

A close-up photograph of a hand with fingers painted in a rainbow gradient, resting on a dark wooden surface. The colors transition from purple at the tips to red, orange, yellow, green, and blue towards the base of the fingers. The background is a dark, textured wood grain.

# PRIVACIDADE NA INTERNET

**Um guia para pais e  
responsáveis**

SMARTE

# PRIVACIDADE NA INTERNET

**Um guia para pais e  
responsáveis**

CAMILA SALLES DOS SANTOS  
SMARTE ESTRATEGIAS EMPRESARIAIS



## Sobre a SMARTE

A SMARTE é uma empresa focada em consultoria, implementação de processos, compliance, desenvolvimento de projetos e de negócios digitais.

Em tempos de mudanças políticas, econômicas, sociais e tecnológicas, em um mercado altamente competitivo, sobreviver com resultados diferenciados exige organização, controle, qualidade, inovação e construção de parcerias sólidas.

Comprometidos com valores humanos, sociais, morais e éticos, apoiamos você e o seu negócio na construção de uma trajetória de crescimento sustentável e valoroso.

Também nos preocupamos com a entrega de informações e conhecimento úteis e confiáveis a todos, para contribuir com a nossa sociedade.

## Sobre a autora

Camila Salles dos Santos é advogada, especialista em segurança digital, governança e gestão de dados.

Mediadora Judicial e participante de programas e estudos sobre Justiça Restaurativa.

Palestrante, com foco na Lei Geral de Proteção de Dados.

Encarregada de Proteção de Dados pessoais na SMARTE e em outras organizações, sendo responsável pela implementação de programas de adequação à LGPD, nos mais variados segmentos econômicos.





## Sumário

Introdução

Papel dos Pais e Responsáveis

Cenário de interação

Ações, comportamentos e riscos

Sinais de Atenção!

Ameaças, riscos e crimes

Orientação e prevenção são o melhor remédio!

Conclusão

# Introdução

A sociedade e as relações estão em constante mutação. A virtualização das relações e da forma de comunicação trouxeram novas modalidades de relacionamentos, de negócios, de serviços, integrando-se totalmente à nossa vida social, profissional, escolar e familiar.

Por isso, tornou-se essencial que o nosso sistema jurídico tivesse normas específicas direcionadas a esta nova realidade.

A Lei ° 13.709/2018 - Lei Geral de Proteção de Dados (LGPD) - regulamenta o uso da informação pessoal e cria um conjunto de novos conceitos jurídicos (ex.: dados pessoais, dados sensíveis, etc.), estabelece condições nas quais os dados pessoais podem ser tratados, define conjunto de direitos para os titulares dos dados, gera obrigações específicas para quem os utiliza e cria uma série de procedimentos e normas de tecnologia, segurança e governança para haver maior cuidado com o tratamento de dados pessoais, sobretudo os dados de crianças e adolescentes.

Contudo, somente a lei não basta. É preciso mudar a cultura. É preciso de educação e orientação.

Por isso, essa nova realidade exige dos pais e/ou responsáveis a adaptação de cuidados básicos que sempre foram repassados às crianças e adolescentes, tais como: *“atravessar a rua somente na faixa de segurança”, “olhar para os dois lados antes de atravessar a rua”, “não aceitar alimentos de estranhos”, “manter as portas trancadas quando estiver em casa sozinho (a)”, “não pegar aquilo que não é seu”, “usar o cinto de segurança”, etc.*

A realidade virtual é uma cópia da vida analógica e, por isso, requer as mesmas orientações, porém adequadas ao meio, sobretudo em razão da agilidade do tráfego de informações, da oferta indiscriminada de bens e serviços e da atuação criminosa e abusiva no ambiente digital e na internet.

**A segurança digital começa em casa!**



# Papel dos pais e responsáveis

# Papel de Pais e Responsáveis

Como referido na introdução, a segurança digital começa em casa.

Cabe a nós, os adultos, orientar e tutelar os direitos das crianças e adolescentes, principalmente, quando elas estão longe dos nossos olhos e presentes em outras realidades, como é o mundo digital.

Por isso, devemos não só saber como monitorar, amparar, orientar e, algumas vezes, balizar o uso de dispositivos de tecnologia e o acesso e uso da internet, notadamente, os ambientes das redes sociais e de aplicações.

