Cidadania digital, segurança na rede e o comportamento de futuros professores

Simão P. P. Marinho[1], Flávia C. Carneiro[2], Ricardo M. Nicolau[3], Ramon F.[4]

[1]Programa de Pós-Graduação em Educação – Pontifícia Universidade Católica de Minas Gerais (PUC MINAS) – 30.535-901 – Belo Horizonte – MG – Brasil

[21]Programa de Pós-Graduação em Educação – Pontifícia Universidade Católica de Minas Gerais (PUC MINAS) – 30.535-901 – Belo Horizonte – MG – Brasil

[3]Departamento de Engenharia de Computação – Fundação Presidente Antônio Carlos – Campus Conselheiro Lafaiete – 36.400-000 – Conselheiro Lafaiete – MG - Brasil

[41]Programa de Pós-Graduação em Educação – Pontifícia Universidade Católica de Minas Gerais (PUC MINAS) – 30.535-901 – Belo Horizonte – MG – Brasil

marinhos@pucminas.br, flaviacar@yahoo.com, ricnic.br@gmail.com, ramon.flauzino@gmail.com

Abstract: *Digital technologies have been causing profound changes in society. The use of these technologies without proper care exposes the users to various types of risks. Then comes the need to develop skills for a culture of safe use of digital technologies. In this context, considering the role of new generations' education for digital culture, this work investigates habits of internet use by undergraduate students of the Biological Sciences, Philosophy and Pedagogy courses of a private educational institution. The data reveal a significant unpreparedness of the future teacher for the safe use of the Internet, which results in damage to his task of educating the new generations.*

Resumo**:** *As tecnologias digitais vêm provocando profundas mudanças na sociedade. O uso cotidiano dessas tecnologias sem os devidos cuidados expõe o usuário a diversos tipos de riscos. Surge então a necessidade de desenvolver competências para que se constitua uma cultura de uso seguro das tecnologias digitais. Nesse contexto, considerando o papel de formador das novas gerações para a cultura digital, este trabalho investiga hábitos de uso da internet por alunos de licenciatura dos cursos de Ciências Biológicas, Filosofia e Pedagogia de uma instituição privada de ensino. Os dados revelam um significativo despreparo do futuro professor para o uso seguro da Internet, o que resulta em prejuízos em sua tarefa de educador das novas gerações.*

1. Sociedade e Educação no século XXI

A partir da última década do século XX, o mundo assistiu a uma das maiores mudanças sociais, econômicas e comportamentais de sua história: o advento da Internet. O acesso à rede mundial de computadores, condição *si ne qua non* para a participação cidadã efetiva na nova era do conhecimento, ainda se apresenta como um desafio para muitos países. A

impossibilidade de garantir esse acesso fere os princípios de Direitos Humanos, quando se considera que o ambiente virtual, ou ciberespaço, representa parte essencial da esfera do convívio humano, onde toma forma a criação e compartilhamento do conhecimento e o exercício dos direitos e deveres dos cidadãos.

Populações expostas a diferentes níveis de acesso à rede terão, com o passar dos anos, diferentes níveis de desenvolvimento dentro da tecnologia do conhecimento, fato que poderá acarretar um agravamento das já persistentes diferenças sociais, econômicas e políticas em uma esfera global. Por outro lado, essa exposição traz também a possibilidade de ampliação do saber e do conhecimento jamais registrada na humanidade.

E, dentro desse cenário a educação surge como um dos principais setores impactados pelo surgimento das Tecnologias Digitais da Informação e Comunicação (TDIC). A perspectiva da diversidade, inclusão e inovação, aqui alcançam um potencial imensurável, que, se bem conduzido, pode auxiliar na formação de uma sociedade conectada, original e menos desigual. Por outro lado, se não atender de maneira adequada as demandas que recaem sobre ela, teremos muitas dificuldades em preparar as novas gerações para usufruírem dos benefícios que a grande rede traz ao mesmo tempo em que aprendam a se proteger dos perigos que essa tecnologia traz consigo.

