UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
ESPECIALIZAÇÃO EM INFORMÁTICA: ÁREA DE CONCENTRAÇÃO: GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

Marcelo Dias de Sá

Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas.: Aplicações mobile do governo

Brasilia
2019

MARCELO DIAS DE SÁ

Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas.: Aplicações mobile do governo

Monografia apresentada ao Curso de Especialização em Informática do Departamento de Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do grau de Especialista em Informática.

Área de Concentração: Gestão de Tecnologia da Informação

Orientador: Prof. Dr. Virgílio Augusto Fernandes Almeida

Brasília

2019

© Marcelo Dias de Sá
Todos os direitos reservados

Ficha catalográfica elaborada pela Biblioteca do ICEx – UFMG

Sá, Marcelo Dias de

S111a Análise do impacto da nova lei de proteção de dados pessoais nas aplicações de internet das coisas. / Marcelo Dias de Sá – Brasília,2019.
ix, 78 f., il.

Monografia (especialização) – Universidade Federal de Minas Gerais. Departamento de Ciência da Computação.

Orientador: Virgílio Augusto Fernandes Almeida

1.Computação – Monografias. 2. Políticas do ciberespaço. 3. Privacidade e proteção de dados. 4. Lei de proteção de dados. I. Orientador. II. Título

CDU 519.6*

FOLHA DE APROVAÇÃO.

UNIVERSIDADE FEDERAL DE MINAS GERAIS

INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
ESPECIALIZAÇÃO EM INFORMÁTICA: ÁREA DE CONCENTRAÇÃO GESTÃO EM TECNOLOGIAS DA INFORMAÇÃO

Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas: Aplicações mobile do governo

MARCELO DIAS DE SÁ

Monografia apresentada aos Senhores:

Prof. Virgilio Augusto Fernandes Almeida
Orientador
DCC - ICEx – UFMG

Prof. José Nagib Cotrim Árabe
DCC - ICEx - UFMG

Prof. José Marcos Silva Nogueira
DCC - ICEx - UFMG

Belo Horizonte, 14 de março de 2019

- *Dedico este projeto à minha família e amigos que sempre estiveram presentes direta ou indiretamente em todos os momentos de minha formação.*
- *Dedico este trabalho a todos aqueles que de alguma forma contribuíram com meu desenvolvimento. Principalmente aos meus pais e irmãos que são sempre presentes.*

AGRADECIMENTOS

Agradeço a minha família e amigos por ter me dado condições para realizar este trabalho, aos professores Virgílio Almeida e Nagib Cotrim pela colaboração e a todos que de alguma forma contribuíram para que eu pudesse realizar com sucesso este trabalho.

Resumo

A Lei Geral de Proteção de Dados (LGPD), 13.709/2018, foi sancionada no dia 15 de agosto, e traz novas regras sobre a coleta e o tratamento de dados pessoais por empresas e por órgãos públicos. O objetivo deste trabalho é apresentar uma análise sucinta da LGPD e um estudo de caso com as aplicações mobile do governo. O desenvolvimento deste projeto será realizado com base em análise documental dos principais normativos que tratam as leis de proteção de dados, Marco Civil da Internet e a LGPD. A análise dos aplicativos será feita através da ferramenta (Lumen) que é desenvolvida pela Data Transparency Labs (DTL). A partir dos resultados obtidos poderemos concluir se os serviços digitais do governo estão em conformidade com a LGPD.

Palavras-chave: Privacidade. Proteção. Governo. Dados.

Abstract

The General Data Protection Act (LGPD), 13,709 / 2018, was sanctioned on August 15, and brings new rules on the collection and processing of personal data by companies and public bodies. The objective of this work is to present a brief analysis of the LGPD and a case study with the government mobile applications. The development of this project will be carried out based on documentary analysis of the main norms that deal with data protection laws, the Civil Internet Framework and the General Law on Data Protection. The analysis of the applications will be done through the tool (Lumen) that is developed by Data Transparency Labs (DTL). From the results obtained, we can conclude that government digital services are in compliance with the LGPD.

Keywords: Privacy. Protection. Government. Data.

Lista de ilustrações

Figura 1 – Direitos fundamentais 13
Figura 2 – Resumo dos Principais Pontos 14
Figura 3 – Hipóteses que legitimam o tratamento de dados 15
Figura 4 – Aplicativo IRPF - Solicitação de permissão de acesso 24
Figura 5 – Aplicativo FGTS - Tela de solicitação de permissão de acesso 25
Figura 6 – Tabela completa com as permissões solicitadas pelos apps analisados.
Preenchimento em vermelho significa que o app possui a permissão 26
Figura 7 – Tela com as permissões de acesso do app IRPF 27
Figura 8 – FGTS permissão GET_ACOUNTS 28
Figura 9 – Contas ativas no dispositivo 29
Figura 10 – Vazamento de informações da aplicação CNH Digital 31
Figura 11 – Vazamento de informações da aplicação Sigepe 32
Figura 12 – vazamento de informações da aplicação Meu digiSUS 33

Lista de Siglas

CNH Carteira Nacional de Habilitação
CSS Cascading Style Sheets
DF Distrito Federal
DNS Domain Name System
DPO Dynamic Position Operator
DTL Data Transaction Language
FGTS Fundo de Garantia do Tempo de Serviço
ICSI Itracytoplasmatic sperm injection (Injeção intracitoplasmatica de esperma)
IP Internet Protocol
IRPF Imposto de Renda Pessoa Física
IX Século 9
LGPD Lei Geral de Proteção de Dados
LGPDP Lei Geral de Proteção de Dados Pessoais
OCDE Organização para a Cooperação e Desenvolvimento Econômico
SNE Sistema Nacional de Educação
SUS Sistema Único de Saúde
TLS Transport Layer Security
VPN Virtual private network

