



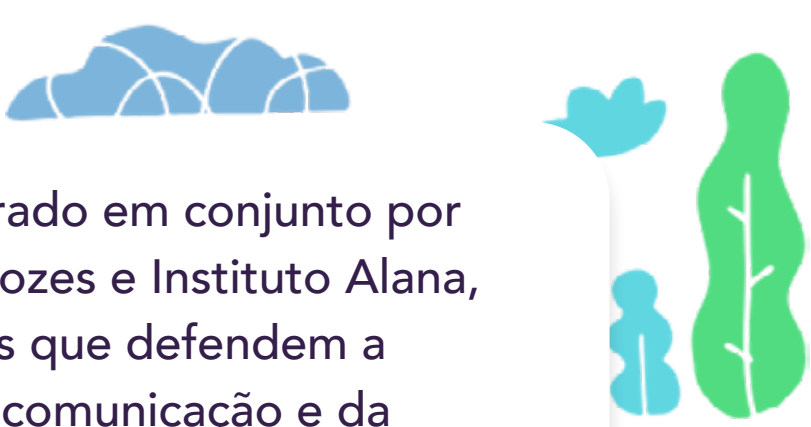
A ESCOLA NO MUNDO DIGITAL

Dados e Direitos de estudantes





Um guia sobre proteção de crianças e adolescentes no uso de tecnologias nas escolas

A blue cloud is positioned above the text. To the right, there are stylized figures: a small blue figure and a taller green figure, both with simple line details.

Este Guia foi elaborado em conjunto por Educadigital, Intervozes e Instituto Alana, organizações sociais que defendem a democratização da comunicação e da educação, bem como a garantia do acesso universal à internet, da liberdade de expressão e da infância.

A series of colorful geometric shapes are located at the bottom left: a blue and white striped triangle, a green shape with white dots, an orange shape, and a green shape with white dots, along with a small blue circle.

O objetivo deste material é auxiliar mães, pais, educadores e gestores escolares a entender melhor o contexto atual de uso da internet. Além disso, trataremos da importância da proteção de dados pessoais estudantis, que vai além das tendências tecnológicas e do mundo online, explicando como eles já são e podem ser protegidos. Por fim, apresentaremos alguns modelos alternativos para uma educação livre de exploração comercial e respeitosa à privacidade e segurança de crianças e adolescentes, enquanto estudantes e pessoas em formação, participantes ativos do ambiente digital. Boa leitura!

Índice

Introdução	Pág. 05
Antes de começarmos: o que é, afinal, a internet?	Pág. 08
Quem acessa a internet? E quem acessa a educação mediada pela internet?	Pág. 13
Os dados pessoais estudantis	Pág. 19
Por que devemos nos preocupar com o uso correto de dados pessoais estudantis?	Pág. 24
Quais leis já existem para proteger os dados pessoais estudantis?	Pág. 33
Na prática, como podemos saber se os dados pessoais estudantis estão sendo protegidos?	Pág. 39
Alternativas para uma educação livre de exploração comercial e respeitosa às crianças e adolescentes	Pág. 47
Educação para a Mídia e Empoderamento Digital	Pág. 50
Diante de tantos desafios, como cada um de nós pode agir?	Pág. 54
Para se aprofundar mais	Pág. 58
Glossário	Pág. 62

Introdução

A pandemia de covid-19 impôs a necessidade, inédita em muitos locais, de medidas de isolamento social, obrigando estados e municípios brasileiros e de todo o mundo a correrem na busca por alternativas e estratégias de [Ensino Remoto](#).



Esse movimento abrupto, em um contexto como o nosso, marcado por extremas desigualdades estruturais, expôs ainda mais a fragilidade do direito à educação, especialmente de crianças e adolescentes, **e acentuou a vulnerabilidade de grupos que já tinham o acesso a esse direito negado ou dificultado.** ↘



É o caso das [crianças e adolescentes](#) com deficiência. Levantamento anterior à pandemia indica que apenas 3,88% dos sites educacionais não apresentam barreiras de acesso. Além disso, o Brasil, assim como a maior parte do mundo, não criou nenhum tipo de protocolo oficial para a educação inclusiva no período de pandemia. [Saiba mais](#)

A educação a distância (EaD), enquanto modalidade de ensino mediada pela internet, vem se **intensificando e sendo ampliada em possibilidades** ↘ num contexto de cibercultura, sendo adotada pelas redes pública e privada. Algumas escolas e secretarias de Educação, inclusive, já tinham plataformas próprias e as utilizavam de maneira complementar às atividades presenciais.



Pesquisa realizada por Instituto Alana, Educadigital e Intervenções sobre o ensino remoto na rede pública de educação básica dos estados e capitais mostra que todas as secretarias estaduais adotaram plataformas de EaD, sendo que 85% utilizam plataformas privadas. Somente o Google está presente em mais de 60% dos serviços de tecnologia adotados. A maioria - quase 90% da rede - complementa as atividades por TV, rádio ou material impresso. Veja os dados levantados [aqui](#).

É importante dizer que a pandemia acelerou um processo que já era crescente: a introdução de tecnologias digitais da informação e comunicação (TDICs) no dia a dia da sociedade e nas escolas. Trata-se de um movimento importante, considerando que a internet e as TDICs, grandes marcos do avanço científico das últimas décadas, podem proporcionar novas oportunidades de ensino e de aprendizagem. Podemos destacar o potencial de ampliação, rapidez e mobilidade da produção de informações e do acesso a uma diversidade de conteúdos, nunca visto antes. Por isso, o acesso à internet é considerado um direito fundamental de todas as pessoas, inclusive de crianças e adolescentes.



Por outro lado, para que esse direito seja garantido de verdade e que a experiência de cada um no ambiente digital - educacional ou não - seja positiva, é importante que todos estejam cientes também dos problemas que

existem na internet. Há várias cartilhas de segurança digital para crianças e adolescentes que trazem alertas para riscos da navegação na internet, como: exposição a conteúdos inadequados, publicidade infantil, desinformação (fake news), uso excessivo, problemas de saúde associados (tais como sedentarismo, obesidade infantil, miopia, distúrbio do sono, depressão, ansiedade, estresse e vício em jogos), cyberbullying, racismo, machismo, discurso de ódio, sextorsão e outros.

No entanto, pouco ainda se fala - e, pior, pouco ainda se sabe - sobre uma das principais e mais silenciosas atividades, que acontece a partir das plataformas digitais, que pode ser uma ameaça à sociedade, especialmente às crianças e adolescentes: a vigilância massiva da população e a **exploração de dados pessoais para finalidades comerciais e de previsão de tendências de consumo e/ou comportamento.** ↘



Recentemente, a Netflix lançou o filme Dilema das Redes, que reúne informações e conta um pouco mais sobre esse tema. Para entender mais, recomendamos também o documentário Privacidade Hackeada.

Este guia foi elaborado em conjunto por Instituto Alana, Educadigital e Intervezes, organizações sociais que defendem a democratização da comunicação e da educação, bem como a garantia do acesso universal à internet, da liberdade de expressão e da infância.

O objetivo deste material é auxiliar mães, pais, famílias, educadores e gestores escolares a entender melhor o contexto atual de uso da internet por crianças. Além disso, trataremos da importância da proteção de dados pessoais estudantis, explicando como estes são protegidos por nossas leis e como podem, na prática, ser ainda mais resguardados. Por fim, apresentaremos alguns modelos alternativos para uma educação livre de exploração comercial e que respeite a privacidade e segurança de crianças e adolescentes, enquanto estudantes e pessoas em formação, participantes ativos do ambiente digital.



1º Módulo

Antes de começarmos, o que, afinal, é internet?

O que chamamos de internet é um sistema de comunicação entre dispositivos eletrônicos (celular, computador, tablet etc.) em torno de uma rede global de infraestrutura. Sites e

aplicativos compõem a camada de conteúdos disponibilizados via web. Servidores armazenam os dados e provedores são responsáveis pela conexão dos dispositivos à rede, por meio de mecanismos de transmissão, como cabos, satélites ou via rádio (este vídeo [aqui](#) conta um pouco mais sobre como funciona a internet).

De acordo com a revista “Submarine Telecoms Forum”, quase 99% do tráfego intercontinental de dados na internet passam por **cabos submarinos de fibra óptica**. Empresas de telecomunicação, como a americana AT&T, e plataformas digitais têm realizado grandes investimentos nessas redes de transmissão. Segundo o site “BroadBandNow”, em 2019, o Google se tornou acionista majoritário de 100 mil quilômetros de cabos submarinos, tendo alguma participação em 8,5% do total existente. Já o Facebook possui uma rede de 90 mil quilômetros, além de 30 mil da Amazon e 6,6 mil da Microsoft.

O que antes demandava uma enorme biblioteca ou grandes compartimentos para armazenar, hoje cabe em um chip. Uma carta que ontem levaria dias para chegar a uma pessoa do outro lado do mundo, hoje leva poucos segundos, por meio de aplicativos de mensagem. A internet permitiu, de certa forma, reduzir a distância entre pessoas e conteúdos e o próprio acesso à informação.

Essas vantagens se tornaram importantes **inclusive no momento de isolamento físico** imposto pela pandemia da covid-19.

Além de ser um dos principais meios para comunicação entre familiares e amigos, a internet tornou-se um grande canal para o ensino, reunindo estudantes e professores em um contexto de incertezas e distanciamento. Inspirado pelos acontecimentos deste período complexo e sem precedentes na educação, o conteúdo deste guia visa a fomentar uma internet livre e segura.

Quanto se paga para usar a internet?



A partir do momento em que se tem acesso à internet - com a senha de um ponto de wi-fi, por exemplo - muitas vezes podemos ter a ilusão de que a navegação em sites e aplicativos é pública e gratuita. Mas a verdade é que, para acessar a rede, mesmo em páginas e plataformas abertas, utilizamos camadas de infraestrutura e conteúdo privadas e isso é pago com uma moeda de troca muito valiosa: nossos [dados pessoais](#).

