PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina

Gabinete da Presidência
Conselho de Segurança Institucional

CARTILHA DE SEGURANÇA COMPORTAMENTAL NA INTERNET

Sumário

1 Introdução

O emprego da tecnologia e da internet exclusivamente nas atividades profissionais tornou-se uma discussão vencida já no fim da década de noventa. Do início dos anos dois mil até hoje a evolução das conexões, softwares e hardwares tem permitido o desenvolvimento de dispositivos e aplicativos que multiplicaram exponencialmente o tempo que passamos interagindo com o mundo virtual, tornando-nos altamente dependentes desses avanços.

Como consequência natural dessa dependência tecnológica, a exposição de dados profissionais e pessoais se tornou inevitável, gerando até mesmo um nicho de mercado próprio (*data markets*), que foi objeto de regulamentação por meio da Lei Geral de Proteção de Dados Pessoais (LGPD).

A forma como as pessoas se comunicam, sejam contatos profissionais, pessoais ou familiares, mudou radicalmente em razão das redes sociais e dos aplicativos

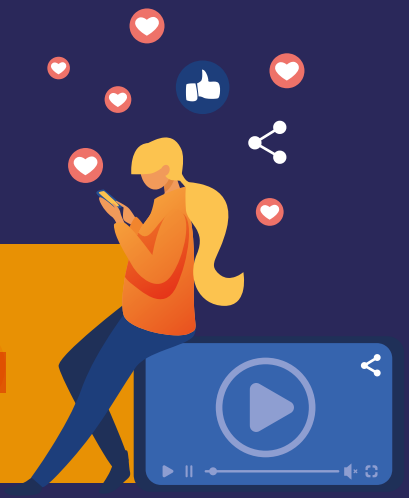
de mensageria, fazendo com que o conteúdo de conversas, publicações e interações nesses ambientes atraíssem a atenção das *Big Techs* e de toda a indústria, sob o pretexto de otimizarem a oferta de produtos direcionados.

Contudo, a exposição do nosso dia a dia, de hábitos, de gostos e de locais que frequentamos, comportamentos confidenciados tão somente em diários pessoais em tempos passados, tornou-se a regra e, de certa forma, passou a exercer até mesmo certa pressão psicológica e sensação de anacronismo para muitos pela não adequação à modernidade.

Sob esse contexto emerge a preocupação com a segurança pessoal, e não mais puramente cibernética, como já abordada na Cartilha de Segurança Cibernética (2020), desenvolvida pelo Núcleo de Inteligência e Segurança Institucional (NIS) do TJSC.

Assim, desta vez, apontam-se comportamentos pessoais e familiares que podem comprometer a segurança física de magistrados e servidores, a fim de mitigar os riscos e potenciais ameaças, prevenindo e reduzindo a vulnerabilidade do ativo mais importante do Poder Judiciário: as pessoas.

2 Dados captados



> “Quando o serviço é gratuito, o produto é você!”

As *Big Techs* (Apple, Microsoft, Alphabet, Amazon, Tesla, Meta, IBM, Samsung, HP, Sony, LG, Google, etc.) estão constantemente despejando produtos e serviços no mercado de tecnologia, em sua grande parte gratuitos.

Não há problema algum em utilizar um serviço ou produto gratuito. Entretanto, é importante que se saiba que, para utilizá-los, é necessária a aceitação dos seus termos de uso e política de dados, o que permite às empresas a captação de informações pessoais das mais diversas naturezas, que indubitavelmente terão caráter comercial.

A título de exemplo, veja os seguintes trechos extraídos dos “Termos de Serviço” da empresa Meta Platforms, Inc. (Facebook):

> *Não cobramos você pelo uso do Facebook ou de outros produtos e serviços cobertos por estes Termos. Em vez disso, empresas e organizações nos pagam para lhe mostrar anúncios de seus produtos e serviços. Quando você usa nossos produtos, concorda que podemos mostrar anúncios que consideramos relevantes para você e seus interesses. Usamos seus dados pessoais para ajudar a determinar quais anúncios mostrar.*
>
> *[...] Nossa Política de Dados explica como coletamos e usamos seus dados pessoais para determinar alguns dos anúncios que serão exibidos e fornecer todos os outros serviços descritos abaixo.*

Cada plataforma, rede social, aplicativo ou serviço via web possui os seus próprios termos de uso e política de dados e capta informações diferentes dos seus usuários. Por isso, é muito importante a leitura quando da instalação ou primeira utilização desses serviços ou produtos, seja para anuir ou discordar, deixando de utilizá-los caso não seja conveniente.