A Internet é a instituição de maior grau anárquico que a humanidade já conheceu (Marcacini, 2016). Na medida em que se expande e penetra nos mais variados segmentos sociais, torna-se cada vez mais importante. Se por um lado essa tecnologia possui uma arquitetura que praticamente inviabiliza seu controle centralizado — daí seu caráter anárquico —, ela não é invulnerável e por si só ela não é capaz de oferecer proteção a quem faz uso dela. Não se pode menosprezar que, em algum grau, é possível exercer controle sobre ela, sobre os dados que trafegam nela, como também sobre as relações que se dão nela (e através dela). Por isso, conhecer melhor não apenas a tecnologia, mas suas implicações em nossa vida tornaram-se imprescindíveis. O que caracteriza a atual revolução tecnológica não é a centralidade de informações e conhecimentos, mas a aplicação desses conhecimentos e informações para a construção de novos conhecimentos e dispositivos com ciclos de realimentação cumulativo entre a inovação e uso (Castells, 1999).

Reduz a cada dia o contingente de pessoas que não possui pelo menos um conhecimento empírico do que é Internet. Em que pese a modesta posição que ocupa o Brasil quando se fala em percentual da população com acesso à Internet (78º lugar), e as desiguais taxas de acesso nas diferentes camadas sociais (CERT.br, 2012), toma-se conhecimento dessa tecnologia por todos os meios de comunicação e em praticamente qualquer contexto do cotidiano de nossas vidas. Porém, conhecer não significa saber como fazer uso adequado dela, sobretudo em relação à segurança. Essa situação não é exclusividade da Internet e das TDIC, afinal, quantos de nós usamos o rádio, a tv, o automóvel, e até mesmo um chuveiro sem saber detalhes de seu funcionamento. Entretanto, quando se trata do uso de TDIC, é necessário considerar que elas se disseminaram de tal forma nos mais variados segmentos sociais que fazer uso delas vai além de atender necessidades pessoais. Atualmente, o exercício da cidadania, em muitas situações, requer domínio das TDIC. Há, por exemplo, serviços públicos cujo principal canal de acesso se dá pela Internet. A própria globalização implica que os seres humanos estejam mais conectados em rede, pois a internet não tem limites ou fronteiras (Veen, 2009).

2. Cibercrime, educação e cibercidadania

Apenas o direito de se exercer plena (ciber)cidadania seria suficiente para não mais se admitir completo desconhecimento das TDIC, ou se negligenciar a formação das novas gerações para a vida na Sociedade do Século XXI. Porém, há outras implicações: o uso inadequado ou inadvertido das TDIC, e em particular, da Internet traz riscos nas mais variadas situações: exposição de dados pessoais, imagens, vídeos, roubo de informação e de recursos financeiros, ciberviolência, vícios, para citar alguns de uma lista gigantesca.

Na medida em que cada vez mais relações sociais, econômicas ou políticas inerentes à vida do cidadão, passaram a acontecer na, ou através da Internet, as implicações jurídicas do uso desse tipo de tecnologia passaram a ser foco crescente de interesse de estudiosos de diversas áreas, inclusive do direito. Tanto que surgiram várias denominações para esse campo de estudo: Direito Eletrônico, Direito Digital, Direito Virtual e Direito da Informática. Marcacini (2016) considera que Direito da Informática define um "estudo interdisciplinar das relações entre a Informática e todos os ramos do Direito, voltado para a compreensão e enquadramento normativo dos *novos fatos* trazidos pela expansão da tecnologia e pela formação de uma sociedade em rede". Os fatos traduzidos e intermediados pelo computador, o autor denomina como fato informático e defende que o fato informático é o ponto de partida para o ramo do Direito da Informática.

A eleição presidencial de 2018 foi um exemplo claro de *novos fatos* que revelou a importância da grande rede na vida do cidadão brasileiro e que requerem uma base jurídica adequada. Uma parte significativa desse processo eleitoral se desenvolveu através de mídias digitais: as articulações políticas realizadas através de canais digitais, a manifestação popular e os protestos nas redes sociais, e até o uso de informações falsas, tais como as *fakenews* e os boatos (Hoax), com o objetivo de influenciar a opinião pública. Estas últimas em especial revelam como a rede pode, em determinadas situações, ser utilizada como instrumento de controle e até de ações ilegais requerendo, portanto, algum tipo de regulação. Não se trata de regular a Internet, a tecnologia em si, mas regular as relações que se dão através dos meios digitais, sejam elas jurídicas, sociais ou econômicas. E isso deve ser feito através de mecanismos construídos de maneira democrática, legítima e com ampla participação da sociedade ,o que sem dúvida alguma impõe à escola, e em especial ao professor, um fundamental papel na formação para o exercício da cidadania.