São informações sobre a nossa rotina e personalidade, na rede e também fora dela, que incluem cadastros, contatos, endereço, mensagens privadas, públicas, registros de acesso, voz, identificação de nossos celulares ou computadores, sistema de posicionamento global - o GPS -, compras etc.

Via de regra, tudo o que fazemos na internet fica registrado, ainda que não tenhamos dado permissão específica para esse registro ou feito um login em determinado site. Todos nós, portanto, temos um “rastro digital”, que inclui informações que nós mesmos colocamos ou escrevemos na internet, como posts, curtidas ou comentários em plataformas e redes sociais, e informações que ficam registradas sem sequer sabermos, como o tempo que gastamos em cada página da internet, o caminho que fazemos com o cursor do nosso mouse ou o dispositivo pelo qual acessamos a rede on-line.

E qual é o grande problema disso? Todas essas informações são interpretadas por algoritmos, operados por técnicas de inteligência artificial (IA), em um processo que chamamos de tratamento ou processamento de dados. Basicamente, a partir do rastro digital de cada pessoa, esses robôs conseguem traçar perfis individuais, mapeando suas relações interpessoais, preferências e gostos em determinados temas, principalmente em relação ao consumo.

A moeda de troca aqui são os dados e preferências de cada pessoa que usa a internet e as TDICs, que alimentam práticas comerciais e geram lucro para as empresas de tecnologia, que oferecem essas informações a outras empresas anunciantes.



Então, grandes corporações de tecnologia, que possuem enorme capacidade de coleta e do processamento de dados, registram lucros gigantes, direcionando por meio de algoritmos de IA, conteúdos específicos, sob medida, a cada usuário. São diversas as contradições relacionadas ao abuso de **anúncios**



sob demanda ↘ e,

inclusive, hoje se discute a real liberdade que temos de escolha de conteúdos que aparecem em nosso uso da internet e de tecnologias digitais de informação e comunicação, que são o tempo todo direcionados a partir de IA.



Talvez você já tenha ouvido sobre o caso em que algoritmos descobriram a gravidez de uma adolescente **antes mesmo de seu pai.**

E todas essas questões se aplicam também quando tratamos da educação mediada por tecnologias e pela internet.

Um estudo de acadêmicos e organizações sociais, sob o título “Educação Vigiada”, mostra que 65% das universidades públicas e secretarias estaduais de educação no Brasil estão expostas ao chamado **“capitalismo de vigilância”**. Isto porque estas instituições têm seus servidores ancorados em grandes empresas de tecnologia, como Google e Microsoft. Um relatório, na mesma linha, da organização Freedom House, intitulado Freedom on the Net – 2019, apontou, a partir de 65 análises, 40 países não livres em termos de monitoramento e vigilância na internet.



2º Módulo

Quem acessa a internet? E quem acessa a educação mediada pela internet?

Há no Brasil e no mundo uma enorme desigualdade de acesso à internet, que privilegia grandes centros urbanos, famílias com maior poder aquisitivo, homens e pessoas brancas. Outra característica marcante é a **concentração do acesso à internet** ↘

em poucas plataformas digitais, que se tornaram as principais intermediadoras da comunicação entre pessoas, empresas e Estados.



Segundo a pesquisa [monopólios digitais](#), elaborada pelo Interozes em 2017, os sites de produção e distribuição de conteúdo mais acessados no Brasil são do Google e Facebook. Em relação aos aplicativos, as plataformas digitais representam 63% dos downloads da loja do Google e 75% da loja da Apple.

A pesquisa [TIC Domicílios 2019](#), realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), mostra que 58% das pessoas que usam a internet no Brasil se conectam somente pelo celular, sendo que na área rural esse número é de 79%, e nas classes DE, de 85%. Além disso, segundo estudos da Agência Nacional de Telecomunicações (Anatel), 55% dos acessos móveis no país se dão a partir de planos pré-pagos, muitos com pacotes de dados bem limitados.

Mas, se para o acesso à educação, que é um **direito básico**,  seja no contexto da pandemia ou nas projeções para o futuro, a internet vem sendo usada como um importante ou principal recurso, como ficam os quadros de desigualdade no Brasil, pensando principalmente na qualidade do acesso e na inclusão? Diante de uma situação de pandemia, como mães,

pais, gestores e educadores podem participar da educação escolar de crianças e adolescentes em casa, em meio a tantos desafios e acúmulos de trabalho?



Segundo o artigo 6º da Constituição Federal, “são direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados...”.

E o que fazer ainda em muitos lugares nos quais as barreiras sociais, econômicas e ambientais, como o acesso à renda e à internet e a própria segurança e sobrevivência das famílias, antecedem o ensino? ➤ Essas são reflexões de difícil resposta, mas muito importantes para pensar o uso da internet e das tecnologias digitais da informação e comunicação na educação.



Pesquisa realizada no Colégio Técnico da Unicamp (Cotuca) e divulgada pelo Intervozes mostra que muitos estudantes possuem conexão através de aparelhos com pouca memória e compartilhados entre membros da família. O levantamento identifica, ainda, que 27,9% dos alunos têm alguma responsabilidade sobre cuidado de crianças e 19,7% de idosos. Nesse contexto, assistir vídeoaulas ou baixar materiais de estudo torna-se uma atividade desafiadora e excludente.

Segundo dados da pesquisa TIC Educação 2019 (Cetic.br), apenas 14% das escolas públicas brasileiras tinham um “ambiente ou plataforma virtual de aprendizagem” antes da pandemia, sendo 64% na rede particular. A desigualdade de acesso também se dá em nível regional: enquanto no Sudeste 88% dos estudantes estão conectados à internet, no Nordeste são 73%. Na área rural, apenas 40% das escolas possuem um computador com acesso à rede.

Esse debate se estende ainda para a formação de professores e estudantes, para o tema da privacidade e da proteção dos dados estudantis, liberdade de expressão e cuidados com segurança digital, entre outras questões que abordaremos neste guia.

Algumas soluções para democratizar o acesso digital e de qualidade, apontadas historicamente por organizações da



sociedade civil, passam pela ampliação da rede e diminuição do custo da banda larga, assim como a garantia da neutralidade da rede, privacidade dos dados pessoais e transparência das corporações, pilares da liberdade de expressão e do direito à comunicação. É dever do Estado estabelecer mecanismos de participação social e educação para promover a diversidade e a pluralidade de pessoas, lugares e contextos também na internet, para além de ofertas comerciais.

Se antes o acesso à internet já era um direito básico de todos os brasileiros e brasileiras, a partir do momento em que a educação é mediada por tecnologias digitais, sua importância redobra. É essencial que seja garantido a todos, desde a infância, acesso à internet com qualidade.

Rastro digital, algoritmos, desigualdades de acesso... E agora?

Se você começou a se dar conta de que tudo o que faz na internet está registrado em grandes bancos de informações, que são manipuladas automaticamente por algoritmos de controle das plataformas digitais, a partir dos seus dados pessoais, está entendendo bem até aqui. Neste caso, é provável que você esteja se sentindo em constante vigilância e monitoramento. Mas, calma! Vamos ajudar a entender e minimizar os impactos negativos de toda essa estrutura tecnológica, política e comercial que está presente em nossa sociedade e, também, na educação.



Diante do cenário recente de centralização das plataformas digitais no cotidiano das pessoas, alguns países, organismos internacionais e movimentos sociais passaram a debater a **regulação da internet**. ➤ Assim, foram estabelecidos princípios éticos e algumas diretrizes para promover o livre acesso e a garantia dos direitos humanos.



No Brasil, desde 2014, existe o Marco Civil da Internet, que estabelece diretrizes básicas de governança multissetorial da internet, ou seja, uma composição coletiva dos setores: governo, empresas, universidades e sociedade civil. Além disso, pontua os princípios de uma internet livre, que garanta liberdade de expressão, privacidade e neutralidade da rede.

A partir de agora, passaremos a falar mais sobre a proteção de dados pessoais e propor caminhos práticos para ampliar a segurança e o potencial do uso da internet, especialmente por crianças e adolescentes no contexto escolar.



3º Módulo

Os dados pessoais estudantis

Até pouco tempo atrás - e em alguns lugares até hoje -, todas as informações e registros pessoais de alunos, professores e das próprias escolas ficavam armazenados em pastas, armários e gavetas. Atualmente, boa parte desses dados foram parar no que se convencionou chamar de “nuvens”, tecnologias que permitem guardar dados através de servidores (máquinas de armazenamento) capazes de suportar **grande quantidade de informações, para que as trocas na internet funcionem.** ↘



Pouca gente fala disso, mas o mundo digital também utiliza recursos naturais. Se você tiver interesse em saber mais sobre isso, [recomendamos esta entrevista.](#)

Parece apenas uma forma mais eficiente de organizar as informações nesta “era digital”, mas você já parou para pensar o que isso impacta na vida de estudantes, mães, pais e famílias, professores, gestores e toda a comunidade escolar? Se a sua resposta for “não”, não se preocupe. Continue aqui que vamos explicar tudo.

O que são dados pessoais estudantis?

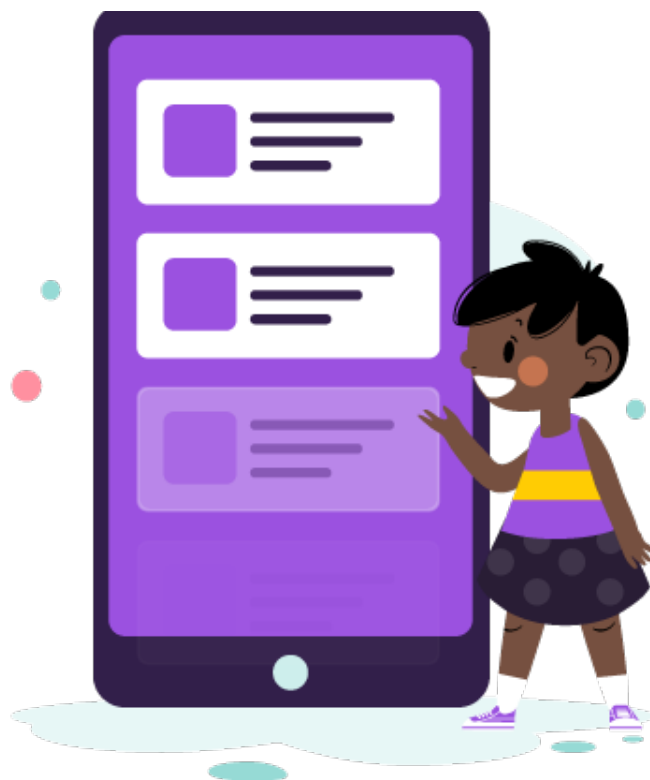
Chamamos de dados pessoais estudantis todas as informações que identificam cada estudante e cuja coleta e uso estejam relacionados à sua vida escolar.

