RESUMO

O presente trabalho tem como propósito analisar o gerenciamento de riscos em contratos de aplicativos de celulares e demais dispositivos. Que permissões estão envolvidas nesse tipo de relação? O que elas permitem que os aplicativos façam com os nossos dados? O que isso acarreta para a nossa intimidade? E para a nossa segurança? Essas permissões estão de acordo com as novas regras estabelecidas para o manuseio deste tipo de informação no ambiente digital, notadamente as estabelecidas pela Lei Geral de Proteção de Dados (LGPD)?

O estudo procurar entender a relação dos riscos e o gerenciamento de riscos em contratos de aplicativos, evitando a contribuição de insegurança para os contratantes.

Aborda ainda que quais são os aplicativos mais perigosos, do ponto de vista da obtenção de dados de forma ilegal de quem os instala, e que ações de segurança podem lançar mão quando da instalação desse tipo de serviço.

Enfim, em um mundo cada vez mais digital, que teve o aprofundamento do online em todas as áreas por conta das restrições impostas pela pandemia de Covid-19, ainda em andamento, mesmo que de forma mais branda, ater-se à nossa relação com os diversos aplicativos atualmente à nossa disposição é fundamental para resguardamos nosso direito à privacidade, à segurança e ao uso correto e responsável de nossos dados por parte dos provedores deste tipo de serviço tecnológico. É sobre este tópico de tamanha magnitude que discorreremos nas próximas páginas.

1. INTRODUÇÃO

É evidente que com o avanço da tecnologia, tudo no mundo mudou. Impossível imaginar nos dias de hoje alguém sem acesso à internet e a smartphones. Passamos a nos comunicar através de sites e aplicativos. O que antes era feito presencialmente agora são feitos virtualmente, surgindo assim, novos negócios jurídicos.

O objetivo desse trabalho é informar aos usuários sobre sua privacidade no campo virtual, esclarecer as medidas de segurança que devem ser tomadas e mostrar, a título informativo aplicativos, que parecem ser inofensivos, mas que tem como objetivo ter acesso ao máximo das suas informações pessoais.

2. PRIVACIDADE

Desde que a internet, e mais precisamente os smartphones, passou a fazer parte da nossa vida cotidiana, falar em privacidade está cada vez mais difícil, por parte de todos nós, membros dessa sociedade altamente conectada e globalizada, seja em que canto do planeta estiver.

Sobre os aplicativos de celular especificamente, é sabido que ao instalarmos algum em nosso dispositivo certamente compartilharemos algum dado a nosso respeito com o desenvolvedor do mesmo. Mesmo que não dermos permissão ao aplicativo para uma série de questões – como compartilhamento contínuo da localização, dos contatos em nossas agendas telefônicas ou do acesso às fotos armazenadas na memória –, ao fazermos o seu download estamos compartilhando, no mínimo, nosso nome, localização (quando do download do aplicativo), senha para acesso e dados financeiros (muito cuidado aqui), por exemplo, caso se trate de alguma operação de compra.

Essa "devassa" da privacidade da sociedade permeia o mundo contemporâneo e é uma das características de nossa sociedade. Muitas vezes, somos nós mesmos que assim desejamos, ao postar fatos corriqueiros, ou não, de nossas vidas nas mais diversas redes sociais. Mesmo esse 'exibicionismo' consentido, no entanto, precisa ser resguardado e se ater a alguns cuidados básicos para que a exposição não vire, na verdade, uma verdadeira dor de cabeça.

2.1. LGPD e a privacidade

Nesse sentido, portanto, deu-se a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709, de 2018, cujo propósito, de acordo com o que está disciplinado em seu artigo 1º, é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

A legislação discorre sobre o tratamento de dados pessoais (em meio físico e/ou digital) compilados tanto por pessoas físicas ou jurídicas (de direito público ou privado), levando em consideração uma diversidade de situações em que possa ser aplicada e, desse modo, resguardar a privacidade dos titulares dos dados.

A LGPD disciplina, em seu artigo 5º, inciso X, que o tratamento de dados por ela referida diz respeito a "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". Como se pode ver, a gama é imensa, abarcando, por assim dizer,

praticamente todas as operações em que um indivíduo e/ou empresa revela alguma informação a seu respeito para o desenvolvimento da transação.

