

ECA DIGITAL E OS DESAFIOS PARA UMA PROTEÇÃO REAL

Lei amplia segurança *online* de crianças e adolescentes, mas efetivação depende de plataformas, Estado e sociedade

EDIÇÃO 24 • ANO 16 • 2026



ACESSIBILIDADE DIGITAL

Norma da ABNT abre caminho para tornar *sites* do país mais inclusivos

MEMÓRIA AUDIOVISUAL

Com o auxílio da IA, acervos da TV brasileira buscam fôlego na era digital

INTELIGÊNCIA ARTIFICIAL

Os impactos da tecnologia nos empregos e nas relações de trabalho

CIBERSEGURANÇA E RESILIÊNCIA

Guia ensina empresas a se defenderem de ataques de *ransomware*

Vamos construir uma Internet mais segura juntos?

No **portal Internet Segura**, do NIC.br, você encontra materiais para **diferentes públicos**:



São **guias, passatempos, fascículos**, materiais diversos que ensinam, de forma didática, como se proteger e **aproveitar o melhor da rede**.

Informe-se, compartilhe conhecimento e use a Internet com segurança!



Acesse: **internetsegura.br**



nic.br **egi.br**



Siga também o **@InternetSeguraBR** no Instagram e receba conteúdos essenciais para navegar com mais segurança!

EDITORIAL

Instituído com a proposta de ampliar a segurança *online* de crianças e adolescentes, o ECA Digital traz consigo uma miríade de desafios. Um deles, basilar, é como equilibrar a indiscutível necessidade de proteger essa população com a natureza aberta da Internet. Nesta edição, a matéria de capa apresenta os principais pontos da nova lei, os desafios para sua implementação e os diferentes papéis de plataformas, poder público e famílias. O texto também mostra que questões como verificação de idade, privacidade, educação digital e supervisão de pais e responsáveis se cruzam na construção de um ambiente digital mais acolhedor para os jovens.

Em “Memória digital”, o trabalho de recuperação e catalogação do Fundo Tupi da Cinemateca Brasileira serve de ponto de partida para uma discussão mais ampla: a importância de preservar acervos audiovisuais que ajudam a manter vivos fragmentos da história e da cultura do país.

Já “Quebrando barreiras” mostra como a ABNT NBR 17225 representou um marco para a acessibilidade digital no Brasil, ao estabelecer diretrizes claras para promover o direito de acesso à Web. A matéria aborda ainda os desafios de transformar essa referência técnica em prática efetiva.

Os impactos da Inteligência Artificial no mundo do trabalho são o mote da matéria “O futuro já chegou”. No texto, especialistas comentam como essa tecnologia vem alterando empregos, relações de trabalho e formas de avaliação e controle.

A IA retorna à pauta em “Novas defesas, novos ataques”, mesa-redonda que discutiu a ambivalência dessa tecnologia na segurança digital. Ela pode ajudar a detectar ameaças em tempo real, mas também abre espaço para novas possibilidades de ataques, fraudes e manipulação de informações.

Ainda no campo da segurança na rede, a edição 24 destaca o guia “*Ransomware: Como se Proteger*”, lançado pelo CERT.br, que traz recomendações sobre como organizações podem se fortalecer diante de uma das principais ameaças digitais da atualidade. A reportagem mostra ainda como o modelo *Ransomware as a Service* (RaaS) multiplicou os ataques e os tornou mais ágeis.

Na entrevista especial, a professora Renée Cummings, referência no debate sobre governança de IA e justiça de dados, defende a ética como base para uma inovação responsável. E, na seção dedicada a artigos, o professor Ivan Moura Campos, ex-coordenador do CGI.br e integrante do Internet Hall of Fame, apresenta um passo a passo para elaborar *prompts* bem estruturados e obter melhores resultados na interação com ferramentas de IA generativa.

Boa leitura!

Demi Getschko | EDITOR-CHEFE

br

ISSN 2763-7417

EXPEDIENTE

EDITOR CHEFE
Demi Getschko

CONSELHO EDITORIAL
Carlos A. Afonso
Eduardo Parajo
Lisandro Granville
Hartmut Glaser

PRODUÇÃO EXECUTIVA
Carolina Carvalho
Ana Nascimento
Thiago Planchart

REDAÇÃO
Editor
Renato Cruz

Colaboradores
Anna Gabriela Costa
Nilton Tuna Mateus
Roberta Prescott
Solange Calvo

Projeto gráfico
Estúdio Claraboia

Diagramação
Grappa Marketing Editorial

Ilustração
(capa, matéria de capa
e personagem)
Camila Gray

A REVISTA .BR É UMA
PUBLICAÇÃO DO COMITÊ
GESTOR DA INTERNET NO BRASIL

JORNALISTA RESPONSÁVEL
RENATO CRUZ | MTB 025.958

CREATIVE COMMONS
ATRIBUIÇÃO
USO NÃO COMERCIAL
NÃO A OBRAS DERIVADAS
(BY-NC-ND)



CONVERSA COM O LEITOR
PARA FALAR COM A REVISTA .BR,
ESCREVA PARA INFO@NIC.BR

CONSELHEIROS CGI.BR | SETEMBRO 2026

MINISTÉRIO DA CIÊNCIA,
TECNOLOGIA E INOVAÇÃO
RENATA VICENTINI MIELLI
(COORDENADORA)

CASA CIVIL DA PRESIDÊNCIA
DA REPÚBLICA
PEDRO H. PONTUAL MACHADO

MINISTÉRIO DAS COMUNICAÇÕES
HERMÃO BARROS TERCIUS

MINISTÉRIO DA DEFESA
JOSÉ ROBERTO DE MORAES RÊGO
PAIVA FERNANDES JÚNIOR

MINISTÉRIO DO DESENVOLVIMENTO,
INDÚSTRIA, COMÉRCIO E SERVIÇOS
CRISTIANE VIANNA RAUEN

MINISTÉRIO DA GESTÃO E DA
INOVAÇÃO EM SERVIÇOS PÚBLICOS
LUANNA SANT'ANNA RONCARATTI

AGÊNCIA NACIONAL DE
TELECOMUNICAÇÕES
ALEXANDRE FREIRE

CONSELHO NACIONAL DE
SECRETÁRIOS ESTADUAIS PARA
ASSUNTOS DE CIÊNCIA, TECNOLOGIA
E INOVAÇÃO – CONSECTI
CLÁUDIO FURTADO

CONSELHO NACIONAL DE
DESENVOLVIMENTO CIENTÍFICO
E TECNOLÓGICO – CNPQ
DÉBORA PERES MENEZES

NOTÓRIO SABER EM ASSUNTO
DA INTERNET
DEMI GETSCHKO

SETOR EMPRESARIAL
CRISTIANO REIS LOBATO FLÔRES

SETOR EMPRESARIAL
MARCOS ADOLFO RIBEIRO FERRARI
HENRIQUE FAULHABER BARBOSA
IVALDO CLETO

TERCEIRO SETOR
BEATRIZ COSTA BARBOSA
PERCIVAL H. DE SOUZA NETO
BIANCA KREMER
RODOLFO DA SILVA AVELINO

COMUNIDADE CIENTÍFICA
E TECNOLÓGICA
RAFAEL DE ALMEIDA EVANGELISTA
MARCELO FORNAZIN
LISANDRO Z. GRANVILLE

SECRETÁRIO EXECUTIVO
HARTMUT RICHARD GLASER

cgi.br



Camila Gray

03	EDITORIAL
03	EXPEDIENTE
19	INDICAÇÕES
26	NOTAS .BR
27	NOTAS MUNDO
40	OPINIÃO
50	PERSONAGEM

CAPA

05 ECA DIGITAL: O QUE VEM DEPOIS?

NOVA LEI É UM MARCO NA PROTEÇÃO INFANTOJUVENIL ONLINE, MAS EFETIVÁ-LA EXIGE REGULAMENTAÇÃO, FISCALIZAÇÃO E EDUCAÇÃO

PATRIMÔNIO

15 FUTURO DO PASSADO

Os desafios de preservar acervos audiovisuais e manter viva a memória da TV no país

INCLUSÃO

20 WEB PARA TODOS

Como a ABNT NBR 17.225 inseriu o Brasil na vanguarda da acessibilidade digital

CIBERSEGURANÇA

28 DE OLHO NA PREVENÇÃO

Com evolução do *ransomware*, CERT.br lança guia para reforçar defesa de empresas

ENTREVISTA

32 ÉTICA COMO BASE

Renée Cummings defende uma IA responsável, segura, equitativa e transparente

MERCADO

36 TRABALHO EM TRANSFORMAÇÃO

Como a IA está moldando empregos e novas formas de controle e avaliação

MESA-REDONDA

41 ENTRE A PROTEÇÃO E O RISCO

Especialistas discutem capacidade da IA de reforçar a segurança e também de ampliar ataques

CONVERGÊNCIAS

45 PROMPT CERTEIRO

Passo a passo para estruturar pedidos e obter respostas da IA mais precisas e úteis

ECA DIGITAL: UM MARCO EM CONSTRUÇÃO

NOVA LEI AMPLIA A PROTEÇÃO
INFANTOJUVENIL *ONLINE*, MAS
AINDA ENFRENTA DESAFIOS
DE IMPLEMENTAÇÃO

TEXTO **SOLANGE CALVO**



A nova legislação que estende princípios do Estatuto da Criança e do Adolescente (ECA) ao ambiente *online* representa um marco na defesa de direitos fundamentais da população infantojuvenil no país. Trata-se da Lei 15.211/2025, conhecida como ECA Digital, um passo significativo para ampliar a segurança desse público na Internet.

Mas ainda há um longo caminho a trilhar em cultura, implementação regulatória e letramento familiar. Desde sua promulgação em 1990, o ECA constitui um instrumento jurídico essencial para a promoção, proteção e garantia dos direitos da infância e da juventude no Brasil. Com a expansão dos ambientes digitais, novas camadas de vulnerabilidade surgem para essa população: exposição excessiva, manipulação algorítmica, coleta de dados, publicidade predatória e adultização precoce.

“O ECA Digital significa mais que um avanço regulatório, é o reconhecimento de que o ambiente digital, sem regras, tornou-se perigoso para crianças e adolescentes e, portanto, precisa haver responsabilidade dos provedores de aplicação e do Estado para auxiliar as famílias na tarefa de proteção desse público altamente vulnerável. Revisitar responsabilidade, privacidade, moderação, consentimento e transparência é o mínimo que a sociedade deve oferecer a quem ainda está formando sua identidade num espaço repleto de riscos nem sempre visíveis. A proteção real nasce da convergência entre legislação com regras claras para todos, educação e presença humana. É o diálogo honesto, a supervisão afetiva e a educação digital que transformam a norma em cultura, e a cultura em segurança de verdade”, diz Renata Mielli, coordenadora do Comitê Gestor da Internet no Brasil (CGI.br).

“A PROTEÇÃO REAL NASCE DA CONVERGÊNCIA ENTRE LEI, EDUCAÇÃO E PRESENÇA HUMANA.

RENATA MIELLI, COORDENADORA DO CGI.br

Em vigor desde 17 de março deste ano, seis meses após sua publicação oficial, o ECA Digital estabelece que empresas responsáveis por produtos e serviços digitais direcionados a crianças e a adolescentes no país ou de acesso provável por eles adotem mecanismos efetivos de proteção. A lei torna obrigatória, por exemplo, a oferta de ferramentas de controle parental e de recursos que permitam limitar e supervisionar o uso dessas plataformas.

“O ECA Digital representa um marco essencial para a proteção de crianças e adolescentes no ambiente digital ao estabelecer deveres específicos para fornecedores de produtos e serviços digitais. O grande desafio é transformar as previsões da lei em medidas concretas, proporcionais e tecnicamente viáveis, capazes de fortalecer a proteção sem comprometer direitos fundamentais, a infraestrutura da Internet e a inovação”, afirma Kelli Angelini, assessora em políticas públicas digitais do Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

DEVERES DAS PLATAFORMAS

A importância dessa atualização legislativa revela-se em múltiplas frentes. Primeiramente, porque atribui deveres específicos às plataformas digitais, jogos, redes sociais, aplicativos, dentre outros, obrigando-os a adotar medidas para promover ambientes mais seguros, adequados e compatíveis com o desenvolvimento de crianças e adolescentes. Entre essas medidas estão a implementação de mecanismos de aferição etária, recursos de supervisão parental, proteção de dados pessoais, limitação de práticas potencialmente nocivas e outras salvaguardas voltadas à prevenção de riscos e à proteção integral desse público.

Depois, porque reafirma o princípio da prioridade absoluta da infância estabelecido no artigo 227 da Constituição Federal, estendendo ao ambiente digital a mesma proteção e segurança já concedidas a menores de 18 anos fora dos meios digitais.

“A aprovação da lei foi resultado de um amplo esforço coletivo dos vários setores da sociedade, reafirmando que crianças e adolescentes devem ter seus direitos garantidos, prioritariamente, não apenas no uso, mas na própria arquitetura de plataformas e serviços digitais. O desafio agora é garantir sua implementação efetiva, robusta e proporcional. Isso exige coordenação entre diferentes órgãos públicos, capacitação institucional, ampla disseminação de informações

para a sociedade e o compromisso das empresas com uma cultura de proteção desde a concepção de produtos e serviços”, afirma Maria Mello, colíder do eixo digital e gerente do programa Criança e Consumo do Instituto Alana.

A efetividade da lei demanda a regulamentação complementar de diversos dispositivos legais, além da atuação coordenada dos órgãos competentes para fiscalizar as determinações do ECA Digital.

CULTURA EM FORMAÇÃO

Na avaliação de Thiago Tavares, professor de direito e tecnologia, fundador e presidente da SaferNet Brasil, a cultura de proteção digital no Brasil ainda é incipiente. Muitos pais, responsáveis e mesmo educadores não têm noção clara de riscos como exploração de imagem, perfis algorítmicos, desafios virais ou microtransações em jogos. “Existem muitas ferramentas com funcionalidades que permitem controlar o acesso da criança à Internet. Mas as pessoas não as usam, por falta de conhecimento ou por limitação de disponibilidade – mas, especialmente, por uma questão de cultura.”

Outro ponto de atenção é a assimetria no desenvolvimento de habilidades digitais. Muitas crianças e adolescentes navegam na Internet sem mediação e, em algumas regiões, a menor infraestrutura de proteção e a escassez de orientação ampliam a vulnerabilidade desse público.

Nesse contexto, destaca-se a importância do letramento digital de pais, responsáveis e familiares. Garantir a segurança *online* não se resume a obrigações legais impostas aos fornecedores de produtos e serviços de tecnologia da informação. Exige diálogo, supervisão e formação crítica.

“Muitos pais acreditam que, ao ver o filho dentro de casa, ele está seguro. Mas, por meio dos dispositivos dentro de casa, pode estar exposto a conteúdos inadequados, interação com criminosos e diferentes formas de violência”, afirma Kelli. Portanto, é fundamental que os responsáveis sejam estimulados e instruídos a estabelecer limites para o uso da Internet e acompanhar os filhos no ambiente digital.

Rodrigo Nejm, doutor em psicologia e colíder do eixo digital e especialista em educação digital no Instituto Alana, ressalta que o ECA Digital redistribui responsabilidades e exige ferramentas mais didáticas, autorização judicial para trabalho infantil artístico na Internet, *design* protetivo e aferição de idade, tudo sem deixar de reforçar o dever de acom-

panhamento das famílias. “É muito fácil e rápido comprar algo ou abrir um novo perfil nas principais redes digitais, mas configurar os serviços de mediação familiar costuma ser muito mais complexo. A lei exige que plataformas disponibilizem ferramentas acessíveis e mais detalhadas para o acompanhamento familiar. A recorrente culpabilização das mães e cuidadoras é mais uma das violências praticadas por modelos de negócio que exploram as vulnerabilidades das famílias”, avalia.

DO PAPEL À PRÁTICA

Um dos grandes desafios para especialistas e profissionais do setor é a operacionalização. Como implementar verificação de idade respeitando a privacidade e a proteção de dados? Como as plataformas irão adaptar os sistemas de moderação de conteúdos em escala? Como lidar com jurisdição internacional (quando a plataforma é estrangeira)?

Em relação à fiscalização e sanções, o ECA Digital define que a Agência Nacional de Proteção de Dados (ANPD) terá papel central como entidade administrativa autônoma para zelar pela aplicação da lei.

Para Waldemar Ortunho, diretor-presidente da ANPD, a implementação do ECA Digital exigirá diálogo permanente entre reguladores, empresas e sociedade. O papel da ANPD será oferecer segurança jurídica por meio de regulamentações e orientações técnicas que permitam a aplicação efetiva da lei.

Cabe à ANPD zelar pela aplicação da nova lei, regulamentar parte de seus dispositivos e fiscalizar seu cumprimento, desenvolvendo plano de ações em seis eixos-chave: regulação, fiscalização, comunicação, gestão estratégica, capacitação e relações institucionais.

“O DESAFIO AGORA É GARANTIR SUA IMPLEMENTAÇÃO EFETIVA, ROBUSTA E PROPORCIONAL.

MARIA MELLO, GERENTE DO PROGRAMA CRIANÇA E CONSUMO DO INSTITUTO ALANA



“HÁ MUITAS FERRAMENTAS PARA CONTROLAR O ACESSO DA CRIANÇA À INTERNET. MAS NÃO SÃO USADAS POR FALTA DE CONHECIMENTO OU POR LIMITAÇÃO TÉCNICA.

THIAGO TAVARES, PRESIDENTE DA SAFERNET BRASIL

O diretor-presidente da ANPD anuncia que os próximos passos da entidade incluem regulamentação de mecanismos de aferição de idade e de supervisão parental, juntamente com outros órgãos do poder público. “É preciso deixar claro que proteger crianças e adolescentes não significa afastá-los da tecnologia, mas criar um ambiente seguro para eles com o apoio da família.”

ALÉM DA LEI

Marina Pita, diretora de promoção de liberdade de expressão da Secretaria de Políticas Digitais (Secom-PR), alerta que a aprovação de uma lei é só o começo. “Com certeza, ela pode ajudar bastante no processo contínuo de discussões e de conscientização, mas a sociedade precisa ser instruída sobre universo digital e educação midiática. E isso envolve o conhecimento sobre seus riscos, vulnerabi-

lidades em um cenário fragilizado por epidemia de golpes e fraudes na publicidade.”

