A Urgente Necessidade da Literacia Digital

Glaucio de Sousa Santos^{1,2}, Claudia Lage Rebello da Motta¹

¹Programa de Pós-Graduação em Informática
Universidade Federal do Rio de Janeiro (UFRJ)
Rio de Janeiro – RJ - Brasil

²Diretoria de Tecnologia da Informação e Telecomunicação
Polícia Civil do Estado do Rio de Janeiro, RJ, Brasil.

{glaucio75@hotmail.com, claudiam@nce.ufrj.br}

Abstract. *The ubiquity of technology brings significant new benefits to modern society, but also presents new challenges to the ongoing safety and well-being of users who have not been properly educated to understand the risks they face in the digital world—or how to mitigate them. This essay offers a critical reflection on the absence of a national public policy for digital literacy aimed at protecting ordinary citizens within the cyber ecosystem. It ultimately argues that the scientific community—particularly in the field of Computing—has a duty to lead the development of broad educational strategies that promote critical, ethical, and secure digital citizenship.*

Resumo. *A ubiquidade da tecnologia traz novos grandes benefícios à sociedade moderna, mas também traz novos desafios no constante a segurança e bem estar dos usuários, que não foram educados adequadamente para ter consciência dos riscos a que estão expostos no mundo digital e nem como mitigá-los. Este ensaio propõe uma reflexão crítica sobre a ausência de uma política pública nacional de literacia digital voltada à proteção do cidadão comum no ecossistema cibernético. Argumenta-se ao final que a comunidade científica, especialmente no âmbito da Computação, tem o dever de liderar a construção de estratégias educacionais de largo alcance que promovam a cidadania digital crítica, ética e segura.*

1. Contextualização

Nos dias atuais, a tecnologia está constante e massivamente presente na vida das pessoas, ultrapassando barreiras como idade, classe social e nível educacional, devido a enorme utilidade que proporciona. O telefone celular é a maior interface para interação humano computador, com uma disponibilidade jamais vista na história da humanidade. A conectividade não está mais limitada pela disponibilidade de infraestrutura de redes de torres de telefonia. A conexão via satélite está disponível aos locais mais remotos. Com essa ubiquidade, difícil imaginar alguém vivendo um dia de vida sem qualquer contato com a tecnologia.

Todavia, há aspectos negativos na disseminação da tecnologia e sua democratização. Como toda evolução tecnológica – e aqui a palavra ‘tecnológica’ é

usada em uma acepção mais ampla -, desde a descoberta do fogo, passando pela escrita, pela energia hidráulica, energia elétrica, o motor a combustão, o mundo sempre precisou se educar em como tirar o melhor proveito delas e também como evitar o mau uso.

A tecnologia avança em uma velocidade sem precedente. Na mesma toada, as ameaças cibernéticas. Frise-se, o termo ‘cibernético’ aqui é utilizado com o alcance mais amplo possível, para além das ameaças e proteção a sistemas, redes e dados, mas também abarcar todo ecossistema cibernético, seus usuários e as comunicações entre eles. É nesse ponto que fazemos o recorte da nossa abordagem.

A sociedade brasileira está preparada para lidar com as tecnologias mais recentes de maneira minimamente segura? A quem compete estabelecer e implementar esta educação?

O objetivo da presente proposição é demonstrar que, apesar da certeza da sociedade estar exposta a inúmeros riscos e ameaças cibernéticas, ainda não se tem uma definição clara de um programa educacional com alcance suficiente para colocar a sociedade ciente de tais riscos e preparadas para minimizá-los e, desta forma, assegurar um ecossistema cibernético mais seguro nesta nova era tecnológica da humanidade.

A seguir, vamos elencar os principais riscos a que todos estamos expostos, dada a ubiquidade da tecnologia.

Por fim, nosso objetivo será alcançado se a presente proposição levar a uma reflexão da comunidade acadêmica representada pela Sociedade Brasileira da Computação que, salvo melhor juízo, detém a legitimidade para trazer a luz este assunto tão caro ao desenvolvimento da sociedade brasileira.

2. Relevância

A ciência e a sociedade empregam muito esforço no que diz respeito às ameaças e proteção de sistemas, redes e dados. O tópico é tratado por profissionais altamente especializados, que empregam técnicas e procedimentos que estão na fronteira do saber. Esse campo é impulsionado por um mercado competitivo e lucrativo, onde a lei da oferta e demanda fomenta uma corrida incessante pelo desenvolvimento de novas soluções de segurança.