No caso de ações ilícitas vale também mencionar o problema dos cibercrimes, o trato jurídico que exigem. Não bastasse o medo que atinge a todos em função dos constantes noticiários que nos mostram uma realidade que muitas vezes supera os horrores de guerras entre nações, sentimo-nos também ameaçados por diversos tipos de crimes cibernéticos. Rossini (2004, p. 32) conceitua crime cibernético como

> ação típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

O CERT.Br (2012) adverte que aquele que se conecta à Internet fica, em algum grau, exposto a uma série de riscos: acesso a conteúdos impróprios ou ofensivos; contato com pessoas mal-intencionadas; furto de identidade; furto e perda de dados; invasão de privacidade; divulgação de boatos; dificuldade de exclusão; dificuldade de detectar,

compreender e expressar sentimentos; dificuldade de manter sigilo; uso excessivo; plágio e violação de direitos autorais. Impõe-se mais uma vez se a necessidade de educação para o uso ético e seguro da tecnologia. Evidentemente, para cumprir seu papel de preparar as novas gerações para o exercício da cidadania e para o trabalho na Era Digital, cabe à escola esclarecer e orientar os alunos. Porém, quando se pensa em segurança na rede, a questão torna-se ainda mais delicada. Na medida em que a escola incluir tecnologias digitais em seu currículo, ao se conectarem à Internet, professores e alunos, se não tomarem os devidos cuidados, ficarão cada vez mais expostos. A fim de cumprirem seu papel, educadores não podem menosprezar o problema da segurança na Internet. Em que pese o ritmo próprio da escola para se apropriar de novidades tecnológicas e mudanças culturais, a tecnologia avança, disponibiliza recursos e cria possibilidades e riscos, aumentando a pressão sobre a escola, uma vez que se espera que ela prepare as novas gerações para o exercício da cidadania e para o mundo do trabalho.

Dentro dos tópicos que constam como condições *si ne qua non* para o exercício da cidadania dentro do mundo digital, dois, em especial, abordam o tema deste artigo: o acesso à internet e a segurança digital. O acesso à internet, figura aqui como fator imprescindível a esse exercício visto que a própria negação do acesso já configura uma limitação à livre participação cidadã do indivíduo. Por mais que nos pareça comum, o acesso à internet ainda é limitado para algumas populações do planeta, seja por questões políticas, geográficas, infraestruturais ou econômicas. Muitas vezes a escola, instituição referência de desenvolvimento da convivência dos indivíduos e da formação cidadã, precisa contornar obstáculos quase intransponíveis para garantir o acesso e a formação digital de seus alunos. Dentro dessa formação digital, a segurança se apresenta como um fator de grande desafio, tanto para escolas quanto para famílias, devido à vastidão de oportunidades de conexão, uma vez estabelecido o acesso. Cada vez mais jovens, os usuários da internet carecem de uma preparação que os previna diante das ameaças intrínsecas a ambientes virtuais. O anonimato e o caráter exponencial das ações tomadas no ambiente virtual, configuram, por si só, uma ameaça real que ronda os mais incautos. Dessa maneira, é papel da escola e da família coordenar ações para a formação digital das novas gerações.

A necessidade de inclusão curricular das TDIC é cada vez mais evidente nos documentos elaborados pelos órgãos responsáveis pelo sistema educacional do país. A Base Nacional Comum Curricular (BNCC) foi construída a partir da Lei nº 9.394/96 de Diretrizes Curriculares Nacionais da Educação Básica (Brasil, 2017) como uma peça central para a construção de aprendizagens com qualidade e excelência correspondendo adequadamente às demandas do estudante e sua preparação para o futuro. Em sua estruturação as TDIC passam a integrar as disciplinas do campo curricular de forma a garantir o desenvolvimento integral por meio de competências previstas para a Educação Básica (Brasil, 2018). No olho desse furacão uma parcela considerável dos professores, sentindo-se arrastada por esse tsunami digital, receosa de se expor, ou expor seus alunos, enquanto pode, opta por não correr riscos na rede. Outros, muitas vezes sem se darem conta dos perigos a que se expõem, se arriscam, alguns deles burlando a proibição sumária que paradoxalmente ainda vige em muitas escolas (Nicolau, 2017).