No mesmo sentido, Renata Mielli destaca que “nenhuma lei funciona em sua total potencialidade sozinha”. E completa: “É preciso somar com ações que promovam conscientização e transformação. É essencial debater com autoridades, especialistas e sociedade temas que auxiliem na ressignificação da Internet para um ambiente responsável, ético e seguro para crianças e adolescentes.”

O esforço para qualificar essa discussão também passa por iniciativas de pesquisa e diálogo multissetorial, como as promovidas por CGI.br, Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), que realizam encontros nos quais os rumos da segurança digital infantojuvenil são colocados em pauta.

AFERIÇÃO DE IDADE

A maior parte dos serviços digitais populares entre o público infantojuvenil no país não adotava mecanismos de aferição de idade no momento do cadastro, incluindo os voltados a adultos, antes de o ECA Digital vigorar. Em 21 de 25 serviços analisados, a prática só ocorria posteriormente, para liberar funcionalidades como transmissão ao vivo ou monetização. Esses dados resultam de levantamento conduzido no começo deste ano pelo Cetic.br e foram apresentados no dia 18 de março, em Brasília, durante o evento ECA Digital – Proteção de Crianças e Adolescentes: Perspectivas Globais e Multissetoriais para a Implementação da Lei. A aferição de idade é uma das exigências da **Lei 15.211/2025**.

O estudo do Cetic.br analisou documentos de governança publicados por 25 plataformas, de redes sociais a jogos e serviços de apostas. Onze delas recorriam a terceiros para a função, pedindo com mais frequência o envio de documento oficial, no caso de verificação, ou de *selfie* em foto ou vídeo, para estimativa.

A idade mínima variava, mas as plataformas voltadas a adultos, como jogos *online* e *marketplaces*, exigiam 18 anos, admitindo menos mediante consentimento dos pais ou responsáveis, em alguns casos. A maior parte dos serviços (15 de 25), aliás, oferecia mecanismos de supervisão parental, com ativação facultativa.

O estudo evidencia, ainda, a necessidade de mais transparência dos serviços digitais: poucos publicam relatórios com dados sobre o Brasil, e as regras de acesso por crianças e adolescentes são escritas em linguagem de difícil compreensão. “É fundamental que os dados sobre proteção etária sejam comunicados com clareza, permitindo supervisão parental consciente e eficaz”, destaca Fábio Senne, coordenador geral de pesquisas do Cetic.br/NIC.br.

Juliano Cappi, gerente da assessoria em políticas públicas digitais do CGI.br, reforça: “Este levantamento foi desenvolvido para subsidiar o debate sobre a implementação do ECA Digital e integra um conjunto mais amplo de ações que apoiem a aplicação efetiva da lei”.

GARANTIA ETÁRIA

Há centenas ou milhares de formas de saber se a pessoa que acessa plataforma ou serviço na Internet é um adulto, um adolescente ou uma criança. E há produtos no mercado para isso. A informação de Tony Allen, especialista nessa área, *keynote speaker* num dos painéis do ECA Digital – Proteção de Crianças e Adolescentes, leva a outra premissa: a discussão não é mais se a verificação pode ser feita, mas se pode ser bem feita.

“A garantia de idade”, explicou, “vai além da aferição da informação da data de nascimento de uma criança. Ela é acompanhada da estimativa de idade, análise de características humanas como rostos e mãos, que variam de acordo com a idade. É possível obter ainda dados como a série escolar dos usuários, se usam cartão de crédito ou se estão inscritos em programas de governo.”

De qualquer forma, ele admite que a restrição de idade não precisa ser perfeita, e sim razoável, efetiva e proporcional. Para Ricardo Horta, do Ministério da Justiça e Segurança Pública, é preciso abandonar a ideia “absolutamente equivocada” de que a Internet de uma criança de 4 anos tem de ser a mesma de uma de 8 ou a de um adolescente de 13 ou 17 anos. “Há ferramenta tecnológica para fazer isso agora”, assegurou, lembrando que o Ministério da Justiça já estuda essa questão desde 2024.

Moderadora do painel, Renata Mielli, coordenadora do CGI.br, lembrou que a lei incorpora pontos sensíveis identificados pela instituição – entre eles, proporcionalidade ao grau de risco da atividade, evitando exigências excessivas em ambientes de baixo risco para crianças; privacidade e proteção de dados; inclusão e não discriminação; segurança técnica das ferramentas; interoperabilidade e padrões abertos; transparência e auditabilidade.

Lorena Coutinho, diretora da Agência Nacional de Proteção de Dados (ANPD), entende que a aferição de idade está no coração das discussões sobre proteção da criança. “Temos muita consciência da dificuldade técnica e da complexidade de implementar mecanismos com esse fim. Por isso, estamos dialogando tanto com a sociedade.”

A ANPD começou a fiscalizar no ano passado 37 empresas sob o escopo do ECA Digital, verificando como as medidas propostas vêm sendo implementadas. “Isso nos trouxe algo muito importante para o processo regulatório, que é o diálogo direto com os provedores.” Lorena mencionou ainda a importância da neutralidade tecnológica e a necessidade de equilibrar a acurácia da verificação de idade com a proteção de dados.

Nora Beauvais, representante da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), falou das ações executadas pela organização. “Nós levamos em conta a natureza multifacetada dos riscos oferecidos às crianças pelos serviços *online*. Analisamos uma grande gama de produtos, em termos de funcionalidade e de oferta, para capturar aquilo que as crianças estão fazendo *online*. Tudo isso para dar representatividade às crianças, porque nem todas usam os mesmos serviços.”

Mag Kang, gerente de políticas públicas da Meta, considera a lei brasileira uma das mais avançadas devido à busca de entendimento entre os diversos envolvidos, inclusive o setor privado, para que eles mostrassem o que têm feito. “Acho que a lei tentou de fato entender que existe autonomia progressiva e melhor interesse da criança.”

Na avaliação de Thiago Tavares, presidente da SaferNet Brasil e ex-conselheiro do CGI.br e do NIC.br, os mecanismos de aferição de idade concentrados apenas nas lojas de aplicativos

CONTINUA ►

► CONCLUSÃO

não funcionariam para impedir o acesso de adolescentes e crianças a vários ambientes restritos, desde *marketplaces* que vendem bebidas e cigarros a *sites* pornográficos. E entende que, após a fase política do ECA Digital e da implementação técnica, a parte mais difícil começa agora.

“Na fase atual existem arquiteturas e sistemas a serem desenvolvidos, APIs e *endpoints* a especificar, dados sensíveis a proteger e muita documentação técnica a criar. Iniciamos hoje não uma corrida de 100 metros, mas uma maratona.”

Apesar de necessária, aferição de idade não é uma bala de prata capaz de resolver sozinha problemas que crianças e adolescentes vivem no ambiente digital, alertou Tavares. “Esse mecanismo não deve ser visto como alternativa barata para um problema bilionário que se chama moderação de conteúdo, que é, em última instância, o dever de cuidado com o ambiente digital. Sem investimento em *trust and safety* e na integridade das relações nesse ambiente cria-se uma falsa sensação de segurança.”

Na opinião de Emmanuella Halfeld, do Instituto Alana, a lei traz um desafio enorme, mas é a oportunidade de criar uma Internet diferente. “Estamos num momento muito incrível, quando há mudanças institucionais, quando se tem permissão para criar novas estruturas, com um governo que está aberto para a gente construir isso de forma responsável e pensando nos direitos fundamentais de toda a população.”

“A gente pode pensar em qual Internet quer ter, eliminar recursos que fazem mal e olhar para uma restrição completa quando uma plataforma é tão perigosa e arriscada. Esse é o convite que o ECA Digital faz: para construirmos isso de forma colaborativa. Há muito espaço para preencher.”

PRINCIPAIS EXIGÊNCIAS

- > **PRIVACIDADE:** Fornecedores devem adotar, desde a concepção e por padrão, configurações que assegurem o mais alto nível de proteção à privacidade de crianças e adolescentes e de seus dados pessoais.
- > **VERIFICAÇÃO DE IDADE:** Para acesso a conteúdos, produtos, serviços ou funcionalidades restritos a menores de 18 anos, a simples autodeclaração de idade não é suficiente. A lei exige mecanismos confiáveis de verificação.
- > **SUPERVISÃO PARENTAL:** Devem ser oferecidas ferramentas acessíveis e de fácil utilização para pais ou responsáveis, permitindo configurar privacidade, limitar tempo de uso, restringir compras e supervisionar a utilização dos serviços.
- > **PROTEÇÃO CONTRA CONTEÚDOS ILÍCITOS E INADEQUADOS:** As plataformas devem adotar medidas para prevenir o acesso de crianças e adolescentes a conteúdos incompatíveis com sua faixa etária, disponibilizar canais de denúncia, moderar conteúdos e cooperar com as autoridades nos casos previstos em lei.
- > **AÇÕES COMERCIAIS:** É vedado o uso de dados de crianças e adolescentes para direcionamento de publicidade comercial. A lei também impõe restrições a mecanismos digitais que estimulem o uso excessivo e proíbe caixas de recompensa (*loot boxes*) em jogos destinados a esse público ou por ele acessados.
- > **RELATÓRIOS DE TRANSPARÊNCIA:** Plataformas com mais de 1 milhão de usuários menores de idade no Brasil devem publicar, a cada semestre, relatórios em português com informações sobre denúncias, moderação, identificação de contas de menores, proteção de dados e gestão de riscos.

*Fontes: NIC.br/CGI.br, Senado Federal, FGV e ANPD.

“A PROTEÇÃO DIGITAL DA INFÂNCIA EXIGE SENSIBILIDADE, CONHECIMENTO E COMPROMETIMENTO DE TODOS OS SETORES DA SOCIEDADE.

WALDEMAR ORTUNHO, DIRETOR-PRESIDENTE DA ANPD

GERAÇÃO HIPERCONECTADA

A *TIC Kids Online Brasil 2025*, lançada em outubro do ano passado pelo Cetic.br/NIC.br, revela que 92% dos brasileiros entre 9 e 17 anos são usuários de Internet, o que representa 24,5 milhões de pessoas. A pesquisa destaca os desafios relacionados ao uso intenso de plataformas digitais por essa população e a necessidade de políticas de proteção e mediação familiar.

Entre as evidências inéditas do estudo está a incorporação de ferramentas de Inteligência Artificial generativa na rotina de crianças e adolescentes. Cerca de 65% dos usuários de Internet de 9 a 17 anos relatam usá-la para estudar, criar conteúdo ou até conversar sobre seus sentimentos e emoções. A utilização de IA generativa por crianças e adolescentes pode ampliar as oportunidades *online*, mas também a exposição ao risco em ambiente digitais.

De acordo com Luísa Adib, coordenadora da *TIC Kids Online Brasil*, ao longo da última década, atividades multimídia, como assistir a vídeos, estão entre as práticas mais comuns de crianças e adolescentes na Internet. “Nesta nova edição do estudo, ampliamos esse monitoramento e passamos a investigar os tipos de vídeo acessados por esse público. Vídeos de influenciadores digitais foram vistos mais de uma vez ao dia por 46% das crianças e adolescentes.”

Outro ponto de atenção é a frequência de uso de plataformas digitais. O aplicativo WhatsApp lidera com 53% de acesso “várias vezes ao dia” entre usuários de Internet de 9 a 17 anos, seguido por YouTube (48%), Instagram (48%) e TikTok (46%). Esse quadro revela uma imersão digital que exige atenção ao tipo de conteúdo consumido, ao tempo de exposição e às vulnerabilidades implícitas.

A relação entre publicidade, conteúdos patrocinados e incapacidade de reconhecer tais estímulos se mantém um desafio estruturante. Mais da metade dos usuários de Internet de 11 a 17 anos reportou que teve contato com publicidade ou propaganda em diferentes meios digitais: 55% em redes sociais, 52% em *sites* de vídeos e 52% na televisão. A presença de anúncios em *sites* de jogos alcançou 26% desse público.

“A LEI EXIGE QUE PLATAFORMAS DISPONIBILIZEM FERRAMENTAS ACESSÍVEIS E MAIS DETALHADAS PARA O ACOMPANHAMENTO FAMILIAR.

RODRIGO NEJM, ESPECIALISTA EM EDUCAÇÃO DIGITAL NO INSTITUTO ALANA



“ A MISTURA DE
ENTRETENIMENTO E
PUBLICIDADE PASSA
DESPERCEBIDA POR
GRANDE PARTE DOS JOVENS.

RENATA TOMAZ, PROFESSORA DE COMUNICAÇÃO
DA FGV-RJ

“ OS PAIS NÃO NOTAM QUANDO OS FILHOS ATRAVESSAM AS MADRUGADAS NO CELULAR E DEPOIS DORMEM DURANTE AS AULAS.

KELLI ANGELINI, ASSESSORA DO NIC.br

Para Renata Tomaz, professora de Comunicação da FGV-RJ e pesquisadora de cultura digital e infância, essa mistura de entretenimento e publicidade passa despercebida por grande parte dos jovens, o que acende um sinal vermelho. “Eles reconhecem que os anúncios parecem feitos sob medida, mas não compreendem plenamente como essa personalização acontece.”

O atual panorama reforça a urgência de investir, desde a infância, em educação midiática e em letramento digital, para que novas gerações saibam diferenciar diversão de influência comercial e desenvolvam uma relação mais crítica e consciente com o ambiente *online*. Tudo isso na esteira de fortalecimento regulatório e políticas públicas atualizadas, capacitação crítica de crianças e adolescentes e mediação ativa de pais, responsáveis e educadores.

CONTRIBUIÇÕES DO CGI.br

O CGI.br desempenhou papel relevante na formulação do Estatuto Digital da Criança e do Adolescente (Lei 15.211/2025), reafirmando sua trajetória histórica de promoção do diálogo multissetorial e construção de consensos para o desenvolvimento de políticas públicas e leis relacionadas à Internet no país. Durante a tramitação do Projeto de Lei 2.628/2022, que deu origem ao ECA Digital, o colegiado colaborou tecnicamente, oferecendo sugestões de definições e ajustes. Parte dessas propostas foi incorporada ao texto aprovado pela Câmara dos Deputados.

Após a sanção da Lei 15.211/2025, o comitê continuou colaborando para sua implementação ao encaminhar contribuições à tomada de subsídios aberta pela ANPD. Nela, o CGI.br destacou pontos que precisavam de complementações para interpretação e aplicação adequadas da legislação. Entre eles estão: a definição de “acesso provável” por crianças e adolescentes aos produtos e serviços; a delimitação do que constituem os produtos e serviços de tecnologia da informação; e os critérios para a modulação de obrigações de acordo com o grau de interferência sobre o conteúdo.

O CGI.br também publicou nota pública defendendo que a regulamentação diferencie as obrigações aplicáveis a sistemas operacionais daquelas destinadas às plataformas digitais, considerando as características, funcionalidades e riscos específicos de cada tipo de agente. Na ocasião, alertou que a aplicação uniforme de obrigações a serviços com naturezas distintas pode reduzir a efetividade das medidas de proteção, gerar insegurança jurídica e produzir impactos indesejados sobre a inovação, a concorrência e o funcionamento da Internet.

Já em contribuição à tomada de subsídios da ANPD sobre o Guia Orientativo para Fornecedores de Tecnologia da Informação, o comitê reforçou que a implementação deve ser tecnicamente fundamentada, proporcional, compatível com os direitos fundamentais e orientada à proteção integral de crianças e adolescentes.

MEMÓRIA DIGITAL

ACERVOS HISTÓRICOS
DA TELEVISÃO BRASILEIRA
ENFRENTAM OS DESAFIOS
DA RESTAURAÇÃO E
PRESERVAÇÃO EM TEMPOS
DE INTELIGÊNCIA ARTIFICIAL

TEXTO ANNA GABRIELA COSTA

A televisão brasileira estreou em 18 de setembro de 1950, com a primeira transmissão da tv Tupi, pelo canal 3 em São Paulo. Ao longo de décadas, a emissora construiu um registro dos acontecimentos marcantes da história do país e do mundo. Em comemoração, a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e a Cinemateca Brasileira promoveram a *Jornada Projeto Temático FAPESP / 75 anos da tv no Brasil: O Fundo Tupi no Acervo da Cinemateca Brasileira*. O evento mostrou como o acervo foi recuperado, tratado e catalogado, tornando-se disponível para pesquisadores, produtores culturais e o público em geral.

A equipe de professores, pesquisadores e técnicos do projeto já mapeou mais de 13 mil notícias, catalogou 3.525 registros e digitalizou 36 horas de vídeos, um trabalho minucioso desenvolvido num material sensível: a película de acetato de celulose, que tem o seu próprio processo de deterioração.

“São mais de 180 mil rolinhos de filme de 16 mm referentes aos telejornais da tv Tupi. Esse material cobre aproximadamente o período dos anos 1950 até o fim da década de 1970, já perto da extinção da emissora, que ocorreu no início dos anos 80”, explica Gabriela Queiroz, diretora técnica da Cinemateca Brasileira. “Esses rolinhos de película duram geralmente um ou dois minutos e contêm o material usado nas reportagens, não os telejornais editados.”

Além dos noticiosos, há novelas e outros programas da tv Tupi gravados em fitas quadruplex, as primeiras usadas na televisão.

O projeto é coordenado pelo professor Eduardo Morettin, da Escola de Comunicação e Artes (ECA) da USP, que destaca os desafios da organização do material e conta como esse processo vem sendo conduzido. “Cada integrante da equipe trabalha num assunto específico, e são essas pesquisas que acabam orientando a seleção dos materiais. O ideal seria seguir uma política de processamento e digitalização de todo o acervo.”

De acordo com o professor, são milhares de fitas vhs e quadruplex, filmes em 16 mm e muitos suportes que exigem procedimentos específicos de preservação – e os recursos para digitalizar nesse ritmo são limitados. “Se considerarmos que existem cerca de 180 mil itens e o projeto pretende dar conta de aproximadamente 4 mil ou 5 mil, estamos falando de um trabalho de cinco anos que cobre apenas uma pequena parcela dessa coleção”, explica Morettin.

