ANÁLISE DE PRIVACIDADE DE DADOS EM APLICATIVOS MÓVEIS

KELVIN MENDES DE ARAÚJO[1]
MARIA ALICE DE OLIVEIRA GUINO[2]
RENAN DA SILVA GOULART MOREIRA[3]
LUCIANO GONÇALVES DE CARVALHO[4]

RESUMO

O aumento do uso de sistemas computacionais e aplicativos móveis destaca questões cruciais sobre privacidade e segurança em um mundo interconectado. O trabalho visa avaliar vulnerabilidades na proteção de dados em aplicativos móveis, analisando como eles coletam e utilizam informações dos usuários. O uso da ferramenta MobSF (*Mobile Security Framework)* para análise estática na elaboração do artigo avaliou a conformidade dos aplicativos com os requisitos de política, fornecendo análises de segurança e permissões de acesso a dados pessoais. A análise destaca a importância de alinhar as permissões concedidas pelos usuários aos princípios de transparência, limitação de finalidade e consentimento do usuário estabelecidos pela LGPD (Lei Geral de Proteção de Dados), ressaltando a necessidade de práticas mais seguras na gestão de informações confidenciais em aplicativos móveis.
.

Palavras-chave: Aplicativos móveis; Dados; Privacidade; Vulnerabilidades.

ABSTRACT

The increasing use of computer systems and mobile applications highlights crucial issues regarding privacy and security in an interconnected world. This study aims to assess data protection vulnerabilities in mobile applications by analyzing how they collect and use user information. The use of the MobSF (Mobile Security Framework) tool for static analysis in this article evaluated the compliance of the applications with policy requirements, providing analysis on security and personal data access permissions. The analysis underscores the importance of aligning permissions granted by users with the principles of transparency, purpose limitation, and user consent established by the LGPD (General Personal Data Protection Law), emphasizing the need for safer practices in managing sensitive personal information within mobile applications.

Key words: Mobile applications; Data; Privacy; Vulnerabilities.

[1]Graduando, Tecnologia em Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP. E-mail: kelvin.araujo01@fatec.sp.gov.br
[2]Graduanda, Tecnologia em Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP.
[3]Graduando, Tecnologia em Análise e Desenvolvimento de Sistemas, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP.
[4]Docente, Faculdade de Tecnologia de Mogi das Cruzes – FATEC-MC. Mogi das Cruzes-SP.

INTRODUÇÃO

A crescente utilização de sistemas computacionais e aplicativos móveis está moldando as fronteiras de privacidade de dados, destacando questões cruciais sobre a proteção de informações pessoais e a garantia da segurança da informação em um mundo cada vez mais conectado e dependente da tecnologia.

Atualmente, é muito comum que os softwares requeiram acesso a informações pessoais dos usuários para poderem funcionar adequadamente e, uma grande parcela desses usuários desconhece os motivos ou mesmo o uso que será feito dessas informações, já que não leem as políticas de segurança, como demonstrado na pesquisa de Obar e Oeldorf-Hirsch (2020).

Este trabalho tem como objetivo a identificação e a análise de potenciais vulnerabilidades relacionadas à privacidade de dados em aplicativos móveis. Para tanto, será utilizada a ferramenta MobSF, conhecida por sua capacidade de identificar vulnerabilidades em aplicativos móveis e fornecer *insights* sobre os tipos de dados coletados e os riscos associados a essa coleta. Essas análises serão essenciais para avaliar se as práticas envolvidas na coleta de informações estão em conformidade com as regulamentações existentes no Brasil e na União Europeia, respectivamente a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre Proteção de Dados (GDPR, em inglês).

Os aplicativos selecionados para a análise por meio da ferramenta MobSF, incluem o e-Título, WhatsApp e Instagram, escolhidos com base em sua popularidade, medida pela quantidade de *downloads* na Google Play Store. Busca-se não apenas explorar os detalhes da coleta e do processamento de dados pessoais pelos aplicativos, mas também abordar os riscos inerentes à violação da privacidade.

