CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

GT ON-LINE - DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET (A)

D598
Direito, Políticas Públicas, Tecnologia e Internet – GT on-line[Recurso eletrônico on-line] organização Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores Livio Augusto de Carvalho Santos, Regina Vera Villas Bôas e Valmir Cesar Rossetti – Franca: Faculdade de Direito de Franca, 2023.

Inclui bibliografia
ISBN: 978-65-5648-913-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios da Regulação do Ciberespaço.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2023 : Franca, SP).

CDU: 34

CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

GT ON-LINE - DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET (A)

Apresentação

É com grande satisfação que apresentamos os Anais do Primeiro Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet, realizado entre os dias 12 e 15 de setembro de 2023, na Faculdade de Direito de Franca, composta por trabalhos apresentados nos Grupos de Trabalhos que ocorreram durante o evento, após rigorosa e disputada seleção.

Ditos trabalhos, que envolvem pesquisas realizadas nas mais diversas áreas do direito, mas primordialmente relacionados a temas centrados na relação entre o direito e o impacto das tecnologias, apresentam notável rigor técnico, sensibilidade e originalidade, buscando uma leitura atual e inovadora dos institutos próprios da área.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões que ocorreram no evento por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Coordenação do Evento:

Alexandre Veronese (UnB)

Felipe Chiarello de Souza Pinto (Mackenzie)

José Sérgio Saraiva (FDF)

Lislene Ledier Aylon (FDF)

Orides Mezzaroba (CONPEDI/UFSC)

Samyra Naspolini (FMU)

Sílzia Alves (UFG)

Yuri Nathan da Costa Lannes (FDF)

Zulmar Fachin (Faculdades Londrina)

Realização:

Faculdade de Direito de Franca (FDF)

Grupo de Pesquisa d Políticas Públicas e Internet (GPPI)

Correalização:

Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI)

Faculdades Londrina

Universidade Federal de Goiás (UFG)

Universidade Presbiteriana Mackenzie (UPM)

Mestrado Profissional em Direito da UFSC

ANÁLISE DA ESTRATÉGIA DE TREINAMENTO DE COMPETÊNCIAS DIGITAIS, MIDIÁTICAS E INFORMACIONAIS A PARTIR DA POLÍTICA NACIONAL DA EDUCAÇÃO DIGITAL (PNED) PARA A PREVENÇÃO DO "PHISHING" E DO "SMISHING"

ANALYSIS OF THE COACHING STRATEGY FOR DIGITAL, MEDIA AND INFORMATIONAL SKILLS BASED ON THE NATIONAL DIGITAL EDUCATION POLITICS (NDEP) TO PREVENT "PHISHING" AND "SMISHING"

Giulia Name Vieira [1]
José Luiz de Moura Faleiros Júnior [2]

Resumo

A pesquisa analisa, a partir da Política Nacional de Educação Digital (PNED), estratégias de capacitação de competências digitais, midiáticas e informacionais para prevenir práticas de phishing e smishing. Ambos os ataques cibernéticos visam obter informações confidenciais por meio de diferentes canais (e-mails e SMS). A PNED, como política pública, promove hábitos que reduzem a assimetria informacional e mitigam danos, contribuindo para a prevenção desses crimes. A pesquisa adota uma abordagem jurídico-social, com um enfoque jurídico-projetivo e um método predominantemente dialético.

Palavras-chave: Phishing, Smishing, Política nacional de educação digital, Inclusão digital, Literacia digital

Abstract/Resumen/Résumé

The research analyzes, based on the National Policy for Digital Education (PNED), strategies to develop digital, media, and information literacy skills to prevent phishing and smishing practices. Both cyber attacks aim to obtain confidential information through different channels (emails and SMS). PNED, as a public policy, promotes habits that reduce informational asymmetry and mitigate damages, contributing to the prevention of these crimes. The research adopts a legal-social approach, with a legal-projective focus and a predominantly dialectical method.

Keywords/Palabras-claves/Mots-clés: Phishing, Smishing, National policy for digital education, Digital inclusion, Digital literacy

[1] Graduanda em Direito pela SKEMA Business School.

[2] Doutorando em Direito pela USP e pela UFMG. Professor da SKEMA Law School. Advogado. Orientador.