Mesmo antes de iniciar os primeiros anos escolares, dados pessoais da criança são

compartilhados com instituições de ensino para fins de registro e reserva de vagas. Nome, endereço, dados sobre sua saúde (como alergias, doenças crônicas e tipo sanguíneo), gênero, raça e etnia, fotografia e impressão digital são apenas alguns exemplos do que é fornecido aos colégios. Também serão compartilhadas com as escolas informações sobre as mães, os pais e os responsáveis pelas crianças e adolescentes, que vão desde o contato até características socioeconômicas.

Conforme os anos se passam, os dados vão se acumulando e o banco onde eles são armazenados passa a ser alimentado com novas informações sobre cada estudante - por exemplo, o seu desempenho escolar, inteligência emocional e mesmo eventuais advertências disciplinares.

A partir da inserção de tecnologias na rotina escolar e de ensino, novos dados estudantis entram em jogo. A instalação de câmeras e sensores em ambientes de aprendizagem, por



exemplo, permite a captação de imagens biométricas, ou seja, das faces de toda a comunidade escolar - que são consideradas **dados sensíveis**, e que também vão compor o complexo acervo de dados estudantis.

Quando tratamos do ensino remoto e do ensino a distância, tão presentes no contexto da pandemia, o acúmulo de informações pessoais de estudantes se torna ainda mais significativo. A conta do e-mail e da rede social, o login e a senha de acesso à plataforma de ensino são exemplos de dados pessoais



estudantis. Ainda, a depender do processo, os sites acessados por aquele aluno, arquivos e mensagens que ele envia a outras pessoas, o tempo de visualização que ele passa em cada página da internet, o trajeto da navegação, o clique do mouse e a curtida que deixa em determinados conteúdos, também podem ser instrumentalizados por essa lógica mercantil perversa.

Para que servem - ou deveriam servir - os dados pessoais estudantis?

É importante ter em mente que muitos dados pessoais estudantis devem ser compartilhados com as instituições de ensino. O fornecimento de algumas informações, inclusive, é uma forma de proteger crianças e adolescentes em eventuais

situações de risco (por exemplo: a escola deve saber se um estudante tem doença crônica ou alguma alergia para poder agir em uma eventual situação de risco à sua saúde).

Além disso, pensando no cenário do ensino público, o conjunto de dados estudantis pode ser muito importante para recenseamento e formulação de políticas públicas em educação, identificação de situações de vulnerabilidade e violência, além da elaboração de projetos político-pedagógicos, que devem ser desenhados a partir do perfil de cada comunidade escolar. Quando falamos em dados pessoais estudantis e na importância de protegê-los, não estamos falando que eles devem, em toda e qualquer situação, estar escondidos e trancados a sete chaves.

Mas você se lembra que, quando falamos sobre o rastro digital, o uso da internet e das tecnologias, explicamos que existem princípios éticos e diretrizes para garantir a preservação de direitos em relação a dados pessoais? Pois isso se aplica de forma especial aos dados pessoais estudantis e aos dados de crianças e adolescentes.

Um ponto essencial desses princípios é a **transparência**, ou seja, abertura e clareza sobre quais informações pessoais, que são íntimas e únicas de cada um, estão sendo fornecidas ou compartilhadas com plataformas digitais, aplicativos e provedores de internet, seja no uso de internet e de tecnologias, seja para o acesso à escola, de um modo geral.

Pelo princípio da transparência, sempre que os dados de uma pessoa estiverem sendo coletados, ela - ou sua mãe, pai, ou

responsável, se essa pessoa for uma criança ou adolescente - deve saber disso e, principalmente, o motivo pelo qual essa coleta está sendo feita, ou seja, a finalidade para a qual seus dados serão destinados.

Essa finalidade, por sua vez, deve obedecer a uma relação de necessidade entre o motivo pelo qual uma pessoa está fornecendo aquele dado e a contrapartida que ela terá, o que significa, na prática, que uma plataforma digital de ensino, salvo por necessidade específica, não deve solicitar ou coletar dados sobre a frequência de voz, o rosto, comportamentos em redes sociais ou hábitos de consumo de um estudante e de sua família, por exemplo, já que esses dados não têm nenhuma relação com o acesso de uma criança ou adolescente à educação escolar pela via remota.

Em uma linguagem mais técnica, falamos em minimização de dados: só devem ser solicitados ou coletados, em qualquer

contexto, os dados pessoais que sejam necessários para o acesso a direitos ou serviços, ou então para a proteção de crianças e adolescentes - como seriam, por exemplo, os dados sobre alergias ou doenças crônicas de estudantes, a serem armazenados pelas escolas.



Mas, não sendo esse o caso, por que coletar determinadas informações pessoais quando estas não são necessárias para o uso específico de um aplicativo ou plataforma digital? É mesmo fundamental que uma empresa que fornece tecnologias de ensino guarde qualquer tipo de dado dos estudantes que a utilizam, como suas preferências de consumo? Quem ganha com isso: são mesmo os estudantes ou são interesses comerciais privados? E será que as famílias têm como saber quais dados pessoais estudantis estão sendo coletados, especialmente no uso da internet e de tecnologias escolares? Qual a responsabilidade das redes públicas de ensino e instituições de ensino privadas na proteção dos dados pessoais estudantis? Continue conosco para pensarmos juntos nessas respostas!



4º Módulo

Por que devemos nos preocupar com o uso correto de dados pessoais estudantis?

- 1 Para garantir que eles não se tornem um instrumento de exploração comercial

Já imaginou se os dados pessoais coletados durante o período escolar forem usados por ou vendidos a empresas para o direcionamento de publicidade infantil, induzindo crianças e adolescentes ao consumo abusivo e desenfreado?

A desobediência a princípios éticos essenciais, como a minimização de dados, pode levar à coleta massiva de informações pessoais e, como explicamos como explicamos no 1º módulo, muitas vezes esses dados são utilizados por plataformas digitais para traçar os perfis de consumo de cada um. A partir desses perfis, as grandes plataformas vendem seu espaço para empresas anunciantes, que terão anúncios de seus produtos e serviços direcionados de forma personalizada para pessoas que usam a internet e as tecnologias digitais da informação e comunicação, reforçando hábitos e valores consumistas.

O ato das plataformas digitais de vender dados obtidos a partir de atividades educacionais é ilegal e desvirtua a finalidade social do ensino. Não é justo que, para acessar a educação, uma criança ou um adolescente esteja sendo monitorado constantemente por meio da coleta de tantas informações - privadas, íntimas e sensíveis -, muito menos que elas sejam usadas para bombardeios de anúncios publicitários, que nada têm a ver com as atividades pedagógicas. Além disso, vale lembrar que toda publicidade direcionada especificamente a crianças é abusiva e, portanto, ilegal.

Assim, além de cobrar pela observância de princípios como a minimização de dados, precisamos também estar atentos a parcerias, ditas gratuitas, firmadas entre empresas de

tecnologia, escolas e secretarias de educação para o ensino remoto, exigindo de todos esses atores, especialmente das empresas de tecnologia e plataformas digitais, transparência e privacidade na gestão dos dados pessoais estudantis. Vale lembrar, sempre, que na internet nada é gratuito.

2 Para proteger crianças e adolescentes de riscos à sua segurança e integridade física, psíquica e sexual

Já parou para pensar em um caso de vazamento de dados de cadastro, fotos, vídeos ou mensagens privadas de estudantes, a partir do qual essas informações sejam utilizadas para fins ilegais, como cyberbullying, assédio sexual, racismo, LGBTfobia, entre outras situações violentas ou humilhantes?

A extensão e profundidade dos registros de navegação que compõem o universo dos dados pessoais de crianças e adolescentes, incluindo os estudantis, acaba por permitir a identificação e a caracterização precisa de indivíduos e de seus hábitos, e a exposição indevida dessas informações pode gerar danos irreversíveis.

Normalmente, nessa fase de juventude há maior exposição a riscos gerais, ainda mais no uso da internet, a partir de redes sociais, aplicativos de mensagem e plataformas digitais. O mau uso da rede e uma eventual quebra de segurança de dados pessoais como endereço, fotos e vídeos, ao chegar às mãos de pessoas desautorizadas ou maliciosas, têm potencial de oferecer, inclusive, riscos à integridade física, psíquica e sexual de crianças e adolescentes.

É importante, portanto, estarmos atentos às medidas de segurança que os dados pessoais estudantis estão recebendo - tanto os que contam sobre o comportamento on-line do usuário, como seus registros de mensagens e fotos em redes sociais, quanto aqueles que se relacionam à vida íntima e off-line de crianças e adolescentes, como seu número de telefone e rota percorrida entre a casa e a escola.

3 Para impedir a consolidação da vigilância e o reforço da discriminação

Como será estudar em um local que mede o nível de atenção dos estudantes durante as aulas por meio de suas expressões faciais, identificadas por câmeras ou instrumentos tecnológicos? E ter provas corrigidas por algoritmos, robôs, que reconhecem padrões de linguagem?