É dever dos pais e responsáveis saber se a criança e/ou adolescente:

- acessa dispositivos eletrônicos e digitais seus ou de terceiros;
- quanto tempo permanece utilizando tais dispositivos;
- quais aplicações, softwares e sites são acessados;
- se existem perfis ou cadastros em nome da criança e/ou adolescente;
- possui relacionamento ou “amizades” virtuais;
- utiliza dispositivos com câmera (smartphones, computadores, tablets, ...);
- possui hábito de fotografar e gravar imagens e vídeos de seu cotidiano ou de terceiros;
- armazena qualquer tipo de conteúdo em seus dispositivos;
- possui acesso a compras virtuais e downloads;
- participa de atividades curriculares on-line;
- se é estimulado ao uso da internet para atividades de estudo e pesquisa;
- se substitui materiais didáticos, livros para a confecção de seus trabalhos por materiais prontos disponíveis na internet;
- se acessa a Deep Web;
- possui ou utiliza senhas próprias, ou de terceiros, inclusive dos próprios pais e responsáveis.

# Cenário de Interação



# Cenário de Interação

Atualmente, assim como a nossa realidade tramita em torno da tecnologia, a das crianças e adolescentes não é diferente. Muito pelo contrário!

As crianças e adolescentes estão muito mais conectadas do que nós, já que nasceram nessa nova era.



Até as salas de aula já estão digitais.

A diversão também é usufruída, em grande parte, no mundo virtual, assim como as amizades e relacionamentos.





# Ações e comportamentos

# Ações e comportamentos

O ambiente virtual ou digital é uma réplica do ambiente analógico.

Assim como nossas crianças e adolescentes podem ser vítimas, também podem ser algozes!

Respeitar os direitos alheios e fazer respeitar os seus próprios direitos são medidas que se impõe.

Embora existam muitas regulamentações sobre o uso da internet, mas a maioria das pessoas ainda acredita que se trata de uma “terra sem lei”, o que incentiva não só a prática de atos ilegais, ofensivos, abusivos e criminosos.

Por isso, estar atento aos cuidados com nossas crianças e adolescentes, requer mais conhecimento, mais comprometimento, mais preparo e instrução dos pais e responsáveis, além de uma atuação multidisciplinar com apoio dos profissionais de saúde, educadores, parentes, amigos e familiares que fazem parte do relacionamento do menor.



## Ações e comportamentos

Além das questões relacionadas ao bom uso das tecnologias e aos riscos de sofrer lesões ou de lesar alguém, a saúde das crianças e adolescentes é extremamente preocupante neste cenário.

Uma pesquisa da ESBRAZIL levantou dados impressionantes. Cerca de 80% das crianças entre 9 e 17 anos estão conectadas à internet, sendo que 97% nas classes sociais A e B, 85% na classe C e 51% nas classes D e E. Os dados são da Tic Kids Online-Brasil, pesquisa realizada pelo Comitê Gestor da Internet (CGI). O levantamento mostra ainda que 66% das crianças acessam a internet mais de uma vez por dia, principalmente pelo celular (83% dos entrevistados usam *smartphones* na hora de se conectar).

No que diz respeito a saúde, o tempo gasto ao celular pode ser prejudicial, já que 21% das crianças e adolescentes deixam de comer ou dormir por causa da internet e 17% dos entrevistados já fizeram buscas sobre formas de emagrecer.

Para os especialistas da Sociedade Brasileira de Pediatria, o ideal é limitar o tempo de exposição às mídias ao máximo de uma hora por dia, isso, para crianças entre 2 a 5 anos de idade. Para os adolescentes é preciso ficar de olho e não os deixar isolados nos seus quartos ou permitir que ultrapassem as horas saudáveis de sono para ficar na internet

Fonte <https://esbrasil.com.br/menores-deixam-comer-dormir-internet/>



# Sinais de Atenção!



## Sinais de Atenção



- Cansaço, sonolência e desânimo em horários que não são destinados ao sono;
- Insônia e pesadelos frequentes;
- Se opõe a frequentar locais que não possuem acesso à internet;
- Não realiza outras atividades de lazer ou esportes para permanecer na internet;
- Deixa de executar suas atividades (estudo, deveres domésticos, asseio próprio) para permanecer na internet;
- Limita suas amizades aos relacionamentos virtuais;
- Baixo rendimento escolar;
- Isolamento das rotinas familiares e festivas.
- Comportamento retraído na presença de outras pessoas.
- Aversão ao convívio social presencial;
- Resistência à frequentar o colégio.

Tais circunstâncias podem indicar tanto o uso excessivo da internet, inclusive uma ciberdependência ou, ainda, evidenciar que a criança ou o adolescente pode estar sendo vítima de alguma prática abusiva ou criminosa.