FUNDAMENTAÇÃO TEÓRICA

Leis de Proteção de Dados

Em 2018, uma vulnerabilidade nos termos de uso do Facebook foi explorada pela Cambridge Analytica, empresa britânica de consultoria política. Essa falha permitiu o acesso a dados pessoais de milhões de usuários e de seus amigos, incluindo fotos, curtidas e participações em grupo. A partir de um teste de personalidade, foi solicitado acesso aos dados dos usuários, que, após concedido, foram coletados e utilizados como base para estratégias de segmentação e manipulação para as eleições presidenciais norte americana (MARTINS; TATEOKI, 2019). Esse incidente foi um dos fatores que impulsionaram o debate sobre a segurança dos dados em plataformas digitais. O uso indevido dessas informações para manipular usuários e influenciar eleitores trouxe a questão da privacidade para o centro das discussões, conforme destacado por Confessore (2018). Com a ocorrência de um novo incidente semelhante, a preocupação com o uso dos dados aumentou, e, no mesmo ano do escândalo, a GDPR foi sancionada, estabelecendo um padrão para o tratamento de dados no ambiente digital.

Em 25 de maio de 2018, foi instituída uma legislação que se tornou um marco global na proteção da privacidade de dados no cenário digital. O Regulamento Geral de Proteção de Dados (GDPR, em inglês) da União Europeia exige que todos os serviços *online* que lidam com dados de cidadãos europeus cumpram suas normas.

Não basta apenas informar quais dados estão sendo processados, é necessário dar ao usuário um controle total sobre as informações, como informado no Artigo 15º do capítulo III da GDPR.

> “O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento [...]” (UNIÃO EUROPEIA, 2016, Art. 15°).

No mesmo ano, em agosto, foi promulgada no Brasil a Lei n°13.709, conhecida como Lei Geral de Proteção de Dados (LGPD). Esta legislação definiu diretrizes para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais,

estabelecendo penalidades mais rigorosas para aqueles que não cumprem com os requisitos estabelecidos (BRASIL, 2018).

Uma vez que se baseou amplamente na GDPR, ambas compartilham conceitos e diretrizes semelhantes. Um aspecto fundamental da LGPD é a compreensão de que a privacidade está intrinsecamente ligada ao consentimento concedido pelo usuário (LORENZON, 2021). Consequentemente, é imperativo que os responsáveis pelo sistema solicitem esse consentimento de forma transparente e completa, assim como está fundamentado no Art 9º da Lei nº13.709:

> "O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso" (BRASIL, 2018, Art. 9°).

Muitas vezes, embora a maioria das aplicações móveis solicitem a permissão dos usuários durante a primeira utilização para lidar com os seus dados, os termos de uso que os definem são escritos de maneira excessivamente formal, com linguagem rebuscada, o que pode dificultar a compreensão do usuário sobre como a plataforma irá tratar as suas informações pessoais (JARDIM *et al*., 2022). Isso cria uma lacuna de clareza acerca dos métodos utilizados pelo aplicativo no tratamento dos dados dos usuários, o que entra em conflito com um dos pilares da LGPD: a transparência com o usuário.

Políticas de privacidade

As políticas de privacidade em aplicativos móveis servem como documentos essenciais que articulam como um aplicativo coleta, usa e protege os dados do usuário. Estas políticas são cruciais para estabelecer transparência e confiança entre desenvolvedores de aplicativos e usuários. Normalmente acessíveis no aplicativo ou durante o processo de criação de uma conta, as políticas de privacidade descrevem os tipos de informações coletadas, as finalidades para as quais os dados são utilizados e quaisquer terceiros com quem os dados possam ser compartilhados.

A conformidade com as regulamentações de privacidade, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, é essencial para essas políticas. As empresas devem assegurar que suas políticas de privacidade sejam escritas de forma clara para facilitar a compreensão dos usuários. Ao seguir as melhores práticas na criação de políticas de privacidade, os responsáveis pelos aplicativos podem contribuir para um ecossistema digital mais seguro e transparente, promovendo a confiança dos usuários no tratamento de suas informações pessoais.