1. CONSIDERAÇÕES INICIAIS

É notório que, com o advento da Internet, a vida foi facilitada e as tarefas diárias, otimizadas. O crescimento dos meios digitais aumenta o fluxo de dados digitais, podendo colocar em risco a segurança cibernética e ocasionar um empecilho para esse novo modo de vida. Tal vulnerabilidade está associada à recorrência de práticas fraudulentas como as que se convencionou denominar de "*phishing*" e "*smishing*", que são técnicas de ataque cibernético que visam enganar pessoas para obter informações confidenciais, como senhas, números de cartão de crédito e dados pessoais. Ambos os ataques têm o objetivo de subtrair criminosamente informações das vítimas, mas são realizados por meio de diferentes canais (e-mails e torpedos SMS, respectivamente).

Não se pretende discutir, do ponto de vista do Direito Penal, o enquadramento dessas práticas nas figuras do furto qualificado do art. 155, §4º, inciso II, ou do estelionato do art. 171, ambos do Código Penal brasileiro. Ao invés disso, a pesquisa em questão tem o objetivo de analisar, a partir da Política Nacional de Educação Digital – PNED (Lei nº 14.533, de 11 de janeiro de 2023), estratégias de capacitação de determinadas competências, tais como a digital, a midiática e a informacional, a fim de descrever a função que passam a ter, no cumprimento de política pública especificamente direcionada ao desenvolvimento da literacia digital da população, para a prevenção das práticas de "*phishing*" e de "*smishing*" selecionadas no recorte temático.

Uma vez que crimes cibernéticos não deixam rastros, o que dificulta a identificação do autor do delito, trabalhar-se-á com a hipótese de que a PNED, enquanto política pública, tem o efeito de promover hábitos que contribuem para a redução da assimetria informacional e para a mitigação difusa de danos.

A pesquisa que se propõe, na classificação de Gustin, Dias e Nicácio (2020), pertence à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa foi predominantemente dialético e quanto ao gênero de pesquisa, foi adotada a pesquisa teórica.

2. ORIGENS E DEFINIÇÕES DE "*PHISHING*" E DE "*SMISHING*"

O termo "*phishing*" teve sua origem em meados de 1990, sendo uma referência ao termo "*fishing*", em inglês, "pescaria". Possui a característica de o praticante "pescar", ou seja, roubar dados de outros, sobretudo via *e-mails* com o intuito de captar informações a respeito

das vítimas e usá-las para acesso a bancos digitais ou outros usos que deveriam ser feitos apenas pelo possuidor de tais dados (ALEROUD; ZHOU, 2017). Essas informações são obtidas através da junção de meios técnicos e da engenharia social (CERT, 2012), que é a expressão que denomina a manipulação e enganação de pessoas para que essas forneçam informações ou executem determinada ação (MANN, 2011). O executor de tal costume recebe o nome de "engenheiro social" e são esses os responsáveis por manipularem as ações de outros indivíduos com o objetivo de acessar às informações privadas desses (MITNICK; SIMON, 2003).

Por outro lado, o termo "*smishing*" é uma forma de *phishing* através de SMS, *Short Message Service*, que se trata de links recebidos por meio do serviço de mensagem em questão com mensagens falsas. A partir do recebimento de tais avisos, a vítima clica em links falsos e passa dados confidenciais, que serão utilizados erroneamente por terceiros.

Visto as origens dos termos em análise, é cabível inferir que os ataques podem ocorrer de diversas maneiras, por diversos meios, possuindo, então, grande abrangência. Dessa forma, é possível afirmar que na maioria dos casos, a vítima sequer sabe o que está havendo, sendo difícil descobrir sobre o acontecimento e não sendo possível bloquear o sistema, por exemplo, assim que os dados foram passados, tendo que lidar com consequências futuras que, geralmente, são mais graves.

3. COMPETÊNCIAS DIGITAIS, MIDIÁTICAS E INFORMACIONAIS A PARTIR DA POLÍTICA NACIONAL DA EDUCAÇÃO DIGITAL (PNED)

O saber tecnológico é solução necessária para a promoção do direito fundamental de acesso à Internet na sociedade da informação. Sem que se tenha cidadãos bem instruídos sobre os usos e práticas da tecnologia e das redes comunicacionais, qualquer medida destinada à mitigação dos efeitos negativos da malversação tecnológica cairá no vazio.