O CERT.Br (2012, p.3) adverte que

> o primeiro passo para se prevenir dos riscos relacionados ao uso da Internet é estar ciente de que ela não tem nada de “virtual”. Tudo o que ocorre ou é realizado por meio da Internet é real: os dados são reais e

> as empresas e pessoas com quem você interage são as mesmas que estão fora dela. [...] É preciso, portanto, que você leve para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia, como por exemplo: visitar apenas lojas confiáveis, não deixar públicos dados sensíveis, ficar atento quando "for ao banco" ou "fizer compras", não passar informações a estranhos, não deixar a porta da sua casa aberta, etc.

A facilidade e o baixo custo da tecnologia criam condições para que atos ilícitos proliferem na rede. Segundo o CERT.br (2012), ataques cibernéticos, conforme estimativa feita pela McAfee em 2013 podem causar prejuízos da ordem de US$300 bilhões por ano à economia mundial. Cifras atraentes como essa dão origem a uma categoria de negócio: *Crime-as-a-Service.* Nesse negócio, prestadores de serviço e clientes mantém contato em fóruns *online* especializados. No Brasil, um número significativo de ataques tem como motivação os protestos, cujos alvos são sites governamentais, bancos e empresas de comércio eletrônico. Outro tipo de ataque frequente são os realizados como competição entre grupos de hackers. É preciso esclarecer que muitos ataques são feitos a partir de dispositivos previamente invadidos, cujo dono na maioria das vezes ignora completamente que seu aparelho participe do ataque.

Segundo, Moraes (2015), a escola não está imune aos atos ilícitos da Era Digital. Na Europa, por exemplo, jovens do ensino médio contratam hackers para derrubar servidores de provas de suas escolas. No Brasil, prossegue o autor, este tipo de ataque pode ser contratado via web ou pela *deep web* e os custos podem variar de R$10 a R$500 dependendo da extensão e duração do ataque. O que aumenta ainda mais a preocupação é que entre 2010 e 2014 o número de ataques cibernéticos aumentou em 176%, avançando de uma média de 50 ataques por semana em 2010 para 138 em 2014. Esse tipo de conduta dolosa foi tipificada pela Lei nº 12.737/2012, mediante a inserção do parágrafo 1º ao artigo 266 do Código Penal, sendo incluída no crime que, então, passou a se chamar "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública". Conclui-se, portanto, que o tema segurança na Internet não é um assunto a ser tratado em treinamentos esporádicos, requer orientação contínua, sobretudo na escola e na família.

Uma vez que os riscos são reais e há uma necessidade cada vez mais premente de incorporar as TDIC ao dia a dia da escola, o que pode ser feito? A tarefa é complexa. Porém, adaptando-se as melhores práticas apontadas pelo CERT.Br (2012), um dos passos fundamentais para a apropriação da cultura da Era Digital na escola é: adotar uma postura preventiva e que a atenção com a segurança seja um hábito incorporado à rotina de todos os atores do ambiente escolar, independente de questões como local, tecnologia ou meio utilizado. Nesse sentido, o papel dos professores é fundamental, a fim de que essa postura seja exercitada e desenvolvida nas atividades pedagógicas de modo que sua importância seja reconhecida e se torne habitual. Evidentemente, se os professores adotarem esse tipo de postura no cotidiano de suas atividades pessoais, será mais fácil introduzi-la no currículo escolar.

Nesse sentido, como se comportam os alunos de licenciatura ao utilizarem TDIC? Eles adotam posturas preventivas como rotina? Ao utilizarem serviços e aplicativos na Internet eles demonstram se preocuparem com a própria segurança? Apresentando questionário online a alunos de três cursos de licenciatura este trabalho investiga como

esses futuros professores se comportam em relação à segurança ao se conectarem à Internet.