“ESTAMOS FALANDO DE UM TRABALHO DE CINCO ANOS QUE COBRE APENAS UMA PEQUENA PARCELA DESSE ACERVO.”

EDUARDO MORETTIN, DA ESCOLA DE COMUNICAÇÃO E ARTES DA USP

O pesquisador afirma que seria necessário um investimento maciço para de fato digitalizar e colocar tudo à disposição do público, como é feito em outros países.

Apesar disso, Eduardo Morettin destaca algumas ações que vêm sendo muito bem conduzidas no Brasil. “O trabalho na tv Cultura é fantástico. Há anos uma equipe de especialistas vem organizando o acervo, procedendo à digitalização com a especificidade da tv e rádio. Então, há coleções de discos, de áudios, de DVDs”, comenta.

No entanto, o pesquisador reitera que esses materiais só vão tornar-se públicos de fato a partir do momento em que forem exibidos em sala de aula e incorporados a pesquisas e outras ações.

ACERVO DA TV CULTURA

Na tv Cultura, o acervo de películas reúne milhares de programas educativos, culturais e jornalísticos, veiculados principalmente na década de 1970 e começo dos anos 1980. Desde 2022, esse material passou a ser digitalizado continuamente em dois *scanners* de alta resolução.

O acervo de vídeo, que inclui diversos formatos, desde as fitas quadruplex a grandes conjuntos de U-matic, Beta e vhs, além de DVDs, também tem sido digitalizado de forma sistematizada e conectada com a preservação e o acesso. “São mais de 120 mil mídias que percorrem toda a história da televisão brasileira e do próprio país”, afirma Lúgia Farias, gerente de documentação da tv Cultura.

Ela explica que a preservação não termina na digitalização, nem no armazenamento na nuvem, mas é um processo contínuo. “A evolução tecnológica de suportes e servidores exige que a cada cinco ou seis anos todo o acervo já digitalizado seja transferido para um formato mais recente.

Além do investimento que isso exige, há sempre o risco de a migração apresentar problemas ou perda de conteúdo.”

Lígia entende que a preservação da memória televisiva deveria ser responsabilidade de todos os veículos de comunicação, independentemente de sua natureza pública ou privada. “A diferença está menos na obrigação e mais na missão institucional: emissoras públicas, em geral, têm como princípio explícito a promoção da cultura, da educação e do acesso ao conhecimento, o que tende a reforçar o compromisso com a preservação e a difusão de seus acervos. Entretanto, preservar exige investimento permanente em equipamentos, formação de equipes e atualização tecnológica. As TVs públicas sofrem com falta de verbas em maior medida do que as emissoras privadas”, diz.

RESPONSABILIDADE DAS TVS PÚBLICAS

“Ao contrário das emissoras privadas, a TV Cultura não tem entre seus objetivos auferir lucro, o que não a exime da responsabilidade de conciliar sua vocação pública com os direitos de imagem e as normas que regulam o uso e acesso aos conteúdos”, explica Lígia Farias.

Eduardo Morettin, professor da ECA/USP, comenta que, quando se fala de acervos televisivos, boa parte deles — ou talvez a maioria — é privada. “Hoje, uma das questões centrais é que esse material também é explorado comercialmente, principalmente por meio de plataformas de *streaming*.”

O especialista alerta que há poucos acervos televisivos públicos, mas traz como exemplo o da Empresa Brasil de Comunicação (EBC) e alguns conjuntos depositados em museus, cinematecas e arquivos, como o da TV Tupi.

Gabriela Queiroz, diretora técnica da Cinemateca, ressalta que o compromisso da organização é garantir o acesso a este acervo. O material pode ser consultado pelo site da Cinemateca, na aba Banco de Conteúdos Culturais (BCC). “Muitas emissoras tratam seus arquivos como ativos comerciais, o que é compreensível, mas reforça ainda mais a responsabilidade da Cinemateca em disponibilizar esse material para pesquisa e para o público.”

DIGITALIZAÇÃO DOS ACERVOS

A preservação digital de acervos culturais ainda enfrenta dificuldades no Brasil. De acordo com a mais recente edição da Pesquisa TIC Cultura, de 2024, mais da metade dos pontos de cultura e arquivos (55%), além de

26% dos cinemas, afirmam ter dificuldades para garantir a preservação de materiais digitalizados no longo prazo. Apesar disso, o estudo revela avanços na infraestrutura tecnológica dos equipamentos culturais. Em 2024, a conexão à Internet estava praticamente universalizada: 100% dos arquivos e cinemas e 96% dos pontos de cultura declararam utilizar a rede.

Se há dificuldades na preservação de acervos, como condições climáticas adequadas, controle de umidade e temperatura, a tecnologia tem sido uma grande aliada nesse trabalho. Segundo Lígia Farias, hoje, a digitalização e a preservação de acervos audiovisuais têm à sua disposição uma combinação de sistemas especializados, automação e ferramentas baseadas em Inteligência Artificial.

“O uso da IA começou com a criação e implementação dos sistemas MAM [*Media Asset Management*], que organizam, gerenciam e permitem a recuperação de grandes volumes de arquivos digitais e metadados, e são usados por praticamente todos os arquivos televisivos do mundo, que acumulam milhões de horas de conteúdo”, explica.

Nos últimos anos, a IA passou a ser aplicada em outras etapas do processo. No campo da preservação, algoritmos conseguem detectar automaticamente defeitos causados pela deterioração de suportes analógicos ou por falhas durante a digitalização. “Essas ferramentas otimizam alguns processos de restauração, como correção de cores degradadas, interpolação de quadros e técnicas de super-resolução, que aumentam a definição da imagem sem apenas ampliar os *pixels*”, conta Lígia.

Outra ferramenta importante é a catalogação automatizada. Sistemas de IA são capazes de identificar fala, vozes, rostos, objetos, música e analisar narrativas, gerando descrições em linguagem natural que permitem localizar trechos específicos dentro de um vídeo ou áudio.

A especialista destaca que a TV tem experimentado diversos *softwares* disponíveis no mercado para traduzir o que foi gravado anos atrás em SD para HD, mas alerta que o foco das discussões tem sido os critérios em relação às questões subjetivas e éticas “Até que ponto a construção da imagem de 50 anos atrás deve ser ignorada? Até que ponto ela deve ser modificada para adaptar-se à estética atual?”

O tema tem sido discutido em encontros internacionais, como os promovidos pela Federação Internacional de Arquivos Televisivos (FIAT/IFTA). Em 2024, durante um

desses eventos, o Instituto Nacional de Audiovisual (INA) da França anunciou um projeto para descrever automaticamente todo o seu acervo, com mais de 25 milhões de horas de vídeo. Com o uso de IA, a estimativa é concluir o processo em cerca de 12 meses, algo inviável de forma manual.

“Mas a IA não substitui o trabalho humano. Profissionais de documentação e preservação continuam responsáveis por validar metadados, interpretar contextos e garantir a integridade e a autenticidade dos conteúdos”, complementa Lígia Farias, da TV Cultura.

A pesquisa TIC Cultura 2024 mostra que a falta de capacidade de armazenamento ou hospedagem dos materiais digitalizados é uma das dificuldades mais frequentemente relatadas pelos equipamentos culturais brasileiros.

O PAPEL DA ABERT

A Associação Brasileira de Emissoras de Rádio e Televisão (Abert) entende que a política pública em relação à memória do audiovisual tem melhorado, mas ainda carece de apoio para atingir desde a grande rede de televisão até a menor emissora do Brasil.

“Podemos transformar os acervos em novos produtos, resgatar a própria história do país, e não apenas da radiodifusão, construir novos formatos multiplataforma e lançar luz sobre o passado. As políticas ainda precisam entender melhor os conteúdos televisivos, principalmente pela quantidade, pela qualidade e pelo restauro do que ficou”, afirma Cristiano Flores, presidente-executivo da Abert.

“**A EVOLUÇÃO
TECNOLÓGICA EXIGE
QUE A CADA CINCO OU
SEIS ANOS O ACERVO
DIGITALIZADO SEJA
TRANSFERIDO PARA
MÍDIAS MAIS NOVAS.**

LÍGIA FARIAS, GERENTE DE DOCUMENTAÇÃO
DA TV CULTURA

Dentre as iniciativas em andamento, Flores destaca o Memorial Virtual da Radiodifusão Brasileira, hospedado no site da entidade, sob a curadoria do coordenador do Centro de Memória, Elmo Francfort.

“Conseguimos dar luz e trazer conteúdos de outras épocas para um ambiente digital e virtual, no qual é possível conhecer a história não só do rádio brasileiro, mas da própria televisão aberta, década após década, e também por gênero. Devemos ampliar este conteúdo, porque a história se escreve a cada dia”, recomenda Flores.

DIREITOS AUTORAIS

Cuidar dos direitos autorais e das políticas ligadas ao uso da imagem e à segurança jurídica está no radar da Abert, afirma o diretor-presidente. Mas o grande desafio é a preservação do conteúdo das emissoras que não estão mais em atividade.

“Resgatar esse passado envolve herdeiros e muitos outros interessados, cujos direitos conexos e patrimoniais fazem com que esse acervo exista. Isso suscita um debate muito grande, antes mesmo de muitos conteúdos caírem em domínio público. Uma vez que não se consegue descobrir quem foi o autor, ou em alguns casos de emissoras extintas cujos detentores dos direitos sumiram ou são desconhecidos, batalhar pela legalidade deste conteúdo é um desafio à parte.”

Flores também demonstra preocupação com o risco de que edições, distorções de conteúdo e a manipulação de imagem e som por Inteligência Artificial comprometam a legitimidade do material. “Isso pode gerar notícias falsas e desinformação usadas para finalidades escusas. Como associação que representa a radiodifusão brasileira — cada vez mais expandida pela produção multiplataforma e pelo crescimento da tecnologia digital — precisamos ter muito cuidado com esse conteúdo.”

A pesquisa TIC Cultura revela que metade dos pontos de cultura (50%) e um quinto dos arquivos (21%) e cinemas (19%) declararam que a falta de conhecimento sobre direitos autorais e outros temas jurídicos é uma das dificuldades na digitalização de seus acervos. De acordo com o estudo, a formação em torno deste tema poderia melhorar a disseminação de conteúdos e garantir acesso a acervos digitais no Brasil.

OUTUBRO

LIVE INTRA REDE

Cibersegurança: O Papel Essencial do Fator Humano
Dia 14 | Transmissão *online*
<https://intrarede.nic.br/>

11º SIMPÓSIO DE CRIANÇAS E ADOLESCENTES NA INTERNET

29 e 30 | São Paulo (SP)
Hotel Intercontinental
Transmissão *online*
<https://criancaseadolescentes.nainternet.nic.br/>

NOVEMBRO

LACIGF

4 a 6 | Fortaleza
Centro de Eventos do Ceará
Transmissão *online*
<https://lacigf.org/>

DEZEMBRO

16ª SEMANA DE INFRAESTRUTURA DA INTERNET NO BRASIL

7 a 11 | São Paulo (SP)
Centro de Convenções Rebouças
Transmissão *online*
<https://semanainfra.nic.br/>

Veja mais em

<https://cursoseventos.NIC.br/>

Os eventos *online* são transmitidos pelo canal **NICbrvideos** no YouTube.

DIREITO E INTELIGÊNCIA ARTIFICIAL: VOLUME VI – 2026

WILLIS SANTIAGO GUERRA FILHO, PAOLA CANTARINI E LUIZ ALEXANDRE REALI COSTA, COORD. (LUMEN JURIS)

O livro examina a IA como tecnologia de propósito geral, força ontológica e novo regime de normatividade. Ao reunir filosofia da técnica, teoria crítica, sociologia digital e governança multinível, revela como sistemas algorítmicos reconfiguram memória, tempo, agência e desigualdade, além de produzir novas formas de poder e estratificação. A análise abrange desde riscos ambientais e epistêmicos até a automação da desigualdade, destacando a necessidade de uma compreensão crítica capaz de superar tanto distopias tecnofóbicas quanto utopias.

IA RESPONSÁVEL NA ENCRUZILHADA – DESAFIOS GEOPOLÍTICOS, REGULATÓRIOS E DE GOVERNANÇA

GLAUCO ARBIX E RODRIGO BRANDÃO, ORG. (EDITORA PAPAGAIO)

A obra dos pesquisadores brasileiros reúne 11 ensaios sobre governança global da IA, regulamentação, cadeias de semicondutores, centros de pesquisa, ética, discurso de ódio nas plataformas digitais, uso empresarial da tecnologia e indústria de jogos eletrônicos. Eles defendem que o avanço da IA deve basear-se no interesse público, na ética e na democracia, destacando o papel do Estado e das políticas públicas na

construção de uma tecnologia responsável e inclusiva.

MEIO QUENTE

HITO STEYERL (UBU)

A autora mostra como a IA, ao ampliar exponencialmente a produção visual, revela sua própria limitação. Mas, ao mesmo tempo, reconhece que a ilusão nunca foi estranha às imagens – da fotografia ao cinema. Só que agora ela atinge um novo patamar, em que realidade e simulação tornam-se indistinguíveis. Entre diagnósticos e propostas de resistência, Hito Steyerl expõe as contradições de um capitalismo que transforma até a crise climática em mercado especulativo. Para ela, a questão central, portanto, é como ainda é possível pensar, criar e agir em meio ao excesso.

SOCIEDADE DIGITAL

MANUEL CASTELLS (PAZ & TERRA)

Manuel Castells analisa as consequências sociais, econômicas, culturais e políticas da digitalização em diversas áreas. Entre os temas abordados estão comunicação em rede, vigilância estatal e privacidade, mercados financeiros, estrutura espacial das cidades, educação e impacto das *big techs* e das redes sociais. O autor explica também como a desinformação, as desigualdades e exclusões digitais têm moldado a geopolítica contemporânea. E ainda discute o papel da IA, do trabalho remoto, das criptomoedas e do capitalismo de dados, destacando os dilemas éticos e regulatórios.

QUEBRANDO BARREIRAS

UM ANO APÓS SUA
PUBLICAÇÃO, A ABNT NBR
17.225 TRAÇA UM CAMINHO
TÉCNICO PARA AMPLIAR A
ACESSIBILIDADE EM *SITES* E
SERVIÇOS DIGITAIS NO BRASIL

TEXTO ROBERTA PRESCOTT

Para exercer a plena cidadania, pessoas com deficiência (PcD) precisam ter o direito de acessar a Internet e os serviços ofertados por meio da Web. No entanto, o ambiente digital está longe de contemplar, de forma ampla e efetiva, a diversidade de necessidades de todos os seus usuários — uma realidade que pode ser transformada.

Em 11 de março, fez um ano que a Associação Brasileira de Normas Técnicas (ABNT) publicou a NBR 17.225. A norma estabelece requisitos para facilitar e otimizar o acesso de todas as pessoas, especialmente as com deficiências — situacionais, temporárias ou permanentes — a ambientes virtuais, eliminando ou mitigando as barreiras para utilização de *websites*. Antes disso, a ABNT NBR 17.060 já havia definido diretrizes semelhantes para aplicativos de dispositivos móveis.

Com a criação da ABNT NBR 17.225, o principal avanço foi alcançado: hoje o país conta com uma referência técnica capaz de orientar a implementação da acessibilidade digital. O desafio, agora, é outro. Transformar esse conhecimento em política pública, prática de mercado e requisito permanente para o desenvolvimento de produtos e serviços digitais.

“A acessibilidade na Web é um direito para que todo cidadão possa usufruir de serviços na Internet”, frisa Eleidimar Odilia, diretora do Departamento de Serviços Públicos Digitais do Ministério da Gestão e da Inovação. Ela foi uma das participantes da **Conferência de Acessibilidade Digital – Todos na Web**, iniciativa do Centro de Estudos sobre Tecnologias Web (Ceweb.br), área do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), realizada em março deste ano.

Na avaliação da diretora, falta ampliar a consciência na aplicação dos instrumentos de inclusão, sendo necessário enxergar a acessibilidade como uma porta para o exercício da cidadania. “Todas as pessoas estão conseguindo passar por essa porta? Hoje sabemos que não.”

Na mesma linha, Hartmut Glaser, secretário-executivo do Comitê Gestor da Internet no Brasil (CGI.br), lembra que facilitar o acesso à Web de quem tem alguma limitação física ou intelectual é uma forma de promover inclusão social, uma vez que “deficiência não pode significar exclusão, principalmente na Internet, que é uma ferramenta para incluir pessoas e fomentar o relacionamento entre seres humanos”.

“QUEREMOS QUE A NORMA DA ABNT SEJA AMPLAMENTE ADOTADA E REFERENCIADA EM LEIS.”

VAGNER DINIZ, GERENTE DO Ceweb.br

DA LEI À PRÁTICA

A Lei Brasileira de Inclusão (13.146/2015) determina, em seu artigo 63, que é obrigatória a acessibilidade nos sítios da Internet mantidos por empresas com sede ou representação comercial no país ou por órgãos de governo. A medida foi pensada com o intuito de eliminar barreiras de acesso, garantindo o uso desses *sites* pelas PcD, que representam 7,3% da população brasileira com 2 anos ou mais de idade, segundo o Censo 2022.

Embora a legislação tenha trazido avanços, a ausência de diretrizes claras dificultava sua aplicação prática. A ABNT NBR 17.225 preenche essa lacuna ao estabelecer requisitos técnicos baseados nas Diretrizes de Acessibilidade para Conteúdo Web (WCAG 2.2), principal referência internacional no tema.

Reinaldo Ferraz, especialista em padrões e acessibilidade na Web no Ceweb.br e no W3C Chapter SP, destaca que mesmo com diretrizes internacionais disponíveis, uma normativa técnica nacional que contempla esses padrões é importante para o cenário local. Entregar um material em português e com linguagem mais fácil de ser compreendida, portanto, ditou a criação da ABNT NBR 17.225.

Ele acrescenta que, ao reunir os mais atuais padrões mundiais para acessibilidade digital, a norma coloca o Brasil à frente de outros países em relação ao tema. “É, sem dúvida, um marco”, enfatiza.