Aspectos de segurança

Para garantir a segurança de um aplicativo, é fundamental utilizar um certificado de assinatura digital. Esse certificado assegura a autenticidade e a integridade do aplicativo, sendo essencial que ele seja válido, confiável e devidamente protegido.

Em relação à proteção da comunicação entre o aplicativo e servidores externos, a segurança de rede é um aspecto fundamental. Ela é formada por um conjunto de ferramentas concebidas para proteger os dados durante uma transmissão (DA ROCHA JR, 2013). Uma análise da segurança de rede permite identificar se a aplicação está configurada de forma segura para lidar com conexões de rede.

Segundo Cintra e Nascimento (2019, pg. 4), “é possível dizer que uma vulnerabilidade surge quando há uma fraqueza nas medidas de proteção de um sistema computacional, podendo ser explorada por um usuário ou mecanismo mal-intencionado”. A presença de vulnerabilidades de alto risco é particularmente preocupante, pois essas podem causar danos significativos se exploradas. Exemplos de tais danos incluem a possibilidade de invasão de privacidade, roubo de identidade, acesso não autorizado a dados pessoais sensíveis e até manipulação de informações armazenadas ou transmitidas pelo aplicativo. Essas falhas de segurança podem ser utilizadas por atacantes para monitorar atividades dos usuários, acessar dados pessoais como endereço, número de telefone, e até mesmo detalhes mais sensíveis como documentos pessoais e informações financeiras.

Outro aspecto que levanta questões sobre a privacidade dos dados coletados pelo aplicativo é a detecção de rastreadores de usuário/dispositivo. De acordo com XAVIER (2021), “os algoritmos programados para rastrear dados têm uma massa de informações subjetivas”. Essas informações podem ser usadas para várias razões, como análise de uso do aplicativo, personalização de conteúdo ou até mesmo para fins maliciosos, como roubo de dados pessoais.

MATERIAL E MÉTODO

A análise de vulnerabilidade a ser executada nos aplicativos e-Título, WhatsApp e Instagram foi feita por meio da ferramenta MobSF (Mobile Security Framework), disponível em um repositório do GitHub de nome “Mobile-Security-Framework-MobSF”.

Para que fosse possível executar a análise de vulnerabilidades pretendida, foi necessário fazer o *upload* dos arquivos do tipo “.apk” de cada um dos aplicativos a serem analisados. Os *downloads* desses arquivos foram feitos a partir da Google Play Store.

Foi utilizada apenas a análise estática da ferramenta MobSF, que examina o código fonte dos aplicativos, sem a necessidade de interagir com a aplicação a ser testada. Nesta análise, abrangeu-se as permissões consideradas “perigosas”, certificados utilizados, análise de segurança na rede, existência de rastreadores e classificação de segurança dos aplicativos.

RESULTADOS E DISCUSSÕES

Através da ferramenta, foi possível verificar que os 3 aplicativos possuem um certificado de assinatura digital e datas de expiração em dia, o que significa que os aplicativos não foram adulterados desde quando foram assinados.

Durante a análise de segurança, somente o Instagram e o WhatsApp apresentaram alguns resultados com severidade alta, como mostrados na Figura 1.

Um dos problemas detectados foi a permissão de tráfego de texto não criptografado (HTTP) para todos os domínios. O tráfego HTTP é vulnerável a ataques de interceptação, onde um assaltante pode acessar e manipular os dados transmitidos entre o aplicativo e o servidor. Para corrigir isso, o aplicativo deve ser configurado para usar HTTPS, que protege a confidencialidade dos dados, criptografando o tráfego de rede.

Além disso, foi apontado também que a configuração básica do aplicativo está configurada para confiar em certificados instalados pelo usuário. Isso pode ser considerado um risco de segurança, pois os certificados instalados pelo usuário podem não ser confiáveis e podem ser usados para realizar ataques. Recomenda-se que o aplicativo implemente sua própria verificação de certificados.