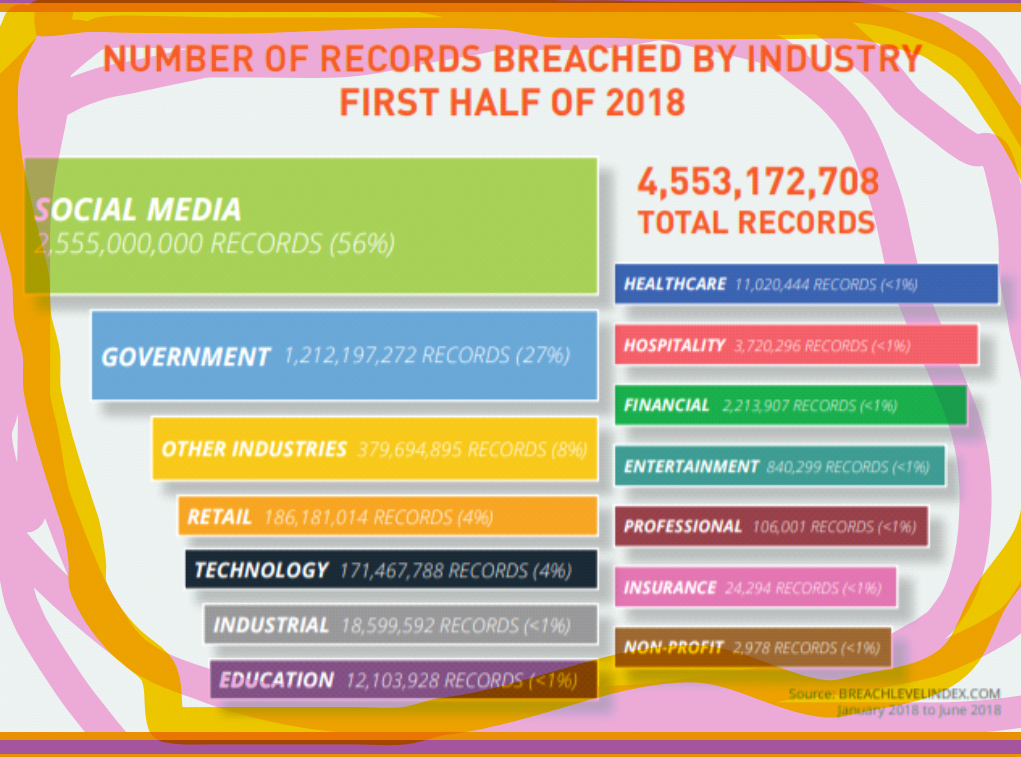
Considerando a opção pela sua utilização, sugere-se a adoção de medidas preventivas e mitigadoras das informações fornecidas já no cadastro inicial. Isso porque, apesar da grande maioria das *Big Techs* serem empresas de confiança, não se pode desconsiderar a hipótese de funcionários mal-intencionados ou cooptados por organizações criminosas repassarem esses dados.

Os aplicativos de entregas, como o 99 Food e iFood, por exemplo, captarão o seu nome, CPF (quando aplicável), e-mail, endereço de entrega, número de telefone e preferências para contato. Pelo menos o nome e o endereço estarão acessíveis aos entregadores, para que, obviamente, consigam realizar a entrega.

Assim, em razão da natureza dos serviços prestados pelo Poder Judiciário, principalmente no caso dos magistrados, uma medida paliativa é cadastrar a conta com os dados de um familiar, já que, com uma simples pesquisa em fontes abertas, é possível identificar a atividade profissional do usuário.

Ainda, não se deve esquecer dos constantes vazamentos de dados em razão das atuações de *crackers* justamente para alimentação dos *datamarkets* ilegais. Durante o período da pandemia de covid-19 ocorreram vazamentos de *database* do Banco Central (chaves Pix), Ministério da Saúde (DataSUS), Netshoes, Enel e Mercado Livre, que expuseram dados de duzentos e vinte e três milhões de usuários.

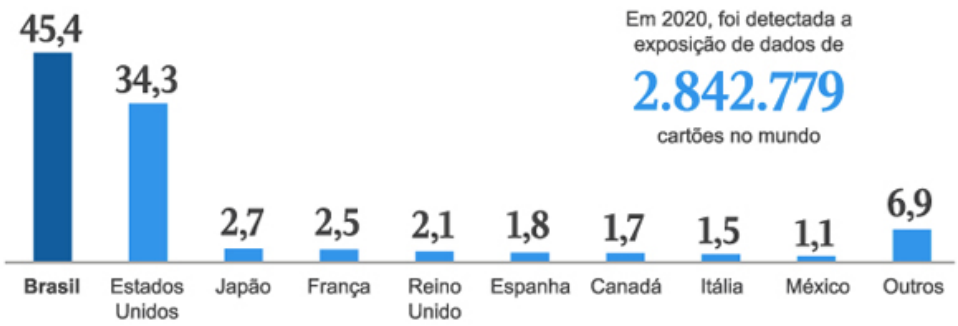
Estudo da Gemalto, uma das maiores companhias de segurança digital do mundo, considerou as redes sociais como um dos **ambientes mais inseguros para informações.**



Redes Sociais lideraram números de dados vazados do primeiro semestre de 2018 (Foto: Canaltech)

De acordo com o Relatório Anual 2020 de Atividade Criminosa *On-line* no Brasil, elaborado pela empresa de cibersegurança Axur, naquele ano o Brasil foi o campeão em vazamentos de dados de cartões, acumulando sozinho 45,4% do total de casos registrados no mundo, distante do segundo colocado, os EUA, com 34,3%, razão pela qual se recomenda, sempre que possível, geração de cartão virtual para cada compra *on-line*.

Países com mais cartões de crédito e débito vazados on-line no ano de 2020 (Em %)



Em 2020, os dados de cartões de crédito vazados no Brasil foram quase metade de todo o mundo.