Vivemos em um mundo com cada vez mais sensores de reconhecimento corporal. Desde câmeras de vigilância e catracas de acesso por meio de impressões digitais, as tecnologias de monitoramento se fazem presente no nosso cotidiano e, muitas vezes, nem mais as notamos. Junto a isso, cresce também o número de estudos e pesquisas que demonstram sua ineficiência e viés - ou, em outras palavras, o tratamento desigual que elas fornecem a indivíduos -, que pode abrir margem para ações discriminatórias e, sobretudo, discriminatórias e, sobretudo, **racistas**. ➤ Cada vez se tem notícia de mais casos de falhas em sistemas de tecnologias de reconhecimento facial, que já resultaram até mesmo em prisões injustas - via de regra, de pessoas negras.



Existem estudos que indicam que as tecnologias de reconhecimento, principalmente as utilizadas por grandes plataformas digitais, têm um padrão racista. Isso acontece, em alguma medida, porque os bancos de dados a partir dos quais essas tecnologias são programadas não são desenhados a partir de padrões étnicos diversos, o que acaba fazendo com que elas criem perfis distorcidos no caso de pessoas negras ou não brancas. Assim, essas tecnologias geram margem para atos discriminatórios muito graves, como [a acusação de uma pessoa por um crime que ela não cometeu.](#)

Uma pesquisa produzida pelas organizações PretaLab/Olabi e ThoughtWorks sob o título #quemcodabr sobre a diversidade no mercado de tecnologia mostrou que apenas 36,9% da população empregada no setor estão formadas por pessoas negras/pretas e pardas, enquanto as brancas representam 58,3%. Há uma sub-representação da população negra, que representa 53,9% do total de habitantes no país, contra 45,2% de brancos. Também há uma super-representatividade de homens, que são 68,3% das pessoas empregadas no setor, enquanto são apenas 48,5% da população total brasileira. Mais de 20% das equipes de tecnologia não possuem nenhuma mulher e mais de 30% nenhuma pessoa negra. Para saber mais sobre o assunto, recomendamos o livro “Comunidades, Algoritmos e Ativismos Digitais: olhares afrodiaspóricos”, de Tarcízio Silva.

Quando instaladas em escolas, essas tecnologias biométricas podem se tornar instrumentos de vigilância massiva e ininterrupta, capazes de desnaturalizar o ambiente da sala de aula e da unidade escolar em geral, ao torná-lo controlado e pouco confortável para crianças e adolescentes exercerem livremente suas vivências de aprendizado.

Portanto, é importante ter em mente que a discussão sobre o uso de tecnologias tão invasivas, como as de reconhecimento facial, passa por uma questão ética em disputa, que tem levado, inclusive, algumas empresas e plataformas, como Google, Facebook e Amazon, a enfrentar problemas na justiça, perder investimentos de clientes globais e até suspender pesquisas na área. O uso de tecnologias em escolas deve ser precedido de muito debate envolvendo toda a comunidade escolar (incluindo as famílias), governos, poder público e organizações especializadas.

4

Para diminuir riscos e ameaças à privacidade

Já imaginou ter problemas em uma entrevista de emprego na vida adulta por uma simples postagem inadequada nas redes sociais quando mais jovem, ou por ter ficado de recuperação em uma matéria na época do ensino fundamental?

Qualquer dado pessoal, por definição, é uma informação íntima da vida de cada um e, portanto, é essencial que seja garantida sua segurança para a preservação da privacidade, cada vez mais posta em risco em nosso mundo atual.

Esse caso de reprovação em uma entrevista de emprego por conta de uma postagem feita na internet quando ainda se era adolescente, ou por ter ficado de recuperação em alguma matéria na época do colégio, não é impossível acontecer no contexto em que vivemos, de coleta massiva de dados, inclusive estudantis, violando a confidencialidade das informações e a intimidade das pessoas. No caso de estudantes, o respeito à privacidade é ainda mais significativo. Enquanto seres em fase de desenvolvimento físico, mental, intelectual, psíquico e social, poder cometer erros em ambientes seguros, e contar com o devido suporte para compreendê-los e mudá-los, é parte do processo de autonomia, autoconfiança e identidade atravessado por crianças e adolescentes.

Se tudo que uma criança ou adolescente fizer em sua vida escolar e no processo de aprendizado ficar registrado, à mercê do uso de terceiros, podendo gerar consequências negativas futuras, não estaríamos privando-lhes do direito ao erro e à experimentação?

Para assegurar a privacidade estudantil, devem existir mecanismos de minimização dos dados coletados e tratados por plataformas e aplicativos de ensino e por qualquer tecnologia utilizada em sala de aula ou no espaço escolar. Além disso, é fundamental que os dados coletados sejam devidamente protegidos, o que pode ser feito por medidas como [verificação em duas etapas](#) sistema de proteção contra [malware](#), [criptografia](#) e também formações educativas em segurança digital.

5 Para proteger também a segurança, integridade e privacidade de professores e gestores escolares

Você já parou para pensar que, além dos estudantes, os dados dos educadores e da gestão escolar também podem estar sujeitos a estas ameaças?

Vale lembrar que os dados pessoais de professores e de gestores escolares, em muitos casos, também são coletados. Isso acontece, por exemplo, quando são instaladas câmeras em escolas e também no uso de plataformas digitais de ensino.

Portanto, a preocupação com a proteção de dados pessoais estudantis e a garantia de que não serão coletados dados excessivos, para além da finalidade daquele uso, e que os dados coletados não serão utilizados para fins injustos, ilegais ou incompatíveis com as atividades de ensino e aprendizado, também representam uma proteção a professores e gestores escolares, agentes essenciais para a vivência da experiência educativa.

6 Para desenvolver práticas educativas em cidadania digital nas escolas

Diante da importância de os dados pessoais estudantis serem bem utilizados, não é, então, essencial que conversemos sobre o tema nas escolas, desde a infância e adolescência?

O ensino sobre cidadania digital e o desenvolvimento de práticas educativas sobre segurança na internet e no uso

de tecnologias digitais da informação e comunicação são fundamentais, porque precisamos mostrar às crianças e adolescentes o funcionamento do mundo digital, inclusive para que possam entender suas oportunidades e riscos.

As **leis brasileiras** ↘ estabelecem que o pluralismo de ideias e concepções deve ser garantido, não sendo possível, assim, a utilização de somente uma plataforma, ou um conjunto de ferramentas digitais de uma mesma empresa, com os estudantes.

Nossa legislação também ressalta a cultura digital, o pensamento crítico, o autoconhecimento e o exercício da cidadania como parte do desenvolvimento integral dos estudantes. Em resumo, aprender a participar de forma cidadã dentro e fora da internet é imprescindível para lidar com os desafios do século 21, e a educação para a cidadania se estende também ao ambiente digital.



O artigo 26 do Marco Civil da Internet dispõe que é dever do Estado na prestação de serviços públicos educacionais desenvolver formação para uso seguro, responsável e consciente da internet. Além disso, desde a Lei de Diretrizes e Bases da Educação, de 1996, o pluralismo de ideias e concepções deve ser garantido, ou seja, não se pode utilizar somente uma plataforma ou um conjunto de ferramentas de uma mesma empresa com os estudantes. A Base Nacional Comum Curricular (BNCC), em suas 10 competências gerais, ressalta a cultura digital, o

pensamento crítico, o autoconhecimento e o exercício da cidadania como parte do desenvolvimento integral dos estudantes.

Assim, crianças e adolescentes têm o direito de entender que existem plataformas que compõem um cenário de concentração de poder das grandes corporações de tecnologia - localizadas especialmente no hemisfério norte, mas que, ao mesmo tempo, existe um movimento colaborativo de criação e distribuição de tecnologia baseado em padrões técnicos abertos e [software livre](#) que permite o aprimoramento de ferramentas e possibilidades sem a dependência de um único fornecedor. Falaremos mais sobre isso adiante.



5º Módulo

Quais leis já existem para proteger os dados pessoais estudantis?

Para reconhecer possíveis violações dos direitos de estudantes, conheça as leis brasileiras que protegem crianças e adolescentes no ambiente digital, e fora dele:

● 1988

📎 Constituição Federal - 1988: prevê que a proteção a crianças e adolescentes deve ser encarada como prioridade absoluta; atribui responsabilidade compartilhada entre Estado, família e sociedade - o que inclui escolas e também empresas e plataformas digitais - nessa proteção; estabelece o direito à educação e à privacidade.

Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

● 1989

📎 Convenção sobre os Direitos da Criança da ONU - 1989: ratificada pelo Brasil, a Convenção prevê que os Estados se comprometam a preservar em suas ações o melhor interesse das crianças.

● 1990

📎 Estatuto da Criança e do Adolescente (ECA) - 1990: prevê o direito de crianças e adolescentes à privacidade e à educação; pontua que é direito dos pais ou responsáveis por crianças e adolescentes ter ciência de seu processo

pedagógico e participar da definição das propostas educacionais.

O Estatuto reafirma a prioridade absoluta à proteção dos direitos de crianças e adolescentes; institui a responsabilidade compartilhada entre Estado, família, comunidade e sociedade para tal; prevê o direito de crianças e adolescentes à privacidade e à educação; pontua que é direito das mães, pais ou responsáveis por crianças e adolescentes ter ciência de seu processo pedagógico e participar da definição das propostas educacionais; além disso, determina que a criança e o adolescente têm direito a produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento - o que, no uso da internet, se conecta ao conceito de [direitos da criança por design](#) no qual o desenvolvimento e a execução de serviços e produtos digitais utilizados por crianças devem atender verdadeiramente ao seu melhor interesse.

 Código de Defesa do Consumidor (CDC) - 1990: garante aos consumidores o direito à informação clara e adequada sobre os produtos e serviços que consome, protegendo-os contra práticas abusivas - como aquelas que colocam em risco a privacidade de crianças e adolescentes.

O CDC se aplica principalmente às relações estabelecidas entre crianças e adolescentes (representados por seus pais ou responsáveis) e provedores de tecnologias de ensino, como as plataformas digitais. O CDC garante aos consumidores o direito à informação clara e adequada sobre os produtos e serviços que consomem, protegendo-

os contra métodos comerciais coercitivos ou desleais, além de práticas e cláusulas abusivas - como aquelas que colocam em risco a privacidade de crianças e adolescentes; determina que toda publicidade direcionada ao público infantil é abusiva, de forma que é ilegal a presença de comunicação mercadológica direcionada à criança, inclusive no contexto escolar e nas tecnologias e plataformas de ensino; além disso, prevê o direito dos consumidores acessarem seus próprios dados quando estes forem detidos por empresas.