Figura 1. Segurança de Rede do Instagram e do WhatsApp.

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

Fonte: Elaborado pelos autores, (2024).

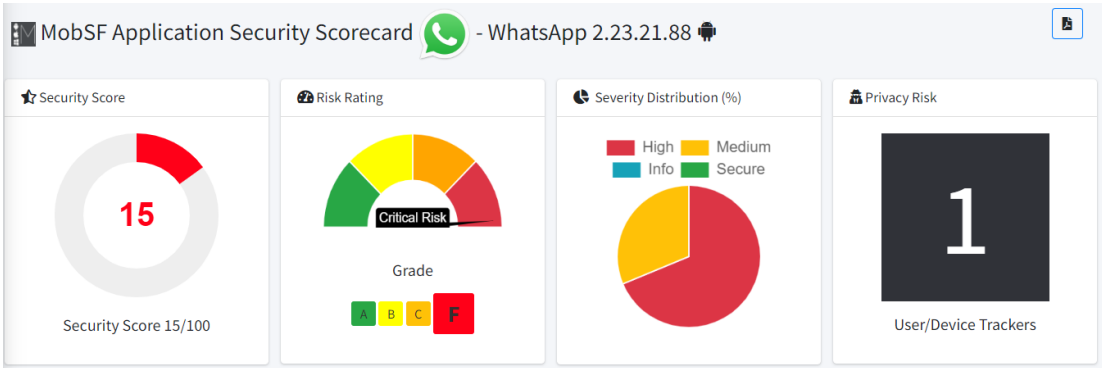
As Figuras 2, 3 e 4 mostram os aplicativos WhatsApp, e-Título, Instagram, com pontuações 15/100, 40/100 e 48/100 correspondentemente. Essas pontuações são baseadas em uma série de critérios de segurança, como aplicação de técnicas de criptografia, práticas de autenticação e medidas de privacidade de dados.

Os resultados indicam que os aplicativos estão abaixo do ideal de segurança, evidenciando a presença de vulnerabilidades que podem ser exploradas por atacantes. O WhatsApp, classificado como “Grave”, aponta para questões sérias que precisam ser abordadas, enquanto a nota “F” sugere que o aplicativo pode estar em um estado crítico em termos de segurança. A classificação de risco "Médio" e a nota

"B" atribuídas aos aplicativos e-Título e Instagram indicam que, embora não estejam no nível mais crítico, ainda apresentam riscos consideráveis associados ao seu uso.

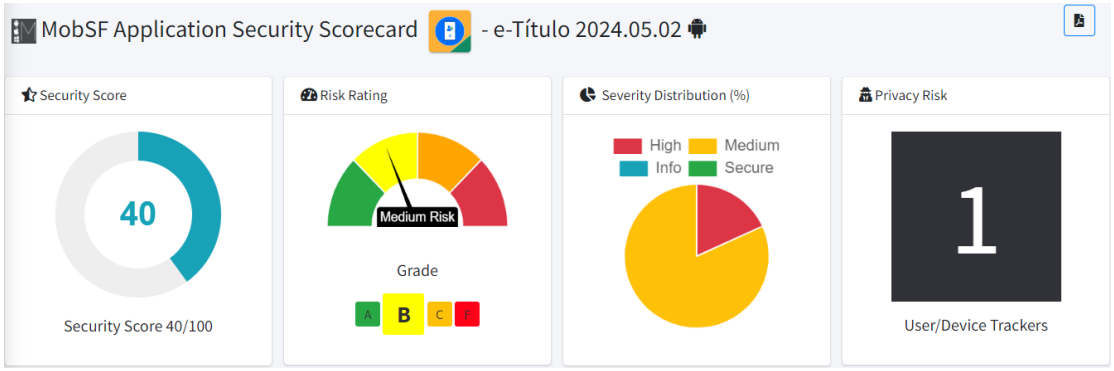
A distribuição de severidade dos problemas detectados revela que a maioria das vulnerabilidades se encontra em categorias de risco médio a alto. Isso indica que há várias questões que, se exploradas, podem comprometer a segurança do aplicativo.