A própria LGPD, em seu artigo 6º, também define quais são os princípios aos quais os tratamentos de dados pessoais precisam observar:

Finalidade – "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades";

Adequação – "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento";

Necessidade – "imitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dado";

Livre acesso – "garantia de consulta livre dada aos (às) titulares dos dados, de forma fácil e sem custo";

Qualidade dos dados – "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais";

Transparência – "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial";

Segurança – "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão";

Não discriminação – "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos";

Prevenção – "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais";

Responsabilização e prestação de contas – "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

Ou seja, a consecução da LGPD deu-se no sentido de resguardar a sociedade como um todo naquilo que temos de mais importante: dados e informações que nos caracterizam como seres, ou empresas, portadores do direito de ter essas informações, quando

coletadas, tratadas de forma correta e utilizadas, exclusivamente, para a finalidade à qual se destinam.

É justamente aqui que entra o direito à privacidade, inclusive no caso de downloads de aplicativos de celulares, cujo cerne do negócio é manejar as informações que recebem de seus usuários com vistas a um fim específico – transação bancária, relacionamento entre pessoas, apostas esportivas, games etc.

Direito à privacidade esse que, muito antes da LGPD e da própria internet, já está regulado pela nossa Carta Magna de 1988, em seu artigo 5º, inciso X, onde, na lista de direitos invioláveis, está "a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Isto posto, haja vista as mudanças tecnológicas pelas quais o mundo tem passado e o imenso compartilhamento de dados diários de pessoas físicas e jurídicas diariamente, há que se empreender enorme esforço para a correta preservação da intimidade dos dados daqueles que baixam aplicativos de celular. No Brasil, especificamente, temos o importante auxílio de nossa legislação mor e de leis novas, como a LGPD, que buscam sedimentar um terreno adequado para que aproveitemos das benesses da tecnologia sem termos nossa privacidade invadida de forma incorreta e ilegal.

3. MEDIDAS DE SEGURANÇA

Como testar a segurança de um aplicativo?

O teste de segurança em aplicativos móveis pode ser feito de forma estática – é analisado o código do programa, sem executá-lo. Basicamente, ele vai buscar por erros e códigos maliciosos, que abram brechas de segurança no aplicativo.

Como ter segurança nos aplicativos?

- "Proteger a comunicação entre apps";
- "Pedir credenciais antes de mostrar informações confidenciais";
- "Aplicar medidas de segurança de rede";
- "Usar objetos WebView com cuidado";
- "Usar *intents* para adiar permissões";
- "Compartilhar dados de forma segura entre apps".

Como proteger app de banco no celular?

- “Use uma senha de bloqueio no seu celular”;
- “Não deixe seus dados de cartão salvos no celular”;
- “Use biometria como camada extra, não como principal acesso”;
- “Cadastre um e-mail separado para recuperação de conta”;
- “Esconda apps importantes”.

Como saber se um aplicativo é perigoso?

- “O app não está em uma loja confiável”;
- “As permissões não fazem sentido”;
- “Verifique as análises e reputação do app”;
- “Reporte apps suspeitos ao Google”;
- “Não confie em apps que oferecem benefícios”;
- “Confira o número de usuários”;
- “Use um antivírus”.

Celular: como se proteger de golpes e aumentar a segurança.

- “Mantenha o sistema operacional e os aplicativos atualizados”;
- “Escolha senhas fortes, mas não anote no celular”;
- “Use proteções integradas de segurança e autenticação de dois fatores”;
- “Não clique em links sem origem nem instale apps fora das lojas oficiais”.

4. OS 15 TIPOS DE APLICATIVOS CONSIDERADOS MAIS PERIGOSOS

Determina a Constituição Federal de 1988 que a privacidade é um direito inerente a todos. No entanto, com o advento da internet bem como dos aparelhos smartphones o exercício pleno de tal direito pode ser ameaçado por conta de aplicativos que buscam ter acesso aos dados pessoais sem a devida consciência do usuário, pois mesmo com a disposição dos termos contratuais conseguem ludibriar a maioria das pessoas com aplicativos de aparência inofensiva porém que buscam ter acesso até ao registro de chamadas bem como à galeria de fotos e vídeos pessoais e outras informações extremamente íntimas.