A UTILIZAÇÃO DE CARTÃO VIRTUAL DIMINUI A POSSIBILIDADE DE "CLONAGEM"

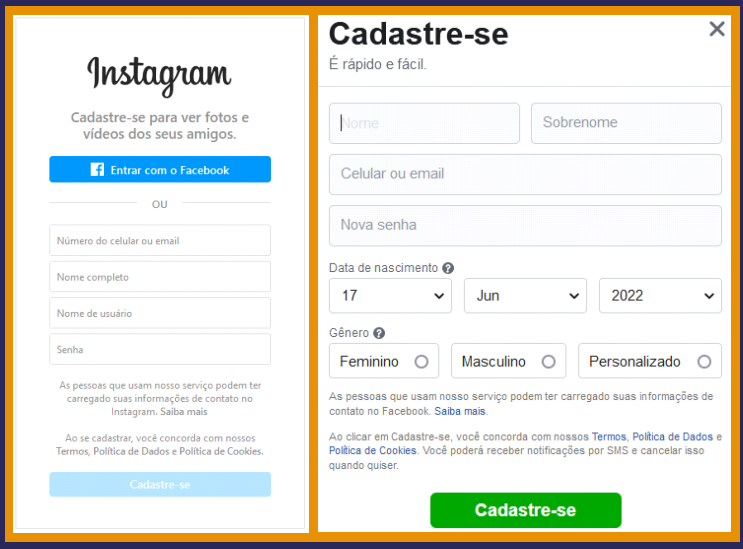
O cartão de crédito virtual só pode ser gerado e usado digitalmente, pelo aplicativo do banco ou *internet banking*. Como pode ser de uso único, ser excluído após o uso e, dependendo do banco, ter seu limite máximo fixado, diminui as chances de golpes e fraudes.

3 Os cuidados já começam nos cadastros iniciais

Preencher alguns campos com dados incompletos, como apenas parte do nome, informar apenas um e-mail, e não o telefone, criar uma conta de e-mail exclusivamente para esse tipo de cadastro, utilizar abreviações, apelidos, etc., são medidas altamente recomendáveis.

Nesse caso, não se está a incentivar a prática de falsidade ideológica, mas, sim, de omitir determinados dados, quando possível, a fim de dificultar a busca ilegal de informações sobre o usuário.

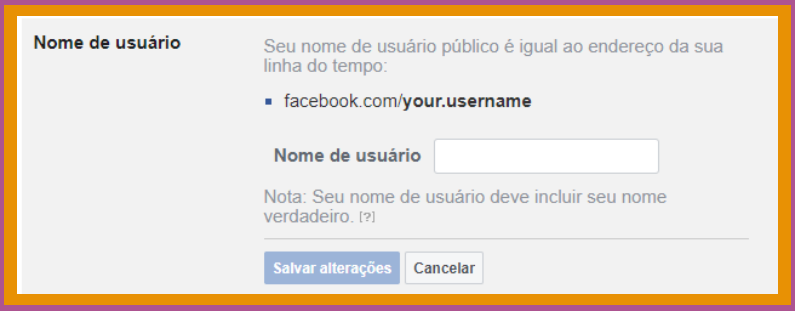
CADASTRO INICIAL NAS REDES SOCIAIS FACEBOOK/INSTAGRAM



Sugestões:

- Omitir o nome completo. Ex.: em vez de Mark Elliot Zuckerberg, “Mark Elliot” ou “Mark Zuckerberg”.
- Utilizar apelidos ou formas pelas quais é conhecido, desde que seja variação do nome. Ex.: Eduardo – Edu, Marcos – Marquinhos.
- Evitar digitar o nome e o sobrenome em sequência.
- Não informar o número de telefone caso seja possível.
- Criar uma conta de e-mail exclusivamente destinada aos cadastros e recuperação de senha de redes sociais.

CONFIGURAÇÕES GERAIS DA CONTA FACEBOOK – NOME DE USUÁRIO

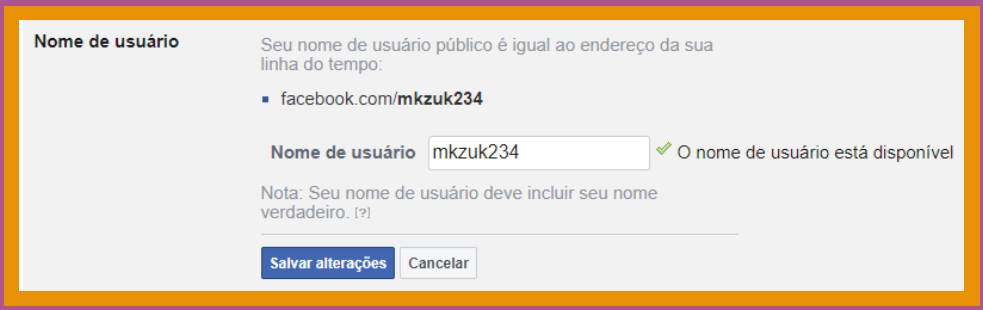


Quando a plataforma permitir a escolha do nome de usuário ou de *link* do perfil, não se deve vinculá-los a dados reais.