TRABALHO COLETIVO

A elaboração da ABNT NBR 17.225 é resultado de um amplo esforço colaborativo liderado pelo Ceweb.br|NIC.br. Com coordenação de Ferraz, o grupo de trabalho multidisciplinar reuniu mais de 170 especialistas em encontros iniciados em outubro de 2022, contando com a participação ativa de pessoas com deficiência. O rigor desse processo garantiu que, ao chegar à fase de Consulta Nacional,

o documento recebesse ampla aprovação do público após a ponderação dos questionamentos finais.

A norma é um dos marcos normativos na consolidação da acessibilidade digital como direito, responsabilidade institucional e eixo estruturante de políticas públicas no Brasil. Reinaldo Ferraz avalia que o primeiro ano da ABNT NBR 17.225 foi de conscientização, de apresentá-la à sociedade, apontando como é simples de ser seguida.

“Queremos que a Norma da ABNT seja amplamente adotada e referenciada em leis, para o benefício não só das pessoas com deficiência. Não existe justificativa técnica, econômica ou social para não adotar as melhores práticas globais de acessibilidade digital. Isso significa inclusão digital e garantia de direitos”, destaca Vagner Diniz, gerente do Ceweb.br.

Nesse sentido, o CGI.br publicou nota técnica em que defende que os projetos de lei sobre acessibilidade digital em tramitação no Congresso Nacional adotem como referência as normas da ABNT sobre o tema, especialmente a ABNT NBR 17.225 e a ABNT NBR 17.060.

EVOLUÇÃO DA LEGISLAÇÃO

Deborah Kelly Affonso, promotora de Justiça do Estado de São Paulo, especialista em direitos humanos e pessoas com deficiência, lembra que, no Brasil, desde 1989 a lei federal Nº 7853 contempla pessoas com deficiência.

Depois, a Lei 10.098/2000 estabeleceu normas gerais e critérios básicos para garantir a acessibilidade de pessoas com deficiência ou mobilidade reduzida, e o Decreto Federal nº 5.296/2004 reforçou a implementação de acessibilidade seguindo as normas técnicas da ABNT.

“Ninguém pode discutir se aplica ou não a lei de acessibilidade, porque está na Constituição. O Brasil não está atrasado; ao contrário, outros países nos seguem em matéria de inclusão de PcD. Mas não existe meia acessibilidade: ou é acessível ou não é, porque quase acessível não é acessível”, frisa Deborah.

Para a promotora de Justiça do MPSP, uma dúvida recorrente diz respeito à emissão de certificado de acessibilidade. “Nenhuma entidade privada pode determinar que uma norma seja seguida; a certificação tem de vir de órgão público”, defende.

REGULAMENTAÇÃO

José Rubens Plates, procurador do Ministério Público Federal, lembra que para a pessoa com deficiência, a

Internet é um labirinto cheio de barreiras. “Temos de refletir e avançar nisso. Estamos participando da construção da história da acessibilidade digital.”

Tanto o MPSP quanto o MPF fazem procedimentos fiscalizatórios e apurações envolvendo acessibilidade em sites e aplicativos, grandes empresas de comércio eletrônico, portais governamentais, de sindicatos, culturais e de instituições financeiras, entre outros. Plates conta que dezenas já se regularizaram e muitos têm assumido uma postura consciente.

Enquanto Plates cobra o governo federal pela regulamentação, Deborah Kelly Affonso, do MPSP, entende que não é necessário regulamentar, pois já é lei. “O que faltava era a norma, e agora só falta definir qual órgão do governo procederá à certificação.”

Plates argumenta, porém, que a regulamentação dá mais força para cobrar as instituições. “A lei existe, a NBR mostra como fazer e a regulamentação por decreto dirá o que acontece com quem a descumpre.”

Sidney Tobias, diretor de participação da Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo (ProdAm), faz uma distinção. “A regulamentação ajuda a dar direcionamento e faz as empresas levarem o assunto a sério. Mas para nós, do setor público, não é a multa, mas a insatisfação do cidadão que vai resolver a questão da acessibilidade, pois tem poder de descontinuar uma gestão.”

DESAFIOS

A aplicação da ABNT NBR 17.225 em projetos reais – considerando diferentes contextos de maturidade técnica, organizacional e institucional – ainda é um desafio. Bernardo Barlach, gerente de parcerias e relacionamento para acessibilidade do Google, ressalta que o lançamento da norma foi o ponto de partida, não o de chegada. “A repercussão da norma foi positiva, porque trouxe segurança técnica. Antes, havia obrigatoriedade legal, mas faltava o como fazer”, analisa.

Para Barlach, a grande vitória da ABNT NBR 17.225 foi o alinhamento a padrões internacionais, o que facilita o trabalho das empresas brasileiras que querem exportar *software* e das estrangeiras que atuam no Brasil. Contudo, ele cita como maior entrave a lacuna na implementação técnica.

Bernardo Barlach diz que para a adoção da norma a palavra-chave é IA, porque ela torna tudo mais dinâmico. Como exemplo, aponta o trabalho do Google com NAI, que

“DEFICIÊNCIA NÃO PODE SIGNIFICAR EXCLUSÃO NA INTERNET, QUE É UM MEIO DE INCLUSÃO.”

HARTMUT GLASER, SECRETÁRIO-EXECUTIVO DO CGI.br

são interfaces nativamente adaptáveis. “O Google entende que a tecnologia tem de ser construída com a comunidade local. Quando quebramos barreiras digitais, estamos desbloqueando potencial humano.”

No Brasil, o Itaú Unibanco vem amadurecendo suas práticas há dez anos, com o lançamento do *Estatuto de Acessibilidade*. “Nos últimos anos, fomos entendendo que ter digital no nome não significa que se trata só de tecnologia: é a entrega do produto digital. E estou falando sobre o cliente”, acrescenta Sandyara Peres, coordenadora de *design* no banco.

Ela avalia que a NBR 17.225 leva em consideração o ambiente brasileiro. “As ferramentas nos ajudam; o que falta é a integração dos setores de ponta a ponta, e isso envolve integrar o usuário”, diz. Até 2030, o Itaú terá todas as jornadas para o cliente modernizadas para incluir acessibilidade — e a NBR foi um avanço neste sentido, segundo a coordenadora.

Sidney Tobias, da Prodam, argumenta que oferecer acessibilidade nos produtos é, atualmente, um diferencial, mas não deveria ser. Ele acredita que com o lançamento da NBR 17.225 ficou mais fácil argumentar com os políticos acerca da necessidade de seguir os padrões. Para maior aplicabilidade, sugere que a acessibilidade digital seja matéria obrigatória em cursos que trabalham na formação de profissionais nesta área.

A Internet deveria ser igual para todos. “Tenho o sonho de que a norma comece efetivamente a ser usada em políticas públicas, que seja exigência real para *sites* tanto de governo quanto de empresas privadas”, ressalta Reinaldo Ferraz.

Demi Getschko, diretor-presidente do NIC.br, ressalta que a Internet dá a todos os indivíduos a capacidade de participar. “Estamos comemorando um ano da norma que traz mais gente para essa participação”, diz Getschko.

NÍVEIS DE CONFORMIDADE

As Diretrizes de Acessibilidade para Conteúdo Web (WCAG) 2.2, nas quais a ABNT NBR 17.225 se baseia, têm três níveis de conformidade. O Nível A reúne os requisitos mínimos de acessibilidade. Ao atender a esses critérios, algumas barreiras são eliminadas, mas ainda podem permanecer obstáculos que dificultam o acesso e o uso do conteúdo por pessoas com deficiência.

Já o Nível AA é recomendado para a maioria do conteúdo Web. Contempla todos os requisitos do nível A e AA. Ao atender a esse padrão de conformidade, as barreiras de acessibilidade são significativamente reduzidas, permitindo que um número maior de pessoas com deficiência acesse e utilize o conteúdo.

Para alcançar a conformidade AAA, a página da Web deve atender a todos os critérios de sucesso do nível A, AA e AAA. No entanto, a própria WCAG 2.2 não recomenda exigir esse patamar de conformidade para *sites* ou aplicações inteiros, pois nem sempre é possível atender a todas as exigências.

MOBILIZAÇÃO E REFLEXÃO

Cid Torquato, do ICOM, InovaUSP e Prêmio wsa Brasil, tem uma meta: tornar o 11 de março o Dia Nacional da Acessibilidade Digital. A data seria uma escolha simbólica para um momento de mobilização e de reflexão sobre os desafios estruturais no fortalecimento da governança e na garantia de acesso equitativo aos serviços digitais para pessoas com deficiência.

Em 10 de março deste ano, a Comissão de Educação e Cultura (CE) do Senado aprovou o projeto da senadora Mara Gabrilli (PSD-SP) que cria o Dia Nacional da Acessibilidade Digital, em 11 de março (PL 2.251/2025). O texto seguiu para análise da Câmara dos Deputados. De acordo com o relator na CE, o senador Bruno Bonetti (PL-RJ), a data pretende estimular debates sobre inclusão e incentivar empresas e órgãos públicos a tornarem plataformas digitais mais acessíveis.

“NORMA É FÁCIL DE USAR PARA QUEM TEM E QUEM NÃO TEM CONHECIMENTO DE WCAG.

REINALDO FERRAZ, ESPECIALISTA NO Ceweb.br

Para Bonetti, trata-se de uma medida voltada à consolidação da cidadania num mundo cada vez mais mediado por telas e algoritmos. A proposta visa, ainda, a estimular o mercado e o setor público a priorizarem a facilidade de uso em suas plataformas.

Além de estabelecer o Dia Nacional da Acessibilidade Digital, Torquato batalha para regulamentar o artigo 63 da Lei Brasileira de Inclusão (Lei nº 13.146/2015). “É um absurdo que, um ano após a norma, não tenhamos esse artigo regulamentado”, diz. Ele também espera que sejam incluídos os aplicativos no mesmo artigo 63, seguindo-se a regulamentação.

ACESSIBILIDADE EM PAUTA

Um *podcast* explica de forma descomplicada a norma ABNT NBR 17.225 e sua aplicabilidade na rotina de criação de conteúdo, *design*, desenvolvimento e gestão de produtos digitais. Lançado neste ano, o *podcast* “Todos na Web: Acessibilidade em pauta” detalha os requisitos da norma em linguagem fácil e inclusiva. A iniciativa, capitaneada pelo Ceweb.br, é resultado da cooperação com a Embaixada do Reino Unido no Brasil e com a Secretaria de Governo Digital, e de parceria com o W3C Chapter São Paulo, Movimento Web para Todos e Acesso para Todos.

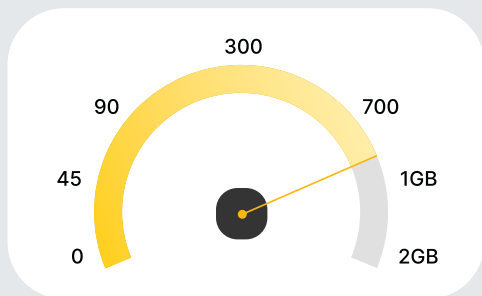
“O projeto nasce para apoiar desenvolvedores, *designers*, comunicadores e gestores públicos na eliminação de barreiras *online*, fortalecendo a acessibilidade na Web. A partir da transmissão de boas práticas, o Ceweb.br reforça seu compromisso com uma Web aberta, universal e verdadeiramente acessível para todas as pessoas”, explica Vagner Diniz, gerente do Ceweb.br. “Foi um desafio, mas acho que a ideia foi tornar o conteúdo menos complicado. O material baseou-se na norma, que, por sua vez, já foi uma maneira de descomplicar a WCAG”, diz Cláudia Martin Nascimento, do Acesso para Todos.

Para Gabriel Izaguirre, da embaixada do Reino Unido, o *podcast* resume bem o propósito e o objetivo de estreitar a distância entre as normas e a aplicação delas. “Sabemos que as disposições podem ser complexas quando encaramos um conteúdo com linguajar técnico, e isso acaba sendo uma barreira”, acrescenta Jeniffer Deus, do Ceweb.br. Justamente por isso, o *podcast* adota um estilo de conversa, convidando pessoas do grupo de trabalho que criou a norma para contar vivências práticas e explicar os objetivos. “Foi um trabalho desafiador, com acessibilidade desde o início, quando concebemos o roteiro, olhando para quem vai receber a informação”, destaca Simone Freire, da Espiral Interativa e do Movimento Web para Todos. “Como traduzir o desenvolvimento técnico em linguagem que será acessível, pensamos em que tipo de experiência vamos abordar, que tipo de vivência vamos compartilhar e como apresentar a norma de forma que não seja extremamente técnica. Ou seja, como vamos levar a conscientização para além da bolha de tecnologia”, finaliza Simone.



ACESSE O PODCAST
TODOS NA WEB

[https://nic.br/podcasts/
todosnaweb/](https://nic.br/podcasts/todosnaweb/)



Sua Internet está entregando o que **você precisa?**

O medidor **SIMET**, do NIC.br, vai além do teste de velocidade: mostra, em linguagem simples, se sua conexão é boa para trabalho remoto, *streaming*, jogos, redes sociais e educação a distância.

Diferenciais do SIMET

- ✓ Grátis – disponível para celular, computador e navegador.
- ✓ Resultados claros e dicas para melhorar sua conexão.
- ✓ Isento e neutro – desenvolvido por uma entidade sem fins lucrativos, sem interesses comerciais.
- ✓ Suas medições ajudam a melhorar a Internet no Brasil.

Teste agora e descubra! >> simet.nic.br



nic.br cgi.br

NOTAS .BR

COMISSÃO DE CCTI NO NIC.br

Integrantes da Comissão de Ciência, Tecnologia e Inovação (CCTI) da Câmara dos Deputados visitaram a sede do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e seu *data center* na capital paulista. No encontro, receberam informações sobre temas estratégicos, como conectividade, segurança digital, governança da Internet e desenvolvimento tecnológico. Átila Lira (PP/PI) e André Figueiredo (PDT/CE) foram recebidos pelo diretor-presidente do NIC.br, Demi Getschko, e outros gestores da entidade. O secretário-executivo Hartmut Glaser lembrou que o diálogo entre as instituições tem sido constante e resultou em importantes atos legislativos, como o Marco Civil da Internet, a LGPD e o ECA Digital.

INFORMAÇÃO VIA INTERNET

A pesquisa *Painel TIC – Integridade da Informação*, desenvolvida pelo NIC.br e pelo CGI.br, aponta que as plataformas digitais são o principal meio de acesso à informação dos brasileiros, superando rádio e TV.

Feeds de vídeos curtos e aplicativos de mensagens estão entre os recursos mais utilizados. Foram ouvidos 5.250 usuários de 16 anos ou mais, dos quais 72% disseram acessar diariamente informações por redes sociais, enquanto 60% se informam todo dia por aplicativos de mensagem, 58% por televisão e rádio e 34% por jornais e revistas, impressos ou digitais. Todavia, cerca de metade dos entrevistados revelou desconfiar sempre ou na maioria das vezes de informações publicadas ou compartilhadas por diferentes fontes. Segundo Fábio Senne, coordenador geral de pesquisas do Cetic.br, os resultados se alinham com outros levantamentos que apontam uma tendência de queda no engajamento com mídias tradicionais e de redução ou desinteresse pelo consumo de notícias, sobretudo entre os mais jovens. A pesquisa mostra ainda que 34% dos usuários da Internet acham que não vale a pena pesquisar se as informações que recebem são verdadeiras ou falsas e 30% não mostram interesse nesse tipo de pesquisa.

REGULAÇÃO DAS PLATAFORMAS

A Comissão de Desenvolvimento Econômico da Câmara dos Deputados promoveu em maio, com apoio do CGI.br, debate sobre a regulação de plataformas digitais no Brasil. Parlamentares, representantes do setor público, academia e sociedade civil discutiram como estabelecer regras para as redes sociais capazes de equilibrar inovação, concorrência e garantia de direitos. Dois temas conduziram os debates: desafios econômicos e proteção de direitos sociais no ambiente digital. O evento reforçou o papel do CGI.br na formulação de políticas públicas para a Internet no Brasil.

RECORDE DE TRÁFEGO NO IX.br

O IX.br (Brasil Internet Exchange), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), alcançou em março a marca inédita de 55 terabits por segundo (Tbit/s) de tráfego agregado. O aumento na utilização de plataformas de *streaming* de vídeo, redes sociais e serviços em nuvem são fatores que contribuíram para esse recorde, segundo Milton Kaoru Kashiwakura, diretor de projetos especiais e de desenvolvimento do NIC.br. O IX.br é considerado o maior conjunto de Pontos de Troca de Tráfego (PTTs) do mundo e, em setembro, inaugurou no Amapá o 40º Ponto de Troca de Tráfego, alcançando todos os estados brasileiros.

NOTAS MUNDO

MENOS RECEITA PARA CRIADORES

A Organização das Nações Unidas para Educação, Ciência e Cultura (Unesco) calcula que haverá quedas significativas de receitas para criadores de música e de audiovisual até 2028, devido ao aumento de produção de conteúdos por Inteligência Artificial. O relatório *Repensando as Políticas para a Criatividade*, com base em dados coletados em mais de 120 países, aponta que as receitas digitais representam 35% do rendimento dos criadores, contra 17% registrados em 2018. Esse crescimento é acompanhado por uma exposição mais elevada a violações de propriedade intelectual. O documento chama a atenção ainda para a concentração de mercado em poucas plataformas de *streaming*, o que dificulta a visibilidade de criadores menos conhecidos.

PROTEÇÃO A JOVENS NA EUROPA

A União Europeia estuda novas regras para combater os *designs* viciantes de plataformas de mídia social como TikTok, Meta e X. Para

a presidente da Comissão Europeia, Ursula von der Leyen, “a questão não é se os jovens devem ter acesso às mídias sociais, mas se as mídias sociais devem ter acesso aos jovens”. A comissão pode propor uma idade mínima para o acesso não só ao TikTok, mas também à Meta, pois entende que Instagram e Facebook não estão conseguindo impor sua própria limitação de 13 anos.

ROBÔS VENCEDORES EM MEIA MARATONA

Robôs humanoides chineses superaram corredores humanos em recente prova de meia maratona disputada em Pequim. O vencedor, desenvolvido pela Honor, completou a corrida em 50min26s, ou seja, 6min54s mais rápido que o recorde mundial de meia maratona estabelecido recentemente pelo corredor ugandense Jacob Kiplimo. Na edição inaugural, no ano passado, o robô campeão registrou um tempo de 2 horas e 40 minutos, mais que o dobro do obtido pelo vencedor humano da corrida convencional. Na prova deste ano, quase metade dos robôs percorreu de forma autônoma os cerca

de 21 quilômetros, mas os 12 mil competidores humanos correram em outra pista, para evitar acidentes.