O ensino hodierno está intimamente ligado ao preenchimento das necessidades humanas, definidas por Abraham Maslow (1970) e perfeitamente enquadráveis no contexto da atual sociedade da informação, na qual se impõe o convívio com um novo ambiente chamado ciberespaço, em que a tecnologia atua como um poderoso componente do ambiente de aprimoramento individual.[1] Nesse contexto, é preciso ressaltar que as relações sociais e

[1] Anota: "If we examine carefully the average desires that we have in daily life, we find that they have at least one important characteristic, i.e., that they are usually means to an end rather than ends in themselves. We want money so that we may have an automobile. In turn we want an automobile because the neighbors have one and we do not wish to feel inferior to them, so that we can retain our own self-respect and so that We can be loved and respected by others. Usually when a conscious desire is analyzed we find that we can go behind it, so to speak, to other, more fundamental aims of the individual. In other words, we have here a situation that parallels very much the role of

pedagógicas, assim como os benefícios e malefícios trazidos pelas Tecnologias de Informação e Comunicação, são desdobramentos de comportamentos da própria sociedade, e não consequências da simples existência da Internet. (MONTEIRO; CARVINO, 2015, p. 242)

Magda Pischetola registra três tipos de "competências digitais":

> 1) As *operacionais*: ou seja, o conjunto de habilidades técnicas que permitem ao usuário acessar as aplicações básicas das TICs on-line e off-line, como, por exemplo, o editor de texto, o e-mail, as atividades de busca on-line.
> 2) As *informacionais*: habilidades para pesquisar, selecionar e elaborar as informações que se encontram nos recursos da rede.
> 3) As *estratégicas*: habilidades para determinar metas específicas orientadas a alcançar outras mais amplas, com o fim de manter ou melhorar sua própria posição social. (PISCHETOLA, 2016, p. 42)

O desenvolvimento dessas competências (ou '*skills'*, para citar o termo utilizado por van Dijk e van Deursen[2]), é uma das chaves para a transição à sociedade da informação. Viver sem computadores está se tornando cada vez mais difícil, pois se perde um número crescente de oportunidades. Em várias ocasiões, as pessoas serão excluídas de acesso a recursos vitais. Todo candidato a emprego sabe que a capacidade de trabalhar com computadores e a Internet é crucial para encontrar e obter um emprego e, cada vez mais, para concluir um trabalho. O número de trabalhos que não exigem habilidades digitais está diminuindo rapidamente. A localização de empregos exige cada vez mais o uso de locais de vagas e aplicativos eletrônicos. Nas entrevistas de emprego, os empregadores solicitam cada vez mais certificados ou outras provas de habilidades digitais.[3]

---

symptoms in psychopathology. The symptoms are important, not so much in themselves, but for what they ultimately mean, that is, for what their ultimate goals or effects may be." (MASLOW, 1970, p. 21)

[2] Registram: "In the first decade of the twenty-first century, the attention given to the so-called digital divide in developed countries gradually decreased. The common opinion among policy makers and the public at large was that the divide between those with access to computers, the Internet, and other digital media and those without access was closing. In some countries, 90 percent of households were connected to the Internet. Computers, mobile telephony, digital televisions, and many other digital media decreased in price daily while their capacity multiplied. On a massive scale, these media were introduced in all aspects of everyday life. Several applications appeared to be so easy to use that practically every individual with the ability to read and write could use them. Yet, we posit that the digital divide is deepening. The divide of so-called physical access might be closing in certain respects; however, other digital divides have begun to grow. The digital divide as a whole is deepening because the divides of digital skills and unequal daily use of the digital media are increasing." (VAN DIJK; VAN DEURSEN, 2014, p. 1)

[3] Comentando o cenário legislativo brasileiro, Renato Opice Blum explica que "(...) pouco adiantará a aprovação de leis para garantir uma segurança maior ao usuário da rede mundial de computadores se ele, antes de iniciar a conexão com um mundo tão rico, tão vasto, tão cheio de informações, mas por vezes perigoso, não for educado digitalmente. Primeiro, é necessário que o usuário, tanto no âmbito pessoal, quanto profissional, e de forma preventiva, seja educado para isso. Por meio de educação voltada para o uso correto da Internet e de suas informações. Esse aprendizado deveria começar na fase escolar e perdurar por toda a vida do ser humano, ante o dinamismo e a abrangência do mundo virtual. Da mesma forma, as escolas devem fazer uso de uma Política de Segurança da Informação, aplicando sistemas eficientes para resguardar o sigilo de suas informações, especialmente de seus alunos. Entretanto, é importante observar que de nada adiantará a escola empresa ter uma

Hoje, segundo van Dijk e van Deursen, todas as escolas dos países desenvolvidos, em todos os níveis de ensino, incluem o uso de computadores e a Internet em seus currículos, de modo que frequentar a escola equivale a usar essas mídias e poder operá-las. Na educação primária dos países ricos, as crianças aprendem amplamente a usar computadores e a Internet em casa, antes mesmo de entrarem na rotina escolar. Na escola, por sua vez, recebem instruções adicionais e um foco no uso dessas mídias digitais para a consolidação do aprendizado – não apenas para entretenimento. (VAN DIJK; VAN DEURSEN, 2014, p. 47)

Sendo certo que "a escola dos séculos XIX e XX foi uma importante instituição difusora de uma sociedade letrada e, agora, adentra o século XXI com novos desafios, porquanto a sociedade baseada na escrita está rapidamente se transformando em uma sociedade informática" (MENESES; JIMENE, 2015, p. 67), o papel da escola e dos educadores dentro de suas áreas de atuação passa a lhes exigir que definam, reflitam, instituam e coordenem o cumprimento das regras que forem impostas.