SUMÁRIO

1 Introdução 13
2 Lei Geral de Proteção de Dados 15
2.1 Apresentando a Lei 15
Controlador e Operador: 17
Escopo da Aplicação - Art.1.º 17
Autorização para tratamento de dados 18
Direitos dos titulares de dados 18
Relatório de impacto 19
Encarregado pelo Tratamento de Dados 19
Autoridade de Proteção de Dados 19
Sanções e Multas 20
3 Caso de uso sobre vazamento de dados 21
3.1 MP-DF acusa empresa pública de vender dados pessoais de brasileiros 21
3.2 Colégio bandeirantes e vazamento de dados de alunos 22
4 PD e as aplicações moveis do governo 23
4.1 Metodologia de Pesquisa 24
4.2 Politica de privacidade dos apps 25
4.3 Análise dos aplicativos 26
4.4 Compartilhamento de informações com terceiros 32
5 Conclusão 35
Referências 37

1 Introdução

Considerando que hoje vivemos em um cenário altamente dependente de Tecnologia da Informação, este trabalho visa analisar o que acontece com os dados dos usuários (cidadãos) na ‘internet’ e os aspectos de vigilância, controle e privacidade.

A lei do Marco Civil da Internet regula o uso da ‘internet’ no Brasil e visa apontar os atos criminosos no ciberespaço, além de prezar pelos direitos de neutralidade da rede, liberdade de expressão, da privacidade dos usuários e dos direitos humanos.

A proteção e privacidade foram os principais motivos do Marco Civil, onde o projeto inicial era uma resposta direta à “Lei Azeredo”, que tipificava os crimes digitais e previa que os dados dos usuários fossem guardados por três anos para a auditoria criminal. Após essa ideia, a internet se posicionou contra o projeto pois o considerava um modo de vigiar o cidadão.

O Marco Civil da Internet garante o princípio da liberdade de expressão, onde impede a censura por partes dos sites e redes sociais, por exemplo, que ficam impedidos de remover os conteúdos dos usuários sem determinação exclusiva de uma ordem judicial (com exceção de conteúdo de nudez ou atos sexuais e explícitos).

A privacidade do usuário é tratada e garantida no Marco Civil da ‘internet’, evitando que as informações sejam vendidas ou trocadas com empresas terceiras (nacional e internacional) sem a prévia autorização do usuário (que deve ser informado no momento de um cadastro em sítio web, por exemplo).

Com o crescimento expressivo de novas tecnologias e a inserção delas no dia a dia das pessoas em diversos momentos, fica cada vez mais fácil coletar dados visando a um maior conhecimento sobre o consumidor e o seu próprio negócio. Uma das tecnologias que pode ser usada nesse processo é a ‘internet’ das coisas (IoT), que, através de diversas categorias de dispositivos, possibilita uma infinita possibilidade de captura de dados.

No entanto, os projetos de IoT enfrentam novos desafios como a Lei Geral de Proteção de Dados Pessoais (LGPDP), lei que foi sancionada em 2018 e entrará em vigor em 2020 e estabelece regras para a garantia da privacidade das informações de cidadãos brasileiros.

O princípio fundamental do uso de dados pessoais é o consentimento da pessoa, que deve ser obtido a partir de uma solicitação clara, simples e objetiva, explicando quais dados serão capturados, como serão utilizados e por quanto tempo serão mantidos.

É importante observar que o consentimento deve ser armazenado como uma evidência e que a pessoa tem o direito de solicitar a sua revogação a qualquer momento. As empresas geralmente complementam o consentimento com uma Política de Privacidade e Termos de Prestação do Serviço.

2 Lei Geral de Proteção de Dados

2.1 Apresentando a Lei

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que determina como os dados dos cidadãos podem ser coletados e tratados, e que prevê punições para transgressões. No dia 14 de agosto de 2018, foi sancionado no Congresso Nacional o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoas e altera a Lei 12.965/16 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira.

A LGPD cria toda um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos. Importante salientar que o país já dispunha de mais de 40 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, a LGPD vem substituir e/ou complementar esse arcabouço regulatório setorial, que por vezes era conflituoso, pantanoso, trazia insegurança jurídica e tornava o país menos competitivo no contexto de uma sociedade cada vez mais movida a dados. Ao ter uma Lei Geral, o Brasil entra para o rol de mais de 100 países que hoje podem ser considerados adequados para proteger a privacidade e o uso de dados.

Tal como a General Data Protection Regulation (GPDR) que é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu, a LGPD motivará mudança de paradigma na gestão dos dados, evidenciando a necessidade de adequações internas e da construção de uma cultura de proteção de dados no Brasil. Lembrando que as entidades públicas e privadas terão o prazo de 18 meses para se adequarem ao novo regulamento.

Os principais fatores que motivaram a criação de uma lei de proteção de dados foram:

- Uso cada vez maior de dados pessoais
- O recurso mais valioso do mundo não é mais petróleo, mas dados. (The Economist).
- Era digital, redes sociais, “analytics”.
- Possibilidade de impactos nas vidas das pessoas, negócios e até eleições
- Ausência de um marco regulatório nacional quanto à proteção de dados

- Acontecimentos recentes e outros fatores
- Cambridge Analytic
- GDPR (General Data Protection Regulation - União Européia)
- OCDE (Organização para a Cooperação e Desenvolvimento Econômico)
- Lei do Cadastro Positivo
- Ano Eleitoral

Composta por 65 artigos divididos em 10 capítulos, abaixo segue uma descrição sucinta dos conceitos que a LGPD aborda.

Direitos Fundamentais

Figura 1 – Direitos fundamentais.

Fonte: Cópia de Tela de slide Power point.

Alguns dos principais termos definidos pela Lei em seu Artigo 5º.

- **Dado Pessoal:** Qualquer dado relacionado a pessoa natural diretamente identificada ou identificável.
- **Dado Pessoal** sensível: dado genético, biométrico, de saúde, vida e orientação sexual, origem racial ou étnica; de convicção política, sindical, filosófica ou religiosa.
- **Tratamento de Dados***:* Qualquer operação que possa ser realizada nos dados. Ex.:coleta, armazenamento, utilização, transmissão, modificação, eliminação.