● 2002

📎 Código Civil - 2002: estabelece que crianças e adolescentes menores de 16 anos devem ser representados por suas mães, pais ou responsáveis para celebrar contratos, o que, na prática, significa que são os adultos que devem concordar com o uso de tecnologias e plataformas de ensino que irão coletar ou solicitar o fornecimento de dados.

● 2014

📎 Marco Civil da Internet (MCI) - 2014: a lei define princípios éticos para o uso da internet; estabelece a privacidade e a proteção de dados pessoais de todos os usuários como princípios gerais para o uso da internet; determina o princípio da finalidade na coleta de dados.

A lei define princípios éticos para o uso da internet; estabelece a privacidade e a proteção de dados pessoais

de todos os usuários como princípios gerais para o uso da internet; prevê a importância da segurança na rede e a universalidade do acesso; sinaliza a exigência do consentimento prévio dos usuários para a coleta e tratamento de seus dados pessoais e da transparência dos controladores de aplicações e plataformas on-line em relação a essa coleta; determina o princípio da finalidade na coleta de dados, de acordo com o qual deve haver uma relação direta de finalidade entre o uso de uma plataforma ou aplicação de internet e os dados que ela coletará do usuário - isso significa, na prática, que uma plataforma de ensino remoto não pode traçar perfis de consumo de estudantes, por exemplo.

● 2018

🔗 Lei Geral de Proteção de Dados (LGPD) - 2018: a LGPD protege os dados pessoais de crianças e adolescentes, inclusive os estudantes, de forma separada e especial; prevê que a coleta e tratamento de dados deve sempre estar de acordo com o melhor interesse da criança ou adolescente, exigindo o consentimento prévio e esclarecido de pais ou responsáveis legais pelo menor de 16 anos para qualquer coleta; determina que Termos de Uso, Política de Privacidade ou qualquer outro documento que preveja a coleta de dados deve ser redigido em linguagem acessível (às crianças e adolescentes, inclusive).

A LGPD protege os dados pessoais de crianças e adolescentes, inclusive os escolares, como dados sensíveis, o que restringe as hipóteses de permissão de sua coleta

e tratamento; estabelece entre os princípios para a coleta e tratamento de dados pessoais o direito à privacidade, à intimidade, à imagem e ao exercício da cidadania, que engloba o direito à educação; reforça a exigência de finalidade, bem como de adequação e necessidade para a coleta e tratamento de dados; determina a segurança e a prevenção a riscos na coleta, tratamento e armazenamento de dados pessoais, assim como a transparência quanto às ações; prevê que a coleta e tratamento de dados deve estar sempre de acordo com o melhor interesse da criança e adolescente, exigindo o consentimento prévio e esclarecido de pais ou responsáveis legais por crianças e adolescentes para qualquer coleta; determina que Termos de Uso, Política de Privacidade ou qualquer outro documento que preveja a coleta de dados deve ser redigido em linguagem acessível (às crianças e adolescentes, inclusive); prevê o dever de eliminação ou anonimização de dados pessoais após o término de seu tratamento; reforça o direito dos titulares de dados pessoais a obter do controlador dos dados a confirmação e o acesso aos dados detidos, bem como a correção, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou incompatíveis com a finalidade do meio de sua captação - na prática, isso significa que se você identificar, pela leitura dos Termos de Uso e da Política de Privacidade de plataformas de ensino remoto, que a coleta de dados não se relaciona com o acesso à educação, é possível solicitar o apagamento; prevê o direito do titular dos dados de revogar o consentimento à sua coleta e tratamento; e, por fim, reforça o dever dos agentes de tratamento de adotar medidas de segurança para proteger os dados pessoais de

acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, tal como a criptografia.



6º Módulo

Na prática, como podemos saber se os dados pessoais estudantis estão sendo protegidos?

Para saber se os dados pessoais de estudantes estão sendo protegidos, algo que pode ser feito, nesse sentido, é a **leitura dos Termos de Uso e Política de Privacidade** ↘ de aplicativos ou plataformas digitais de ensino que estejam sendo utilizadas pela gestão pública de seu município ou estado, por sua escola ou pela escola de seu filho. Sabemos que, ao baixar aplicativos ou preencher cadastros na internet, quase ninguém lê esses documentos.



Nos Termos de Uso estão as regras do funcionamento do site ou aplicativo e também os direitos do fornecedor e

do usuário, a exemplo de informações sobre propriedade intelectual. Já a Política de Privacidade contém normas sobre a coleta e o tratamento de dados pessoais, ou seja, são indicadas quais informações serão armazenadas e como serão utilizadas - desde nome, endereço, telefone, CPF e idade, até registros de acesso e navegação.

Os textos costumam mesmo ser longos e densos, escritos em linguagem jurídica e técnica, e, muitas vezes, sequer são abertos pelo usuário, que apenas marca aquela caixa no final dizendo “concordo”. Em muitos casos, inclusive a própria maneira como aplicativos e plataformas digitais nos apresentam esses Termos de Uso, em letras pequenas e em páginas separadas, pode ser considerada uma estratégia que induz o usuário a não lê-los.



Apesar disso, ao concordar com esses termos, em seu nome ou no de seus filhos, você assina um contrato, assumindo obrigações e, inclusive, cedendo dados pessoais diversos. E não concordar com os Termos de Uso e a Política de Privacidade de um aplicativo ou site significa não poder fazer uso do serviço. No caso de plataformas para o ensino, discordar desses documentos significa não ter

acesso aos conteúdos educativos que lá serão disponibilizados. Na prática, então, dá para dizer que mães, pais, responsáveis e, geralmente, professores, têm um espaço muito limitado de escolha para concordar com Termos de Uso e Políticas de Privacidade, independentemente de seu conteúdo.

Ainda assim, é direito de todas as mães, pais, famílias, professores e gestores o acesso a tais documentos e lê-los pode ser uma forma de entender se há ou não alguma prática abusiva acontecendo, especialmente em relação à proteção de dados pessoais estudantis.

Uma vez munidos dessas informações, podemos cobrar por mudanças, de forma específica e direcionada, exigindo que as empresas de tecnologia que desenvolvem “nuvens” de armazenamento de dados pessoais estudantis, e fornecem aplicativos e plataformas de ensino, respeitem os direitos de crianças e adolescentes em sua máxima extensão. Além disso, podemos acessar as gestões públicas de educação e as escolas, cobrando delas o uso de produtos e serviços que protejam verdadeiramente os dados pessoais estudantis. Vamos falar mais sobre isso no próximo módulo.

No que podemos prestar atenção quando estivermos lendo os Termos de Uso e Políticas de Privacidade?

Apesar de as leis brasileiras determinarem que os Termos de Uso e as Políticas de Privacidade devem ser escritos em linguagem acessível, sabemos que esta não é a realidade. Então, separamos algumas dicas das principais informações e palavras-chave contidas nesses documentos para apoiar você nessa leitura.

Vale lembrar que as escolas e as gestões públicas de educação também devem estar atentas a esses contratos. E uma vez que a proteção de dados pessoais estudantis vai além da vida online e do mundo digital, algumas das perguntas e reflexões que pontuamos a seguir podem ser feitas inclusive às escolas, sobre como elas armazenam os dados cadastrais de crianças, adolescentes e de suas mães, pais e responsáveis.

Quais dados pessoais estão sendo coletados e tratados pela plataforma?

Geralmente, você encontra essas informações em:
Política de Privacidade

Se não encontrar, você pode tentar um “ctrl+f” nos termos: “dados”; “coleta”; “cookie”

FINALIDADE DA COLETA - as leis brasileiras prevêm que os dados que serão coletados e tratados no uso de uma plataforma ou aplicativo devem estar direta e estritamente relacionados à finalidade do serviço, sendo sua coleta necessária para o funcionamento da aplicação.

REGISTROS DE ACESSO - é importante entender se

há coleta e armazenamento de registros de acesso a outras aplicações de internet, para além da plataforma de ensino; ou seja, se aquela plataforma digital reunirá informações sobre todos os sites e aplicativos digitais que você ou seu filho está utilizando, mesmo fora dos horários escolares. Isso pode estar sinalizado como “instalação de [cookies](#)”.

Quem irá armazenar esses dados?

Procure entender se será a escola, a plataforma ou uma empresa terceira.

Geralmente, você encontra essa informação em: Termos de Uso ou documentos da própria escola

Se não encontrar, você pode tentar um “ctrl+f” nos termos: “armazenar”; “armazenamento”; “controle”; “controlador”; [“operador”](#).

CONTROLADOR E OPERADOR - essa informação é importante para saber a quem cobrar em caso de violações de direitos. Competem ao controlador as decisões referentes ao tratamento de dados pessoais, sendo ele quem vai definir quais dados dos estudantes vão ser coletados no uso ou na interação com alguma tecnologia digital de informação e comunicação (TDIC). Já o operador realiza o tratamento de dados pessoais em nome do controlador. Idealmente, a instituição de ensino deve ocupar o papel de controladora dos dados, o que nem sempre acontece.

Por quanto tempo esses dados serão armazenados?

Geralmente, você encontra essa informação em: Termos de Uso

Se não encontrar, você pode tentar um "ctrl+f" nos termos: "tempo"; "excluir"; "exclusão"; "apagar"; "apagamento"

ACESSO E EXCLUSÃO DE DADOS - sempre que for utilizar uma plataforma digital ou aplicativo, vale atentar-se para a possibilidade de alterar as configurações de acesso a dados para limitar a abrangência das informações suas ou de seu filho que poderão ser coletadas. Isso pode ser feito, por exemplo, não concedendo acesso à câmera, microfone, localização, arquivo de mídias. Além disso, veja se os Termos preveem que, ao final do uso dessa tecnologia ou ao final dos anos escolares, os dados estudantis serão excluídos das bases da empresa.