No Brasil, o Marco Civil da Internet cuidou de determinar ao Estado o dever de promover a educação e a inclusão digital:

> Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.
>
> Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:
> I - promover a inclusão digital;

E, cumprindo o mister definido no comando normativo contido nos artigos 26 e 27 do Marco Civil da Internet, o legislador finalmente promulgou a Política Nacional de Educação Digital – PNED (Lei nº 14.533, de 11 de janeiro de 2023), com o objetivo de ampliar o acesso da população brasileira a recursos, ferramentas e práticas digitais, com foco nas populações mais vulneráveis. A PNED é composta por programas, projetos e ações de diferentes entidades governamentais, tanto a nível federal quanto estadual e municipal, e abrange também os programas de inovação e tecnologia na educação que recebem apoio técnico ou financeiro do governo federal. A política é estruturada em quatro eixos principais: Inclusão Digital, Educação Digital Escolar, Capacitação e Especialização Digital, e Pesquisa e Desenvolvimento em Tecnologias da Informação e Comunicação.

---

estrutura adequada na área de Tecnologia da Informação se os professores, alunos e pais não tiverem consciência da importância de se garantir a segurança da informação." (BLUM, 2015, p. 189-190.)

Insofismavelmente, na medida em que a Internet “aumenta o poder da sociedade civil para atuar mediante cooperação e solidariedade frente aos demais poderes que atuam de forma vertical” (BENACCHIO; SANTOS, 2015, t. I, p. 168), a promoção da educação digital desempenha papel essencial para o reforço da liberdade expressão bem manifestada. A PNED não substitui outras políticas existentes, como as políticas nacionais, estaduais, distritais ou municipais de educação escolar digital, de capacitação profissional para novas competências e de ampliação de infraestrutura digital e conectividade. Em vez disso, ela atua como uma instância de articulação, buscando potencializar os resultados dessas políticas. Cada eixo da PNED tem estratégias prioritárias definidas, e o primeiro eixo, o da inclusão digital, estabelece diretrizes para promover competências digitais e informacionais, oferecer treinamento, facilitar o acesso a plataformas e recursos digitais, e promover certificação nessa área.

O eixo "promoção de competências digitais e informacionais" da Política Nacional de Educação Digital (PNED) busca sensibilizar os cidadãos brasileiros sobre a importância das competências digitais, midiáticas e informacionais. Essa iniciativa tem o potencial de reduzir a propensão dos cidadãos incluídos digitalmente a práticas criminosas, como o *phishing* e o *smishing*, devido aos seguintes fatores: *(i)* conscientização sobre ameaças: Ao sensibilizar os cidadãos sobre as competências digitais, midiáticas e informacionais, a PNED pode educá-los sobre os riscos associados a práticas criminosas online, como o *phishing* e o *smishing*. Os cidadãos terão maior conhecimento sobre os métodos usados pelos criminosos para enganar e roubar informações pessoais, como senhas bancárias e dados de cartões de crédito; *(ii)* reconhecimento de técnicas de fraude: A promoção de competências digitais e informacionais pode capacitar os cidadãos a identificar técnicas de fraude utilizadas no *phishing* e *smishing*. Eles aprenderão a reconhecer sinais de alerta, como e-mails ou mensagens suspeitas, links maliciosos, solicitações de informações confidenciais e abordagens enganosas. Essa conscientização pode ajudá-los a evitar cair em armadilhas e a proteger suas informações pessoais; *(iii)* uso seguro da tecnologia: A PNED pode fornecer orientações sobre o uso seguro da tecnologia, incluindo práticas de segurança digital e proteção de informações pessoais. Os cidadãos incluídos digitalmente terão acesso a informações sobre a importância de manter seus dispositivos e aplicativos atualizados, utilizar senhas fortes, evitar compartilhar informações confidenciais em sites não confiáveis e adotar medidas de segurança ao lidar com transações online. Essas competências ajudam a reduzir a vulnerabilidade a ataques de *phishing* e *smishing*.