Controlador e Operador:

- **Operador**: agente que realiza tratamento de dados a pedido do controlador.
- **Controlador:** agente (pessoa física ou jurídica) que toma decisões sobre tratamento de dados.

Diretrizes e previsões da Lei 13.709/18

Figura 2 – Resumo dos Principais Pontos

Fonte: Cópia de Tela slide Power Point

Principais Pontos

Escopo da Aplicação - Art.1.º

Afeta qualquer atividade que envolva utilização de dados pessoais, incluindo o tratamento pela 'internet', de consumidores, empregados, entre outros.

- Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular.
- Necessidade: Limitação do tratamento de dados ao mínimo necessário.
- Livre acesso: Consulta facilitada e gratuita aos titulares sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados.
- Qualidade dos Dados: Exatidão, clareza, relevância e atualização dos dados.

- Transparência: Informações claras, precisas e facilmente acessíveis sobre o tratamento de dados, observados os segredos comerciais e industrial.
- Segurança: Utilização de medidas técnicas e administrativas para evitar acesso não autorizados e situações acidentais ou ilícitas de perda, alteração, etc.
- Prevenção: Adoção de medidas para prevenir a ocorrência de danos aos titulares.
- Não Discriminação: Não utilização de dados pessoais para fins discriminatórios ilícitos ou abusivos.
- Responsabilização e prestação de contas: demonstração das medidas adotadas para cumprimento das diretrizes de Lei, inclusive a eficácia destas medidas.

Autorização para tratamento de dados

Figura 3 – Hipóteses que legitimam o tratamento de dados

Fonte : Cópia de Tela de slide Power point.

Para dados sensíveis, algumas destas hipóteses podem não estar disponíveis (ex.: interesse legítimo) ou terem diretrizes mais rígidas (ex.: consentimento específico e destacado), conforme Artigo 11.

Análogo se aplica a dados de crianças e adolescentes, conforme Artigo 14. Atenção especial à necessidade de consentimento ser de um pai ou responsável.

Direitos dos titulares de dados

- Confirmação da existência de tratamento;
- Acesso aos dados;

- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimidade, bloqueio ou eliminação de dados desnecessário;
- Portabilidade dos dados a outro fornecedor de serviço ou produto;
- Eliminação dos dados pessoais tratados com consentimento;
- Informação das entidades públicas e privadas com as quais o controlador compartilhou dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento.

Relatório de impacto

O relatório de impacto consiste em uma documentação que descreve os processos de tratamento de dados pessoais que podem gerar algum risco aos direitos dos titulares, além das medidas e mecanismos empregados para mitigar esses riscos. Deverá ser avaliado o ciclo de vida completo de tratamento de dados (coleta, armazenamento, uso, exclusão). O relatório contemplará também as medidas de segurança da informação e mitigação de riscos associados.

Encarregado pelo Tratamento de Dados

Conforme o artigo 41 da LGPD, deverá ser nomeado um responsável para ser o Encarregado pelo Tratamento de Dados. O Encarregado é a pessoa que atuará como canal de comunicação perante os titulares dos dados pessoais e aos órgãos reguladores. Ele deverá supervisionar todas as práticas de tratamento de dados pessoais dentro da organização e verificar se estas estão em conformidade com a Lei de proteção de dados. O Encarregado é semelhante ao Data Protection Officer (DPO) do Regulamento Geral sobre a Proteção de Dados (GDPR).

Autoridade de Proteção de Dados

A autoridade Nacional de Proteção de Dados (ANPD) foi criada a partir da medida

provisória 869, de 27 de dezembro de 2018 e trouxe algumas outras alterações à Lei Geral de Proteção de Dados – Lei nº13.709/2018. A sua criação tem efeito imediato a partir da publicação no diário oficial e fará parte do órgão da administração pública federal, tendo sua organização, competências, governança e hierarquia dispostas por adições ao artigo 55 da LGPD.

As principais atribuições da ANPD são: o estabelecimento de padrões técnicos, a avaliação de cláusulas e jurisdições estrangeiras no que tange a proteção de dados, a determinação para a elaboração de Relatórios de Impacto, a fiscalização e aplicação de sanções, atividades de difusão e educação sobre a lei, bem como demais atribuições que visam a correta aplicação da lei e os princípios da proteção de dados pessoais.

Sanções e Multas

A LGPD prevê sanções para quem não tiver boas práticas. Elas englobam advertência, multa ou até mesmo a proibição total, ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões, passando por penalidades diárias. A Lei também prever a obrigação de divulgação de incidentes, a eliminação de dados pessoais e a inversão de ônus da prova a favor do titular do dado.

3 Caso de uso sobre vazamento de dados

3.1 MP-DF acusa empresa pública de vender dados pessoais de brasileiros

Empresa pública de tecnologia, vinculada ao Ministério da Fazenda, é apontada como responsável por divulgar bases de dados da Receita Federal para um sítio web chamado Consulta Pública.