Esses dados serão compartilhados com - ou vendidos para - terceiros?

Geralmente, você encontra essas informações em: Política de Privacidade

Se não encontrar, você pode tentar um "ctrl+f" nos termos: "compartilhar"; "compartilhamento"; "venda"; "terceiros"

COMPARTILHAMENTO COM TERCEIROS - aplicações e plataformas podem ser acessadas por crianças ou adolescentes ainda que seus pais ou responsáveis não consentam a captação e tratamento de seus dados pessoais necessários à atividade. Procure saber se a plataforma compartilha ou vende essas informações para outros fins e agentes comerciais (por exemplo: para o direcionamento de publicidade).

Quais as medidas de segurança adotadas na coleta e no armazenamento?

Geralmente, você encontra essas informações em:

Termos de Uso

Se não encontrar, você pode tentar um “ctrl+f” nos termos: “consentimento”;

“criptografia”; “anonimização”; “anonimizado”;

“vazamento”; “quebra”; “segurança”; “notificação”

CONSENTIMENTO - é importante checar se a plataforma destinada ao uso de crianças e adolescentes cumpre o dever de colher o consentimento prévio, expresso e irrestrito de pelo menos um dos pais ou responsável legal.

SEGURANÇA - vale atentar-se também para quais medidas técnicas e administrativas são tomadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda,

alteração, comunicação ou difusão de informações. Uma delas é a criptografia.

ANONIMIZAÇÃO - uma medida simples de segurança aos usuários pode ser a anonimização, em conformidade com as políticas de minimização da coleta e do tratamento de dados.

POLÍTICA DE RESPOSTA - outra checagem importante é se há informações sobre a política de resposta no caso de vazamento de dados da plataforma para que, no caso de uma quebra de segurança e potencial exposição de crianças e adolescentes, ao menos suas mães, pais, responsáveis ou escolas sejam alertados e possam ficar cientes.

Mudanças nos Termos de Uso e na Política de Privacidade serão notificadas ao usuário e será solicitada uma nova manifestação de consentimento?

Geralmente, você encontra essas informações em:
Termos de Uso

Se não encontrar, você pode tentar um “ctrl+f” nos termos: “modificação”, “modificações”, “alteração”, “alterações”

DIREITO À INFORMAÇÃO CLARA E ADEQUADA - é fundamental que qualquer mudança nesses documentos seja notificada ao usuário ou, no caso de o usuário

ser pessoa com menos de 16 anos, à sua mãe, pai ou responsável. Caso contrário, podemos falar que existe uma brecha para que as empresas distorçam a natureza desses termos da forma que preferirem e o usuário deixe de ter uma informação clara e adequada sobre o serviço ou produto que está utilizando. Nesse caso, os Termos de Uso provavelmente mencionariam essa informação falando em modificação ou alteração “unilateral”, o que pode até mesmo ser considerado ilegal.



7º Módulo

Alternativas para uma educação livre de exploração comercial e respeitosa às crianças e adolescentes

São muitas e complexas as questões que envolvem a segurança digital e a livre circulação de crianças e adolescentes na internet. Se você também se assustou com tantos problemas, acalme-se e preste atenção às estratégias, políticas e dicas sobre tecnologias de ensino que promovem usos mais

responsáveis e adequados ao desenvolvimento infantil. Elas existem e queremos apresentá-las, resumidamente, a você!

Diante da situação de concentração da tecnologia e dos meios de comunicação agravada na pandemia, mas que já vinha ocorrendo em diversos lugares, é fundamental garantir a educação e a comunicação como direitos e o conhecimento como um bem comum, algo debatido mais firmemente desde 2002, em um evento realizado pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO).

Nesse evento, foi cunhado o termo recursos educacionais abertos (REA): materiais de ensino, aprendizado e pesquisa disponibilizados em qualquer suporte ou mídia, sob domínio público ou licenciados de maneira aberta, o que significa que podem ser utilizados ou adaptados livremente por qualquer pessoa. Os REA são parte integrante do movimento de Educação Aberta, que compreende a partilha de boas ideias entre educadores, agora permeada pelas novas possibilidades de interação trazidas pela cultura digital. Esses recursos podem ser livros, capítulos de livros, planos de aula, softwares, jogos, resenhas, trabalhos escolares, artigos, dissertações, teses, manuais, vídeos, áudios e imagens, dentre outros tipos.

O uso de formatos abertos e a criação com base em software livre são elementos importantes para o processo construído no âmbito da estrutura existente de direitos de propriedade intelectual, tais como se encontram definidos por convenções internacionais.

Em sua 40ª Conferência Geral, realizada em novembro de 2019, em Paris, a UNESCO aprovou por unanimidade uma **Recomendação sobre Recursos Educacionais Abertos** ↘, a partir da qual espera-se o compromisso dos países com a produção e compartilhamento de materiais educacionais com licença aberta, beneficiando estudantes e educadores em todo o mundo.



Trata-se de um instrumento normativo que determina que os estados-membros devem promover e reportar avanços no desenvolvimento de políticas de educação aberta a partir do Plano de Ação de Liubliana, resultado do 2º Congresso Mundial de REA da UNESCO na Eslovênia. A adoção oficial de uma Recomendação sobre REA vem ao encontro das diretrizes sobre educação de qualidade, inclusiva e equitativa destacadas no 4º Objetivo de Desenvolvimento Sustentável da ONU.



No Brasil, desde 2018, existe a Portaria nº 451 do Ministério da Educação, que determina o uso de licença aberta para materiais educacionais comprados ou subsidiados pela pasta, voltados para a educação básica. Há também um projeto de lei, criado em 2011 e atualizado em 2018,

já aprovado nas comissões de Educação e de Cultura da Câmara dos Deputados, que agora segue para a [Comissão de Constituição, Justiça e Cidadania](#).

Busque Recursos Educacionais Abertos para recomendar ou utilizar em sua escola e sala de aula em relia.org.br

Conheça soluções em código aberto e software livre:
escolhalivre.org.br
comunica.aberta.org.br

Busque prestadores de serviço em software livre e recursos abertos:
msa.aberta.org.br



8º Módulo

Educação para a Mídia e Empoderamento Digital

Este guia tentou mostrar como a internet e as tecnologias de informação ampliaram os desafios da comunicação, da educação e da proteção de dados. Nesse sentido, é importante entender que o direito à comunicação está absolutamente

ligado aos demais direitos sociais, já que o acesso e a produção de informações possibilitam expandir os debates sobre moradia, saúde, meio ambiente, raça, etnia, gênero e sexualidade, além da educação.

Com a internet, pautas relacionadas à diversidade e à pluralidade, centrais no âmbito dos meios de comunicação tradicionais (TV, rádio e impresso), ganham novos contornos. Infelizmente, como vimos, a rede tem sido um espaço restrito e privilegiado para o consumo, a vigilância, a concentração e a formação de bolhas sociais, que implicam em um cenário de desinformação, polarização política e disseminação de boatos/inverdades (fake news) e discursos de ódio.



Para enfrentar essas barreiras sociais, que criam violações e exclusões transpostas para as redes digitais, diversas organizações da sociedade civil propõem a efetivação da liberdade de expressão e educação, para além das ideias de liberdade de imprensa e cátedra. Dessa forma, a universalização do acesso e a privacidade e a proteção dos dados pessoais estudantis aparecem como elementos básicos para a formação cidadã e o exercício do direito de se informar, aprender e expressar livremente opiniões e ideias por quaisquer meios. E é essencial que isto seja passado adiante, inclusive para nossas crianças e adolescentes, que já nascem em um mundo hiperconectado.

Precisamos estender para a internet princípios de representatividade e participação ativa norteadores da sociedade, como a cidadania - ou seja, a garantia de direitos e segurança na rede, incluindo a privacidade e a proteção de dados - e a democracia - a partir da construção de debates e conhecimentos públicos amplos sobre as tecnologias digitais da informação e comunicação.

Destacamos dois conceitos importantes para lidar com essa invasão das tecnologias na educação e na sociedade: o “empoderamento digital”, dado pela participação ativa da sociedade na criação e no controle das tecnologias; e a “educação para a mídia”, que vai além da simples recepção e manipulação passiva de informações e tecnologias, privilegiando uma leitura crítica dos meios de comunicação.

Consideramos como premissas da noção de empoderamento digital: (1) a indivisibilidade entre o direito à comunicação e outros direitos humanos, cuja garantia deve se dar também no ambiente on-line; (2) a diversidade e o pluralismo como formas de demonstração da liberdade de expressão de indivíduos e coletividades; (3) o conhecimento como uma construção coletiva e compartilhada; (4) a constituição das Tecnologias da Informação e da Comunicação como instrumentos democráticos a serem apropriados de forma ativa pelos sujeitos; (5) o combate a opressões e a defesa da justiça social e da democracia política como valores e objetivos associados a essas práticas.

A educação para a mídia busca construir uma mudança cultural nos espaços de ensino, que impulsiona os alunos a se tornarem agentes comunicativos, deixando de lado a passividade com relação à informação. Ela parte do pressuposto de que todos devem ter acesso à mídia - muitas vezes, no contexto atual, disseminada no meio digital e das tecnologias - e, além disso, entender como ela funciona, tendo condições de analisar e refletir criticamente sobre os seus conteúdos e participar da produção midiática. Afinal, o exercício da cidadania no contexto digital exige um conhecimento amplo sobre as oportunidades de aprendizagem e as ameaças e danos envolvidos no uso das tecnologias de comunicação.



9º Módulo

Diante de tantos desafios, como cada um de nós pode agir?

Trazemos aqui algumas sugestões do que cada um de nós pode fazer para promover a proteção de dados pessoais estudantis, lembrando novamente que é responsabilidade compartilhada de todos os agentes da sociedade - família, Estado, escolas e empresas - a promoção máxima dos direitos de crianças e adolescentes.