3. Análise dos dados da pesquisa

Alunos de três cursos de graduação, Ciências Biológicas (18%), Filosofia (11%) e Pedagogia (71%) de uma instituição privada de ensino participaram da pesquisa respondendo questionários online. Os dados coletados revelaram que quase dois terços deles fazem uso intensivo da Internet (63%) e praticamente um terço (30%) faz uso moderado. O grupo estudado apresenta comportamento compatível com os brasileiros usuários de Internet, conforme mostra pesquisa realizada pelo CETIC.BR (2018): 87% dos brasileiros usuários de Internet fazem uso diário ou quase diário dela. Vale relatar que 6% dos sujeitos não respondeu sobre sua frequência de uso da Internet. É um contingente que pode ser estudado com maior profundidade para se descobrir porque não quiseram se manifestar a respeito de seu perfil de acesso à Internet. Teriam os futuros professores receio de responder essa pergunta? É oportuno lembrar: não faz muito tempo era corrente a crença de que o professor não sabia usar computador e por isso tinha medo de fazer uso dele em atividades com os alunos.

Quando se pensa em segurança na Internet uma das primeiras questões que vêm à tona refere-se às senhas. O uso de senhas seguras (ou senhas fortes) é importante tanto como forma de proteger os dados de um usuário em particular quanto como política de segurança de empresas, escolas ou instituições. O hábito de usar senhas que não podem ser facilmente descobertas, tais como, datas de aniversários, sequências numéricas, anagramas do nome do usuário, nomes de filhos e familiares, dificultam golpes como "furto de identidade" (CET.br, 2012). Considerando-se que os sujeitos são futuros professores, chama a atenção o fato de que dentre os respondentes um terço (33%) nem sempre se preocupa em criar senhas seguras. É ainda mais alarmante: aproximadamente um em cada dez (8%) alegou que não havia atentado para a importância de usar senhas seguras. Ou seja, a despeito de tudo que já se falou a respeito do uso de senhas e de sua importância como elemento de segurança, quase a metade dos respondentes ainda não incorporou como hábito a postura preventiva que recomendam especialistas na área. Esses alunos de licenciaturas provavelmente possuem senhas que podem ser facilmente "quebradas". Além do manifesto desconhecimento a respeito da importância do uso de senhas fortes, a postura desses futuros professores poderá levar os alunos à perigosa crença de que esse assunto não exige maiores cuidados, o que seria uma lamentável lacuna na formação de cibercidadãos. Não se pode abrir mão da cultura de segurança. Reforçando o papel de orientação do professor, na escola, políticas de segurança devem exigir que todos atendam pelo menos à requisitos básicos, tais como, criar senhas obedecendo regras de formação previamente estabelecidas (tipo e quantidade de caracteres, tamanho mínimo e máximo) e periodicamente trocá-las (CERT.br, 2012).

Um dos serviços que exige do usuário maior cuidado na definição de senhas é o serviço de internet banking. Uma parcela considerável dos sujeitos (58%) respondeu usar esse serviço e mais de um terço dos participantes (34%) fazem uso frequente dele. Quase um terço (33%) respondeu que não utiliza o internet banking e praticamente um em cada dez alunos (9%) afirmou nunca ter feito uso do serviço. Mesmo que lancem mão de literatura específica, uma parcela significativa desses licenciandos (42%) poderá chegar à sala de aula com pouca (33%) ou nenhuma experiência (9%) no assunto. Essa falta de experiência prática com o uso do serviço pode resultar em dificuldade para orientação aos

alunos. Pesquisas futuras poderão investigar se o professor se sente capaz de identificar se sua conexão ao serviço internet banking é segura e se ele se considera preparado para orientar os alunos sobre essa temática.