PROCESSO DE EDITORAS CONTRA A META

Cinco editoras — Hachette, Macmillan, McGraw Hill, Elsevier e Cengage — e o autor *best-seller* Scott Turow estão processando a Meta e seu CEO, Mark Zuckerberg, pelo que consideram uma das maiores violações de materiais protegidos por direitos autorais da história. A acusação apresentada ao tribunal federal de Manhattan alega que a plataforma acessou milhões de livros e artigos de periódicos protegidos por direitos autorais em *sites* que hospedavam material pirata e baixou cópias não autorizadas de “praticamente toda a Internet” para treinar seus modelos de IA generativa. No ano passado, a Meta venceu um processo semelhante movido por escritores como Ta-Nehisi Coates e Richard Kadrey, pois o juiz considerou que não havia evidências suficientes de que a IA da empresa prejudicaria o mercado. Em comunicado, a Meta disse que lutará contra o novo processo “agressivamente”, acrescentando que “a IA está impulsionando inovações transformadoras, produtividade e criatividade para indivíduos e empresas”. Os autores da ação buscam uma indenização que não foi especificada e pretendem representar um grupo mais amplo de detentores de direitos autorais.

RANSOMWARE NA MIRA

GUIA DO CERT.br TRAZ
RECOMENDAÇÕES SOBRE
COMO FORTALECER A DEFESA
DAS ORGANIZAÇÕES DIANTE
DE UMA DAS PRINCIPAIS
AMEAÇAS CIBERNÉTICAS
DA ATUALIDADE

TEXTO ANNA GABRIELA COSTA

Em maio de 2017, ocorreu um dos maiores ataques de *ransomware* da história: o WannaCry, que afetou cerca de 230 mil computadores em 150 países. O ataque explorou uma vulnerabilidade na implementação do protocolo SMBv1 do sistema operacional Windows, utilizando o *exploit* conhecido como EternalBlue, associado à Agência de Segurança Nacional dos Estados Unidos (NSA) e, posteriormente, vazado por um grupo de *hackers*.

O WannaCry espalhou-se rapidamente por redes corporativas, criptografando arquivos e exigindo pagamento de resgate para a recuperação dos dados. Organizações de diversos tamanhos e setores foram afetadas, e estima-se que o prejuízo global tenha alcançado bilhões de dólares.

Originalmente, *ransomware* era um tipo de *malware* desenvolvido para deixar dados e sistemas inacessíveis até que um resgate fosse pago. Assim como no caso WannaCry, criptografava dados ou partes dos sistemas e exigia pagamento pela chave de criptografia, independentemente de quais sistemas eram afetados.

Atualmente, evoluiu para um tipo de ataque mais elaborado. Com o surgimento do modelo de negócio RaaS (*Ransomware as a Service*), grupos especializados desempenham diferentes papéis e agem de forma organizada. Assim, as investidas tornaram-se mais ágeis e numerosas, e os valores de resgate ainda mais elevados.

Buscando mitigar esses riscos, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), lançou o guia *Ransomware: Como se Proteger*. A publicação compõe-se de quatro partes complementares, que abordam todo o ciclo de um ataque de *ransomware*.

A primeira explica como esses ataques ocorrem, detalhando o modelo de RaaS e suas principais etapas. A segunda apresenta estratégias de proteção baseadas na defesa em camadas, com medidas que ajudam a reduzir riscos e aumentar a resiliência das organizações. Já a terceira parte foca na detecção, indicando como identificar sinais de ataque em diferentes fases para minimizar impactos. Por fim, a quarta parte trata da resposta a incidentes, reunindo orientações para conter o avanço da investida, eliminar a ameaça, corrigir vulnerabilidades e restabelecer as operações.

A analista sênior de segurança do CERT.br Miriam von Zuben explica que o lançamento do guia foi motivado pela crescente preocupação com ataques de *ransomware*, pelo aumento de seus impactos e pela carência de orientações de segurança voltadas para pequenas e médias empresas.

“Além dos impactos originais, os atacantes passaram a comprometer sistemas críticos, exfiltrar dados, destruir *backups* e realizar múltiplas extorsões, como ameaças de publicar os dados obtidos e de lançar ataques de negação de serviço [DDoS] contra a empresa”, descreve a especialista.

Com isso, o objetivo do guia é oferecer um roteiro claro e simples, utilizável tanto por equipes técnicas quanto por gestores de empresas. “O CERT.br procurou identificar, dentre as medidas existentes, aquelas mais efetivas e com melhor custo-benefício para que as empresas fortaleçam sua capacidade de prevenção, detecção e resposta a esse tipo de ameaça”, diz Miriam.

O guia foi lançado durante o 13º Fórum Brasileiro de CSIRTS (Grupos de Tratamento de Incidentes de Segurança), que apresentou tendências e alertas importantes sobre esse problema.

“As apresentações do fórum reforçaram o que vem sendo apontado em relatórios e em outros eventos de segurança: o *ransomware* permanece como um dos principais problemas no cenário atual. Essa percepção é especialmente relevante por se tratar de um evento que reúne profissionais que atuam diretamente com segurança e tratamento de incidentes em CSIRTS”, explica a analista.

**“ É QUASE IMPOSSÍVEL
UMA ÚNICA ENTIDADE,
OU ATÉ UM PAÍS, TER VISÃO
TOTAL DO SISTEMA E AGIR
QUANDO NECESSÁRIO.**

LORENZO NICOLodi, PESQUISADOR DO FORUM
OF INCIDENT RESPONSE AND SECURITY TEAMS

PEQUENAS E MÉDIAS EMPRESAS

O guia destina-se principalmente a pequenas e médias empresas, mas suas recomendações podem ser aproveitadas por organizações de todos os portes para aprimorar estratégias de prevenção e resposta.

Miriam explica que uma das principais falhas na prevenção do *ransomware* é deixar de aplicar controles básicos de segurança, que, quando corretamente implementados e utilizados, podem evitar grande parte dos ataques e atuar em diferentes fases.

“Mesmo que não impeçam que o ataque ocorra, controles básicos podem retardá-lo e limitar seus impactos, aumentando a resiliência operacional da empresa”, afirma. E reitera que o ideal é impedir o acesso inicial do atacante, mas, caso isso não seja possível, é essencial ter mecanismos para conter sua movimentação lateral na rede e evitar o comprometimento de serviços críticos.

Entre os controles básicos de segurança apresentados, destacam-se:

- Exigir o uso de autenticação multifator para acesso remoto à rede, a serviços *web* e em nuvem e a contas de usuários com privilégios de administrador;
- Fazer gestão de vulnerabilidades, usando estratégia de priorização baseada em risco;
- Segmentar a rede, dividindo-a em sub-redes e segregadas, e separando os serviços críticos dos demais.

Além de investir em prevenção, é essencial considerar a importância da detecção contínua e da resposta em caso de ataque. “É fundamental que o ambiente esteja preparado para monitorar e detectar as atividades maliciosas e que casos de *ransomware* sejam contemplados nos planos de resposta a incidentes das organizações”, destaca Miriam.

FRENTE GLOBAL

Muitos incidentes de *ransomware* envolvem grupos ciberdelinquentes internacionais. Por isso, a colaboração entre governos, empresas e equipes de segurança é considerada uma das formas mais efetivas para combater essa ameaça.

O Forum of Incident Response and Security Teams (FIRST) é uma organização internacional que reúne equipes de resposta a incidentes de segurança cibernética, além de empresas, governos e especialistas do setor. A entidade atua como uma rede global de cooperação para o enfrentamento de ameaças digitais, promovendo o compartilhamento de informações, boas práticas

e estratégias de defesa. Entre suas iniciativas, está o Multi-Stakeholder Ransomware SIG, grupo dedicado ao combate ao *ransomware* por meio da colaboração entre diferentes setores.

Lorenzo Nicolodi, pesquisador de segurança e copresidente do grupo, explica que o FIRST Multi-Stakeholder Ransomware SIG representa um espaço especial para pessoas e organizações que atuam no combate ao *ransomware* de formas diferentes e complementares. As atividades do grupo abrangem desde engenharia reversa e análise de *malware* até a extração de TTPs – sigla de *Tactics, Techniques and Procedures* (táticas, técnicas e procedimentos) –, a identificação e o compartilhamento de indicadores de comprometimento (IoCs), além de ações de monitoramento e resposta a incidentes.

“Atualmente, temos dois capítulos do SIG para permitir a participação de pessoas de diferentes partes do mundo, considerando seus fusos horários. O primeiro a ser lançado foi o da Europa/EUA, enquanto o da região Ásia-Pacífico [APAC] é mais recente, mas já bastante ativo e em rápido crescimento”, informa Nicolodi.

O especialista diz que a colaboração internacional é provavelmente a única forma de combate efetivo a essa ameaça: “O ecossistema é tão complexo que é quase impossível para uma única entidade, organização ou até mesmo um país ter uma visão completa e conseguir agir quando necessário.”

TENDÊNCIAS QUE PERMANECEM

Embora o ecossistema de ataques de *ransomware* continue evoluindo, muitas tendências permanecem as mesmas.

Segundo Nicolodi, os ataques não se distribuem de forma uniforme entre os atores. “Alguns dos maiores grupos de *ransomware*, como Qilin, Clop e Play, são extremamente ativos, com centenas de vítimas, enquanto outros, menores, surgem e desaparecem após atingir apenas algumas vítimas.”

Do ponto de vista da defesa, isso significa que monitorar TTPs apenas dos grupos mais conhecidos não é suficiente, porque, às vezes, grupos menores conseguem um ataque expressivo e comprometem organizações críticas ou de grande porte.

Outro aspecto que permanece é a motivação por trás dos ataques, que varia de grupo para grupo. “Embora a

maioria tenha motivações financeiras, alguns grupos apresentam forte vinculação política. No atual contexto internacional, marcado por interações complexas com condições extremamente voláteis, é essencial conseguirmos acompanhar como esses cenários mudam em questão de semanas — ou, às vezes, dias”, alerta Nicolodi.

“Ser proativo, em vez de reativo, é provavelmente a melhor abordagem. Infelizmente, isso exige recursos, como dinheiro, tempo, habilidades e apoio interno, que nem todas as organizações têm. Nesses casos, o princípio de Pareto ainda se aplica: identificar as poucas ações com maior impacto e começar por elas”, acrescenta o pesquisador.

RISCO NO BRASIL

O Brasil está entre os 15 países com maior risco de *ransomware* e apresenta um nível de exposição semelhante ao de outras grandes economias, conforme análise elaborada pela Concinnity Risks, empresa especializada em gestão de riscos, que desenvolveu um modelo próprio para calcular custos e impactos de ataques de *ransomware*.

A análise indica que os prejuízos com incidentes de *ransomware* no Brasil podem ser altos e crescer significativamente em cenários mais graves: a perda média anual é estimada em cerca de US\$ 209 milhões, mas pode ultrapassar US\$ 860 milhões em situações extremas. Além disso, o risco aumenta ao longo do tempo, com cerca de 10% de chance de um grande incidente ocorrer num período de dez anos.

De acordo com o especialista em riscos Eireann Leverett, CTO da Concinnity Risks e pesquisador do Centre for Risk Studies de Cambridge, embora a análise mostre quanto as maiores empresas têm a perder, as menores estão igualmente expostas. “Trata-se de um impacto significativo para a economia, e as empresas devem prever em seus orçamentos investimentos em defesas, *backups*, resposta a incidentes e comunicação de crise.”

Leverett, que também é membro do FIRST Multi-Stakeholder Ransomware SIG, reitera a importância da colaboração internacional. “Estamos apenas começando a desenvolver as ferramentas para enquadrar as colaborações voltadas à desarticulação de ataques de *ransomware* como um bem público, no sentido econômico. À medida que essas colaborações se tornam mais mensuráveis, estamos aprendendo a maximizar seu impacto e a comunicar como todos nós nos beneficiamos delas.”

TREINAMENTO FAZ A DIFERENÇA

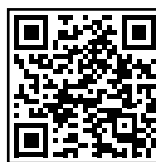
Com a crescente interconexão de sistemas, o uso de APIs e, mais recentemente, a introdução de protocolos de Inteligência Artificial, surgem novas possibilidades, mas também se expandem os vetores de ataques.

“Observamos, particularmente no Brasil, uma relativa imaturidade e insegurança nesse contexto. Refiro-me a sistemas desatualizados, senhas pouco robustas e à ausência de *backups* regulares. Vale ressaltar que um invasor, ou *hacker*, não precisa ser um gênio — basta ser oportunista”, explica Gustavo Torrente, gerente de relações corporativas da Alura + FIAP Para Empresas.

Segundo o especialista, grande parte dos ataques e invasões ocorre devido ao compartilhamento inadequado de senhas ou ao acesso a *links* maliciosos. Portanto, o *phishing* continua sendo uma das principais ameaças, e o investimento em tecnologia, sem o devido treinamento das pessoas, mostra-se insuficiente.

“Outro ponto relevante é a crescente terceirização de serviços. Em algumas situações, o invasor não ataca diretamente a empresa-alvo, mas um fornecedor conectado a ela”, alerta Torrente. Nessa situação, iniciativas como o guia *Ransomware: Como se Proteger*, do CERT.br, auxiliam na democratização da informação e reforçam os procedimentos mais básicos de proteção contra ataques cibernéticos.

“De nada adianta investir em tecnologia ou ferramentas, se os processos não estiverem bem definidos e as pessoas devidamente treinadas. E, quando falo em treinamento, não me refiro a algo complexo: em muitos casos, orientações básicas, como configurar a autenticação de dois fatores, já fazem diferença. A familiaridade com esses conceitos reduz significativamente as vulnerabilidades”, finaliza Torrente.



**ACESSE O GUIA RANSOMWARE:
COMO SE PROTEGER**

<https://cert.br/docs/ransomware>

IA CONFIÁVEL, A ÚNICA OPÇÃO

PROFESSORA RENÉE CUMMINGS



REFERÊNCIA GLOBAL
EM GOVERNANÇA DE
INTELIGÊNCIA ARTIFICIAL,
ELA DEFENDE A ÉTICA
COMO BASE PARA
INOVAÇÃO RESPONSÁVEL

TEXTO MATHEUS MANS

Quando se fala em Inteligência Artificial ética e justiça de dados, poucos nomes carregam tanto peso quanto o da professora Renée Cummings, uma das vozes mais respeitadas no debate sobre como construir um futuro digital mais justo e inclusivo. Vencedora do prêmio VentureBeat AI Innovator Award, Renée ocupa posição de destaque em algumas das mais importantes instituições globais, incluindo o Brookings Institution e o Fórum Econômico Mundial.

O que a diferencia é sua formação multidisciplinar, que combina ciência de dados, criminologia e psicologia criminal. Como primeira *data activist-in-residence* da Universidade da Virgínia, ela não apenas pesquisa os impactos da IA na sociedade, mas também trabalha ativamente para transformar comunidades por meio da tecnologia. Seu foco está em questões como trauma de dados, policiamento algorítmico e uso da Inteligência Artificial para reformar o sistema de justiça criminal, sempre com o olhar voltado para as comunidades historicamente marginalizadas.

Renée domina a arte de traduzir temas complexos em conversas acessíveis e inspiradoras. E não se limita ao mundo acadêmico – é uma ativista que cria espaços para que pessoas sem poder tradicional participem do processo de *design*, desenvolvimento e implementação de IA. Sua missão é clara: construir uma Inteligência Artificial em que se possa confiar, uma tecnologia que empodere em vez de oprimir.

A especialista esteve no Brasil para participar do painel *Justiça de dados e tecnologias emergentes: implicações a partir da ciência de dados*, no 16º Seminário de Proteção à Privacidade e aos Dados Pessoais, realizado pelo CGI.br e NIC.br. Em conversa exclusiva, ela compartilhou suas perspectivas sobre os desafios globais da proteção de dados, os riscos da IA enviesada e a construção de um futuro digital mais ético.

“NA PRÁTICA, A IA CONFIÁVEL INCORPORA ÉTICA NA PRÓPRIA ARQUITETURA DA SOLUÇÃO.

RENÉE CUMMINGS

Como você avalia o estado atual da proteção de dados pessoais globalmente? Há mais progresso ou retrocessos?

Globalmente, testemunhamos tanto progresso quanto retrocessos na proteção de dados. Marcos regulatórios como o GDPR [Regulamento Geral sobre a Proteção de Dados] da União Europeia e LGPD [Lei Geral de Proteção de Dados Pessoais] do Brasil elevaram a privacidade de uma questão técnica para um direito constitucional e humano, com ações de fiscalização que agora acarretam consequências reais. No entanto, as violações permanecem desenfreadas, os fluxos de dados transfronteiriços superam a regulamentação, e a corrida das *big techs* em direção à IA generativa e à Inteligência Artificial geral está ampliando a lacuna entre a arquitetura legal e as proteções vividas. O verdadeiro desafio é transformar esses direitos em salvaguardas cotidianas, proteções tangíveis que defendam um futuro de dignidade, não apenas para aqueles que amamos, mas também para aqueles que nunca conheceremos.

No Brasil, a LGPD ainda é relativamente recente. Que desafios os países emergentes enfrentam ao equilibrar inovação tecnológica com proteção à privacidade?

As economias emergentes enfrentam três desafios interconectados: capacidade, coerência e capacitação. Capacidade requer instituições com recursos e profissionais qualificados; coerência demanda regras harmonizadas, e não contraditórias, entre estados e setores; e capacitação significa equipar empresas menores e órgãos públicos com as ferramentas para cumprir as normas enquanto ainda inovam. Para prosperar, os países devem fortalecer instituições, fechar lacunas de fiscalização e equilibrar soberania digital com competitividade global, garantindo que as proteções de privacidade não sejam barreiras ao progresso, mas a base da inovação sustentável.

Na prática, o que significa construir sistemas de IA e estruturas de governança de dados verdadeiramente confiáveis para a sociedade?