A necessidade de inovação constante e de respostas rápidas às ameaças emergentes estimula tanto o aprimoramento das tecnologias existentes quanto a criação de novos métodos para proteger as infraestruturas digitais e os dados críticos. Mas é comum ouvir que o usuário é o elo mais fraco de qualquer sistema de proteção. As consequências disso estão muito além da proteção de tais sistemas. É urgente discutir a necessidade de proteção de todos os aspectos da vida do usuário de tecnologia.

O *Center for Humane Technology*, organização independente sem fins lucrativos, tem como foco expor os mecanismos por trás de todas as tecnologias aplicadas para capturar e influenciar nossos pensamentos, comportamentos, emoções e ações. Seus fundadores são os autores do documentário ‘O dilema das Redes’, assistido por mais de 100 milhões de pessoas e ganhador do Prêmio Emmy, exibido na plataforma Netflix e do vídeo *THE AI DILEMMA*, disponível na plataforma youtube,

exibido em 09 de março de 2023, com mais de 3,4 milhões de visualizações até 20 de setembro de 2024 [HARRIS & RASKIN, 2023].

Em um breve resumo, os autores relatam que tudo começa com engenheiros criando e aplicando algoritmos para aumentar o engajamento de usuários nas redes sociais através da predição de outputs personalizados que conseguissem capturar a intenção dos usuários por mais tempo. Todavia, isso gerou efeitos indesejados: *Doomscrolling* ('doom' - catástrofe, ruína; 'scrolling' – ato de rolar página) ou 'rolagem da perdição' ou 'rolagem para a desgraça', assim entendido como a prática de consumir compulsivamente notícias ruins; Diminuição da capacidade concentração infantil; Adição em pornografia; Pedofilia digital; Sobrecarga informacional; Polarização; *Fake news*; Ameaça a democracia; Colapso da realidade, da verdade e confiança; Criação de cyber weapons, guerra assimétrica; Relacionamentos superficiais.

Os autores alertam que estes problemas não foram devidamente enfrentados e que serão agravados exponencialmente com o surgimento dos *Gollem – Generative Large Language Multi-Modal Models* – Modelos Geração de Linguagem Multi-Modais de Larga Escala, com capacidade de gerar sons, imagens. Relatam preocupação com o fato de que em 2022 o número de pesquisas em segurança no uso da Inteligência Artificial foi 30 vezes menor do que as pesquisas em Sistemas de Processamento Neural, sugerindo um preocupante aumento na busca pela habilidade de modelar o pensamento humano em detrimento da segurança no uso da IA [HARRIS & RASKIN, 2023].

O usuário não representa apenas o elo mais fraco na proteção dos sistemas de informação. Ele é, em si, na qualidade de ser humano, o mais frágil e mais exposto a perigos. Será que as pessoas comuns percebem a gravidade dos riscos cibernéticos? Qual o nível de conscientização sobre boas práticas de segurança digital? Qual o impacto do uso massivo de tecnologia sem a consciência dos perigos que esta traz? Com que frequência nos deparamos com comportamentos de risco, como o uso de senhas fracas, clicar em links suspeitos ou compartilhar informações pessoais sem cuidados? Quais os impactos na saúde mental das pessoas com o uso inconsciente de tecnologia? As pessoas estão cientes de problemas como polarização, filtros de bolha, medo de ficar de fora (*Fear of Missing Out*)?

3. Impactos do Desafio na Sociedade

A sociedade está vivenciando as consequências da ausência de educação digital. Ameaças à verdade, à democracia, ao bem-estar e saúde mental das pessoas. Crianças, adolescentes, idosos, adultos, absolutamente todos, estão expostos a diferentes tipos e graus de vulnerabilidade. A tecnologia não respeita espaços sociais, privados, a separação de classes, os limites territoriais.

Em muitos casos, a segurança cibernética é vista como custo e não investimento. A regulamentação insipiente do espaço cibernético contribui para este cenário de risco. A conveniência oferecida por muitos dispositivos e serviços tecnológicos incentivam um comportamento menos cuidadoso. Por exemplo, o uso de autenticação automática e a confiança excessiva em dispositivos sem considerar as configurações de segurança

adequadas expõem a vulnerabilidade. As pessoas muitas vezes priorizam conveniência sobre segurança, o que as torna suscetíveis a fraudes.