Sugestões:

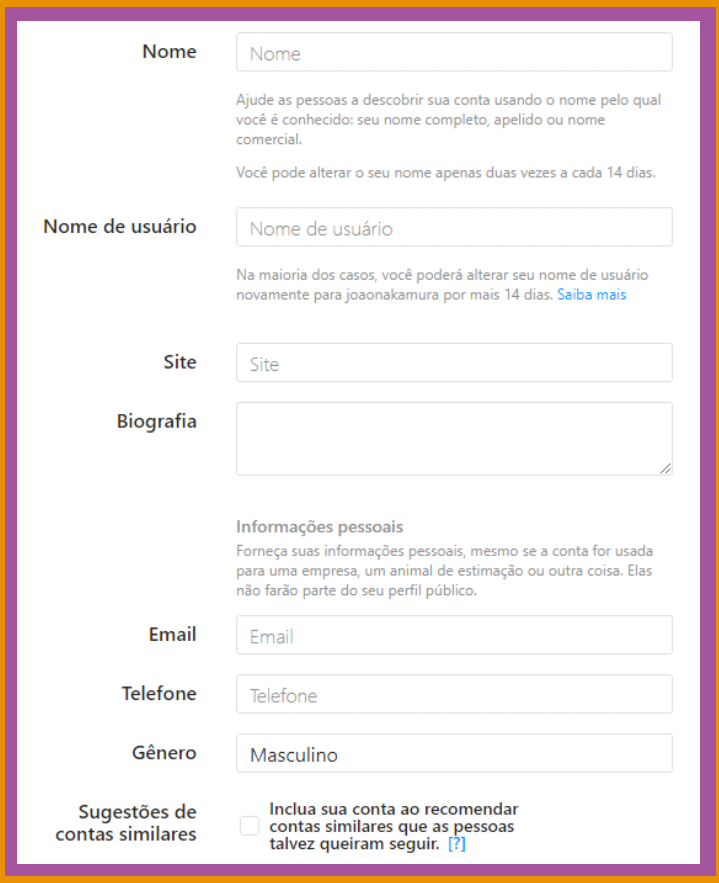
- Não utilizar o nome completo.
- Não utilizar datas de nascimento.
- Utilizar abreviações ou apenas iniciais dos prenomes, nomes e sobrenomes.

Um bom exemplo para o usuário “Mark Zuckerberg” seria:



Configurações gerais da conta facebook – sugestão de nome de usuário (link de perfil)

CONFIGURAÇÕES GERAIS DA CONTA INSTAGRAM



Omitir, sempre que possível, todo e qualquer dado solicitado, desde que isso não implique violação aos termos e condições de uso do serviço.

No caso do Instagram, considerados os campos de cadastro da imagem acima, a publicação de informações como site, biografia, e-mail e telefone não é obrigatória e deve ser evitada, pois todo e qualquer dado serve de

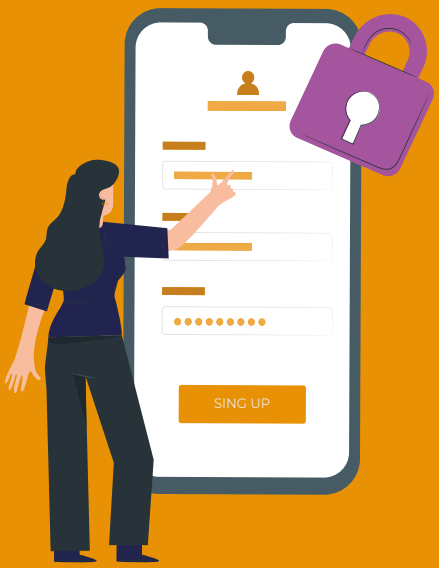
referência para pesquisa e confirmação de identidade por terceiros.

Também se sugere a não marcação da caixa “Inclua sua conta ao recomendar...”, a fim de evitar que o seu perfil de usuário seja sugerido a outras pessoas para interação.

O ideal é que os seus perfis nas redes sociais sejam visualizados e sejam objeto de interação somente pelas pessoas que realmente façam parte do seu círculo de interesses.

Ainda, se possível, não escolha uma foto perfil, uma imagem que identifique de plano o seu rosto nestes aplicativos.

Apesar de sentir orgulho da sua profissão, seja magistrado ou servidor, não se deve especificá-la, a não ser que seja obrigatório, sugerindo-se o emprego de nomenclaturas genéricas como “servidor público estadual” em vez de “juiz, magistrado, desembargador, oficial de justiça, serventuário da justiça, auxiliar do Poder Judiciário”. Esta recomendação vale para todo e qualquer cadastro.



Caso não viole os termos e condições de uso, omita a maior quantidade de informações possível.

4 Muito cuidado com o conteúdo das publicações *(posts)*

O conteúdo das nossas publicações revela muito mais do que gostaríamos. Através deles podem-se identificar padrões de consumos, localizações, relacionamentos pessoais e familiares, telefones e até mesmo residências.

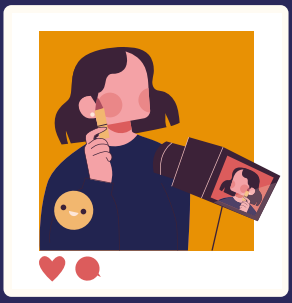
Fotografias, vídeos e transmissões ao vivo (*lives*) feitas em nossas residências, indiretamente podem expor não somente bens e valores que possuímos, mas também a arquitetura e sua localização, atraindo olhares indesejados.

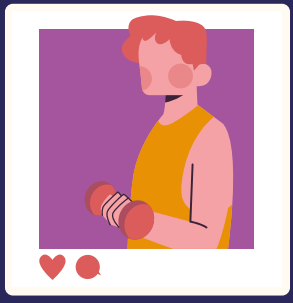
O uso de *#hashtags* deve ser evitado, pois permite que a publicação seja listada de forma acessível a todos. Ainda que o perfil seja privado, caso a publicação contenha menções ou marcações de outros usuários em que as postagens sejam públicas, a utilização de uma *#hashtag* permitirá a visualização por terceiros não desejados.