Aprofundando a investigação, os alunos foram questionados se tinham o hábito de clicar em anúncios que aparecem na tela de seus navegadores. Apenas 2% dos respondentes alegou clicar com frequência nesses links, 40% o fazem raramente e 58% respondeu nunca clicar nesses anúncios. Esses dados chamam a atenção para um estudo mais aprofundado no sentido de se identificar as razões que justificam esse comportamento. Esses estudantes têm receio de clicarem em links falsos por não saberem diferenciá-los de outros legítimos, ou não se sentem seguros para realizarem compras online? Teriam esses licenciandos dificuldade de reconhecerem se o ambiente em que navegam é ou não seguro? Como futuros formadores das novas gerações é imprescindível que eles conheçam esses perigos e sejam capazes de identificar sinais de fraude durante a navegação na rede de modo que sejam capazes de orientar seus alunos. No campo das transações comerciais é grande o número de golpes. Além dos sites fraudulentos criados por alguém que não envia as mercadorias compradas, há sites que realizam falsos leilões e outros que realizam falsas compras coletivas. Outro tipo de golpe é o *Pharming:* apresenta-se ao usuário uma página web falsa parecida com a verdadeira, solicitando seus dados pessoais. Utilizando esses dados de identificação capturados por algoritmos maliciosos, os golpistas "furtam a identidade da vítima" e passam então a fazer compras, abrem empresas fantasmas, criam contas bancárias ilegítimas, acessam sites que exigem identificação pessoal, etc.

É oportuno lembrar que se discute o excesso de anúncios comerciais que atingem crianças e jovens, promovendo uma cultura de consumismo. Essa é uma questão importante na formação de cidadãos da Era Digital, uma vez que com "um clique" pode-se realizar uma "compra por impulso". Por isso, antes de apresentarmos dados da pesquisa a esse respeito, abramos aqui um parêntese para advertir que o atual volume de anúncios comerciais nas páginas web ultrapassou o cenário de poluição visual que enfrentamos nas cidades. Não seria esse volume de propaganda um abuso dos departamentos de marketing das empresas que estão obrigando usuários a visualizarem suas marcas e produtos sem que eles manifestem objetivamente seu interesse? Do ponto de vista técnico não seria difícil reservar uma área dos navegadores para propaganda, deixando ao internauta o direito de ativar ou não sua exibição. E como evitar que crianças e jovens sofram esse tipo de assédio quando acessam a internet?

Uma parcela significativa dos respondentes (81%) afirmou fazer compras online e quase a metade (43%) faz compras frequentemente. É oportuno acrescentar que aproximadamente um em cada cinco alunos alegou não fazer compras online (18%) e há também aqueles que alegaram nunca terem feito esse tipo de transação (1%).

Uma transação comercial online quando realizada em condições seguras impõe autenticação do usuário e do estabelecimento comercial e emprega criptografia dos dados trocados durante a transação. Para auxiliar os internautas, os navegadores apresentam um ícone que identifica se foi estabelecida uma conexão segura com o site em que se realizará a transação. Mostraram-se vulneráveis a algum tipo de ataque em transações comerciais aproximadamente um terço dos respondentes (32%) uma vez que 14% dos sujeitos responderam nunca verificar esse ícone e outros 18% alegaram raramente fazê-lo.

Felizmente mais da metade dos alunos participantes da pesquisa (52%) responderam que já verificam com frequência se o site é seguro quando fazem compras online.

Assim como nas compras online, é significativo o contingente de usuários que não dão a devida importância ao quesito segurança. O acesso ao serviço internet banking também requer conexão em ambiente seguro. Impressiona que apenas 44% dos professores frequentemente verifiquem se sua conexão ao serviço é segura antes de enviar dados e que, quase um terço dos participantes da pesquisa (29%) estão vulneráveis, uma vez que raramente (14%) ou nunca (15%) verificam se sua conexão ao serviço é segura.

Os dados mostram que uma parcela significativa dos sujeitos não se comporta de modo adequado quando se considera atitudes preventivas de proteção à ataques maliciosos na rede. Porém, há ainda outro tipo de problema que os professores devem ser capazes de orientar seus alunos: além dos problemas causados pelo "furto" de dados importantes não se pode negligenciar a importância de se protegerem dados importantes. A cada dia surgem novas formas de se armazenar dados na rede. Assim, o que antes ficava num cofre, ou bem guardado em um armário trancado, agora, digitalizado, fica nos discos (rígidos, externos, ou portáteis), ou na rede (nos sites ou na nuvem). Perder informações de avaliações, notas e frequência de alunos, registros de controle financeiro e dos colaboradores da escola pode comprometer seriamente o funcionamento de uma escola. A perda de informações pode acontecer em função de ataques maliciosos, geralmente realizados por (ex)alunos, (ex)funcionários ou terceiros ou por furto de dispositivos, mas também por acidentes (imperícia no uso de aplicativos, formatação acidental de disco rígido) ou falhas de equipamentos, como por exemplo, a queima de discos rígidos, ou a corrupção de bases de dados.