Muitas fraudes e ataques cibernéticos não ocorrem por causa de falhas técnicas, mas sim porque as pessoas são manipuladas para fornecer informações, baixar arquivos ou clicar em links maliciosos. Ensinar as pessoas a reconhecerem e evitarem técnicas de engenharia social é um dos maiores desafios, pois esses ataques exploram a psicologia humana, e não apenas falhas tecnológicas. Vivemos uma verdadeira epidemia de fraudes no Brasil.

O crime de estelionato, assim definido como aquele previsto no art. 171 do Código Penal vem aumentando a incidência ano a ano por todo o Brasil, segundo o Anuário Brasileiro de Segurança Pública de 2024, publicado pelo Fórum Brasileiro de Segurança Pública.

No Estado do Rio de Janeiro, observamos o mesmo fenômeno do aumento da incidência dos crimes de estelionato ao longo dos últimos anos.

Uma análise do comportamento de outros indicadores de crimes no Estado do Rio de Janeiro mostra um comportamento semelhante entre os crimes de Estelionato e os crimes de Roubo e Furto de Celular:

Os aumentos nos anos de 2022 e 2023 sugerem uma correlação entre os crimes de estelionato com os crimes de furto e roubo de celular. A hipótese sugerida é que criminosos estão se aproveitando da falta de educação digital do cidadão para criar mecanismos de proteção de seus dispositivos, que estariam sendo utilizados pelos criminosos para prática de crimes de estelionato.

Essa hipótese é reforçada pelo comportamento completamente diferente dos outros indicadores de crimes que aferem o comportamento da criminalidade no Rio de Janeiro. A seguir, exibimos os indicadores de roubo de veículos, roubo de carga e ocorrências com morte violenta – letalidade violenta, que são historicamente usados pelo Governo do Estado do Rio de Janeiro.

Os crimes de estelionato digitais provocam prejuízos financeiros e emocionais nas suas vítimas. Com uma educação adequada, dando as pessoas conhecimento necessário para que se protejam da engenhosidade social perpetrada pelos criminosos, esse impacto poderia ser minimizado.

A disrupção do nosso meio de vida trazida pela tecnologia não foi percebida como uma ameaça. Todos os dias, milhares de pessoas entram no espaço cibernético como se estivessem sentados no banco do motorista de um veículo sem saber como guiá-lo. O desafio é descobrir como criar uma cultura de uso seguro da tecnologia, manter a educação sobre cibersegurança sempre atualizada para acompanhar as novas vulnerabilidades e técnicas de ataque que surgem constantemente. Hackers estão sempre desenvolvendo novos métodos de exploração, e manter o público informado sobre os perigos emergentes é uma tarefa contínua.

Os dispositivos que utilizam sistemas computacionais estão por toda parte da vida do cidadão comum. Difícil apontar um empreendimento que não faça uso de um sistema. Seja um smartphone, usado pelo microempreendedor, ou data centers enormes,

usados por grandes empresas, a economia deslocou-se do eixo industrial para uma base tecnológica.

A evolução tecnológica sem dúvidas traz incontáveis benefícios para a sociedade, ganhos de produtividade, acesso a informação, expansão do mercado consumidor, automação de atividades, eficiência operacional, controle, etc. Mas, assim como toda tecnologia ao longo da história da humanidade, traz também aspectos negativos, relacionados ao seu mal uso e consequências não pensadas.

Quando se fala em cibersegurança, muito se fala sobre a proteção contra ataques aos sistemas de informação, a proteção dos dados, privacidade, criação destes mecanismos. Todavia, não importa quão moderno, bem desenvolvido e arquitetado são as soluções de proteção, a maior vulnerabilidade está na falta de conhecimento dos usuários comuns. Assim como ele é o elo fraco desta corrente, também é, em si, o mais vulnerável e necessitado de proteção. Saber como se comportar, usar, o que evitar, é imperioso para evitar ataques cibernéticos

Tabela 1 – FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 18º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2024. Disponível em: <https://publicacoes.forumseguranca.org.br/handle/1234> , consultado em 21/09/2014

TABELA 15

Estelionato e Estelionato por meio eletrônico ⁽¹⁾
 Brasil e Unidades da Federação – 2022-2023