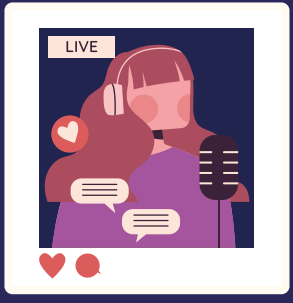
A soma dessas publicações no *feed* (espaço da página principal que oferece visão geral dos posts mais recentes) fornece pequenas peças para a montagem de um quebra-cabeças que permite aos criminosos a obtenção de dados que passam despercebidos no cotidiano.

A mesma cautela deve ser empregada em serviços de mensageria (WhatsApp, Telegram, Signal, etc.), principalmente quando da sua publicação em grupos e no *status* de usuário.

Uma simples publicação como “estou de férias” traz como consequência lógica o raciocínio de que a pessoa não será encontrada no trabalho ou de que a sua residência poderá estar vazia, o que facilita um plano de furto.

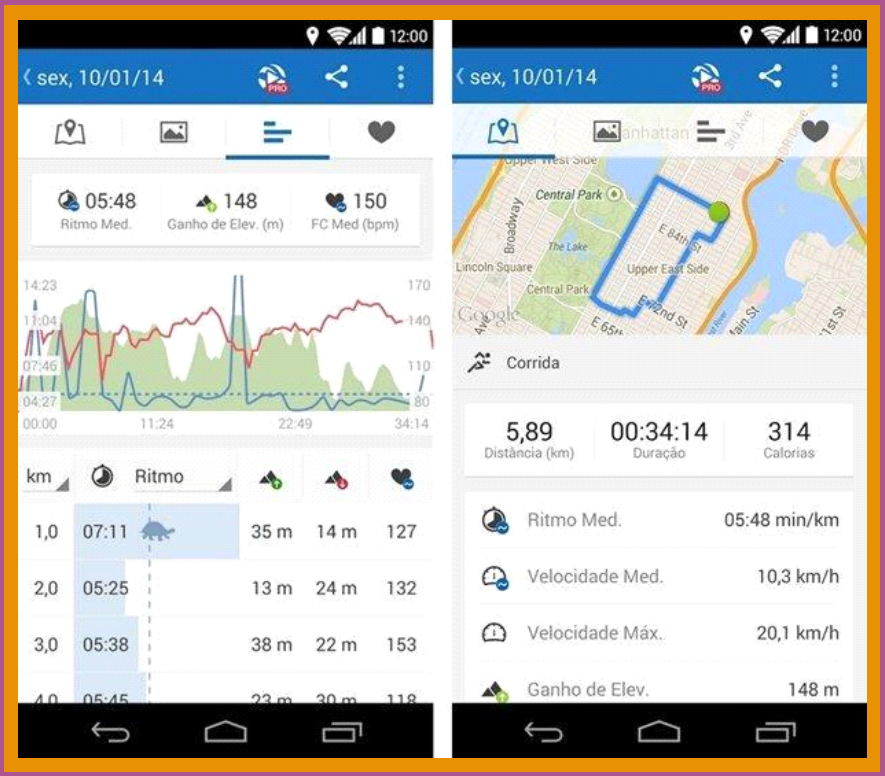






Redes sociais como Twitter, TikTok e Instagram, por vezes, acabam funcionando como um diário da vida pessoal. Não é difícil encontrar publicações de usuários que expõem constantemente os seus restaurantes preferidos,

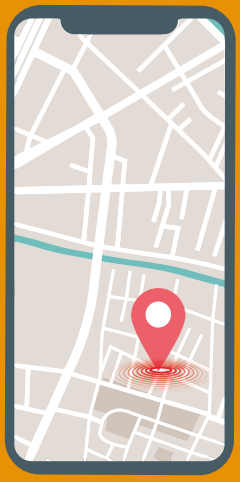
cafeterias, academias e *print-screens* de aplicativos que registram a prática de exercícios físicos (Runtastic, Google Fit, MiFit, Strava, RunKeeper, Nike Run Club, MapMyRun, Map My Tracks, 10K Runner, etc.) Publicações como essas permitem a identificação dos hábitos pessoais, como o horário e a rotina (corridas, caminhadas e pedaladas), e até mesmo a exata localização do trajeto percorrido.



Muitas vezes, os aplicativos possuem atrativos inclusive financeiros, como o Sweatcoin e Step'n, que chegam a remunerar atividades físicas por meio de criptoativos como forma de atrair utilizadores. Entretanto, deve-se tomar cuidado com as postagens.

Outro comportamento não recomendado é fazer *check-in* em uma conta de rede social, o que é exigido para acessar a rede wi-fi de alguns estabelecimentos comerciais. Ao fazer o *check-in*, o local onde se encontra o usuário será informado em alguma rede social. Caso seja necessária conexão com a internet por esse meio, imediatamente após a publicação na rede social, recomenda-se excluí-la a fim de minimizar a exposição.

Aplicativos como o Foursquare devem ser evitados, pois, uma vez que o *check-in* é efetuado, a sua localização exata será publicada em todas as redes sociais vinculadas.



5 Interações

Interações como curtidas, comentários e republicações, assim como seguir certos perfis, exprimem sentido conotativo, como preferências políticas, ideológicas, gostos, padrões de consumo e relacionamentos próximos.

Da mesma forma, recomenda-se a não participação ou a utilização de pseudônimos em grupos de discussão abertos, incluindo-se os fóruns, que não são propriamente redes sociais.