O que chamou a atenção em relação ao site foi a atualidade dos dados disponibilizados e a forma com que os dados são apresentados. “A estruturação dos dados foi um indicativo de que a base de dados utilizada tinha origem na administração pública”, de acordo com ofício do MP-DF enviado ao Ministério Público Federal.[1]

> A empresa pública de tecnologia, vinculada ao Ministério da Fazenda, é apontada como responsável por repassar ao site Consulta Pública bases de dados da Receita Federal.
>
> O que chamou a atenção em relação ao site foi a atualidade dos dados disponibilizados e a forma com que os dados são apresentados. “A estruturação dos dados foi um indicativo de que a base de dados utilizada tinha origem na administração pública”, de acordo com ofício do MP-DF enviado ao Ministério Público Federal.
>
> Por se tratar de empresa pública ligada ao governo federal, o Ministério Público do Distrito Federal não pode analisar a legalidade da prática de extração perpetrada pelo Serpro. Mas já conclui que o Serpro vende informações, inclusive para a própria administração pública.
>
> A Comissão de Proteção dos Dados Pessoais do MP-DF aponta que o repasse está incluído em contratos com a Controladoria-Geral da União, no valor de R$ 997 mil; com o Conselho da Justiça Federal, cuja negociação foi de R$ 273 mil; e com o Conselho Nacional de Justiça (R$ 56 mil). A comissão cita ainda uma cópia de proposta comercial do Serpro remetida a outro órgão da administração pública.
>
> “Trata-se de um negócio milionário no qual os dados armazenados e geridos pela própria administração pública são vendidos para a mesma administração pública”, afirma o promotor Frederico Ceroy.
>
> Ele afirma que a empresa se aproveita do Decreto 8.789/2016, que trata do compartilhamento de bases de dados na administração pública federal, e faz a Secretaria da Receita Federal do Brasil e a Procuradoria-Geral da Fazenda Nacional disponibilizarem a outros órgãos da administração informações sem sigilo.
>
> Diante dos indícios de irregularidades, o MP-DF diz ter pedido informações ao Serpro sobre o funcionamento da extração das bases de Cadastro de Pessoas Físicas (CPFs) e do Cadastro Nacional de Pessoas Jurídicas (CNPJs), porém alega que a empresa se recusou a respondê-las, alegando sigilo.
>
> O documento do MP-DF afirma que, desde fevereiro de 2018, o domínio do Consulta Pública está congelado, sem possibilidade de acesso.
>
> Fonte: https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros

[1] (2018, 05/2018)

3.2 Colégio bandeirantes e vazamento de dados de alunos

Em 2015, o tradicional Colégio Bandeirantes, de São Paulo, sofreu um vazamento de dados. Eles foram expostos em redes sociais e tinham registros de alunos, desde seu desempenho acadêmico até avaliações emocionais, feitas por professores e pela direção. A publicização desse conteúdo gerou mal-estar em toda a comunidade da escola, que rapidamente teceu críticas duras à direção por não ter um sistema de segurança eficiente para o armazenamento dessas informações. Muitos alunos e pais se sentiram lesados com alguns comentários feitos nas avaliações vazadas. Uma delas diz, por exemplo: “tem olheiras, boca de ódio, cara de criança de filme de suspense”. O Bandeirantes sofreu fortes críticas e teve de mudar seu sistema de armazenamento. Esse episódio revela como a segurança da informação é importante em todos os âmbitos.

4 PD e as aplicações moveis do governo

A recente aprovação do Regulamento Geral de Proteção de Dados no Brasil evidenciou a inquietação que a economia orientada por dados vem gerando sobre os direitos da personalidade. A discussão mais comum e recorrente é sobre a privacidade ou do controle dos dados pessoais, muitas vezes coletados de forma ilícita, sem a ciência e a autorização do titular do dado.

O aumento exponencial na utilização de dispositivos móveis que são capazes de coletar dados sobre o usuário, monitorar suas atividades e até mesmo identificá-los, traz uma nova realidade sobre à proteção de privacidade do cidadão dentro e fora da internet. Os problemas abrangem questões como vigilância em massa e acesso e compartilhamento não autorizado de informações pessoais.

Um aparelho de telefone, por exemplo, hospeda uma rica variedade de informações sobre o seu usuário e suas atividades. Isso inclui uma variedade de identificadores, dados de localização e até mesmo sua lista de contatos. Muitas vezes, os aplicativos coletam essas informações confidenciais e as compartilham com terceiros, como redes de publicidade e serviços de análise, sem o seu consentimento para fins de publicidade e rastreamento.

É possível encontrar nas lojas online de aplicativos móveis uma série de aplicativos da administração pública que oferecem serviços e funcionalidades associados a órgãos e entidades estatais, sejam eles federais, estaduais ou municipais.

Mesmo que disponibilizados por órgãos e entidades da administração pública, enquanto aplicações de internet, esses aplicativos também se submetem às normas de proteção de dados que estabelece uma série de deveres a provedores de aplicações e de direitos a usuários da internet.

Segundo a Lei do Marco Civil (LEI. . .)

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> VII – Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consenti- mento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII – Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou

> em termos de uso de aplicações de internet;
>
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

Partindo das premissas relacionadas às leis que tange a manipulação e proteção de dados no Brasil, esse estudo de caso visa analisar os serviços do governo federal que são disponibilizados através de aplicativos moveis, com o intuito de entender como os apps do governo obtém a permissão, tanto com relação ao tratamento de dados pessoais de modo geral quanto a relação de cada permissão de acesso.

Segundo o artigo 7º da LGPD, o tratamento de dados pessoais somente poderá realizado mediante o fornecimento de consentimento pelo titular; isso significa que, dado o aceite, o responsável pelo o uso do dado está, via de regra, autorizado a fazer todo o combinado no contrato.

O objetivo desta análise possui os seguintes objetivos:

1) Compreender os serviços digitais dos governos fornecidos para o cidadão,
2) Compreender como esses serviços utilizam os dados dos seus usuários
3) Avaliar como esses sistemas tratam os dados dos usuários
4) Avaliar quais os acessos esses sistemas têm acesso no dispositivo do usuário,
5) Apresentar relatório sobre como as permissões solicitadas pelos aplicativos do governo estão operando e e se estão de acordo com as leis de proteção de dados.

4.1 Metodologia de Pesquisa

A pesquisa será realizada com base em análise documental dos principais normativos que tratam as leis de proteção de dados, Marco Civil da Internet e a Lei Geral de Proteção de Dados.

A análise dos aplicativos será feita através da ferramenta Lumen, que é mantida pela Data Transparency Labs(DTL) e outros órgãos governamentais.

A DTL é uma colaboração interinstitucional que busca criar uma comunidade global de tecnólogos, pesquisadores, formuladores de políticas e representantes do setor que trabalham para promover a transparência dos dados pessoais on-line por meio de pesquisa científica, inovação e design.