Nesse aspecto, se faz necessário analisar a importância de informar a todos a respeito das medidas de segurança para a proteção de dados íntimos quando enumerar e listar quais aplicativos pode oferecer maior risco aos indivíduos. Diante disso, torna-se imprescindível fazer uma análise dos quinze tipos de aplicativos mais perigosos para os usuários.

Segundo o site “Apptuts.net” existem 15 tipos de aplicativos extremamente perigosos para o usuário. São eles:

1º: os aplicativos que prometem limpar o smartphone de arquivos inúteis, tais aplicativos buscam ter acesso à galeria de fotos bem como a todos os arquivos pessoais que estiverem na memória do aparelho. Além disso, sua funcionalidade pode ser considerada dispensável uma vez que o próprio usuário pode remover manualmente aquilo que considerar inútil.

2º: apps para escancear vírus, esses podem indicar falsamente a existência de vírus no smartphone obrigando o usuário a baixar arquivos perigosos e desnecessários, para tanto, recomenda-se o uso de aplicativos Antivírus de empresas conhecidas como Avast, Kaspersk, por exemplo.

3º: os apps exploradores de arquivos, esses podem conter muitos anúncios e recursos que podem expor o aparelho a riscos como maware.

4º: apps com permissões estranhas ao seu serviço, por exemplo, é natural que um app editor de fotos queira ter acesso à galeria, no entanto é comum ver tais aplicativos buscando ter acesso ao microfone e registro de chamadas. Nesse sentido vale ressaltar a importância de estar atento aos tipos de permissão que o usuário fornece.

5º: apps para melhorar a bateria, além de sua funcionalidade ser questionável uma vez que tudo que um app pode fazer para melhorar sua bateria o próprio usuário pode fazer manualmente, tais apps trazem consigo inúmeros anúncios que podem ser perigosos.

6º: os aplicativos que precisam ser baixados fora das lojas convencionais, a exemplo da appstore e playstore, uma vez que as empresas responsáveis fazem o controle de quais aplicativos não oferecem risco, por tanto se um app precisa ser baixado fora da forma convencional pode ser sinal de algum problema.

7º: jogos que simulam outros famosos, geralmente tais aplicativos se apresentam como alternativas gratuitas e podem expor o aparelho a mawares.

8º: apps que se passam por aplicativos populares, muitos podem não oferecer riscos em relação a vírus, no entanto, podem coletar dados pessoais e até mesmo informações bancárias.

9º: os aplicativos cheios de anúncios, durante o uso de tais apps podem ser abertas abas no navegador e de download mesmo contra a vontade do usuário.

10º: os aplicativos que pedem informações, estes podem coletar dados de cartão de crédito e demais informações pessoais.

11º: os apps que prometem deixar o aparelho smartphone mais rápido, aqui há o mesmo problema dos apps de limpeza, são funções que o próprio usuário pode fazer manualmente além de trazer anúncios e downloads indesejados.

12º: os apps de transferência de arquivos, eles podem ter acesso a arquivos pessoais bem como contam com diversos anúncios maliciosos, nesse caso também cai no mesmo problema que os aplicativos de limpeza e bateria, uma vez que o próprio usuário do smartphone pode transferir arquivos para o computador através de um cabo USB.

13º: os apps que prometem Wi-Fi de graça, além de se demonstrarem incapazes uma vez que um app não pode ser capaz de burlar senhas de rede, ele pode colocar o aparelho em risco de ser alvo de invasões, uma vez que podem conectar o celular em qualquer rede pública.

14º: os apps usados para gravação de ligações, esses podem trazer riscos ao aparelho quando o usuário não se encontra atento às permissões uma vez que só precisam ter acesso aos contatos e microfone.

15º: os aplicativos de lanterna, sua funcionalidade já se mostra dispensável uma vez que a maioria dos smartphones já tem tal função embutida naturalmente, mesmo assim tais apps continuam sendo baixados por muitos usuários, os perigos desse tipo de aplicativo são o excesso de anúncios e downloads indesejáveis.

