Nextlevel
Westcon-Comstor Americas

# EDUCAÇÃO DIGITAL: RISCOS LEGAIS E RESPONSABILIDADES.

Houve um tempo em que os **principais desafios da sala de aula** eram notas baixas e conversas paralelas. Hoje, com o advento e a presença cada vez mais constante das novas tecnologias da informação e comunicação, os desafios são aqueles e outros tantos mais. Sabemos, pais e educadores, que somos **responsáveis pela moral e cívica** de nossos filhos e educandos, mas que em tempos de internet falhar neste papel pode gerar sérios e, por vezes, irreversíveis desdobramentos, aos quais poucos se dão conta.

Dotamos de liberdade para ir e vir, bem como para praticar quaisquer atos da vida civil, salvo se uma lei expressamente proibir. É o que dispõe o art. 5º, inciso II, da Constituição Federal: "ninguém será obrigado a fazer ou deixar de fazer alguma coisa, senão **em virtude de lei**".

Logo, se agirmos contrariando uma lei, seja na **ação ou na omissão**, mas causando prejuízo a outrem, podemos ser responsabilizados, já que o Código Civil garante a quem sofreu um dano o direito de pleitear uma compensação com o fim de reparar eventual prejuízo. É o que chamamos de **responsabilidade civil** e encontra-se prevista nos artigos 186, 187 e 927 do Código Civil Brasileiro.

No entanto, se e quando este ato é **praticado por um menor**, a responsabilidade recai sobre os pais, responsável legal e, a depender da situação, sobre **estabelecimentos de ensino**, nos termos do que dispõe os incisos I e IV do artigo 932 da legislação civil. E ainda, sendo a conduta praticada pelo menor considerada como crime tipificado no Código Penal, no caso, denominado como ato infracional pelo Estatuto da Criança e do Adolescente, poderá o autor da conduta ser submetido às medidas de proteção ou socioeducativas, que podem ser, desde uma advertência, uma pena restritiva de direitos e até mesmo de liberdade, a depender da situação.

O fato é que hoje é possível o contato dos alunos com o mundo externo mesmo quando sob os **domínios físicos da escola**, o que potencializa a responsabilidade e o compromisso desta em garantir sua segurança e envidar esforços a impedir que se tornem vitimas ou infratores de **crimes digitais**. Aliás, cumpre ressaltar que, em tempos de internet, a responsabilidade da escola extrapola

seus domínios físicos, na medida em que, conflitos digitais envolvendo seus alunos sempre reverberam no âmbito escolar.

A rigor e se bem refletirmos, implementar iniciativas para a educação e **cidadania digital** está longe de constituir prerrogativa das instituições de ensino, posto que além de representar o caminho para o exercício da cidadania e preparo para mercado de trabalho, expectativas para a educação bem estabelecidas na Constituição Federal, Estatuto da Criança e do Adolescente, Lei de Diretrizes e Bases da Educação e no próprio **Marco Civil da Internet**, instigar a reflexão dos alunos acerca dos riscos e oportunidades que oferecem as novas tecnologias, mitigará, substancialmente, os riscos de vê-los envolvidos em **crimes ou ilícitos cibernéticos**.

Neste sentido, observa-se uma tendência dos próprios docentes se valerem das **ferramentas tecnológicas** para sua rotina, o que, sem dúvida, é muito bom, já que as novas gerações demandam aulas mais interativas, **professores mais criativos e conectados**, é claro.

E eis aí mais um ponto de atenção. Tudo que se faz na e por meio da internet fica documentado e constitui, inclusive, meio de prova perante o Poder Judiciário. Daí a importância de se estabelecer regras claras sobre a utilização dos **recursos tecnológicos**, bem como, **infraestrutura adequada** e segura, capazes de institucionalizar da melhor forma possível, por exemplo, as interações realizadas entre aluno e professor neste ambiente digital.

Afinal, muito embora as novas tecnologias representem tão importante marco no processo ensino-aprendizagem, estas só podem ser consideradas ferramentas para **exercício da cidadania** se e quando utilizadas de forma segura, consciente e responsável, conforme estabelece o próprio artigo 26 do Marco Civil da Internet.

Sim, o mau uso das novas tecnologias pode gerar muitos desdobramentos, que podem, inclusive, **demandar ações do judiciário**. Além do furto e desvio de informações, estelionato, violação de direitos autorais, os crimes contra a honra (calúnia, injúria e difamação), o preconceito e discriminação (Lei 7716/89) são alguns dos ilícitos mais recorrentes do **universo digital**. Existe uma linha muito tênue entre a liberdade de expressão e a violação do direito alheio, e a impulsividade inerente ao ser humano e potencializada por esta nova Era (tecnológica). São gerados muitos prejuízos de todas as ordens, uma vez que determinados comentários podem ofender a **honra do indivíduo** e quando realizados na e por meio das redes sociais, os desdobramentos tendem a ser muito piores, tanto que, a pena cominada aumenta de um terço, quando referidos crimes são cometidos na presença de várias

pessoas, ou por meio que facilite a divulgação da difamação ou da injúria, como é o caso da internet (art. 141 CP III).