Brasil e Unidades da Federação	Estelionato					Estelionato por meio eletrônico				
	Ns. Absolutos		Taxas ⁽²⁾		Variação (%)	Ns. Absolutos		Taxas ⁽²⁾		Variação (%)
	2022 ⁽¹⁾	2023	2022	2023		2022 ⁽¹⁾	2023	2022	2023	
Brasil	1.816.438	1.965.353	894,4	967,8	8,2	207.125	235.393	173,1	196,8	13,6
Acre	5.649	5.538	680,6	667,2	-2,0	154	248	18,6	29,9	61,0
Alagoas	20.087	21.058	642,2	673,3	4,8	4.973	5.729	159,0	183,2	15,2
Amapá	8.587	7.146	1.170,3	973,9	-16,8	380	618	51,8	84,2	62,6
Amazonas	15.430	17.464	391,5	443,1	13,2	419	877	10,6	22,2	109,3
Bahia	91.223	98.934	645,1	699,6	8,5	4.183	7.515	29,6	53,1	79,7
Ceará	68.754	68.235	781,7	775,8	-0,8	...	...	...	...	...
Distrito Federal	52.995	50.387	1.881,0	1.788,4	-4,9	15.749	16.060	559,0	570,0	2,0
Espírito Santo	37.391	35.168	975,3	917,3	-5,9	15.277	14.578	398,5	380,3	-4,6
Goias	74.163	74.906	1.051,0	1.061,5	1,0	1.488	2.167	21,1	30,7	45,6
Maranhão	14.799	14.782	218,4	218,1	-0,1	5.781	6.278	85,3	92,6	8,6
Mato Grosso	20.261	20.565	553,8	562,1	1,5	9.253	11.257	252,9	307,7	21,7
Mato Grosso do Sul	13.647	13.357	495,0	484,5	-2,1	5.027	5.414	182,3	196,4	7,7
Minas Gerais	132.120	141.649	643,2	689,6	7,2	35.878	40.906	174,7	199,2	14,0
Pará	35.038	36.845	431,5	453,7	5,2	13.099	16.884	161,3	207,9	28,9
Paraíba	5.669	6.443	142,6	162,1	13,7	406	1.030	10,2	25,9	153,7
Paraná	141.777	145.205	1.238,8	1.268,8	2,4	5.738	7.029	50,1	61,4	22,5
Pernambuco	59.499	58.460	656,8	645,3	-1,7	14.164	13.941	156,4	153,9	-1,6
Piauí	15.310	16.663	468,0	509,4	8,8	276	584	8,4	17,9	111,6
Rio de Janeiro	123.841	120.218	771,3	748,8	-2,9	...	...	...	...	...
Rio Grande do Norte	25.945	26.018	785,6	787,8	0,3	...	...	...	...	...
Rio Grande do Sul ⁽⁴⁾	95.182	87.627	874,6	805,2	-7,9	...	6.577	...	...	...
Rondônia	15.376	18.393	972,4	1.163,2	19,6	5.932	6.532	375,2	413,1	10,1
Roraima	5.396	5.359	847,5	841,7	-0,7	778	1.893	122,2	297,3	143,3
Santa Catarina	95.706	94.944	1.257,6	1.247,6	-0,8	64.646	64.482	849,4	847,3	-0,3
São Paulo	611.572	750.430	1.377,1	1.689,7	22,7	...	...	...	...	...
Sergipe	19.734	17.763	892,9	803,8	-10,0	446	751	20,2	34,0	68,4
Tocantins	11.287	11.796	746,8	780,4	4,5	3.078	4.043	203,6	267,5	31,4

Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Instituto de Segurança Pública/RJ (ISP); Polícia Civil do Estado do Acre; Polícia Civil do Distrito Federal; Polícia Civil do Estado de Roraima; Instituto Brasileiro de Geografia e Estatística (IBGE) – Censo Demográfico 2022; Fórum Brasileiro de Segurança Pública.

(...) Informação não disponível.

(1) Em 2021, o crime de Estelionato - Fraude eletrônica passou a ser tipificado pelos parágrafos 2ºA, 2ºB e 3º do art. 171 do Código Penal.

(2) Taxas por 100 mil habitantes.

Nesse sentido, um dos grandes desafios tecnológicos é a ausência de literacia digital dos usuários de todos os níveis. A tecnologia avança rapidamente e, com ela, as ameaças cibernéticas. A comunidade acadêmica está diante de um desafio enorme. Estas ameaças e vulnerabilidades são bem conhecidas, definidas e estudadas no âmbito acadêmico. Mas todo esse conhecimento precisa ultrapassar os limites da academia. Precisamos pensar nas melhores e mais eficientes estratégias para enfrentar este desafio.

Referências

HARRIS, Tristan and RASKIN, Aza. (2023) “The AI Dilemma. [S.l.]: Center for Humane Technology”

<https://www.youtube.com/watch?v=xoVJKj8lcNQ>. Acesso em: 19 set. 2024.