Figura 2. Pontuação de segurança do WhatsApp.



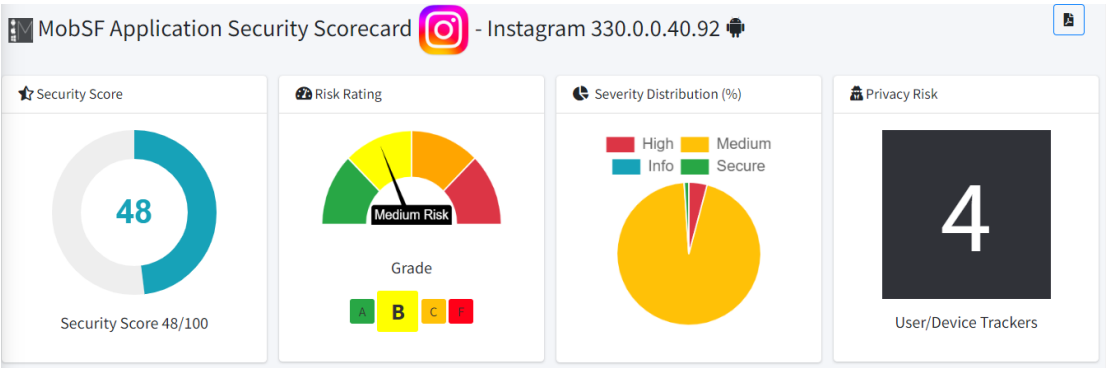
Fonte: Elaborado pelos autores, (2024).

Figura 3. Pontuação de segurança do e-Título.



Fonte: Elaborado pelos autores, (2024).

Figura 4. Pontuação de segurança do Instagram.



Fonte: Elaborado pelos autores, (2024).

Considerando a enorme base de usuários do WhatsApp, a presença de um rastreador levanta questões sobre o alcance e a natureza dos dados que podem estar sendo coletados pelos desenvolvedores ou terceiros associados.

Já no e-Título, a detecção de um rastreador chama a atenção para as implicações de privacidade em um aplicativo que lida com informações sensíveis dos cidadãos, como documentos de identificação.

No Instagram, a presença de múltiplos rastreadores sugere uma coleta extensiva de dados que pode incluir informações sobre interesses, hábitos de consumo, localização e interações sociais dos usuários. Os usuários podem não estar cientes dessas práticas de coleta de dados e das possíveis ramificações para sua privacidade *online*.

O Quadro 1 exibe algumas das permissões listadas durante a análise estática dos aplicativos que foram classificadas como “perigosas” devido a capacidade de acesso às informações pessoais (lista de contatos, histórico de ligações, armazenamento do dispositivo, localização precisa) e ao uso de recursos do dispositivo como *Bluetooth* e a câmera, que pode oferecer risco a integridade de informações pessoais, uma vez que o *Bluetooth* permite a transferência de arquivos entre dispositivos próximos, enquanto a câmera pode resultar em uma utilização indevida de imagem.

Quadro 1. Permissões solicitadas consideradas “perigosas”.