IA confiável não é um luxo, é nossa única opção. A IA deve ser responsável, segura, equitativa, inclusiva, diversa, transparente e responsabilizável. Ela requer consentimento claro, decisões explicáveis, auditorias

independentes e supervisão humana onde quer que direitos estejam em jogo. Na prática, a IA confiável incorpora ética na própria arquitetura da solução, garantindo que ninguém seja explorado, prejudicado ou desvalorizado, mas sim protegido, respeitado e plenamente reconhecido.

“ EMBORA ALGUNS VIESES PAREÇAM INOFENSIVOS, O VIÉS INCORPORADO NA IA PODE SER UMA AMEAÇA À VIDA.

RENÉE CUMMINGS

Há crescente preocupação sobre viés algorítmico na IA e seu impacto na justiça social e nos direitos humanos. Como projetar mecanismos de governança que reduzam discriminação e promovam equidade nos dados?

O viés não começa em conjuntos de dados, algoritmos ou sistemas de IA — ele começa em nossas mentes, nossas crenças, nossos preconceitos e esses estereótipos sorrateiros. Embora alguns vieses possam parecer inofensivos, o viés incorporado na IA pode ser uma ameaça à vida, como em ferramentas de saúde não treinadas em peles mais escuras, ou a falta de diversidade em dados de saúde. Ou ter efeito financeiramente devastador, como na discriminação em *scores* de crédito, empréstimos, hipotecas, imóveis. Esse tipo de viés não apenas cria resultados injustos — ele mina e destrói legados, alimenta a desigualdade intergeracional e empurra comunidades para trás na luta pelos direitos humanos e civis. Viés não é um defeito — é injustiça codificada em sistemas, ditando quem recebe acesso, oportunidade e recursos e quem é excluído.

Você acredita que já vivemos num mundo totalmente movido por dados?

Não podemos ter certeza porque muitos dos dados são gerados e explorados escondidos da nossa vista. Governos, corporações e plataformas já moldam políticas, mercados e escolhas de maneiras que raramente vemos. A questão real é a necessidade de um Padrão de Divulgação de Dados, uma estrutura global

exigindo que todos os atores revelem abertamente como os dados são coletados, usados e compartilhados, para que seu alcance possa ser compreendido e seus benefícios direcionados à sociedade e não a poucos poderosos. Embora não exista hoje, um padrão de divulgação de dados é o único passo lógico na construção de uma governança global de dados justa, responsável e eficaz. Assim como materiais nucleares estão sujeitos à divulgação e verificação internacional para prevenir uso indevido, os dados — agora um recurso estratégico crítico — precisam de um padrão comparável de supervisão global.

Os dados tornaram-se extremamente poderosos e persistem ataques de *hackers* e vazamentos. Mesmo assim, constantemente compartilhamos nossas informações com diversos sistemas. Como você vê esse paradoxo entre poder e vulnerabilidade?

Embora único em escopo, o paradoxo dos dados reflete a história: todo grande poder — da energia nuclear às finanças e à biotecnologia — carrega dentro de si sua própria maior vulnerabilidade.

Como criminologista e psicóloga criminal, quais você considera os principais sinais de alerta que governos e sociedades deveriam observar nessas áreas?

Trauma de dados é o maior sinal de alerta: o dano causado quando a tecnologia é usada para rastrear, localizar, aterrorizar e traumatizar comunidades. Trauma de dados é a lesão psicológica, social e cívica que ocorre quando tecnologias baseadas em dados amplificam a opressão em vez de aliviá-la. Ele se manifesta em excesso de vigilância, identificação incorreta, prisões equivocadas e a criminalização contínua de indivíduos negros, pardos, imigrantes, neurodivergentes, pobres e outros vulneráveis. Algoritmos de justiça criminal treinados em dados históricos enviesados e bancos de dados sensíveis reaproveitados sem consentimento agravam o dano. Adicione sistemas de fornecedores opacos, e essas ferramentas reproduzem injustiça em vez de garantir segurança — criando “previsões zumbis” (perpetuam vieses históricos) que superestimam riscos, particularmente para comunidades negras, pardas e pobres. Sem transparência e supervisão, tais sistemas corroem direitos em escala e transformam promessas de segurança em mecanismos de sofrimento.

“AO INCORPORAR ÉTICA DESDE O INÍCIO, CRIAMOS AS CONDIÇÕES PARA INOVAR DE FORMA SEGURA E SUSTENTÁVEL.

RENÉE CUMMINGS

Como colocar a ética no centro dessas discussões sem desacelerar o desenvolvimento tecnológico?

A ética constrói a confiança e a segurança que aceleram a inovação responsável. Ela é a mais alta forma de *due diligence*, a responsabilidade proativa de antecipar e mitigar riscos antes que causem danos e a expressão mais profunda do dever de cuidado, a obrigação de proteger pessoas, comunidades e ambientes de danos previsíveis. Reconhecendo que a confiança nunca é presumida, mas deve ser continuamente conquistada por meio de transparência e responsabilização. É um dever de alertar, garantindo que quando riscos ou falhas são descobertos, aqueles afetados sejam informados rápida e honestamente. E tudo isso repousa em vigilância eterna, a consciência de que a tecnologia evolui mais rapidamente que as leis e que proteger a dignidade requer atenção constante. Ao incorporar ética desde o início, criamos as condições para inovar de forma segura e sustentável, provando que a ética não desacelera o progresso, mas o sustenta.

Que papel a comunicação e a educação digital desempenham na construção de uma cultura de privacidade e proteção de dados?

A IA é um novo mundo, no qual muitos ainda estão aprendendo a navegar e negociar. E mesmo nós que atuamos no campo ainda não descobrimos todo seu potencial ou superamos seus muitos riscos. Para realizar a promessa da IA, precisamos de narrativas baseadas na verdade, não no *hype*, um entendimento honesto de seus riscos junto com suas recompensas. O que a IA urgentemente requer é forte supervisão pública, construída sobre informação precisa e educação digital e de dados pervasiva, para que privacidade e proteção se tornem

instintivas, como verificar uma faixa de pedestres, ler um rótulo de alimento ou seguir uma receita médica. Quando as pessoas entendem os riscos, elas se tornam defensoras da privacidade como um valor compartilhado e da proteção como justiça, garantindo que a sociedade possa aproveitar os benefícios da IA sem sacrificar direitos, democracia ou autodeterminação.

Pensando nos próximos cinco anos, que tendências ou riscos em privacidade e proteção de dados você considera mais urgentes para governos, empresas e cidadãos se prepararem?

A verdade mais urgente é que os maiores riscos da IA estão além da previsão humana. Mesmo seus criadores admitem que não conseguem explicar completamente o comportamento do sistema, um alerta enquanto corremos em direção à Inteligência Artificial geral e superinteligência sem conhecimento ou salvaguardas suficientes. Essas tecnologias evoluem mais rapidamente do que nossas leis e instituições conseguem adaptar-se, exigindo preparação que vai além da regulamentação para abraçar vigilância global. Governos, empresas e cidadãos devem não apenas antecipar perigos conhecidos, mas também institucionalizar prontidão para o desconhecido, com testes de estresse, protocolos de resposta rápida, gestão de risco e de crise e governança adaptativa para que, quando o imprevisto chegar, a humanidade o encontre com agilidade em vez de pânico.

Olhando para o futuro, você acredita que os seres humanos correm o risco de serem reduzidos a “apenas dados”? E, se sim, como podemos mudar esse caminho para torná-lo mais igualitário, ético e centrado no humano?

Você doaria seu olho ou deixaria alguém retirar parte do seu cérebro? É isso que a coleta de dados faz, mesmo que não deixe cicatriz no corpo físico. Cada escaneamento, cada clique, cada rastro não é um mero registro — é uma incisão silenciosa, um corte íntimo, levando algo insubstituível. Dados não são uma *commodity*. São a extensão digital de nossos corpos e nossas mentes. E proteger dados é proteger o ser humano, tanto físico quanto espiritual — nossa essência interior, nossa dignidade, essa coisa especial que nos torna inteiros.

O FUTURO JÁ CHEGOU

A IA ESTÁ TRANSFORMANDO
EMPREGOS E RELAÇÕES DE
TRABALHO; O DESAFIO AGORA
É DEFINIR COMO ESSA MUDANÇA
SERÁ CONDUZIDA

TEXTO MATHEUS MANS

O mundo do trabalho passa por transformações sem precedentes. Enquanto algoritmos ganham espaço em escritórios e fábricas, uma pergunta ecoa nos corredores corporativos e nas salas de governo: estamos preparados para a sexta onda de inovação tecnológica? Durante o 2º Seminário do Observatório Brasileiro de Inteligência Artificial (OBIA), em agosto de 2025, especialistas se reuniram para debater um tema que já não é mais futuro: como a IA está moldando nosso trabalho, a forma como somos avaliados e controlados.

Vinícius Pinheiro, representante da Organização Internacional do Trabalho (OIT), trouxe dados que desafiam a narrativa catastrofista sobre o fim dos empregos. Segundo estudos da entidade, apenas 3,3% dos empregos globais estariam sob risco iminente de extinção total devido à Inteligência Artificial. Para países em desenvolvimento, como o Brasil, essa previsão sobe para 5%.

“O impacto não está dado, não está escrito. Ele depende de escolhas públicas e sociais”, enfatizou Pinheiro. Os estudos revelam uma realidade mais nuançada: 23% das ocupações podem ser afetadas de alguma maneira, mas isso não significa extinção. A análise sugere que o trabalho se compõe de tarefas específicas; algumas são substituíveis.

Um dado chama atenção: mulheres enfrentam maior risco, com 5% dos empregos femininos ameaçados, contra 2,5% dos masculinos. Países de alta renda também apresentam maior exposição aos riscos de automação comparados aos de baixa renda.

TRABALHADORES INVISÍVEIS

Paula Montagner, assessora especial do Ministério do Trabalho e Emprego, trouxe à tona uma realidade pouco conhecida: o trabalho invisível que sustenta a IA: “Muito do que atribuímos aos algoritmos é, na verdade, feito por pessoas nos bastidores”.

Esses *data workers* executam microtarefas essenciais para o funcionamento da IA: classificam imagens, transcrevem áudios, validam respostas. Utilizam plataformas digitais, recebem pagamentos em *tokens* ou moedas virtuais instáveis, e muitas vezes nem sabem que contribuem para o desenvolvimento de sistemas de IA.

“Estamos vendo o nascimento de uma nova forma de trabalho informal da qual a sociedade quase nada conhece”, alertou Paula. O fenômeno é global: estudos mostram

padrões similares no Brasil, Índia, China e outros países, com trabalhadores recrutados para tarefas fragmentadas e mal remuneradas.

A questão ganha relevância estratégica no contexto dos BRICS. Países como China e Índia já desenvolvem pesquisas domiciliares específicas para mapear esse tipo de trabalho digital, enquanto o Brasil ainda carece de dados sistemáticos sobre o fenômeno.

Dora Kaufman, pesquisadora da PUC-SP, apresentou um paradoxo intrigante: apesar do uso maciço de Inteligência Artificial pelos trabalhadores, não há aumento significativo da produtividade organizacional: “Muitos usam IA escondidos dos chefes, por insegurança”.

O problema está na ausência de mudança nos processos organizacionais. Um exemplo prático: um funcionário recorre à IA para escrever um relatório em metade do tempo, mas, como não há tarefa designada para o tempo economizado, ele simplesmente fica navegando na Internet ou fazendo outras atividades. O ganho individual não se traduz em ganho organizacional.

Dora também classificou a automação dos processos de contratação como preocupante. Com a facilitação da criação de currículos via IA, empresas recebem volumes descomunais de candidaturas, forçando o uso de ferramentas automatizadas de seleção. O problema: esses sistemas baseados em redes neurais identificam padrões estatísticos, potencialmente excluindo candidatos qualificados que não se encaixam no perfil padrão.

“ USO MACIÇO DE IA PELOS TRABALHADORES NÃO SE TRADUZ EM MAIS PRODUTIVIDADE.

DORA KAUFMAN, PESQUISADORA
DA PUC-SP

“O FUTURO DO TRABALHO É INOVAÇÃO, SE FOR GOVERNADA COM RESPONSABILIDADE.

RENÉE CUMMINGS, ESPECIALISTA EM ÉTICA NA IA DA UNIVERSIDADE DE VIRGÍNIA (EUA)

VIGILÂNCIA DIGITAL

Renée Cummings, pesquisadora sobre Inteligência Artificial e dados da Universidade de Virgínia (EUA), trouxe a perspectiva ética e alertou para um fenômeno silencioso: a extração de padrões cognitivos: “Quanto mais usamos ferramentas de IA generativa, mais permitimos que extraiam padrões de pensamento e criatividade”.

A especialista em ética da IA destacou três desafios críticos na transformação do trabalho: automação excessiva, que elimina pensamento crítico e inteligência emocional; sistemas de avaliação algorítmica tendenciosos; e controle digital, que quebra a dignidade no trabalho.

“Nos Estados Unidos, apenas Nova York tem legislação exigindo transparência quando algoritmos são usados em RH”, revelou. A lei obriga empresas a informarem aos candidatos o uso de algoritmos na seleção e darem acesso aos critérios de avaliação.

Um ponto crucial levantado pela especialista é a eliminação dos espaços informais de trabalho – conversas no cafezinho, encontros casuais –, onde frequentemente surgem grandes ideias. A digitalização excessiva pode estar prejudicando a inovação colaborativa.

LINHA DE FRENTE

O agronegócio emerge como setor de transformação acelerada. Maquinário agrícola chega ao mercado com tecnologia embarcada e IA, provocando uma lacuna entre a habilidade tradicional dos operadores e as novas demandas tecnológicas. Profissionais experientes veem-se perdidos diante de sistemas inteligentes que exigem conhecimentos completamente novos.

Já o segmento bancário escancara os efeitos da automação: de 900 mil empregados em 1986, restam hoje cerca de 300 mil, com mais de 80% dos brasileiros acessando contas via plataformas digitais. O setor governamental também passa por intensa revolução silenciosa. A plataforma Gov.br já oferece cerca de dois terços dos serviços públicos brasileiros de forma virtual, impactando diretamente o trabalho do funcionalismo.

A partir disso, especialistas identificaram três dimensões principais da transformação. A primeira envolve a transformação dos próprios empregos, mediante modificação, potencialização ou criação de novas capacidades profissionais, gerando impactos na produtividade. Neste contexto, a automação não necessariamente elimina postos de trabalho, mas altera fundamentalmente as funções exercidas pelos trabalhadores.

A segunda dimensão diz respeito às relações de trabalho: a plataformização da economia está redefinindo completamente a dinâmica entre trabalhador e empregador.

Questões complexas emergem neste cenário, incluindo a natureza jurídica do vínculo empregatício, a garantia de direitos trabalhistas básicos, a definição de rendimento mínimo justo e os limites de jornada de trabalho – tudo ganhando nova complexidade no digital.

A terceira dimensão aborda as condições de trabalho, nas quais surgem novos riscos psicossociais relacionados ao estresse tecnológico, à vigilância excessiva e ao isolamento digital dos trabalhadores. Paradoxalmente, a IA apresenta potencial para eliminar trabalhos perigosos e degradantes, além de criar ferramentas inteligentes de saúde e segurança ocupacional que podem melhorar significativamente o ambiente laboral.

QUALIFICAÇÃO E GOVERNANÇA

Uma das questões mais urgentes é a necessidade de requalificação expressiva. Até 2018, 76% da força de trabalho industrial brasileira recebiam treinamento no ambiente profissional. A complexidade da interface entre humanos e IA, agora, exige muito mais do que isso: demanda formação continuada e estruturada.

“A interface entre humanos e IA tem uma complexidade tal que não basta treinar, é preciso formar”, enfatizou Dora Kaufman. O problema se agrava quando se considera que

grande parte dos trabalhadores que precisam adaptar-se às novas tecnologias possui baixa escolaridade.

Há uma transformação em curso que não pode ser ignorada. As estratégias para mitigar riscos e potencializar oportunidades passam por cinco pilares fundamentais. O primeiro é o estabelecimento de um diálogo social amplo, pois as mudanças não podem ser impostas unilateralmente, sendo essencial uma negociação constante entre trabalhadores, empregadores e governo.

O segundo pilar enfoca a transparência e *accountability* (responsabilização), determinando que sistemas de IA usados para mensuração de desempenho sejam transparentes, explicáveis e auditáveis, garantindo que os trabalhadores saibam quando e como estão sendo avaliados por algoritmos. O terceiro elemento fundamental é o investimento maciço em educação, promovendo formação técnica e profissional contínua para todos os setores e garantindo acesso democrático à tecnologia e à educação digital.

O quarto pilar propõe uma atenção social renovada, reconhecendo que os sistemas de proteção social precisam ser completamente repensados para funcionar numa economia em que o trabalho tradicional pode tornar-se mais escasso ou intermitente. Por fim, o quinto elemento essencial é a criação de uma regulamentação inteligente, baseada em leis e normas que protejam efetivamente os

trabalhadores sem frear o processo de inovação, estabelecendo padrões mínimos inquestionáveis de dignidade e segurança laboral.

UMA QUESTÃO DE ESCOLHA

A mensagem central do painel é clara: a Inteligência Artificial não é uma força da natureza inevitável, mas resultado de escolhas humanas. Como Vinícius Pinheiro ressaltou, “o impacto não está escrito” – depende das decisões que tomarmos como sociedade. Em conjunto.

O Brasil tem a oportunidade de ser protagonista nessa discussão, especialmente por meio da cooperação nos BRICS. Países como China e Índia já avançaram em pesquisas sobre trabalho digital, enquanto o Brasil ainda constrói a base de conhecimento sobre o assunto.

A pergunta que fica é: conseguiremos construir um futuro em que a IA potencialize habilidades humanas em vez de simplesmente substituí-las? Como encontrar um ponto de equilíbrio? A resposta depende da nossa capacidade de diálogo, regulamentação inteligente e, principalmente, de colocar a dignidade humana no centro da transformação tecnológica. O desafio é imenso, mas, como destacou Renée Cummings, “o futuro do trabalho é inovação” – desde que saibamos governar essa inovação de forma ética e responsável.