*“A dependência do uso excessivo da Internet, de acordo com os novos levantamentos, caracteriza-se como uma incapacidade que o sujeito possui para reprimir e controlar impulsos para usar a internet, provocando desconforto e sentimentos de culpa.... CIBERDEPENDÊNCIA: O PAPEL DAS EMOÇÕES NA DEPENDÊNCIA DE TECNOLOGIAS DIGITAIS.*

fonte: <http://periodicos.letras.ufmg.br/index.php/textolivre>.



# Ameaças, riscos e crimes

# Ameaças, riscos e crimes

Ao utilizar a internet, seja para pesquisa, para acessar e-mails, aplicações, softwares ou redes sociais, a criança e adolescente deve ter conhecimento dos tipos de ameaças ou riscos que podem lhe trazer diversos prejuízos, como o uso indevido dos seus dados pessoais (nome, imagem, idade, apelido, ...) e arquivos ou mesmo a captura de dados pessoais de terceiros, como dos próprios pais e/ou responsáveis, sobretudo, no uso de equipamentos compartilhados entre os membros da família.

Os riscos e ameaças mais comuns no uso da internet são fraudes, crimes e espionagem, os quais são praticados mediante o uso de MALWARES (software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores) fonte:

<https://pt.wikipedia.org/wiki/Malware>



# Ameaças, riscos e crimes

Os malwares mais comuns são: vírus, spyware, worm, ransomware, adware, trojan, screenlogger, keylogger, backdoor, rootkit, bot e o uso de engenharia social como o phishing.

São muitos os tipos de riscos, ameaças e crimes praticados na internet, muito direcionados ao público infantil. Exemplo:

A **TURMA DA Mônica** está procurando um novo amigo!



Quer fazer parte da turminha?

Tudo o que você tem que fazer é comentar:

1. o número do cartão de crédito da mamãe
2. os 3 numerozinhos atrás
3. a data de expiração

fonte: <https://www.agazeta.com.br/es/gv/criminosos-usam-turma-da-monica-para-aplicar-golpes-em-criancas-0919>

## Ameaças, riscos e crimes

*É essencial que as crianças e adolescentes sejam orientados sobre as ameaças existentes e suas consequências no uso da internet, tanto na condição de vítimas como na condição de criminosos, apresentando-se como haters, hackers, crackers ou mesmo apenas como usuários mal orientados.*



## Ameaças, riscos e crimes

Em razão do crescente número de danos gerados a outras pessoas, inúmeras leis forma surgindo ao longo do tempo, a fim de tornar determinados comportamentos em ações ilícitas, ou seja, tornar CRIME, cabendo aos pais e/ou responsáveis ter conhecimento e orientar as crianças e adolescentes sobre situações em que podem ser vítimas e, também, nas quais poderão atuar em ação tipificada como crime.



## Ameaças, riscos e crimes



São considerados crimes no Brasil:

- Falsificação e supressão de dados. (Arts.155, 297, 298, 299, 313-A, 313-B do Código Penal)
- Invasão de dispositivo informático e furto de dados. (Art.154-A do Código Penal)
- Cyberbullying - veiculação de ofensas em blogs e comunidades virtuais - (Arts.138, 139, 140 do Código Penal)
- Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional (Art.20 da Lei n°7.716/1989)
- Ameaça (Art.147 do Código Penal)
- Stalking (Art.147-A do Código Penal)
- Crimes contra a propriedade intelectual, artística e de programa de computador. (Art.184 do CP e Lei n°9.609/1998)
- Estelionato e Furtos eletrônicos - Fraudes Bancárias- (arts.155 §§3º e 4º, II, e 171 do Código Penal)
- Incitação e apologia de crime. (Arts.286 e 287 do Código Penal)
- Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infanto-juvenil. (Arts.241 e 241-A, 241-B do ECA- Lei n°8.069/1990)



## Ameaças, riscos e crimes

São considerados crimes no Brasil:

- Falsidade Ideológica (Art. 307 do Código Penal)
- Violação de Direito Autoral (Art.184 do Código Penal)
- Crime de Calúnia (Art. 138, Código Penal)
- Crime de Difamação (Art. 139 do Código Penal)
- Crime de Injúria (Art. 140 do Código Penal)
- Tráfico de Drogas (Art. 33 da Lei n.º 11.343 de 2006)
- Divulgação de Segredo (Art. 153 do Código Penal)
- Dano (Art. 163 do Código Penal)



# Orientação e prevenção são o melhor remédio



# Orientação e prevenção são o melhor remédio!



Cientes de toda essa complexidade e responsabilidade, algumas ações são recomendáveis aos pais e responsáveis:

## Quanto ao uso de dispositivos:

- Estabelecer horário e/ou limites para uso dos dispositivos;
- Configurar o acesso com uso de senha;
- Possuir antivírus;
- Instalar firewall e AntiSpam;
- Utilizar ferramentas de controle parental;
- Manter atualizados os softwares e seguir as orientações dos fabricantes;
- Possuir rotina de backup de informações, arquivos, fotos e vídeos;
- Compartilhar o uso dos dispositivos apenas com seus familiares e desde que haja relação de confiança;
- Orientar para que as crianças e adolescentes não realizem downloads de softwares sem se certificar da procedência;
- Orientar para que as crianças e adolescentes não realizem qualquer forma de manutenção no equipamento sem o conhecimento técnico necessário à sua preservação;
- Procurar não manter os equipamentos em quartos, salas ou ambientes que dificultem a fiscalização;
- Orientar sobre o uso de câmeras, evitando o uso para captação de imagens ou vídeos de outras pessoas, ou com conteúdo íntimo;
- Ao utilizar equipamentos de uso compartilhado, como computadores do Colégio ou em Lan Houses, tomar o cuidado para não salvar senhas de forma automática e encerrar sessões.



# Orientação e prevenção são o melhor remédio!



## Quanto às redes sociais e aplicativos:

- Identificar quais redes sociais são utilizadas pelas crianças e adolescentes;
- Identificar quais aplicativos são utilizados pelas crianças e adolescentes;
- Verificar as Políticas de Privacidade dos sites, aplicações e redes;
- Observar as faixas etárias indicadas para o uso das mídias digitais;
- Realizar a configuração de perfil, certificando-se de fornecer apenas as informações necessárias para uso da rede social ou aplicação;
- Realizar configuração de perfil, limitando o acesso somente à rede de amigos;
- Consultar o conteúdo de publicações realizadas no perfil das crianças e adolescentes, verificando se não há exposição indevida de imagem, intimidade ou informações que gerem vulnerabilidades, tais como check-in, informações relacionadas à rotina, como horários e nomes de familiares;
- Orientar o uso de cartões de crédito ou uso de dados de outras pessoas na internet;
- Orientar a criação de senhas seguras;
- Orientar sobre postagens e compartilhamento de informações, certificando-se de sua veracidade, evitando, assim, injustiças, calúnias e inverdades (fakenews);

# Orientação e prevenção são o melhor remédio!



## Quanto às redes sociais e aplicativos:

- Orientar sobre como se manifestar, utilizando linguagem respeitosa e educada;
- Orientar quanto à publicação de conteúdos ofensivos, difamatórios ou que ridicularizem ou prejudiquem a honra e/ou reputação de outras pessoas. Cuidado com o Cyberbullying!;
- Orientar quanto à publicação, divulgação ou compartilhamento de fotos e vídeos de outras pessoas, sem a autorização destas;
- Orientar quanto ao uso de câmera (não permitir ser filmado ou fotografado) e pedidos de envio de “nudes”;
- Orientar sobre conversas e troca de informações, links e arquivos com pessoas estranhas ou perfis duvidosos;
- Orientar sobre direitos autorais na internet, citando a fonte ou a referência do conteúdo utilizado, a fim de preservar a sua autoria ao criar seus próprios conteúdos;
- Orientar para não gravar, fotografar ou printar imagens, vídeos ou sons das atividades desenvolvidas em ambiente coletivo, como a escola, clubes, colhidas sem autorização dos colegas, profissionais envolvidos e da Direção do local;
- “Cyberbullying é um termo da língua inglesa utilizado para caracterizar a prática agressiva de intimidações e perseguições no ambiente virtual.” <https://brasilecola.uol.com.br/sociologia/cyberbullying.htm>.

# Conclusão





## Conclusão

Como se pode perceber, o cuidado com o uso das tecnologias e das mídias digitais em geral diz respeito não só à saúde, como a integridade física, emocional e patrimonial das crianças e adolescentes, tornando-se essencial a atenção de pais e/ou responsáveis na educação, orientação e condução quanto ao uso, riscos, ameaças e as consequências dos atos praticados ou da ausência de cuidado.

O compromisso com a proteção da privacidade e da segurança de todos nós, a responsabilidade pela divulgação de informações verídicas, cabe a toda a sociedade.

O exemplo é a melhor forma de ensinar e orientar nossos pequenos e jovens adultos sobre aquilo que realmente importa.

A tecnologia e a inovação são maravilhas que devem ser bem aproveitadas, resguardando direitos e preservando vidas e jamais substituirão o ser humano naquilo que somente ele pode proporcionar ao próximo: amor, compreensão, carinho.

Cuide dos seus. Cuide dos nossos!



# SMARTE

CAMILA SALLES DOS SANTOS

[www.smartestrategias.com.br](http://www.smartestrategias.com.br)

siga as nossas redes sociais

