meio de educação e literacia digital; proteção, por meio de canais acessíveis de denúncia, apoio e remoção; e responsabilização, por meio de mecanismos jurídicos e institucionais adequados. A ausência de articulação entre esses níveis pode limitar a eficácia das respostas isoladas.

A dimensão sociocultural também merece atenção. Quando a circulação de conteúdos é acompanhada por culpabilização ou banalização da violência, a procura por apoio pode ser dificultada. Assim, uma resposta centrada na dignidade humana deve evitar práticas institucionais que reproduzam constrangimento e exposição indevida das pessoas afetadas.

SÍNTESE DA DISCUSSÃO

Em conjunto, a discussão mostra que a prevenção da exposição não consentida de conteúdos íntimos não pode ser reduzida a uma única intervenção. A literacia digital atua sobre competências e comportamentos; as plataformas condicionam a circulação e a persistência dos conteúdos; e as instituições definem parte importante das condições de denúncia, proteção e responsabilização.

18

No contexto angolano, os achados apontam para a necessidade de fortalecer a articulação entre educação digital, mecanismos institucionais, proteção jurídica e responsabilidade das plataformas. Esta interpretação deve, contudo, ser lida à luz da natureza qualitativa, bibliográfica e documental do estudo, que permite identificar relações e padrões analíticos, mas não estabelecer incidência estatística ou generalizações para toda a população de Angola.

4. CONCLUSÃO

O presente estudo analisou o papel das Tecnologias da Informação e Comunicação (TIC) na prevenção da exposição não consentida de conteúdos íntimos nas redes sociais, relacionando segurança digital e dignidade humana no contexto de Luanda, Angola. Os resultados demonstram que este fenómeno é multidimensional, envolvendo fatores sociais, culturais, tecnológicos e institucionais, com impactos sobre a privacidade, a imagem, a honra e a dignidade das vítimas (Deslandes, 2022; Sarlet, 2015).

A investigação evidenciou ainda que a literacia digital constitui um importante instrumento de prevenção, devendo promover competências relacionadas com privacidade, proteção de dados e utilização responsável das tecnologias, sem transferir para as vítimas a responsabilidade pela violência sofrida (UNESCO, 2019; UNICEF Brasil, 2019). Verificou-se também que a segurança digital ultrapassa a dimensão técnica, exigindo mecanismos eficazes de denúncia e remoção, redução da redistribuição dos conteúdos e responsabilização dos diferentes atores envolvidos.

No contexto angolano, persistem desafios institucionais relacionados com a prevenção, proteção e resposta às situações de exposição não consentida, tornando necessária uma atuação articulada entre educação digital, instituições, Estado, sociedade civil e plataformas digitais (Congo, 2023).

Apesar das suas contribuições, o estudo apresenta limitações decorrentes da sua natureza *qualitativa, bibliográfica e documental*, não permitindo generalizações estatísticas nem uma avaliação direta das experiências das vítimas e instituições. Recomenda-se, por isso, a realização de estudos empíricos em diferentes províncias de Angola, incluindo investigações sobre literacia digital, mecanismos institucionais de proteção, vulnerabilidades de crianças e adolescentes e sistemas de denúncia, moderação e remoção de conteúdos.

19

Conclui-se que a prevenção da exposição não consentida de conteúdos íntimos exige uma abordagem integrada, que combine segurança digital, educação, proteção institucional, responsabilidade das plataformas e respeito pelos direitos fundamentais. Nesse sentido, promover a segurança digital significa garantir que as TIC contribuam para a comunicação, inclusão e desenvolvimento sem comprometer a privacidade, a autonomia e a dignidade humana.

REFERÊNCIAS

- BARDIN, Laurence. *Análise de conteúdo*. Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.
- BRUNO, Fernanda; BENTES, Anna; FALTAY, Paulo. Economia psíquica dos algoritmos e laboratório de plataforma. *Revista FAMECOS*, Porto Alegre, v. 26, n. 3, e33095, 2019. DOI: <https://doi.org/10.15448/1980-3729.2019.3.33095>.
- CASTELLS, Manuel. *A sociedade em rede*. 12. ed. São Paulo: Paz e Terra, 2009.

CASTRO, Julio Cesar Lemes de. Plataformas algorítmicas: interpelação, perfilamento e performatividade. *Revista FAMECOS*, Porto Alegre, v. 26, n. 3, e33723, 2019. DOI: <https://doi.org/10.15448/1980-3729.2019.3.33723>.