Além disso, o eixo da inclusão digital prevê a implantação de infraestrutura de conectividade nas escolas, garantindo acesso à internet de alta velocidade e equipamentos

adequados para o ambiente educacional, além de promover o acesso móvel à internet para professores e estudantes. Essa Lei busca estabelecer diretrizes e ações para impulsionar a educação digital no país, visando reduzir as desigualdades e promover o desenvolvimento de competências digitais e tecnológicas, especialmente entre as populações mais vulneráveis. Ao articular programas, projetos e ações de diferentes esferas governamentais e áreas de atuação, a PNED visa otimizar os resultados das políticas públicas relacionadas à educação digital, abrangendo desde a inclusão digital até a pesquisa e desenvolvimento em tecnologias da informação e comunicação.

4. CONCLUSÃO

A promoção de competências digitais e informacionais, como previsto na Política Nacional de Educação Digital (PNED), é essencial para combater práticas criminosas como o *phishing* e o *smishing*. O *phishing* é o roubo de dados por meio de e-mails fraudulentos, enquanto o *smishing* é uma forma de *phishing* feita por SMS. Esses ataques ocorrem por meio da manipulação e enganação das pessoas para obter informações confidenciais.

Ao sensibilizar os cidadãos sobre a importância das competências digitais e informacionais, a PNED ajuda a conscientizá-los sobre os riscos dessas práticas criminosas e a identificar sinais de alerta, como mensagens suspeitas e links falsos. Além disso, o desenvolvimento dessas competências capacita as pessoas a utilizar a tecnologia de forma segura, protegendo suas informações pessoais e evitando se tornarem vítimas de *phishing* e *smishing*. A PNED, ao promover a educação digital, contribui para reduzir a propensão a esses crimes e fortalecer a segurança na era digital.

Portanto, ao promover competências digitais e informacionais entre os cidadãos, a PNED pode contribuir para que eles se tornem menos propensos a cair em práticas criminosas, como o *phishing* e o *smishing*. Com uma compreensão aprimorada dos riscos e técnicas de fraude, juntamente com o conhecimento de boas práticas de segurança digital, os cidadãos incluídos digitalmente estarão mais bem equipados para proteger suas informações pessoais e evitar se tornarem vítimas desses tipos de crimes.

REFERÊNCIAS

ALEROUD, Ahmed; ZHOU, Lina. Phishing environments, techniques, and countermeasures: A survey. **Computers & Security**, [S.l], v. 68, p. 160–196, jul. 2017.

ALVES, Mateus de Araújo. **Crimes digitais**: Análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova. São Paulo: Dialética, 2020.

BENACCHIO, Marcelo; SANTOS, Queila Rocha Carmona dos. A Lei nº 12.965/14 como instrumento de promoção dos direitos humanos. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I

BLUM, Renato Opice. O Marco Civil da Internet e a educação digital no Brasil. *In:* ABRUSIO, Juliana (coord.). **Educação digital**. São Paulo: Revista dos Tribunais, 2015.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm Acesso em: 06 jun. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União, Brasília, DF. Disponível http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 06 jun. 2023.

BRASIL. Lei nº 14.533, de 11 de janeiro de 2023. **Institui a Política Nacional de Educação Digital e dá outras providências**. Diário Oficial da União, Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm Acesso em: 06 jun. 2023.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5. ed. São Paulo: Almedina, 2020.

MANN, Ian. **Engenharia Social.** São Paulo: Blücher, 2011.

MASLOW, Abraham H. **Motivation and personality**. 2. ed. Nova York: Harper & Row, 1970.

MENESES, Marcelo Figueiredo de; JIMENE, Camilla do Vale. A tecnologia que permeia a escola: uma breve visão histórica. *In:* ABRUSIO, Juliana (coord.). **Educação digital**. São Paulo: Revista dos Tribunais, 2015.

MITNICK, Kevin; SIMON, William. **The art of intrusion**: the real stories behind the exploits of hackers, intruders and deceivers. Oxford: Wiley, 2003.

MONTEIRO, Renato Leite; CARVINO, Fabrício Inocêncio. Adaptive learning: o uso de inteligência artificial para adaptar ferramentas de ensino ao aluno. *In:* ABRUSIO, Juliana (Coord.). **Educação digital**. São Paulo: Revista dos Tribunais, 2015.

MORAES, Alexandre Fernandes. **Segurança em redes**: fundamentos. São Paulo: Saraiva, 2010.

PISCHETOLA, Magda. **Inclusão digital e educação**: a nova cultura da sala de aula. Petrópolis: Vozes, 2016.

VAN DIJK, Jan; VAN DEURSEN, Alexander. **Digital skills**: unlocking the information society. Nova York: Palgrave Macmillan, 2014.