Em síntese, a maioria dos aplicativos listados já tem sua funcionalidade embutida nos aparelhos ou podem ser feitas manualmente pelos usuários, mesmo assim são baixados aos montes.

Dessa forma, campanhas de conscientização e esclarecimento a respeito dos perigos do uso de tais aplicativos bem como a indicação de quais podem trazer riscos se mostram imprescindíveis para a garantia da segurança dos usuários. Dessa maneira, operando os smartphones com consciência é possível promover a proteção e o exercício do direito à privacidade, mencionado na constituição federal.

5. CONCLUSÃO

Conclui-se que os contratos de aplicativo, muitas vezes, oferecem riscos e armadilhas aos usuários, que muitas vezes não estão cientes dos termos e condições impostos pelas empresas responsáveis pelos aplicativos.

Estes termos podem incluir cláusulas abusivas, que violam direitos dos usuários ou utilizam dados pessoais de forma inadequada. Além disso, os usuários muitas vezes ficam expostos a fragilidades em relação à segurança dos seus dados, já que muitos aplicativos não cumprem as normas e padrões de segurança estabelecidos.

As grandes empresas de tecnologia devem respeitar as normas de direito nos termos de uso levando em consideração que o usuário é a parte hipossuficiente da relação jurídica, e que o contrato deve conter mais cláusulas protetivas e transparentes aos usuários, evitando abusos e ameaças a sua segurança.

A facilidade de aceitar o termo de uso, é desproporcional quando comparada pelas longas redações, com linguagem técnica complicada e de difícil acesso pelos usuários.

Resta aqui dizer que, ler os Termos de Uso ao baixar um aplicativo, é extremamente necessário, pois afeta diretamente os direitos legais dos usuários e que sua privacidade que fica prejudicada por conta das cláusulas contratuais.

Portanto, é indispensável que os usuários estejam atentos aos riscos envolvidos e busquem informações sobre os termos de uso dos aplicativos antes de concordar com eles.

REFERÊNCIAS BIBLIOGRÁFICAS

Constituição da República Federativa do Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm Acesso em: 03 de abril de 2023.

Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 03 abril de 2023.

Permissões de aplicativos no Android e como controlá-los. Disponível em https://www.avg.com/pt/signal/guide-to-android-app-permissions-how-to-use-them-smartly Acesso em: 03 de abril de 2023.

Apptuts. 15 tipos de aplicativos perigosos para Android que deve evitar. Disponível em https://www.apptuts.net/tutorial/android/aplicativos-perigosos-para-android-deve-evitar/ Acesso em: 05 de abril de 2023.

Techtudo. 8 tipos de aplicativos que você deve evitar baixar no smartphone. Disponível em: https://www.techtudo.com.br/listas/2021/05/8-tipos-de-aplicativos-que-voce-deve-evitar-baixar-no-smartphone.ghtml Acesso em: 04 de abril de 2023.

CRR Advocacia para Negócios Inovadores. Saiba como Elaborar um "Termo de Uso" e uma "Política de Privacidade". Jusbrasil. Disponível em https://roseadvocaciaparastartup.jusbrasil.com.br/artigos/507868098/saiba-como-elaborar-um-termo-se-uso-e-uma-politica-de-privacidade-understand-tems-and-conditions-and-privacy-policy Acesso em: 03 de abril de 2023.

Bach, Ronaldo. Conheça os perigos dos aplicativos instalados no seu celular e como evitá-los. Jornal Jurid. Brasília, 28 de fevereiro de 2023. Disponível em: https://www.jornaljurid.com.br/noticias/conheca-os-perigos-dos-aplicativos-instalados-no-seu-celular-e-como-evita-los Acesso em: 03 de abril de 2023.

Carneiro, Ramon Mariano. Direitos fundamentais nos termos de uso das plataformas digitais. Disponível em: https://revista.internetlab.org.br/li-e-aceitoviolacoes-a-direitos-fundamentais-nos-termos-de-uso-das-plataformas-digitais/ Acesso em: 03 de abril de 2023.

EJUDI Soluções Jurídicas. Termo de uso: conheça seus requisitos e sua finalidade. Disponível em https://ejudi.com.br/termo-de-uso-finalidade/ Acesso em: 03 de abril de 2023.