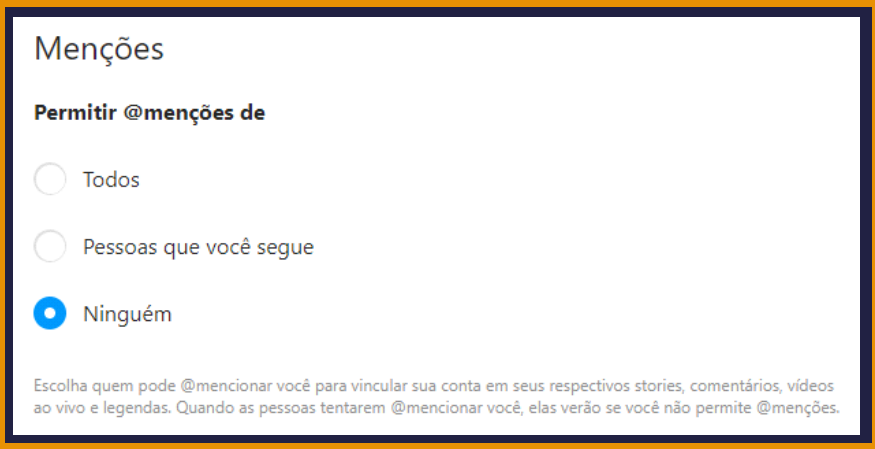
Uma análise rápida das interações pode permitir a identificação dos colegas de trabalho, familiares e amigos, cujos perfis nas redes sociais podem estar abertos (não privados) e, portanto, ser acessados livremente.

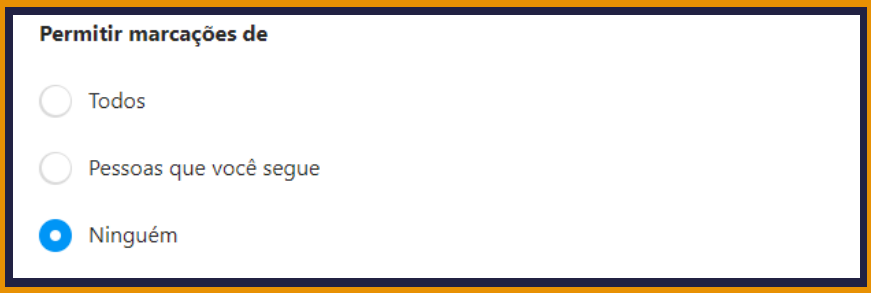
Fatores como esses podem facilitar ataques pessoais, inclusive físicos, se conjugados com a existência de outras informações.

Portanto, recomenda-se:

- evitar comentários que revelem o grau de parentesco com familiares, principalmente caso eles possuam uma conta pública;
- conversar com os familiares e amigos mais próximos e esclarecer sobre a importância de se diminuírem as exposições; e
- comunicar a amigos e, principalmente, familiares que muita exposição em redes sociais pode torná-los alvos indiretos na busca de intimidação de magistrados e servidores do Poder Judiciário.

Além de manter as contas nas redes sociais como privadas, uma boa prática consiste em não permitir a marcação do perfil ou menções em *posts* publicados por terceiros, bem como o compartilhamento de *stories*.



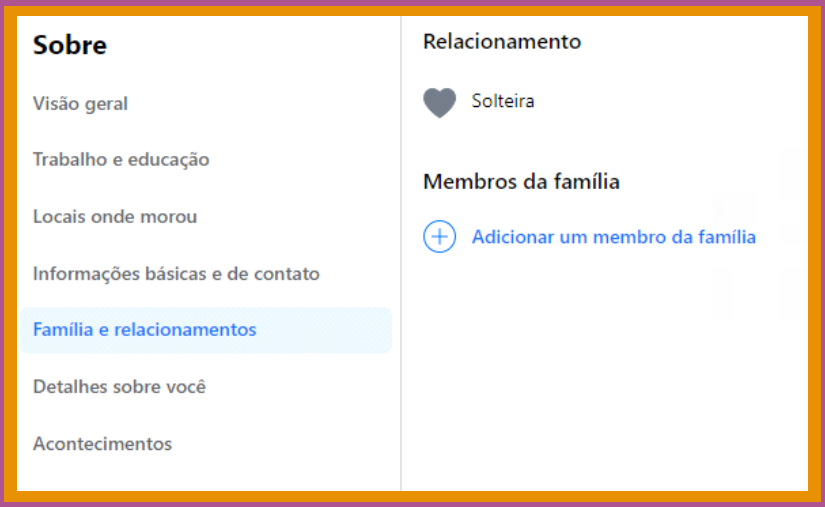


CONFIGURAÇÕES DE PRIVACIDADE E SEGURANÇA – INSTAGRAM

No Instagram é possível criar uma lista de amigos próximos e compartilhar o *story* somente com as pessoas que estão nessa lista, o que restringe o alcance da publicação.

Essa lista pode ser atualizada a qualquer momento, e as pessoas não serão notificadas quando adicionadas ou removidas, o que evita qualquer constrangimento.

Um comportamento bastante negligenciado no Facebook é a identificação de familiares e relacionamentos, que acaba por fornecer os nomes e perfis de mães, pais, tios(as), primos(as) e *status* de relacionamento amoroso. Isso facilita a obtenção de informações de forma indireta.