APLICATIVO	PERMISSÃO	DESCRIÇÃO
Whatsapp	android.permission .CALL_PHONE	Permite que um aplicativo leia todos os dados de contato (endereço) armazenados em seu telefone. Aplicativos maliciosos podem usar isso para enviar seus dados para outras pessoas.
	android.permission .CAMERA	Permite que o aplicativo tire fotos e grave vídeos com a câmera. Isso permite que o aplicativo colete imagens que a câmera vê a qualquer momento.
	android.permission .GET_TASKS	Permite que o aplicativo recupere informações sobre tarefas em execução atuais e recentes. Pode permitir que aplicativos maliciosos descubram informações privadas sobre outros aplicativos.
Instagram	android.permission .BLUETOOTH_CONNECT	Necessário para poder conectar-se a dispositivos Bluetooth emparelhados. Permite a transferência de arquivos entre dispositivos próximos.
	android.permission .READ_CONTACTS	Permite que um aplicativo leia toda a lista de contatos e suas informações armazenadas em seu telefone.
	android.permission .WRITE_EXTERNAL_STORAGE	Permite que um aplicativo grave em armazenamento externo.
e-Título	android.permission .ACCESS_COARSE_LOCATION	Acesse fontes de localização precisas, como o sistema de posicionamento global no telefone, quando disponível.
	android.permission .READ_EXTERNAL_STORAGE	Permite que um aplicativo leia do armazenamento externo.
	android.permission .READ_MEDIA_AUDIO	Permite que um aplicativo leia arquivos de áudio de armazenamento externo.

Fonte: Elaborado pelos autores, (2024).

Análise de privacidade de dados em aplicativos móveis.	Kelvin M. de Araújo; Maria Alice de O. Guino; Renan da S. G. Moreira; Luciano G. de Carvalho.

CONCLUSÃO

As evidências revelam os desafios que muitos aplicativos enfrentam para garantir a proteção necessária aos dados sensíveis dos usuários, juntamente com a necessidade de manter a consistência dos dados que são essenciais para o funcionamento da aplicação. Por essa razão, é substancial a utilização de técnicas eficientes que garantam um uso seguro dos dados. Em contrapartida, os usuários frequentemente se veem obrigados a conceder permissões desnecessárias, que podem ser exploradas indevidamente, expondo informações sensíveis a riscos.

Em consequência disso, um enfoque cuidadoso na gestão de permissões, a implementação de práticas proativas por parte dos usuários (como restringir a instalação de aplicativos a lojas nativas), o oferecimento de orientações sobre os riscos do compartilhamento de dados e o fortalecimento das regulamentações de privacidade de dados são medidas imprescindíveis para abordar efetivamente essas preocupações e promover um ambiente digital mais seguro e confiável.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, 15 ago. 2018.

CONFESSORE, N. Cambridge Analytica Scandal: The Fallout Widens. **The New York Times,** 4 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 10 jun. 24.

DA ROCHA JR, V. C. **Segurança de Rede**. Revista de Tecnologia da Informação e Comunicação, v. 3, n. 1, p. 14-21, 2013. Acesso em: 09 de jun. 2024.

JARDIM, G. P. S. et al. **Uma Caracterização das Políticas de Privacidade Utilizadas em Aplicativos no Brasil.** In: WORKSHOP SOBRE AS IMPLICAÇÕES DA COMPUTAÇÃO NA SOCIEDADE (WICS). Niterói. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, p. 13-25. 2022.

LORENZON, L. N. **Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement.** Revista do Programa de Direito da União Europeia, v. 1, p. 39-52, 2021. Acesso em: 26 nov. 23.

MARTINS, M. G.; TATEOKI, V. A. **Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da cambridge analytica.** Revista Eletrônica Direito e Sociedade - Redes, [S.L.], v. 7, n. 3, p. 135, 2019. Centro Universitario La Salle - UNILASALLE. Acesso em: 09 jun. 24.

NASCIMENTO, F. R. do; CINTRA, F. G. **Vulnerabilidades de segurança em dispositivos Android: análises e estatísticas (2009-2019).** Revista EduFatec: educação, tecnologia e gestão, v.2 n.1. 2019. Acesso em: 09 jun. 24.

OBAR, J. A.; OELDORF-HIRSCH, A. **The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services**. Information, Communication & Society, v. 23, n. 1, p. 128-147, 2020. Acesso em: 30 de mar. 2024.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (GDPR), n. 2016/679, 27 abr. 2016. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. **Diário Oficial da União Europeia**, L 119, p. 1-88, 4 maio 2016.

XAVIER, M. R. P. **O dispositivo de vigilância algorítmica: algoritmos rastreadores, smartphones e coleta de dados**. 2021. Acesso em: 09 jun. 24.