CONGO, Emerson Tavares. A problemática dos “nudes” como violação do dever de fidelidade. *JuLaw*, 2021. Disponível em: <https://julaw.ao/a-problematica-dos-nudes-como-violacao-do-dever-de-fidelidade/>. Acesso em: 27 set. 2026.

CONGO, Emerson Tavares. “Revenge porn” (pornografia de vingança): uma análise do cibercrime sexual no ordenamento jurídico angolano. *JuLaw – Revista Jurídica*, 2023. Disponível em: <https://julaw.ao/revenge-porn-pornografia-de-vinganca-emerson-congo/>. Acesso em: 27 set. 2026.

DESLANDES, Suely Ferreira; SILVA, Claudia Valéria Cardim da; REEVE, Juliana Marins; FLACH, Roberta Matassoli Duran. Vazamento de nudes: da moralização e violência generificada ao empoderamento. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 27, n. 10, p. 3959–3968, 2022. DOI: <https://doi.org/10.1590/1413-81232022710.07112022>.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3. ed. São Paulo: Revista dos Tribunais; Thomson Reuters Brasil, 2021. 368 p.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). ENISA threat landscape 2023. Heraklion: ENISA, 2023. DOI: <https://doi.org/10.2824/782573>. Disponível em: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>. Acesso em: 27 set. 2026.

FLICK, Uwe. An introduction to qualitative research. 4th ed. London: SAGE Publications, 2009.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2019.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global cybersecurity index 2024. 5th ed. Geneva: ITU, 2024. 151 p. Disponível em: <https://www.itu.int/pub/D-HDB-GCI.01-2024>. Acesso em: 27 set. 2026.

LE MOS, André. Cibercultura: tecnologia e vida social na cultura contemporânea. 9. ed. Porto Alegre: Sulina, 2023. 328 p.

LE MOS, André; PASTOR, Leonardo. Experiência algorítmica: ação e prática de dado na plataforma Instagram. *Contracampo*, Niterói, v. 39, n. 2, p. 132–146, 2020. DOI: <https://doi.org/10.22409/contracampo.v39i2.40472>.

LÉVY, Pierre. Cibercultura. Tradução de Carlos Irineu da Costa. 3. ed. São Paulo: Editora 34, 2010. 272 p.

LISBINO, J. K. T. Exposição não consentida de conteúdos íntimos: perspectiva criminológica, jurídica e social. 2021. Dissertação (Mestrado) — Universidade Fernando Pessoa, Porto, 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica: métodos científicos, técnicas de pesquisa e elaboração de referências bibliográficas. 9. ed. São Paulo: Atlas, 2021. 354 p.

MINAYO, Maria Cecília de Souza; GUERRIERO, Iara Coelho Zito. Reflexividade como éthos da pesquisa qualitativa. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 19, n. 4, p. 1103–1112, 2014. DOI: <https://doi.org/10.1590/1413-81232014194.18912013>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Risk management framework for information systems and organizations: a system life cycle approach for security and privacy. Special Publication 800-37 Rev. 2. Gaithersburg: U.S. Department of Commerce, 2018. DOI: <https://doi.org/10.6028/NIST.SP.800-37r2>.

NOVO JORNAL. SIC detém agente da Polícia Nacional por divulgar vídeo de um casal em actividades sexuais. *Novo Jornal*, 11 abr. 2018. Disponível em: <https://novojornal.co.ao/>. Acesso em: 27 set. 2026.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). How's life in the digital age? Opportunities and risks of the digital transformation for people's well-being. Paris: OECD Publishing, 2019. DOI: <https://doi.org/10.1787/9789264311800-en>.

SARLET, Ingo Wolfgang. Direitos fundamentais a prestações sociais e crise: algumas aproximações. *Espaço Jurídico Journal of Law*, Joaçaba, v. 16, n. 2, p. 459–488, 2015. DOI: <https://doi.org/10.18593/ejll.v16i2.6876>.

UNESCO. Alfabetização midiática e informacional: diretrizes para políticas públicas. Paris: UNESCO, 2019.

UNICEF BRASIL. Adolescentes e o risco de vazamento de imagens íntimas na internet. Brasília, DF: UNICEF Brasil, 2019.

ZANINI, Leonardo Estevam de Assis; MACIEL, Silvio Luiz. O combate à pornografia de vingança e a tutela penal da imagem no Brasil. *Revista do Tribunal Regional Federal da 3ª Região*, São Paulo, v. 31, n. 144, p. 15–33, 2020. Disponível em: https://www.revista.trf3.jus.br/index.php/rtrf3/pt_BR/article/view/259. Acesso em: 27 set. 2026.