Sem dúvida alguma, na escola se inicia o mais intenso **processo de socialização** do indivíduo e se muitos adultos lamentam ter aprendido a usar adequadamente as novas tecnologias "na dor", é possível (e é nossa obrigação) fazer diferente para com crianças e adolescentes. A habilidade que possuem com a tecnologia é inversamente proporcional a maturidade e capacidade de compreensão que possuem acerca dos riscos e responsabilidades a que estão sujeitos no vasto universo digital.

Não se pode negar que crianças e adolescentes se tornaram ainda mais vulneráveis com o uso das novas tecnologias, sobretudo a crimes como: sequestros, pornografia infantil, **cyberbullying** (sim, muitas das condutas relacionadas à prática, constituem crimes, tais como: calúnia, injúria, difamação, ameaças, entre outros). Mas, e quando essas crianças e adolescentes deixam de ser vítimas e passam a ser verdadeiros **infratores da honra** e imagem de terceiros, por terem a falsa ilusão de que não serão descobertos, por estarem se valendo de perfis falsos ou aplicativos que prometem o anonimato? A omissão e a negligência dos pais e educadores sob a alegação do desconhecimento da lei pode livrá-los da responsabilização? A resposta é: não.

Logo, considerando as possíveis **implicações jurídicas** dos atos praticados na e por meio da internet, a recomendação, pensando não somente na segurança da criança e do adolescente, mas também na do próprio professor e da escola, é de que interações digitais entre docentes e discentes se deem por meio de **mídias sociais educacionais**, assim como quaisquer meios de acesso às novas tecnologias, sejam sempre e somente disponibilizados utilizando os melhores padrões de qualidade e segurança.

Nesse sentido e em conformidade com o previsto no Marco Civil da Internet, sugere-se que a **inclusão digital** se dê acompanhada de lições de boas práticas, assim como de providencias técnicas, como filtros e monitoramento, que assegurem a impossibilidade de acesso a conteúdo impróprio e alertas quanto a necessidade de tempestivas providências, por exemplo, quando algum usuário fizer mau uso do acesso provido pela escola.

Mas, se de um lado, alunos precisam aprender a tirar o melhor e mais seguro proveito das **novas tecnologias**, instituições de ensino, também precisam estar atentas à maneira como também usufruem dos recursos tecnológicos, não somente alertando seu corpo docente quanto ao papel e referência que representam na vida dos alunos, mas, sobretudo, na escolha das ferramentas e meios que utilizam para **armazenar todos os dados coletados** no exercício de sua atividade.

Isto porque, toda e qualquer informação ou dados relativos a seus alunos, devem ser tratados como confidencial, principal e não exclusivamente, quando referirem-se a menores de idade, nos termos do que dispõem os artigos 17 e 18 do Estatuto da Criança e do Adolescente. Isso significa que, "todo cuidado é pouco" quando o assunto é: **"cloud computing"**, por exemplo.

Por certo, a possibilidade de **armazenamento de dados em Nuvem** representa mais uma, dentre tantas facilidades, propiciadas pela internet. No entanto, considerar o fator "segurança" como premissa preponderante quando da escolha da melhor solução faz toda diferença.

Assim como pen drives podem ser perdidos ou furtados, serviços de Nuvem também podem sofrer ataques ou serem contaminados por vírus. Daí a importância de se verificar junto ao fornecedor do serviço, por exemplo: qual a segurança da informação aplicada, considerando inclusive, que o acesso pode se dar de inúmeros dispositivos; como ocorre a **autenticação dos acessos**; qual o serviço de contingência oferecido na hipótese de um "bug"; quais os cuidados para com as informações armazenadas; o prazo para **recuperação de dados** em casos fortuitos; entre outros.

Além disso, é recomendável que **outras cautelas** também sejam colocadas em prática, tais como: criação de senhas fortes, logout e não salvamento automático de senhas, **backup** contínuo e adoção de outras práticas de segurança, quando tratar-se de um dado ultrassensível.

Enfim, manter-se continuamente informado acerca de todos os **riscos e oportunidades** que as novas tecnologias oferecem é fundamental para que se extraia benefícios e se estabeleçam sólidas e **eficazes estratégias** para a mitigação de prejuízos atrelados aos riscos, não somente com relação às crianças e adolescentes, mas à sociedade de uma forma geral.

*Borelli, Alessandra – OAB/SP 201535 – Diretora Executiva Nethics Educação Digital – Westcon Americas | Abril/2018*