O Projeto Haystack é uma colaboração do Instituto Internacional de Ciência da Computação (ICSI) da Universidade da Califórnia, em Berkeley, entre várias instituições acadêmicas. No centro do projeto está o aplicativo Lumen Privacy Monitor.

O Lumen Privacy Monitor é um aplicativo para Android, disponível gratuitamente pelo Google Play, que ajuda usuários de smartphone a entender como seus aplicativos móveis lidam com suas informações particulares, incluindo os dados confidenciais que seus aplicativos vazam e com quem eles compartilham. O Lumen aproveita a permissão VPN do Android para capturar e analisar o tráfego de rede localmente no dispositivo e no espaço do usuário: implementa uma pilha de rede simplificada através de soquetes padrão do usuário para atuar como um middleware local que transmite pacotes de forma transparente entre o aplicativo e a interface de rede.

Essa ferramenta também oferece um ponto de vista exclusivo para entender o ecossistema móvel em grande escala com estímulos reais do usuário. Operando localmente no dispositivo, o Lumen pode correlacionar informações contextuais ricas e distintas, como identificadores de aplicativos e IDs de processos, com fluxos; por exemplo, ele pode corresponder consultas DNS a fluxos de saída e identificar com precisão o processo que possui um determinado soquete.

Também analisa a carga útil do tráfego de aplicativos e pesquisa informações pessoais que são recuperadas do dispositivo para as permissões do Android. Além disso, com o consentimento do usuário, o Lumen também realiza a interceptação TLS implementando um proxy TLS local que injeta certificados forjados nos fluxos durante o estabelecimento da sessão TLS.

4.2 Politica de privacidade dos apps

Foi realizado uma pesquisa pela política de privacidade dos apps analisados neste estudo e constatou-se que quase todos os apps possuem política de privacidade. Quando o usuário for baixar o app na playstore.com, na própria página de transferência do aplicativo contém o link para acessar a política.

Das políticas avaliadas, a Carteira digital, FGTS e Bolsa Família são os que possuem as informações mais claras.

A Política de Privacidade do FGTS e Bolsa Família são idênticas, visto que a Caixa utiliza uma política comum para todos os serviços digitais. As regras de privacidade da Caixa possuem uma descrição clara e didática, onde informa ao usuário quais dados são coletados, a finalidade dessa coleta, as medidas de segurança aplicadas a esses dados, o uso de cookies, e as possibilidades de compartilhamento de informações com terceiros.

O app CNH Digital também possui uma política de privacidade boa, onde informa que coletará todos os dados cadastrais do usuário, que terá acessos a vários recursos do dispositivo e que utilizará cockies e tecnologia semelhante. Adicionalmente, informa que irá “coletar e armazenar quaisquer informações sobre sua navegação neste aplicativo”. Outra informação interessante é que respeitadas as exceções legais, o Serpro e o Denatran não repassarão a terceiros informação de nível individual que por você seja cedida com este aplicativo. Toda e qualquer informação individual a seu respeito só poderá ser repassada mediante sua aprovação expressa ou, ainda, por outros meios, se permitido em lei.

A política de privacidade do app Meu IRPF é semelhante ao do CNH Digital, difere somente na parte em que não informa se os dados pessoais serão ou não compartilhados com terceiros.

Em contrapartida, os outros apps não disponibilizam uma política de privacidade para acesso. Os apps Na hora - DF, Sigepe e Nota Legal DF possuem o link para acesso, porém, ao clicar no link, é emitido a mensagem de erro “Não é possível acessar esse site”.

4.3 Análise dos aplicativos

Os resultados encontrados no presente estudo foram obtidos dos dados de tráfego gerados e da análise de permissões de acesso dos aplicativos. Foram analisados desde os procedimentos de baixar os ‘softwares’ da loja playstore.com até a instalação e uso ativo das aplicações.

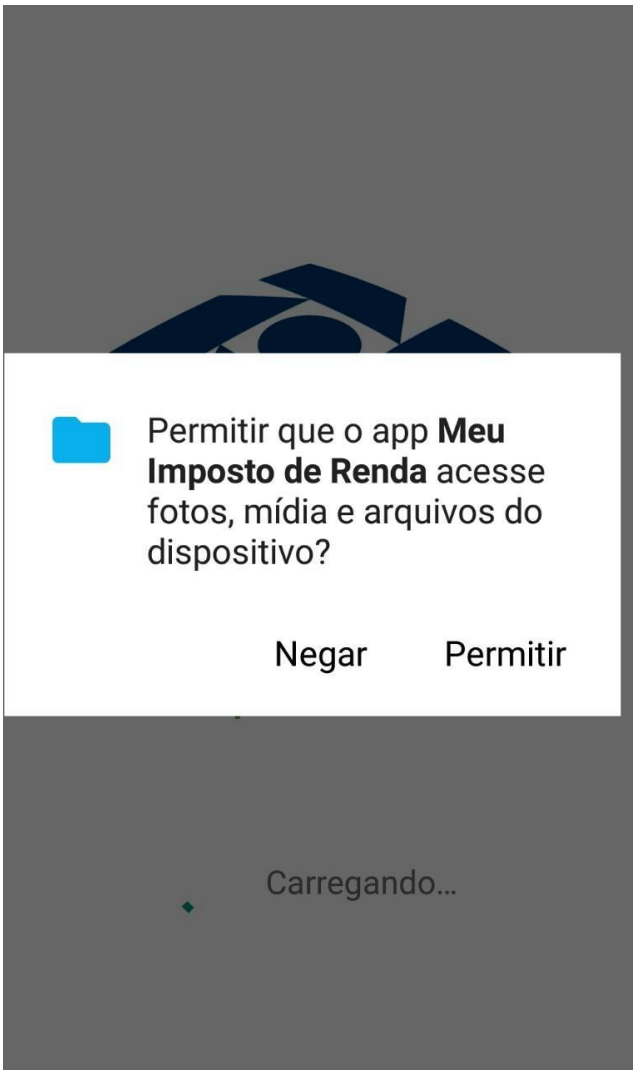
Uma descoberta foi que desde a instalação até o uso efetivo nenhum app pediu o consentimento expresso para o tratamento dos dados pessoais do usuário. Verificou-se que de dentro dos sistemas não é possível acessar a política de privacidade e visualizar os detalhes das permissões de acesso. Para visualizar tais informações é necessário acessar a loja de aplicativos, buscar pelo app e tentar localizar as políticas de acesso e privacidade.