Esse tipo de problema pode ser evitado com o emprego de procedimentos ou políticas de proteção de dados: realizar cópias dos dados importantes em mídias (como CD, DVD, pen-drive, disco de Blu-ray e disco rígido externo), ou armazená-los remotamente (online ou off-site). Isso pode ser feito com o emprego de ferramentas de backup. Antes de mais nada o usuário precisa ter consciência dos riscos que corre.

Quando o assunto é preservação de dados a prática dos sujeitos é preocupante (Grafico 1). Entre os respondentes menos da metade (47%) alegou fazer backup frequente de seus dados importantes. Aproximadamente um em cada quatro (23%) estão completamente vulneráveis, pois nunca fizeram backup (15%) ou simplesmente não sabem como fazê-lo (8%).

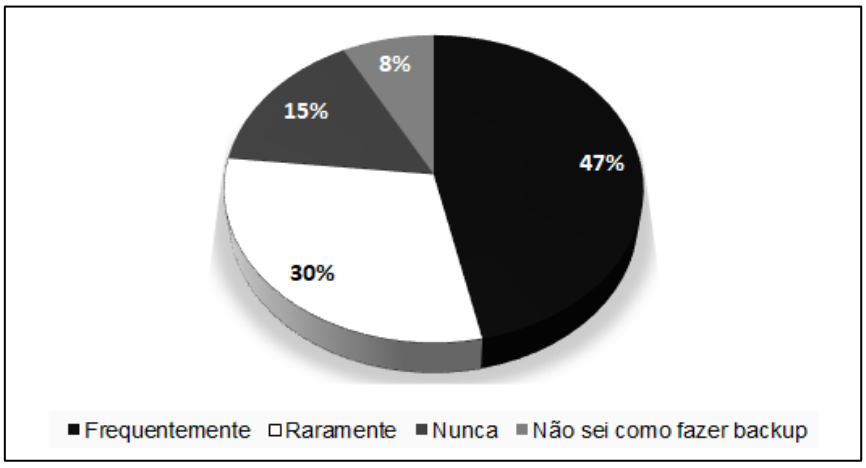

Gráfico 1. Proporção de sujeitos que fazem backup por frequência

Quando se cria um conteúdo digital ― que podem ser textos, fotos, áudios ou vídeos ―, a Lei de direitos autorais (Lei nº 9.610/98) estabelece que o autor tem direitos de natureza moral e patrimonial sobre o conteúdo que criou. Entre os direitos de natureza moral, destaca-se a própria autoria da obra que jamais poderá ser atribuída a outra pessoa que não seja o seu autor. No campo dos direitos patrimoniais, a Lei estabelece circunstâncias de (re)uso, cópia, e/ou divulgação por terceiros. Estabelece, portanto, em que condições esse conteúdo, ou parte dele, pode ser (re)utilizado por terceiros, seja com, ou sem autorização do autor para fins lucrativos ou não.

Para se ter uma noção das ramificações desses problemas, no campo da educação, a infinidade de recursos disponíveis na rede capazes de realizar buscas e indiscriminadamente fazer cópias de conteúdos educacionais, sejam aqueles produzidos por professores ou alunos, muitas vezes caracterizando verdadeiras fraudes, estabeleceu uma verdadeira "indústria do plágio". O plágio tornou-se uma epidemia em todos os níveis escolares. Há um sem número de denúncias de "empresas" que vendem trabalhos escolares, trabalhos de conclusão de curso, dissertações e teses. Estabelece-se um cenário, em que a escola, por seu papel de formação do cidadão, tem responsabilidades cada vez mais urgentes e importantes. A escola e os educadores que nela trabalham poderiam se valer da possibilidade praticamente infinita não somente da disseminação do conhecimento, mas também da construção colaborativa desse conhecimento, porém, quando não estão devidamente informados, correm o risco de verem envolvidos em práticas de fraude e corrupção. O Art. 104 da Lei nº 9.610/1998, entre as sanções civis impostas ao contrafator, define que "Quem vender, expuser a venda, ocultar, adquirir, distribuir, tiver em depósito ou utilizar obra ou fonograma reproduzidos com fraude, com a finalidade de vender, obter ganho, vantagem, proveito, lucro direto ou indireto, para si ou para outrem, será solidariamente responsável com o contrafator, nos termos dos artigos precedentes, respondendo como contrafatores o importador e o distribuidor em caso de reprodução no exterior.