CONFIGURAÇÕES – SOBRE – FAMÍLIA E RELACIONAMENTOS

Por não ser um requisito obrigatório para utilização do Facebook, recomenda-se não informar esses dados. Ainda assim, caso se opte por essas vinculações, deve-se lembrar de manter essas informações disponíveis apenas aos amigos nessa rede social.

- Sempre se deve negar pedido de amizade de pessoa desconhecida e bloquear aquelas que parecem *fakes* (perfis falsos).

Soluções para a promoção de relacionamentos íntimos, como Tinder, Dobradiça, Grindr, Coincidir, Bumble, Inner Circle e Happn, devem ser evitadas, principalmente pelos magistrados. Em razão da sua condição pública, a identificação do seu perfil pode atrair não somente golpistas, mas também assaltantes, sequestradores e pessoas descontentes com decisões judiciais.

Aplicativos de transportes como Uber, Waze Carpool (carona), 99 App, Indriver, etc., além dos cuidados mencionados quando da realização do cadastro, merecem atenção.

O fornecimento e a utilização de caronas, apesar de serem uma boa iniciativa, devem ser evitados com pessoas desconhecidas.

Durante a utilização do Uber, 99 App, Indriver e até mesmo taxis convencionais, conversas que revelem sua profissão, período em que estará fora de casa e local de trabalho não são recomendadas. Se possível, sempre que se utilizarem esses serviços, deve-se dar preferência para entrar e sair do automóvel em local próximo de onde se encontra e para onde vai.

6 Estudo de caso – Marcelo Pecci, promotor paraguaio morto na Colômbia

As recomendações feitas até o momento podem parecer exagero, preciosismo ou até mesmo “neurose”. Entretanto, casos como o do promotor encarregado da Unidade Especializada de Crime Organizado e Narcotráfico do Ministério Público do Paraguai, Marcelo Pecci, revelam a necessidade de cuidados com as exposições na internet.

Sua esposa, Claudia Aguilera, publicava seu dia a dia no Instagram, com perfil aberto, expondo momentos íntimos e informando, inclusive, locais que iria frequentar.

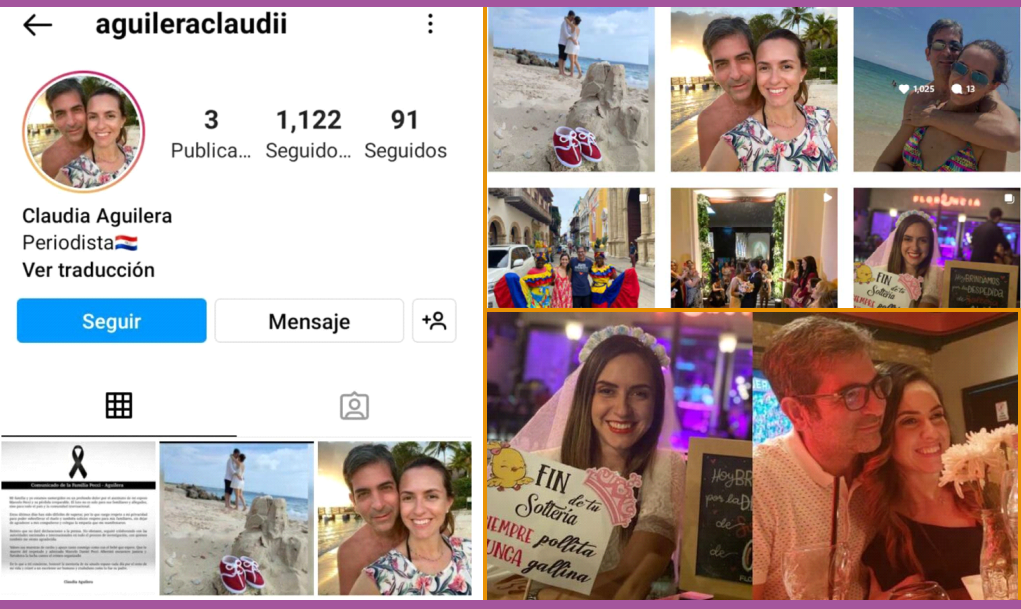


Foto: Instagram @aguileraclaudi

Considerada uma das jornalistas mais populares do Paraguai, Claudia possivelmente encarava sua exposição como algo natural. Inclusive, havia anunciado no periódico Hoy o local em que ocorreria a cerimônia e a recepção dos convidados para seu casamento, Parroquia San José de Asunción e Gran Hotel del Paraguay.

Ainda na mesma publicação, o destino e a data da lua de mel do casal acabaram sendo divulgados:

> *"Como destino de Luna de Miel, eligieron Colombia, y el 4 de mayo viajarán específicamente a Cartagena y Barú."*

A matéria revela a escolha do casal para desfrutar a lua de mel, as cidades de Cartagena e Barú, na Colômbia, a partir de 4 de maio.

Em outra publicação da imprensa paraguaia, Claudia revelou a data da cerimônia, 30 de abril.

O promotor Marcelo Pecci acabou sendo assassinado em 10 de maio de 2022, justamente durante a lua de mel, na ilha de Barú, perto de Cartagena de Índias, local publicado pela imprensa dias antes.

De acordo com as informações da imprensa internacional, duas pessoas se aproximaram em um jet-ski e, ainda da água, abriram fogo contra o promotor.

"Pecci havia se casado com a jornalista Claudia Aguilera no dia 30 de abril. Horas antes do assassinato, ela havia anunciado em uma rede social que os dois esperavam o primeiro filho."