Quanto as permissões, a solicitação ocorre de maneira genérica, onde os aplicativos pedem acesso à funcionalidades importantes do sistema, porém, não existe nenhuma explicação para tal acesso.

Quanto as permissões para que o aplicativo acesse dados e sensores do dispositivo, há duas formas de como pode ser obtido: de forma ampla no momento de instalação, englobando todas as permissões, ou de modo mais específico, durante o uso, quando elas se tornam necessárias para que alguma funcionalidade ou serviço seja corretamente acessado.

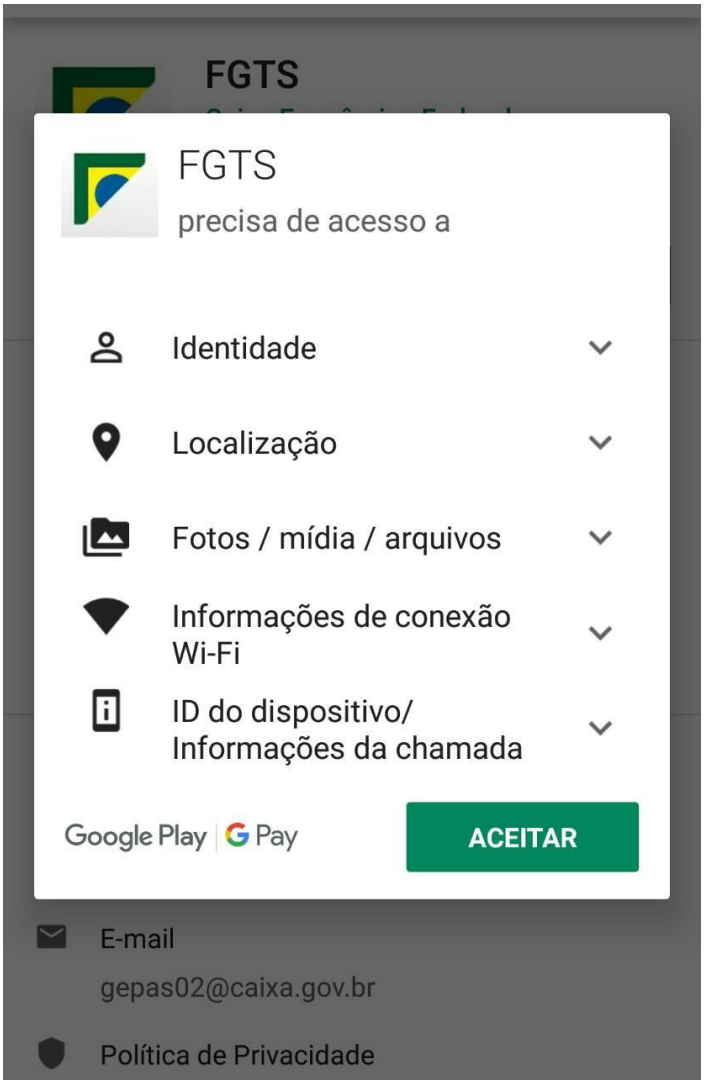
As imagens abaixo possuem uma descrição de solicitação de acesso dos apps, cabe ressaltar que dos 09 sistemas analisados, 06 deles - FGTS, SNE, CNH Digital, Na Hora - DF, Sigepe, Nota Legal - DF e o Bolsa Família - pedem o consentimento genérico do usuário com relação às permissões de acesso na *playstore*, antes do início do download.

Figura 4 – Aplicativo IRPF - Solicitação de permissão de acesso.



Fonte: Fonte: Cópia de Tela de instalação do aplicativo Meu Meu IRPF.

Figura 5 – Aplicativo FGTS - Tela de solicitação de permissão de acesso.



Fonte: Cópia de Tela de instalação do aplicativo FGTS.

Nos aplicativos Meu IRPF e INSS é possível identificar pedidos específicos de consentimento para que a aplicação funcione. No IRPF por exemplo, no momento da instalação é requisitado o acesso aos arquivos armazenados no dispositivo, permissão que é necessário caso o usuário deseja fazer upload ou download de arquivos. Essa permissão é classificada como perigosa e o ideal é que fosse restringida somente quando tal funcionalidade fosse usada pelo usuário.

Um ponto a ser ressaltado é que mesmo clicando em negar o acesso, os app são instalados e funcionam normalmente. Fica a dúvida se essa requisição é meramente informativa, visto que aceitando ou não o sistema irá executar tal função.

Apesar de a hipótese de obtenção de consentimento específico possibilitar que o usuário se informe e concorde com determinadas permissões, isso não é feito para todas as permissões de acesso a dados e funcionalidades do dispositivo. Na

verdade, o consentimento específico acaba sendo obtido apenas com relação a determinadas permissões “perigosas”, a critério do desenvolvedor. Outras, como a permissão de acesso a identificadores do dispositivo, por exemplo, não são submetidas à concordância específica, ou não, do usuário. Se isso até faz sentido quando a permissão é imprescindível para que o app funcione, não se pode dizer o mesmo quando o app funciona normalmente sem que a permissão seja dada.