Mãe, pai, familiar ou educador(a):

- Compartilhe suas inquietudes e preocupações com a gestão e a comunidade escolar;
- Debata com a escola e com a comunidade escolar a escolha de produtos e serviços seguros para a proteção de dados;
- Converse com crianças e adolescentes sobre empoderamento digital e educação para a mídia;
- Analise ou busque auxílio para avaliar os Termos de Uso e

a Política de Privacidade de aplicativos e plataformas de ensino;

- Solicite ao responsável pela base de dados (escola ou empresa) a eliminação de seus dados pessoais ou dos dados pessoais de seus filhos que tenham sido coletados de forma desnecessária, excessivamente invasiva à privacidade ou que sejam direcionados a fins ilegais;
- Denuncie possíveis violações nos órgãos competentes: Ministério Público, Procons, organizações da sociedade civil (como o programa [Criança e Consumo](#), do Instituto Alana) ou diretamente às empresas, por meio do SAC ou de suas redes sociais.

Escola ou gestão pública de educação:

- Analise e abra espaços de discussão com a comunidade escolar (educadores, estudantes e famílias) sobre as oportunidades e os riscos relacionados à adoção de uma tecnologia proprietária, para que a decisão seja fundamentada e regularizada;
- Verifique a possibilidade de adoção de plataformas ou tecnologias alternativas, que não sejam prejudiciais à privacidade e respeitem a proteção de dados de crianças e professores (software livre);
- Não condicione a participação da criança ao consentimento do uso de determinada plataforma ou serviço, dando sempre opções;

- Exija de fornecedores de tecnologia, mesmo em regime de doação (sem custo para os cofres públicos), via termo ou contrato, transparência sobre o tratamento de dados a ser realizado na respectiva ferramenta, aplicativo ou tecnologia. Vale refletir, aqui, se parcerias “gratuitas” não terão mesmo nenhum custo às escolas e, especialmente, aos estudantes;
- Auxilie pais e/ou professores na solicitação de eliminar os dados pessoais coletados de forma desnecessária, excessivamente invasiva à privacidade ou que sejam direcionados a fins ilegais;
- Incorpore de forma transversal os temas de cidadania digital, empoderamento digital e educação para a mídia às discussões com crianças e adolescentes.

Empresa prestadora de serviço digital:

- Obedeça aos direitos da criança por design, o que implica em formular seus produtos e serviços, desde a concepção até a execução, a partir do melhor interesse da criança com absoluta prioridade, em abordagem multidisciplinar;
- Siga à risca as leis e as boas práticas do mercado, não se limitando a elas;
- Estabeleça padrões mundiais para a prestação de seus serviços e entrega de produtos, deixando de privilegiar os direitos de crianças e adolescentes e a proteção de dados apenas em países que regulam o tema de forma mais rígida ou específica - majoritariamente, países do norte global;

- Esteja aberto ao diálogo com toda a sociedade e comunidade escolar, para adequação de suas práticas;
- Parta do princípio da minimização dos dados coletados e tratados, especialmente no caso de crianças e adolescentes, ou seja, não condicione a participação em aplicações de internet ou outras atividades ao fornecimento de informações pessoais que não sejam estritamente necessárias à atividade educativa. Isso significa, também, nunca coletar e tratar dados de crianças, adolescentes e estudantes para fins comerciais, como o direcionamento de publicidade;
- Disponibilize Termos de Uso e Política de Privacidade acessíveis (em termos de idioma, vocabulário, diagramação, design e recursos de acessibilidade);
- Solicite o consentimento prévio para coleta e tratamento de dados em documento separado do consentimento para uso do serviço ou produto;
- Exija o consentimento prévio parental, e não apenas das escolas;
- Realize todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis;
- Não permita a presença de estratégias de comunicação mercadológica, especialmente no ambiente de plataformas e aplicativos desenhados para o ensino remoto ou para o contexto escolar;

- Reforce seus padrões de segurança em relação aos dados pessoais de crianças e adolescentes.

Sociedade civil e organizações sociais:

- Cobre transparência das empresas e gestões escolares sobre a coleta, uso e armazenamento de dados pessoais estudantis;
- Acompanhe, inclusive via Lei de Acesso à Informação (LAI), as ações da gestão pública em relação aos contratos estabelecidos com empresas de tecnologia para uso educacional.



10º Módulo

Para se aprofundar mais

Esperamos que a leitura deste material tenha sido bastante proveitosa para você! Trazemos, aqui, uma lista de referências caso você queira se aprofundar ainda mais no tema.

Aproveitamos para apresentar, também, o que cada uma das organizações que elaboraram este guia tem feito na defesa da educação e das infâncias livres de exploração comercial.

Não esqueça de compartilhar este [guia](#) com mais pessoas que podem se interessar por este conteúdo.

Indicação de materiais para aprofundamento (temas diversos sobre crianças, internet e proteção de dados)

- [Livro-guia de Como Implementar uma Política de Educação Aberta](#)
- [Cartilhas de Segurança para Internet](#), publicadas pela Nic.br/CGI através do Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT)
- [Cartilha Diálogo Virtual 2.0](#), publicado pela Safernet/CGI/MPF
- Guias [Internet Segura](#) e [Internet Segura Para Seus Filhos](#), publicados pela Nic.br/CGI através do Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT)
- Guias [#Internet Com Resposta- Na sua sala de aula](#) e [#Internet Com Resposta](#) - Na sua sala de aula e encarte [#FikDik](#) publicados pela Nic.br/CGI através do Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT).
- [Guia NIC.br sobre uso de internet na sala de aula](#)
- [Cartilha Acessibilidade na Web](#), publicada pela Nic.br/CGI através do Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores (CERT)
- [10 maneiras de enfrentar a desinformação](#) (Intervozes)

- [Site GDPR](#)
- [Media Ownership Monitor Brazil](#) (Intervozes/Repórteres Sem Fronteiras)
- [Monopólios Digitais - Concentração e Diversidade na Internet](#) (Intervozes)
- [CCFC: A Practical Guide for Protecting Your Child's Sensitive School Data](#)
- [Direito à Comunicação e Internet – o empoderamento digital como garantia desse direito no ambiente online](#)
- 5Rights: [The Future of Childhood in the Digital World](#)
- Especial Lunetas: [Um olhar para as infâncias conectadas](#)
- [Aulas remotas: qual o impacto na saúde mental das crianças?](#)

Como buscar e compartilhar boas práticas sobre privacidade e outros temas de cidadania digital?

A plataforma [Pilares do Futuro](#), lançada em agosto de 2020, tem a missão de promover a troca entre educadores e demais profissionais envolvidos com educação, seja no sistema formal ou não, sobre como implementar em escolas e instituições projetos e atividades voltadas para a reflexão e pensamento crítico.

O que Instituto Alana, Educadigital e Intervenções já estão fazendo nesses temas?

- **Instituto Alana:** evento [Ser Criança no Mundo Digital](#); envio de carta de apoio ao Conselho Nacional de Secretários de Educação (Consed) e à União Nacional dos Dirigentes Municipais de Educação (Undime) sobre a importância de não haver publicidade infantil nos materiais didáticos impressos nem intervalos comerciais em transmissões do ensino remoto via radiodifusão; assinatura de carta com outras entidades internacionais para demandar das autoridades, governos e empresas a proteção das crianças da exploração comercial no contexto do aumento de uso de plataformas digitais, inclusive para razões educacionais, durante a pandemia de covid-19; assinatura de carta junto com coalizão internacional exigindo que empresas gigantes de tecnologia cessem a exploração comercial infantil no ambiente digital; envio de contribuição à Organização das Nações Unidas (ONU) sobre o direito à privacidade e a exploração comercial de crianças no ambiente digital, inclusive em atividades educativas.
- **Educadigital via Iniciativa Educação Aberta:** mapa de Recursos Educacionais Abertos, com respectivos prestadores de serviços; servidor para teste de ferramentas de comunicação e colaboração abertas; landing page Escolha Livre - Guia sobre software livre e Recursos Educacionais Abertos para professores e gestores; plataforma de compartilhamento de boas práticas educativas em cidadania digital Pilares do Futuro

- **Intervozes:** ações judiciais (contra a Telefônica/ Vivo, por exposição de dados pessoais; contra o Metrô de São Paulo, por câmeras de reconhecimento facial); pedido à Agência Nacional de Telecomunicações (Anatel) de proibição de bloqueio de franquia de internet durante a pandemia; Campanha Seus Dados São Você; Campanha Internet Direito Seu; Laboratório Tático do Comum (LabTaCo) Guarani; Projeto Ondas da Resistência; Podcast Levante Sua Voz.
- **Instituto Alana, Intervozes e EducaDigital**, em conjunto: levantamento das iniciativas de ensino remoto das secretarias estaduais e municipais de educação das capitais brasileiras; pesquisa de análise dos Termos de Uso e Política de Privacidade dos pacotes Google e Microsoft para educação.