Não é incomum que materiais produzidos por professores sejam publicados em sites da escola, alguns deles com acesso público. Qual seria então o nível de responsabilidade imputável à escola, aos gestores e educadores se determinado material didático fosse considerado ilícito em relação a direitos autorais? Quem deveria responder pelo crime e ressarcir eventuais danos a terceiros? Nossos professores estão preparados para fazer jus do próprio uso de materiais disponíveis na rede, e mais, para ensinar a maneira adequada de utilizá-los?

4. Considerações finais

A necessidade de uma formação para a cidadania na Era Digital exige, das instituições da sociedade, uma postura mais célere e organizada, de modo a coordenar esforços e alcançar os objetivos desejados. A velocidade com a qual a internet se renova, em seu lado positivo e naquele ruim, é vertiginosa. A cada dia, novas oportunidades e ameaças se apresentam a um número crescente de usuários, criando uma sempre crescente comunidade virtual, que entrelaça sua existência com aquela física, coexistindo e co-influenciando a vida humana. Com o crescimento das interações humanas e institucionais dentro do ambiente virtual, aumenta também a necessidade de esclarecimento e capacitação dos usuários para que usufruam do imenso potencial da internet, ao mesmo tempo que possam se proteger dos igualmente imensos perigos.

O desenvolvimento de procedimentos de acesso seguros, integrados em um currículo digital, como o uso de senhas, filtros, a criação de *back-up* de dados, uso de programas *antivirus, firewall*, a atenção no acesso a arquivos com terminações suspeitas como ".exe" ou ".scr", o cuidado quanto à exposição dos próprios dados, por exemplo, garante a navegação criteriosa e profícua do ambiente virtual. A formação para a segurança digital nas escolas torna-se, então, um fator determinante na busca desse objetivo onde todos os usuários, professores e alunos, aprendam sobre o uso adequado e seguro da ferramenta mais potente já criada pela humanidade.

Referências Bibliográficas

Brasil (2017). *Base Nacional Comum Curricular: Educação Infantil e Ensino Fundamental*. Brasília:MEC/Secretaria de Educação Básica.

Brasil (2018). *Base Nacional Comum Curricular: Ensino Médio*. Brasília: MEC/Secretaria de Educação Básica.

Castells, M (1999). *A sociedade em rede*. São Paulo: Paz e Terra.

CERT.br. (2012). *Cartilha de Segurança para Internet*, versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado de: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>.

CETIC.br (2018). *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil*. São Paulo: Comitê Gestor da Internet no Brasil.

Marcacini, A. (2016) *Aspectos fundamentais do Marco Civil da Internet: Lei nº 12.965/2014.* São Paulo. ISBN-13: 978-1541333031

Moraes, A. F. (2015) *Firewalls: segurança no controle de acesso*. São Paulo: Érica.

Nicolau R. M. (2017). *Usos particular e educativo das tecnologias digitais de informação e comunicação pelo professor da educação básica na era digital: um estudo com base no modelo SAMR*. (Dissertação de Mestrado). Belo Horizonte: Pontifícia Universidade Católica de MG, Programa de Pós-Graduação em Educação.

Rossini, A. E. S. (2004). *Informática, telemática e direito penal*. São Paulo: Memória Jurídica.

UNESCO (2012). *Declaração Rea De Paris*. PARIS. Recuperado de: <http://www.unesco.org/new/fileadmin/multimedia/hq/ci/wpfd2009/Portuguese_Declaration.html>.

UNESCO/COL (2011). *Guidelines for Open Educational Resources (OER) in Higher Education*. Vancouver: COL. Disponível em: <http://unesdoc.unesco.org/images/0021/002136/213605E.pdf>.

Veen, W.; Vrakking, B. (2009) *Homozapiens: educando na era digital*. Porto Alegre: Artmed.