No caso do Meu IRPF, por exemplo, o consentimento é requerido apenas com relação ao acesso ao armazenamento, mas neste aplicativo foram identificadas também permissões para encontrar contas no dispositivo e ler o “estado do celular”, que dá acesso ao ‘status’ do aparelho (incluindo número de telefone, informações de rede atuais, status de chamadas, e lista de contatos registrados no aparelho) de forma abrangente.

Figura 6 – Tabela completa com as permissões solicitadas pelos apps analisados. Preenchimento em vermelho significa que o app possui a permissão.

Permissões	FGTS	CNH Digital	IRPF	NaHora	Sigepe	Nota Legal - DF	Digi-Sus	Bolsa Familia	SNE
Acessar a localização aproximada	■			■			■	■	■
Acessar a localização precisa	■			■			■	■	
Acessar as contas	■		■				■	■	
Ler memória externa	■		■	■	■	■	■	■	■
Escrever em memória externa	■		■	■	■	■	■	■	■
Ler estado do telefone	■		■			■			
realizar ligações	■								
Acessar a câmera		■				■			
acessar a internet	■	■	■	■	■	■	■	■	■
Acessar o estado da rede	■	■	■	■	■	■	■	■	■
Acessar o estado do wi-fi	■		■				■	■	
Receber informaçòes do boot do aparelho						■			■
Requisitar instalações e pacotes									
Vibrar		■	■	■	■	■			
Manter o aparelho ativo	■	■	■	■	■	■	■	■	■
Usar hardware de impressão digital									
Acessar a lanterna									
Acessar as tarefas									
Criar janelas									
Desconhecidas	■	■	■	■			■	■	■

Fonte: Cópia de Tela de planilha criada em PowerPoint.

É possível verificar através da tabela de permissões que a maioria dos aplicativos analisados possuem acesso à geolocalização do usuário. Nesse caso, não fica evidente para todos, para que essa funcionalidade seria necessária. Os aplicativos SNE e IRPF que possuem essa permissão não a utilizam em nenhuma funcionalidade do sistema. Já os aplicativos Meu digiSUS, FGTS e Bolsa Família utilizam a funcionalidade de geolocalização para fornecer informações de localização de agências de atendimento para o usuário.

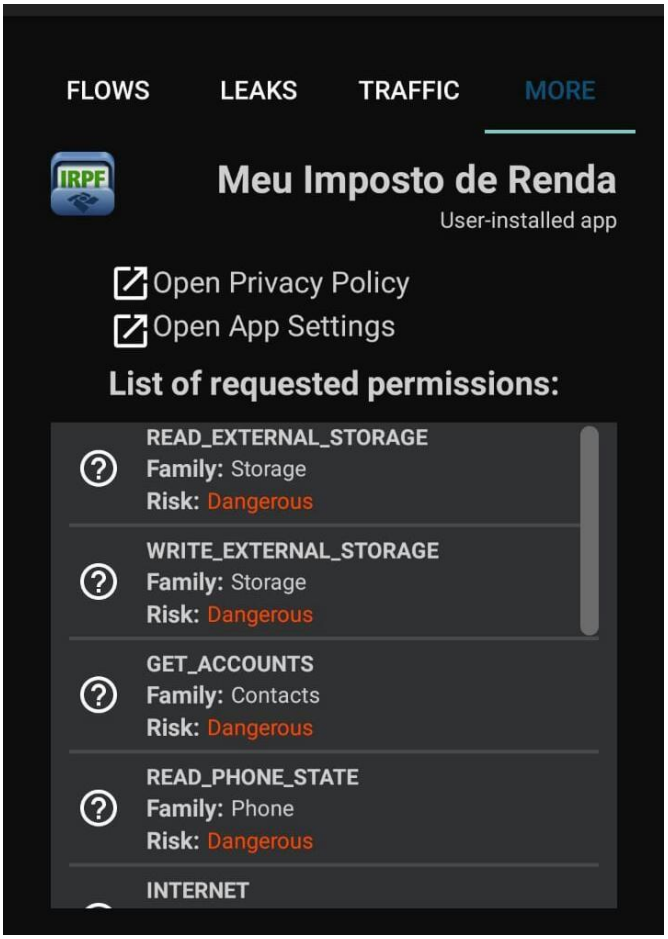
Outra permissão bastante evasiva é a de acesso à câmera do dispositivo, dos apps analisados apenas 02 possuem esse acesso, CNH Digital e Na Hora - DF. A

permissão parece fazer sentido para esses apps, pelo menos em princípio, porque ambos aplicativos possuem funcionalidades relacionadas com a leitura de documentos físicos (sejam boletos ou notas fiscais). Porém, essa permissão gera o risco de um app poder gravar vídeos secretamente ou tirar fotos a qualquer momento.

É possível verificar que os apps FGTS, CNH Digital, Digi-Sus e Bolsa Família possuem o privilégio de acessar contas (GET_ACCOUNTS), com esse acesso um aplicativo pode copiar toda sua agenda. Esses dados são altamente atrativos para *spammers* e falsários. Essa permissão também garante acesso à lista de todos os contatos usados em aplicativos no dispositivo – Google, Facebook, Instagram e outros.

De acordo com o relatório exibido pelo Lumen, outro conjunto de permissão que é classificado como perigoso é a permissão de acesso a memória externa, como cartões de memória ou a memória interna do dispositivo. Isso permite que os aplicativos leiam qualquer arquivo que esteja ali armazenado. Isso, em geral, é feito por aplicativos que precisam salvar e ler diferentes arquivos. No caso do app do Meu IRPF, por exemplo, é feito para permitir que o usuário reaproveite informações já inseridas na sua antiga declaração na elaboração da atual. Outra vez, entretanto, não fica claro porque essa funcionalidade é necessária para utilização de todos os aplicativos analisados.