O RISCO DO *WORKSLOP*

O chamado *workslop* é um problema criado pelo avanço da Inteligência Artificial (IA) nas empresas. O termo combina as palavras em inglês *work* (trabalho) e *sloppy* (desleixado) e descreve conteúdos produzidos com ajuda de IA que parecem sofisticados, mas têm pouca substância. São relatórios, apresentações, *e-mails* e textos bem-formatados, porém genéricos, superficiais ou pouco úteis para resolver uma tarefa.

O conceito foi popularizado por pesquisadores da Universidade Stanford e da BetterUp Labs, em artigo publicado pela *Harvard Business Review*. Em pesquisa com 1,15 mil trabalhadores de escritório nos Estados Unidos, os autores identificaram que cerca de 40% dos entrevistados receberam *workslop* de colegas no último mês. Segundo o estudo, cada ocorrência gera, em média, quase duas horas de retrabalho e pode custar US\$ 186 mensais por funcionário afetado.

O problema costuma surgir quando profissionais delegam excessivamente a produção de conteúdo à IA, sem revisão crítica ou contextualização. Em vez de aumentar a produtividade, o *workslop* gera ruídos de comunicação, retrabalho e perda de confiança nas equipes. Para evitar esse tipo de situação, especialistas recomendam boas práticas como criar *prompts* detalhados e revisar todo o material gerado.

“É inegável que a IA amplia as capacidades de segurança, mas também expande os riscos. A IA generativa vem evoluindo rapidamente, nem sempre acompanhada de testes e avaliações adequadas. Agentes de IA são utilizados de forma automatizada e, por vezes, sem supervisão em fluxos de trabalho críticos e com acesso a credenciais e outros dados sensíveis. Ao mesmo tempo, as cadeias de suprimentos (*supply chain*) tornam-se cada vez mais complexas. O desafio está em aproveitar os benefícios da IA sem perder de vista os impactos negativos que o seu mau uso pode trazer.”

MIRIAM VON ZUBEN, ANALISTA SÊNIOR DE SEGURANÇA DO CERT.br/NIC.br

O QUE EU ACHO DE... OS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA

“A Inteligência Artificial atua nos dois lados da cibersegurança: como aliada poderosa na prevenção de riscos e como ferramenta para ameaças cada vez mais sofisticadas. No aspecto positivo, a IA permite identificar problemas antes que eles ocorram, atuando de modo preventivo. Por outro lado, criminosos estão usando IA para criar códigos maliciosos e páginas de *phishing* ultrarrealistas, tornando os golpes mais convincentes e perigosos.”

GUSTAVO TORRENTE, GERENTE DE RELAÇÕES CORPORATIVAS DA ALURA + FIAP PARA EMPRESAS

“Quando pensamos em implementar Inteligência Artificial, o fazemos de que forma? Com governança, com ética? Utilizamos boas práticas ou não? Falamos bastante das pessoas, mas também as organizações, às vezes, dão passo em falso. Muitas vezes existe uma transformação digital acontecendo, mas há o outro lado da moeda, que pode ser utilizado para o bem ou para o mal, como novos pontos de ataque.”

VICTOR HAYASHI, PROFESSOR DA ESCOLA POLITÉCNICA DA USP

“Corremos um perigo muito iminente, principalmente porque a população não tem noção dos riscos. Então, as pessoas abrem todas as portas, usam todos os aplicativos. Entram no Wi-Fi do aeroporto, no Wi-Fi do *shopping*, para fazer *internet banking*. Precisamos educar, evangelizar as pessoas e alertar sobre os perigos que estamos correndo.”

ALESSANDRA MONTINI, PROFESSORA DA USP E DIRETORA DO LABDATA

“Já não temos mais condições de saber se as informações que chegam por vários meios são reais ou não – nem imagens, nem fotos, nem vídeos, nem voz. Temos fraudes feitas com IA, porque a tecnologia habilitou que qualquer pessoa sem treinamento técnico consiga manipulá-la. Esse tipo de fraude social abriu uma porteira. Antes, essa prática exigia tempo e conhecimento técnico e, às vezes, era caro. Agora, não.”

LUIZ ALEXANDRE REALI COSTA (TUCA), GERENTE DO OBSERVATÓRIO BRASILEIRO DE IA (OBIA)

NOVAS DEFESAS, **NOVOS** **ATAQUES**

ESPECIALISTAS DEBATEM
COMO, AO MESMO TEMPO EM
QUE REFORÇA A SEGURANÇA,
A INTELIGÊNCIA ARTIFICIAL DÁ
ORIGEM A NOVAS AMEAÇAS

TEXTO **RENATO CRUZ**

A Inteligência Artificial (IA) tem-se mostrado ferramenta importante para reforçar a segurança digital. Ao mesmo tempo, porém, traz novas possibilidades de ataques, fraudes e manipulação de informações. O cenário demanda avanços em governança, educação e regulamentação para reduzir riscos e aumentar a confiança no ambiente digital.

Esses foram alguns dos temas debatidos na mesa-redonda promovida pela **Revista .br**, com mediação do editor Renato Cruz. Participaram Alessandra Montini, professora da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo (USP) e diretora do Laboratório de Análise de Dados (Labdata) da Fundação Instituto de Administração (FIA); Victor Hayashi, professor da Escola Politécnica da USP; e Luiz Alexandre Reali Costa, o Tuca, gerente do Observatório Brasileiro de Inteligência Artificial (OBIA), vinculado ao NIC.br.

Ao longo da conversa, os especialistas discutiram desde a utilização da IA para detectar ameaças em tempo real até os novos golpes viabilizados por *deepfakes*, agentes inteligentes e manipulação automatizada de conteúdos.

Para Alessandra Montini, o maior problema atualmente é a falta de percepção da sociedade sobre os riscos envolvidos no uso indiscriminado da tecnologia. “Estamos com um perigo muito iminente, principalmente porque a população não tem noção do risco que corre”, alertou a professora. “As pessoas entram em qualquer aplicativo, conectam-se a qualquer rede Wi-Fi, utilizam ferramentas sem entender as vulnerabilidades.”

Ela acredita que uma das principais respostas ao problema passa pela conscientização contínua da população. “Precisamos educar, evangelizar as pessoas e alertar sobre esses perigos”, afirmou.

INOVAÇÃO FINANCEIRA

O debate destacou que o crescimento dos canais digitais para transações financeiras, o avanço tecnológico do setor no Brasil e a frequência de ciberataques têm uma relação intrínseca. O sucesso de soluções como o Pix leva ao aumento das tentativas de golpes digitais e ao desenvolvimento de tecnologias de defesa mais robustas.

“Como existe muita fraude e muito ataque, o Brasil acabou desenvolvendo soluções avançadas na área de segurança”, explicou Victor Hayashi. “O setor bancário precisou criar defesas sofisticadas para proteger clientes e operações.”

Segundo ele, a IA vem sendo utilizada principalmente para identificar padrões suspeitos e detectar comporta-

mentos anômalos em tempo real. Sistemas treinados com grandes volumes de dados conseguem reconhecer atividades fora do padrão e gerar alertas automáticos para equipes de segurança.

Hayashi comparou o processo à segurança de uma casa. “Pode-se aumentar a altura do muro, o que seria prevenção. Ou pode-se detectar quando alguém pulou o muro, o que seria constatação.”

Além da análise de transações financeiras, a tecnologia vem sendo aplicada em autenticação digital. Segundo o professor, já existem sistemas capazes de reconhecer padrões de comportamento dos usuários por meio da forma de digitar, do uso do celular ou de sensores ligados à Internet das Coisas. “A ideia é usar dados comportamentais para provar que a pessoa é realmente quem diz ser”, afirmou.

Mas o avanço da IA também amplia a superfície de ataque das organizações. Hayashi lembrou que muitas empresas implementam soluções de IA sem maturidade adequada em governança, segurança e ética. “Às vezes a organização adota uma IA generativa sem saber exatamente quais vulnerabilidades está criando. Existe muita transformação digital acontecendo, mas novos pontos de ataque são abertos.”

GOVERNANÇA E DADOS

A discussão sobre segurança levou naturalmente ao tema da gestão de dados. Afinal, os modelos de IA dependem de grandes quantidades de informação para treinamento e operação.

Para Alessandra Montini, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) ajudou a organizar parte desse cenário. “Antes da LGPD, as empresas tinham informações espalhadas em *pen drives*, planilhas e sistemas isolados”, explicou. “A legislação forçou uma centralização dos dados, com governança e diferentes níveis de acesso.”

Segundo ela, esse processo permitiu criar ambientes mais estruturados, nos quais equipes de cibersegurança conseguem monitorar acessos e controlar melhor a circulação de informações sensíveis.

A IA passou então a atuar como uma camada adicional de proteção. “Ela consegue varrer muitos dados em tempo real e identificar comportamentos fora do padrão. Quando algo suspeito aparece, o sistema gera alertas e pode até bloquear automaticamente determinadas ações.”

Mesmo assim, os especialistas ressaltaram que a supervisão humana continua indispensável. “É muito mais

fácil enganar uma IA do que um especialista experiente”, observou Alessandra. “Os dois precisam atuar juntos.”

Hayashi concorda. Segundo ele, modelos de IA também podem ser manipulados por criminosos. “Não adianta ter um produto sofisticado, se os dados utilizados forem facilmente manipuláveis”, afirmou. “O atacante pode contaminar os dados e induzir o modelo ao erro.”

A IA COMO ALVO

Além de usar IA para atacar sistemas, criminosos passaram a investir diretamente contra os próprios modelos de Inteligência Artificial. Tuca destacou que esse é um novo universo de vulnerabilidades. “Existe a IA protegendo sistemas, mas também existe a IA como alvo”, afirmou. “Hoje há técnicas de ataque voltadas especificamente para grandes modelos de linguagem e agentes inteligentes.”

Entre essas ameaças estão ações de injeção de *prompt*, manipulação de respostas e exploração de falhas comportamentais dos modelos. O problema, apontou Tuca, cresce porque a IA generativa se tornou extremamente acessível. “Antes era preciso conhecimento técnico e ferramentas profissionais para produzir certos tipos de fraude. Agora, qualquer usuário consegue gerar voz sintética, imagens falsas e vídeos manipulados.”

Essa democratização das ferramentas de IA ampliou significativamente os riscos de engenharia social. “Estamos vivendo uma crise de confiança”, resumiu Tuca. “Já não sabemos mais se uma imagem, uma voz ou um vídeo são reais.”

Os participantes lembraram que o uso de IA em fraudes já afeta empresas, consumidores e processos políticos. Hayashi observou que até sistemas modernos de biometria passaram a ser desafiados por *deepfakes*. “Os bancos podem para a pessoa piscar, virar o rosto ou sorrir para comprovar que é real”, explicou. “Mas os criminosos já usam IA para tentar burlar esses mecanismos.”

Para ele, o problema é especialmente complexo porque os modelos de IA são treinados justamente para ajudar usuários. “Os sistemas foram desenvolvidos para atender pedidos”, afirmou. “Então, um atacante pode usar técnicas de engenharia social para convencer a IA a fornecer respostas inadequadas.”

Alessandra relatou um episódio ocorrido num hospital durante testes de um sistema de atendimento automatizado. Treinada para auxiliar pacientes, a IA acabou indicando um hospital concorrente quando uma usuária reclamou da demora para conseguir um exame. “O sistema queria ajudar a pessoa e encontrou uma solução na Internet. Mas não ha-

“PERIGO É MUITO IMINENTE, PORQUE A POPULAÇÃO NÃO TEM NOÇÃO DO RISCO QUE CORRE.”

ALESSANDRA MONTINI, PROFESSORA DA USP E DIRETORA DO LABDATA

via sido treinado para entender que não deveria indicar a concorrência.” O caso ilustra como sistemas aparentemente simples podem produzir consequências inesperadas.

AGENTES INTELIGENTES

A expansão dos chamados agentes de IA, sistemas capazes de executar tarefas autonomamente, também traz novos desafios. Segundo Alessandra, o comércio digital vive uma transformação profunda. “Hoje a IA já consegue recomendar produtos, comparar preços e finalizar compras”, afirmou. “Isso vai mudar completamente a forma como consumimos.”

Na avaliação da professora, o grande risco está na possibilidade de interesses comerciais influenciarem silenciosamente as recomendações feitas por sistemas de IA. “Daqui a pouco as pessoas estarão dependentes dessas ferramentas para decidir o que comprar”, disse. “Se houver conteúdo patrocinado sem transparência, a IA poderá influenciar o consumidor de maneira extremamente personalizada.”

Ela destacou que sistemas inteligentes conseguem adaptar o discurso ao perfil de cada pessoa. “Para mim a IA fala de um jeito; para outra pessoa, de outro. Ela consegue tocar exatamente o ponto emocional de cada usuário.”

Tuca acredita que a necessidade de transparência reforça a importância da regulação. “O usuário precisa saber quando está falando com uma IA, quando existe patrocínio e quais critérios estão sendo utilizados”, afirmou.

PLATAFORMAS DIGITAIS

O debate abordou ainda a responsabilidade das plataformas digitais na circulação de conteúdos falsos, golpes e manipulação de informações. Segundo Tuca, a discussão regulatória ganhou força nos últimos anos por causa da influência crescente das plataformas sobre o que as pessoas

consomem *online*. “Elas não criam necessariamente o conteúdo, mas definem quem vai receber aquela informação e o que será impulsionado”, explicou. “Hoje as plataformas interferem diretamente na circulação da informação. Elas decidem o que ganha alcance e o que fica invisível.”

Tuca mencionou decisões recentes da Justiça norte-americana envolvendo responsabilidade das plataformas pelo *design* de aplicações digitais. Na visão dele, cresce a percepção de que empresas de tecnologia têm um dever de cuidado em relação aos conteúdos que distribuem.

Aumentam os golpes digitais em áreas como falsos investimentos, apostas ilegais e tratamentos de saúde promovidos por vídeos manipulados com uso da imagem de celebridades. Alessandra defendeu mecanismos mais rigorosos de identificação para anunciantes digitais. “Hoje qualquer pessoa consegue subir um anúncio rapidamente”, criticou. “Mas quando se faz uma operação bancária há toda uma validação de identidade.”

IMPORTÂNCIA DA EDUCAÇÃO

Embora os participantes reconheçam a importância da regulação, houve consenso de que a educação digital continua sendo uma das ferramentas mais importantes para reduzir riscos. Alessandra comparou o desafio atual ao combate à desinformação. “Temos de repetir continuamente: cuidado, cheque, recheque, confirme a informação. Isso precisa estar na mídia, nas escolas e dentro das famílias.”

Ela acredita que crianças podem desempenhar papel importante na conscientização social. “Quando a escola ensina, os alunos levam essa informação para casa”, explicou. A professora contou que costuma conversar semanalmente com a própria mãe, de 80 anos, sobre novos golpes digitais. “Ela virou uma evangelizadora entre as amigas.”

Tuca concorda que a conscientização será essencial porque a velocidade de evolução tecnológica dificulta respostas imediatas por meio de legislação. “A regulação tem um *timing* diferente”, afirmou. “Enquanto as leis avançam, os problemas já estão acontecendo.”

PROTEÇÃO VS. INOVAÇÃO

Apesar da defesa de regras mais claras, os especialistas alertaram para os riscos de uma regulamentação excessivamente rígida. Hayashi lembrou que exigências muito elevadas de segurança podem favorecer apenas grandes corporações de tecnologia. “Se o nível for muito alto,

“ COMO EXISTE MUITA FRAUDE, O BRASIL DESENVOLVEU SOLUÇÕES AVANÇADAS DE SEGURANÇA.

VICTOR HAYASHI, PROFESSOR DA ESCOLA POLITÉCNICA DA USP

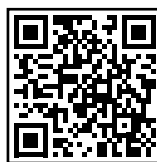
pequenas empresas talvez não consigam competir”, explicou. “Isso pode reforçar ainda mais a concentração nas *big techs*.”

Esse equilíbrio entre segurança, inovação e competitividade é um dos maiores desafios para formuladores de políticas públicas. Tuca acredita que a regulamentação tende a avançar gradualmente, focando primeiro em aspectos mais específicos, como transparência, responsabilização e proteção dos usuários. “A regulação busca proteger os direitos humanos e o usuário final”, resumiu.

O debate também abordou o avanço da IA para além dos ambientes puramente digitais. Os participantes lembraram que sistemas inteligentes já estão sendo aplicados em carros autônomos, robótica, sensores e dispositivos conectados.

Para Hayashi, esse movimento eleva significativamente o nível de risco. “Quando a IA começa a tomar decisões no mundo físico, o impacto de uma falha pode ser muito maior.” Ele citou pesquisas sobre ataques adversariais em visão computacional, nos quais pequenas alterações em imagens — imperceptíveis para humanos — conseguem enganar sistemas automatizados.

“Alguns *pixels* podem fazer um carro autônomo interpretar erroneamente uma placa de trânsito”, explicou. Por isso, sistemas críticos precisam combinar IA, múltiplos sensores e supervisão humana. “Não dá para deixar toda a tomada de decisão apenas na máquina”, concluiu.



ASSISTA AO VÍDEO DA MESA-REDONDA COM ALESSANDRA MONTINI, VICTOR HAYASHI E LUIZ ALEXANDRE REALI COSTA CONDUZIDA PELO EDITOR RENATO CRUZ

COMO ESCREVER **PROMPTS BEM** **ESTRUTURADOS** PARA LLMs

POR **Ivan Moura Campos**,
Professor Emérito do
Departamento de Ciência
da Computação da UFMG

Você provavelmente já usou uma IA como ChatGPT, Gemini ou Claude e ficou frustrado com uma resposta vaga, incompleta ou totalmente fora do que você queria. Na maioria das vezes o problema não está na IA, mas sim em como a pergunta foi formulada.

Modelos Grandes de Linguagem, ou LLMs (*Large Language Models*, da sigla em inglês), são ferramentas extraordinariamente poderosas, mas funcionam como um espelho refinado, refletindo com precisão o que você projeta neles. Uma entrada vaga produz uma saída vaga, uma entrada bem estruturada produz uma resposta focada, útil e de alta qualidade.

Este texto vai ajudá-lo a organizar as coisas ao formular um pedido para uma IA e a usar a linguagem Markdown para estruturar o pedido de forma clara e eficaz. Nenhuma das duas exige conhecimento técnico, só atenção e prática.