Fotos: Instagram @aguileraclaudi

Fotos: Instagram @aguileraclaudi

Como se pode observar, Claudia Aguilera tinha o hábito de publicar no Instagram as suas localizações praticamente em tempo real.

Segundo o procurador-geral colombiano, Francisco Barbosa Delgado, ***"os assassinos seguiram os passos de Pecci, na Colômbia, pelas postagens do promotor nas redes sociais. Eles disseram que por vezes se perderam, mas conseguiram se localizar graças às publicações nas redes sociais"***.

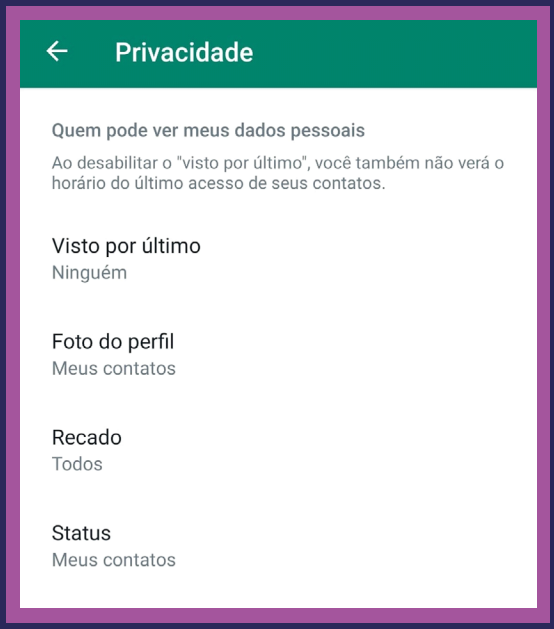
De acordo com a Polícia da Colômbia, **uma organização criminosa brasileira** já havia tentado assassinar o promotor Pecci no Paraguai, o que denota que esse tipo de técnica investigativa por parte dos criminosos também é praticada em território nacional.

7 Recomendações extras

- **Privacidade no WhatsApp**

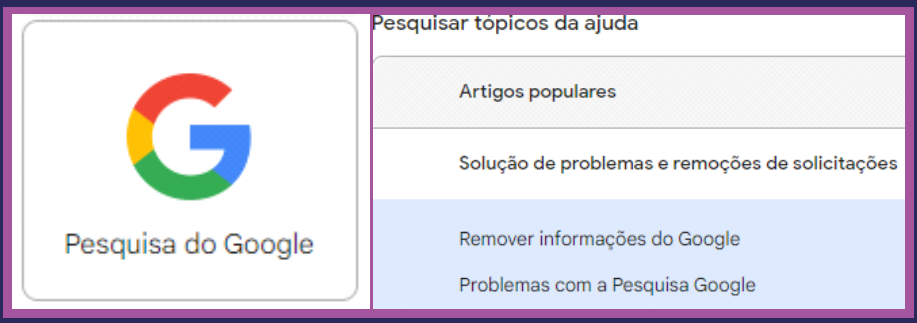
Assim como recomendado em outras redes sociais, se possível, deve-se evitar a utilização de uma foto que exponha o rosto no WhatsApp e em outros aplicativos de mensageria, ou que ao menos sua visualização esteja restrita aos contatos da agenda. Para tanto, seleciona-se em Configurações Privacidade/Foto do Perfil a opção “Meus contatos”.

Recomenda-se a adoção da mesma postura em relação ao *status*, que funciona de maneira similar aos *stories* do Instagram: Configurações Privacidade/Status, opção “Meus contatos”.



• **Excluir informações pessoais das pesquisas no Google**

Caso se deseje, também é possível ir um pouco além e excluir as informações dos resultados das pesquisas do Google. Para tanto, no suporte do Google, clica-se em "Pesquisa do Google" e removem-se as informações.



• **Google Alerts**

Outra ferramenta interessante, disponibilizada pela Google, consiste no monitoramento de publicações através do cadastramento de palavras-chave.

Caso seja inserido um nome completo, por exemplo, toda a vez que o mecanismo de pesquisa do Google identificar uma publicação que o mencione, será enviado um e-mail contendo o *link* em que foi inserida a menção.

8 Conclusão

As atividades desempenhadas por servidores do Poder Judiciário e, principalmente, pelos magistrados impactam diretamente na construção da sociedade e na vida dos jurisdicionados, muitas vezes gerando insatisfação quanto às suas expectativas.

Para que a magistratura seja exercida de maneira plena e independente é imprescindível a adoção de medidas de segurança, não somente no aspecto repressivo, quando a exposição aos riscos e ameaças já ocorreu, mas, principalmente, de forma preventiva.

Uma autoanálise comportamental no ambiente cibernético, com a adoção de posturas mitigadoras de exposição, apesar de parecer anacrônica e ir contra a ideia de maior interação nas redes sociais proposta pela enorme gama de aplicativos e serviços existentes, sem dúvida auxilia na prevenção, principalmente quando evita a identificação de alvos relevantes para o crime organizado.

É nesse sentido que estas recomendações foram elaboradas, a fim de que os Magistrados e servidores do Poder Judiciário compreendam que suas atividades são sensíveis e os expõem (inclusive familiares) a diversos riscos em razão da natureza das suas atividades profissionais.

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina

Gabinete da Presidência
Núcleo de Inteligência e Segurança Institucional

Projeto Gráfico: Assessoria de Artes Visuais - Núcleo de Comunicação Institucional