Glossário

Algoritmos

Conjunto de regras, operações e procedimentos, definidos e ordenados, usados na solução de um problema, ou de uma classe de problemas, em um número finito de etapas. Atualmente, os algoritmos são utilizados, em larga medida, para analisar o comportamento humano na internet, traçando os gostos e preferências dos usuários para, então, poder direcionar a cada um o conteúdo específico que o interessa. [Voltar ao texto ↩](#)

Anonimização de dados pessoais

De acordo com a Lei Geral de Proteção de Dados (LGPD), dado anonimizado é o conjunto de informações relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. A anonimização, portanto, seria o processo que permite a desidentificação do dado a seu titular. [Voltar ao texto ↩](#)

Cibercultura

Cultura que surgiu, surge, ou está surgindo, a partir do uso da internet, da rede de computadores, e das tecnologias, destacando-se os movimentos de comunicação virtual, a indústria do entretenimento e o comércio eletrônico. [Voltar ao texto ↩](#)

Comissão de Constituição, Justiça e Cidadania

É uma das comissões da Câmara dos Deputados e do Senado Federal brasileiros, responsável por avaliar se o texto de uma proposta legislativa está de acordo com a Constituição Federal. [Voltar ao texto ↩](#)

Controladores de aplicações e plataformas on-line

Controladores são as pessoas ou empresas que irão definir o funcionamento de uma aplicação ou plataforma on-line, estabelecendo qual será o escopo e a amplitude

do conjunto de dados pessoais dos usuários que serão coletados e tratados durante seu uso. Em plataformas como o Facebook, por exemplo, é o próprio Facebook quem define quais dados dos usuários irá coletar, além de como irá tratar e utilizar esses dados. [Voltar ao texto ↩](#)

Cookies

Os cookies são utilizados por sites, aplicativos e plataformas para identificar e armazenar informações sobre os usuários que os visitam. São pequenos arquivos de texto que ficam gravados no dispositivo por meio do qual o usuário acessa aquela plataforma ou ambiente digital. [Voltar ao texto ↩](#)

Criptografia

A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da internet. [Voltar ao texto ↩](#)

Cyberbullying

Modalidade virtual do bullying, que toma grandes proporções na internet por meio de celulares, câmeras fotográficas e redes sociais. Consiste em intimidações repetitivas entre crianças e adolescentes, por meio da disseminação de conteúdos de insulto, humilhação e

violência psicológica que provocam constrangimento e prejuízos nos envolvidos. [Voltar ao texto ↩](#)

Dados pessoais

Toda informação relacionada à pessoa natural identificada ou identificável. O nome, telefone, endereço, e-mail e perfis em redes sociais, por exemplo, são dados pessoais. É natural atrelarmos a ideia de dado pessoal à internet, até porque boa parte dessas informações é armazenada no ambiente digital. Mas, é importante ter em mente que o conceito de dado pessoal vai muito além do comportamento de cada indivíduo on-line.

[Voltar ao texto ↩](#)

Dados pessoais estudantis

Toda informação que identifica cada estudante e cuja coleta e uso estejam relacionados à sua vida escolar.

[Voltar ao texto ↩](#)

Dados sensíveis

Dado pessoal sensível, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), é qualquer dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a um indivíduo, inclusive crianças e adolescentes. São protegidos de forma rígida e só podem ser tratados quando houver consentimento do titular - ou

da mãe, pai ou responsável pelo titular, se menor de 16 anos - ou em situações específicas de interesse público, listadas no art. 11 da Lei. [Voltar ao texto ↩](#)

Direitos da criança por design

O padrão dos direitos da criança por design deve ser incorporado por todos os atores que desenvolvem e implementam tecnologias e sistemas digitais voltados para crianças, ou que possam ser usados por elas ou impacta-las de alguma forma. O padrão impõe a esses atores o dever de considerar os direitos de crianças desde o momento em que concebem e desenhar aquela tecnologia ou sistema, até o momento em que a executem. Na prática, resulta em produtos e serviços que possuam design adequado e humanizado para as crianças, o que significa, dentre outras diretrizes práticas, que serão seguros; livre de violências; livre de publicidade infantil; não realizarão coleta de dados para fins comerciais; promoverão o direito das crianças a se desconectar, não incentivando que elas se mantenham ligadas às telas; promoverão experiências educativas, de criação e de brincadeiras. [Voltar ao texto ↩](#)

Domínio público

Uma obra em domínio público pode ser reproduzida, distribuída, traduzida, publicada ou adaptada sem a necessidade de autorização. [Voltar ao texto ↩](#)

Educação a distância (EAD)

O Conselho Nacional de Educação (CNE) define Educação a Distância (EaD) na Resolução nº 1, de 11 de março de 2016, como “modalidade educacional na qual a mediação didático-pedagógica, nos processos de ensino e aprendizagem, ocorre com a utilização de meios e tecnologias de informação e comunicação, com pessoal qualificado, políticas de acesso, acompanhamento e avaliação compatíveis, entre outros, de modo que se propicie, ainda, maior articulação e efetiva interação e complementariedade entre a presencialidade e a virtualidade “real”, o local e o global, a subjetividade e a participação democrática nos processos de ensino e aprendizagem em rede, envolvendo estudantes e profissionais da educação (professores, tutores e gestores), que desenvolvem atividades educativas em lugares e/ou tempos diversos”. Trata-se de modalidade de ensino complementar na educação básica e ilegal na educação infantil. Vale lembrar que, apesar de associarmos rapidamente a EaD com a internet, há registros de experiências de ensino a distância desde o século XVIII. Ao longo do tempo, ela foi se adaptando aos contextos e transformações tecnológicas. A história da EaD tem como principais fases:

- 1) ensino por correspondência;
- 2) ensino pela mídia impressa e rádio;
- 3) teleaprendizagem;
- 4) teleconferência e
- 5) internet

[Voltar ao texto ↩](#)

Ensino Remoto

Termo utilizado para identificar a forma não presencial como as atividades escolares passaram a ser feitas após o isolamento físico imposto pela pandemia. A internet é a principal forma de atingir esse objetivo, mas outras possibilidades são consideradas quando há problemas de conexão. [Voltar ao texto ↩](#)

Inteligência Artificial (IA)

Campo de conhecimento que atua com “sistemas cognitivos” ou “computação cognitiva” para transformar dados não organizados em informações estruturadas, como linhas, colunas ou esquemas. Ao criar e manter perfis em redes sociais, usar aplicativos com geolocalização ou acessar sites de streaming para ver filmes e escutar músicas, estamos constantemente interagindo com robôs. [Voltar ao texto ↩](#)

Malware

Popularmente chamado de ‘vírus’, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações. [Voltar ao texto ↩](#)

Melhor interesse das crianças

Deve ser considerado primordialmente por todos aqueles que estão submetidos ao dever compartilhado de proteger e promover os direitos de crianças e adolescentes com absoluta prioridade, nos termos do art. 227 da Constituição Federal (CF), ou seja, Estado, família e sociedade, na qual se incluem os entes privados como empresas. Deve ser entendido como o fundamento primário de todas as ações direcionadas à população infanto-juvenil – em âmbito público ou privado –, de modo que qualquer orientação ou decisão nesse campo deve ser pautada pelo que é melhor e mais adequado para satisfazer as necessidades e interesses desse público, sobrepondo-se a outros interesses, inclusive os estritamente comerciais. [Voltar ao texto ↩](#)

Minimização de dados

É a limitação do tratamento, estabelecida na LGPD, ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento dessas informações. [Voltar ao texto ↩](#)

Neutralidade da rede

De acordo com a Coalizão Global pela Neutralidade de Rede, trata-se de “princípio segundo o qual o tráfego da internet deve ser tratado igualmente, sem discriminação, restrição ou interferência independentemente do emissor, recipiente, tipo ou conteúdo, de forma que a

liberdade dos usuários de internet não seja restringida pelo favorecimento ou desfavorecimento de transmissões do tráfego da internet associado a conteúdos, serviços, aplicações ou dispositivos particulares”. É, portanto, um dos princípios básicos para o uso da internet. [Saiba Mais](#)
[Voltar ao texto ↩](#)

Operador

A Lei Geral de Proteção de Dados define operador como “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”. [Voltar ao texto ↩](#)

Plataformas digitais

Modelos de negócios intermediados por tecnologias, nas quais se conectam fornecedores e consumidores, elas são ambientes on-line onde pessoas se conectam para relações de troca, que podem ser de trabalho, ensino, lazer ou entretenimento. [Voltar ao texto ↩](#)

Publicidade infantil

Qualquer comunicação mercadológica direcionada às crianças, com o objetivo de divulgar e estimular o consumo de algum produto, marca ou serviço. [Voltar ao texto ↩](#)

Recursos Educacionais Abertos (REA)

materiais de ensino, aprendizado e pesquisa disponibilizados em qualquer suporte ou mídia, sob domínio público ou licenciados de maneira aberta, o que significa que podem ser utilizados ou adaptados livremente por qualquer pessoa. [Voltar ao texto ↩](#)

Sextorsão

Como explica a SaferNet, é a ameaça de se divulgar imagens íntimas para forçar alguém a fazer algo - ou por vingança, ou humilhação ou para extorsão financeira.

[Saiba mais](#)

[Voltar ao texto ↩](#)

Software livre

É o software que concede liberdade ao usuário para executar, acessar e modificar o código fonte, e redistribuir cópias com ou sem modificações. [Saiba mais.](#)

[Voltar ao texto ↩](#)

Tecnologias digitais da informação e comunicação (TDICs)

Todo dispositivo que permita a navegação da internet, como computador, tablet, celular, smartphone etc.

[Voltar ao texto ↩](#)

Transparência

De acordo com a LGPD, é a garantia aos titulares de dados pessoais de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. [Voltar ao texto ↩](#)

Tratamento ou processamento de dados

Segundo a Lei Geral de Proteção de Dados (LGPD), trata-se de “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. [Voltar ao texto ↩](#)

Verificação em duas etapas

A ‘verificação em duas etapas’ é um recurso que adiciona mais uma camada de segurança às contas de cada usuário. Muitas vezes, para além da senha geralmente utilizada para login, o usuário recebe um código por SMS ou por whatsapp, por exemplo. A maior parte dos aplicativos e plataformas digitais permitem e recomendam a habilitação desse tipo de configuração. [Saiba mais](#)

[Voltar ao texto ↩](#)

Elaboração

Iago Vernek

Marina Meira

Priscila Gonsales

Contribuição

Ana Cláudia de Arruda Leite

Belisa Rotondi

Diana Pallares

Isabella Henriques

Olívia Bandeira

Pedro Hartung

Raquel Franzim

Tel Amiel

Coordenação Editorial

Maíra Bosi

Revisão de texto

Marcia Pinto e Regina Cury - Metatexto

Projeto gráfico

Vitor Pinho - Bright Experience

Como citar:

VERNEK, Iago; MEIRA, Marina;

GONSALES, Priscila. *A Escola no mundo digital - dados e direitos de estudantes*.

Instituto Alana, São Paulo, 2020

**Realização
e organização**



Organização



Apoio





A ESCOLA NO MUNDO DIGITAL

Dados e Direitos de estudantes

Acesse a versão online

www.dadosestudiantis.org.br



Esta obra está licenciada com uma Licença
Creative Commons Atribuição - Não Comercial 4.0 Internacional.