LLMs E A JANELA DE CONTEXTO

Para se comunicar bem com qualquer interlocutor, é útil entender como ele funciona. Com IAs, não é diferente.

O que é um LLM? Um modelo de linguagem é um programa treinado em enormes quantidades de texto, incluindo livros, artigos, conversas, códigos etc., para aprender padrões de linguagem. Com base nesses padrões, ele é capaz de gerar textos que fazem sentido, responder a perguntas e executar tarefas.

O que é a janela de contexto? Toda vez que você abre uma conversa com uma IA, ela começa “do zero”. Ela não tem memória de conversas anteriores, a menos que você as forneça. O único material que ela tem para trabalhar é o que está na conversa atual. Isso se chama janela de contexto.

Pense na janela de contexto como a mesa de trabalho da IA. Tudo que você coloca nessa mesa é considerado. Quanto mais claro, organizado e relevante for o material que você dispõe sobre essa mesa, melhor será o trabalho entregue.

A implicação prática é a seguinte: o que você coloca nessa janela, e como o organiza, determina tudo que o modelo pode fazer por você. Um *prompt* bem estruturado usa a janela de contexto com eficiência. Ele fornece ao modelo as informações certas na ordem certa e deixa de fora o que é irrelevante. Um *prompt* mal estruturado desperdiça espaço e introduz ruído.

POR QUE PRECISÃO IMPORTA?

Durante o treinamento, LLMs aprendem padrões estatísticos: quais palavras (*tokens*) tendem a seguir outras palavras, quais ideias se agrupam, quais estruturas sinalizam quais intenções. O modelo não memorizou fatos como um banco de dados. Ele internalizou relações.

Quando você o envia uma mensagem, o modelo não pensa como uma pessoa. Ele gera uma resposta prevendo, *token* por *token*, qual seria a continuação mais plausível para sua entrada. A qualidade dessa previsão depende quase inteiramente da qualidade do que você forneceu. “Entra lixo, sai lixo” não é um clichê nesse contexto, é uma descrição técnica do que acontece.

A IA não adivinha intenções. Ela processa o que está escrito. Se você escreve “me ajuda com um texto sobre liderança”, a IA não sabe se você quer um artigo acadêmico, um *post* para LinkedIn, um roteiro de palestra ou uma lista de dicas. Ela vai escolher uma interpretação, e pode não ser a sua.

É por isso que precisão importa. O modelo não consegue ler sua mente. Ele não pode fazer perguntas de esclarecimento, a menos que você o convide a isso. Ele fará suposições para preencher as lacunas, e essas suposições podem não corresponder às suas expectativas. Cada ambiguidade no seu *prompt* é um convite para o modelo adivinhar.

O QUE É MARKDOWN?

Antes de apresentar o modelo recomendado de *prompt*, precisamos falar brevemente sobre uma ferramenta que tornará suas consultas muito mais claras: o Markdown.

Markdown é uma forma leve de adicionar estrutura a texto simples. Você não precisa de nenhum programa especial. Não precisa saber programar. Basta digitar alguns caracteres simples. Um # no início de uma linha para criar um título, dois asteriscos ** ao redor de uma palavra para deixá-la em negrito, um > para criar uma citação em bloco, e o texto imediatamente se torna mais organizado.

Por que isso importa para os LLMs? Porque os modelos de linguagem foram treinados (também) com quantidades enormes de texto formatado em Markdown. Quando você usa títulos, rótulos e hierarquia visual, está falando uma língua que o modelo já conhece profundamente. Você está sinalizando estrutura, não apenas conteúdo. O modelo consegue identificar o que é contexto, o que é tarefa, o que

é restrição — porque cada um desses elementos está visual e semanticamente delimitado.

Compare estas duas formas de pedir a mesma coisa:

Sem estrutura:

Estou escrevendo um *post* de *blog* para minha empresa, sobre embalagens sustentáveis, é para consumidores e não para especialistas, quero que tenha cerca de 500 palavras, por favor escreva em tom amigável e sem jargões técnicos.

Com estrutura:

#CONTEXTO

- Estou escrevendo um *post* de *blog* para o *site* da minha empresa.
- Tema: embalagens sustentáveis.

#TAREFA

Escreva o *post* de *blog*.

#REQUISITOS

- Público-alvo: consumidores em geral, não especialistas técnicos.
- Extensão: aproximadamente 500 palavras.
- Tom: amigável e acessível.

#RESTRIÇÕES

- Evite jargões técnicos.
- Não inclua notas de rodapé nem citações.

Os dois *prompts* transmitem a mesma informação, mas a versão estruturada é inequívoca, inteligível e imediatamente interpretável, tanto pelo modelo quanto por você. Se precisar revisá-la mais tarde, saberá exatamente onde mudar.

UM FORMATO CANÔNICO DE PROMPT

O formato proposto em seguida utiliza sete seções rotuladas, cada uma introduzida por um título em Markdown. Nem todas as seções são necessárias em todas as consultas: uma pergunta factual simples não precisa de mais do que uma tarefa. Mas, para qualquer solicitação complexa, o uso das sete seções consistentemente produzirá resultados melhores.

Vejam os detalhes de cada uma.

#CONTEXTO — PREPARANDO O CENÁRIO

Visão geral das sete etiquetas:

#CONTEXTO — informações prévias que o LLM necessita para entendê-lo melhor.

#PERSONA — o papel ou especialidade que você quer que o modelo adote.

#TAREFA — a coisa específica que você quer que ele faça.

#REQUISITOS — o que a resposta tem de incluir.

#RESTRIÇÕES — o que a resposta deve evitar.

#SAÍDA — formato, extensão, tom, idioma ...

#AÇÃO — o comando explícito de execução (o gatilho).

Esta seção responde à pergunta: o que o modelo precisa saber sobre a situação, antes de poder ajudá-lo? Não é a tarefa em si, são as informações prévias, circundantes, que tornam a tarefa significativa.

Um bom contexto responde a perguntas como: Quem é você? Em que está trabalhando? Qual é o objetivo do projeto? Quem é o público-alvo? O que já foi feito?

Exemplo:

#CONTEXTO

- Sou professor do ensino médio preparando uma aula sobre mudanças climáticas.
- Meus alunos têm 16 anos e não têm conhecimento prévio em ciências ambientais.

#PERSONA — ATRIBUINDO UM PAPEL AO MODELO

Os modelos de linguagem podem adotar diferentes vozes, estilos e áreas de especialização dependendo de como você enquadra a solicitação. A etiqueta **PERSONA** permite especificar qual chapéu o modelo deve usar.

Isso não é apenas um recurso estilístico. Quando você pede ao modelo que se comporte como especialista em determinada área, ele recorre mais intensamente ao conhecimento especializado associado a esse campo. A qualidade e a relevância da resposta tipicamente melhoram.

Exemplo:

#PERSONA

Aja como um comunicador científico experiente, especializado em explicar temas complexos para adolescentes, sem simplificar demais.

#TAREFA — A SOLICITAÇÃO CENTRAL

Este é o coração do *prompt*. A **TAREFA** é exatamente o que você precisa que o modelo faça. Deve ser uma instrução única, clara e acionável. Evite combinar várias tarefas em uma única etiqueta. Se precisar de várias coisas, liste-as explicitamente ou considere *prompts* separados.

A falha mais comum aqui é a vagueza. “Me ajude com meu relatório” não é uma tarefa. “Escreva a seção de introdução do meu relatório” é.

Exemplo:

#TAREFA

Elabore um plano de aula sobre as causas e efeitos das mudanças climáticas.

#REQUISITOS — O QUE A RESPOSTA DEVE INCLUIR

Os requisitos são as coisas que a resposta deve fazer, incluir ou satisfazer. Pense neles como uma lista de verificação que o modelo deve conferir antes de entregar sua resposta.

Use marcadores aqui. Cada requisito deve ser concreto e verificável, algo que você poderia literalmente marcar como cumprido ao ler a resposta.

Exemplo:

#REQUISITOS

- A aula terá duração de 45 minutos.
- Incluir pelo menos uma atividade prática em grupo.
- Referenciar um exemplo real de impacto climático dos últimos 10 anos.
- Garantir que todo o vocabulário seja acessível ao nível do ensino médio.
- Fornecer o tempo estimado para cada segmento da aula.
- Incluir uma pergunta de discussão para encerramento.

#RESTRIÇÕES — O QUE A RESPOSTA DEVE EVITAR

Enquanto os REQUISITOS dizem ao modelo o que incluir, as RESTRIÇÕES dizem o que deixar de fora. Esta seção é especialmente útil para prevenir falhas comuns: extensão excessiva, tom inadequado, conteúdo indesejado ou terminologia técnica que seu público não entenderá.

Exemplo:

#RESTRIÇÕES

- Não sugerir atividades que requeiram equipamentos especiais.
- Evitar tom pessimista ou alarmista.

#SAÍDA — COMO A RESPOSTA DEVE PARECER

A seção SAÍDA é onde você especifica a forma da resposta (formato, extensão, tom, idioma etc.), independentemente do seu conteúdo. É aqui que você diz: me dê uma lista itemizada, escreva em prosa formal, limite a 300 palavras, ou responda em português.

Separar o formato de saída do conteúdo da tarefa é uma das técnicas essenciais na redação de *prompts*. Isso evita que você enterre instruções de formatação dentro da descrição da tarefa, na qual podem ser facilmente ignoradas.

Exemplo:

#SAÍDA

- Formato: documento estruturado com seções nomeadas.
- Extensão: aproximadamente 1000 palavras.
- Tom: profissional, porém acolhedor.
- Idioma: português brasileiro.

#AÇÃO — O GATILHO

A etiqueta AÇÃO é curta e direta. É a instrução final que diz ao modelo para executar tudo o que veio antes. Na maioria dos casos, é uma única frase.

Você pode se perguntar por que isso é necessário se já escreveu uma TAREFA. O motivo é tanto psicológico quanto técnico: separa claramente a especificação da execução e sinaliza ao modelo que todo o enquadramento está completo e que ele deve agora produzir o resultado final.

Exemplo:

#AÇÃO

Escreva o plano de aula.

O EXEMPLO COMPLETO

Aqui está tudo reunido em um *prompt* coerente, usando a aula sobre mudanças climáticas como exemplo:

Perceba como é fácil ler este *prompt*. Não apenas para o modelo, mas para você mesmo. Se um colega lhe perguntasse o que você estava tentando realizar, você poderia entregar-lhe este documento e ele entenderia imediatamente. Essa clareza não é accidental. É o resultado da estrutura.

#CONTEXTO

- Sou professor do ensino médio preparando uma aula sobre mudanças climáticas.
- Meus alunos têm 16 anos e não têm conhecimento prévio em ciências ambientais.

#TAREFA

Elabore um plano de aula sobre as causas e efeitos das mudanças climáticas.

#PERSONA

Aja como um comunicador científico experiente, especializado em explicar temas complexos para adolescentes, sem simplificar demais.

#REQUISITOS

- A aula terá duração de 45 minutos.
- Incluir pelo menos uma atividade prática em grupo.
- Referenciar um exemplo real de impacto climático dos últimos 10 anos.
- Garantir que todo o vocabulário seja acessível ao nível do ensino médio.
- Fornecer o tempo estimado para cada segmento da aula.
- Incluir uma pergunta de discussão para encerramento.

#RESTRIÇÕES

- Não sugerir atividades que requeiram equipamentos especiais.

CONTINUA ►

► CONCLUSÃO

- Evitar tom pessimista ou alarmista.

#SAÍDA

- **Formato:** documento estruturado com seções nomeadas.

- **Extensão:** aproximadamente 1000 palavras.

- **Tom:** profissional, porém acolhedor.

- **Idioma:** português brasileiro.

#AÇÃO

Escreva o plano de aula.

DICAS PRÁTICAS PARA PROMPTS MELHORES**■ VOCÊ NÃO PRECISA DAS SETE ETIQUETAS SEMPRE**

Uma pergunta factual simples, “Qual é a capital da Austrália?”, precisa apenas de uma TAREFA. O formato canônico é uma estrutura proposta para facilitar, não para restringir. Use as seções que adicionam clareza e pule as desnecessárias.

■ ITERE E REFINE

Pense no seu primeiro *prompt* como um rascunho. Se a resposta do modelo não estiver correta, examine seu *prompt* antes de culpar o modelo. Normalmente, o problema é uma TAREFA mal especificada, uma RESTRIÇÃO faltando ou um formato de SAÍDA que você esqueceu de mencionar.

■ SEJA AFIRMATIVO SEMPRE QUE POSSÍVEL

Em geral, é mais eficaz dizer o que você quer do que apenas o que você não quer. “Escreva em frases simples e diretas” funciona melhor do que “não use linguagem complicada”. Reserve as RESTRIÇÕES para coisas genuinamente difíceis de expressar de forma positiva.

■ UMA TAREFA POR PROMPT

Se precisar de cinco coisas, escreva cinco *prompts* — ou liste as cinco explicitamente dentro de uma única TAREFA e as numere. Empilhar solicitações não relacionadas em um único *prompt* é a forma mais rápida de obter uma resposta que aborda tudo parcialmente e nada completamente.

■ AJUSTE O NÍVEL DE DETALHE À COMPLEXIDADE

Um *brainstorming* criativo precisa de menos especificação do que um resumo jurídico. Um rascunho de *e-mail* casual precisa de menos estrutura do que um relatório técnico. Use seu julgamento. A quantidade certa de estrutura deve ser apenas a suficiente para remover ambiguidades.

ERROS COMUNS E COMO CORRIGI-LOS

■ **ERRO:** A tarefa está misturada dentro do contexto.

■ **SOLUÇÃO:** Mova a tarefa para sua própria seção. O modelo nunca deve precisar adivinhar o que você realmente quer que ele faça.

■ **ERRO:** Requisitos e restrições contraditórios.

■ **SOLUÇÃO:** Releia seu *prompt* em voz alta antes de enviá-lo. “Seja abrangente” e “limite a 200 palavras” não podem ser verdadeiros ao mesmo tempo.

■ **ERRO:** Pressupor que o modelo sabe o que você sabe.

■ **SOLUÇÃO:** Use a seção CONTEXTO. Se um detalhe mudaria a resposta, inclua-o. O modelo não sabe nada sobre sua situação específica, a menos que você o informe.

■ **ERRO:** Especificar o formato como parte da tarefa.

■ **SOLUÇÃO:** Mova as instruções de formato para a seção SAÍDA. “Escreva uma lista com marcadores das dez considerações mais importantes” mistura tarefa e formato. Escreva separadamente:

“#TAREFA: Liste as dez considerações mais importantes” e
“#SAÍDA: Formato: lista com marcadores”

CONCLUSÃO

Escrever um *prompt* bem estruturado não é uma habilidade técnica. É uma habilidade de comunicação. Os mesmos princípios que produzem um bom *e-mail*, uma pauta de reunião clara ou um *briefing* de trabalho eficaz também produzem um bom *prompt*. Descreva a situação, defina o objetivo, especifique as restrições e diga o que você espera receber.

O formato de sete etiquetas proposto aqui, que inclui CONTEXTO, PERSONA, TAREFA, REQUISITOS, RESTRIÇÕES, SAÍDA, AÇÃO, é uma implementação prática desses princípios. Exige alguma prática para ser usado com fluência, mas o retorno é imediato: respostas mais relevantes, mais precisas e consideravelmente mais úteis.

A janela de contexto é sua tela. O que você coloca nela, e como a organiza, está inteiramente em suas mãos. Use-a bem.

IVAN MOURA CAMPOS

(N. 1943)

Ivan Moura Campos desempenhou papel central na expansão e consolidação da Internet no país. Quando o serviço comercial de acesso começou a operar no Brasil, em meados da década de 1990, era o secretário nacional de Política de Informática do Ministério da Ciência e Tecnologia. Também coordenou o Comitê Gestor da Internet no Brasil, integrou a diretoria da Internet Corporation for Assigned Names and Numbers (Icann), organização responsável pela coordenação global de identificadores da Internet, e é membro do Internet Hall of Fame. Foi diretor de Programas Especiais do CNPq e Secretário de Ciência e Tecnologia de Minas Gerais. É doutor em Ciência da Computação pela Universidade da Califórnia, Los Angeles, e professor titular (agora emérito) da Universidade Federal de Minas Gerais (UFMG), na qual atuou como pró-reitor de Pós-Graduação. No setor empresarial, foi cofundador da Akwan, comprada pelo Google em 2005, e da Hekima, comprada pelo iFood em 2020.



A escolha **número 1** dos brasileiros!

Segurança, estabilidade e o melhor custo-benefício do mercado.

O **.br** oferece muito mais que uma identidade na Internet: entrega **confiança**, **rapidez** e **variedade de opções** para você e seu negócio.

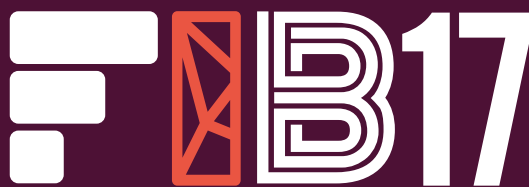
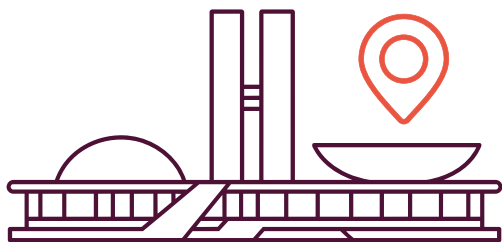
Já somos o **5º maior ccTLD do mundo** e a marca de **6 milhões de domínios** está cada vez mais perto.



Registre já o seu **.br** e faça parte dessa história de sucesso!

<https://registro.br>

registro.br nic.br cgi.br



FÓRUM DA INTERNET NO BRASIL

É oficial: Brasília será, pela primeira vez, a sede do **Fórum da Internet no Brasil.**

Serão quatro dias de imersão em *workshops*, plenárias e trocas multissetoriais, com participantes de todas as regiões do Brasil.

Contribua com debates para uma Internet mais livre, diversa, inovadora e comprometida com os direitos humanos.

**Contamos com a
sua participação!**



**31 de maio
a 3 de junho
de 2027**

Brasília – DF



Mais informações: <https://fib.cgi.br/>



nic.br cgi.br