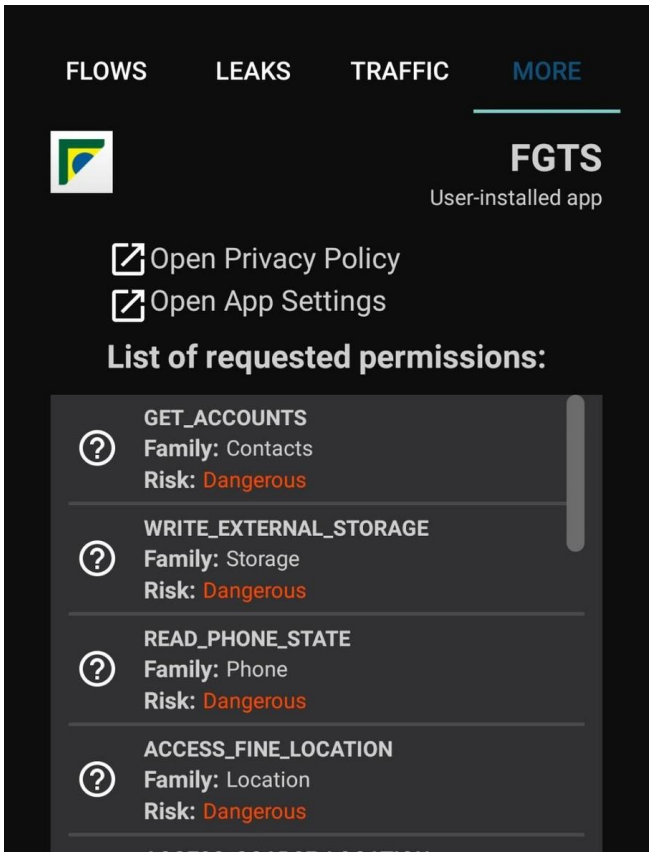
Figura 7 – Tela com as permissões de acesso do app IRPF



Fonte: Cópia de Tela do aplicativo Lumen Privacy Monitor com as descrições das permissões de acesso do sistema IRPF.

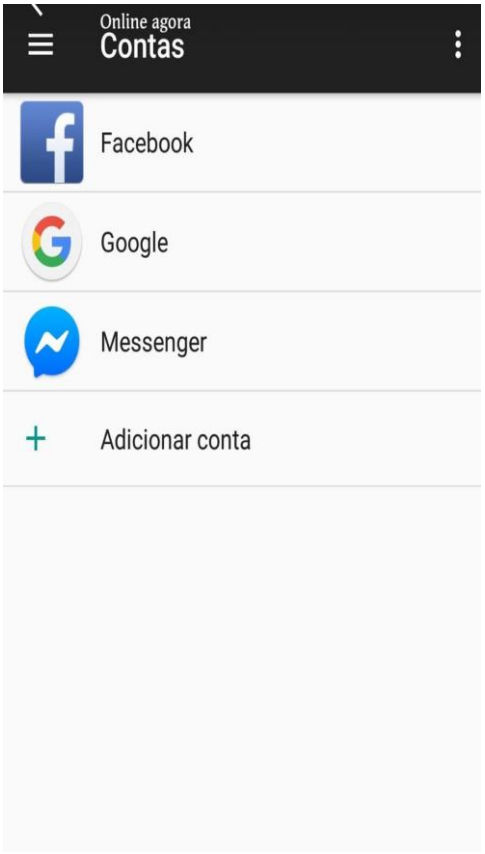
É possível notar também que alguns aplicativos possuem o acesso de ler o estado do telefone (READ_PHONE_STATE), esse privilégio, assim como o nome diz, tem acesso a informações número de telefone do dispositivo, informações de rede atuais, status de chamadas e lista de contatos registrados no aparelho. Os pontos perigosos desse privilégio é que ao liberar o acesso, você autorizava que o app faça praticamente qualquer coisa associada às comunicações por voz. Ele também saberá quando e para quem você ligar – e pode ligar para qualquer lugar, incluindo números pagos.

Figura 8 – FGTS permissão GET_ACOUNTS



Fonte: Cópia de Tela do aplicativo Lumen Privacy Monitor com as descrições das permissões de acesso do sistema IRPF.

Figura 9 – Contas ativas no dispositivo



Fonte: Cópia de Tela do sistema Android com as descrições das contas ativas no sistema operacional.

4.4 Compartilhamento de informações com terceiros

O crescimento das novas tecnologias e a capacidade de captar e utilizar dados pessoais por parte das empresas torna fundamental o debate sobre políticas de proteção de dados e a sua regulação, assim como sobre a privacidade do usuário, que está diretamente ligada aos direitos da personalidade. As plataformas tecnológicas ampliaram a possibilidade de coleta, processamento e vazamento massivo desses dados pessoais, com notórios danos aos direitos dos usuários.

O caso Facebook com a Cambridge Analytica (empresa privada que combina mineração e análise de dados com comunicação estratégica para o processo eleitoral) acendeu o alerta sobre as chamadas tecnologias invasivas das grandes corporações digitais sobre a vida do cidadão, colocando como principal desafio a construção de barreiras legais. Calcula-se que 87 milhões de pessoas foram atingidas, incluindo, nesse universo, 443 mil usuários brasileiros. Tudo começou com um teste de personalidade sobre a vida digital aplicado aos usuários que

concordaram com o teste. A Cambridge Analytica, contudo, coletou os dados dos amigos desses usuários para montar perfis voltados a influenciar eleitores (durante a última eleição americana) e para formar opinião (na campanha pela saída do Reino Unido da União Europeia), em flagrante afronta ao direito à privacidade. A ferramenta propicia indevido e indesejável “controle social”, muito ao gosto dos regimes totalitários.

Em Contrapartida, ao uso indevido de informações pessoais, a lei de proteção de dados não permite o compartilhamento de dados pessoais com terceiros sem o consentimento do titular, a não ser nos casos das exceções previstas em lei. É indispensável que no momento de apresentar seu consentimento, o titular seja informado, de forma clara e objetiva, sobre as ações de transferência de seus dados a terceiros e as possíveis implicações dessa transferência. Toda pessoa deve ter o direito de escolher os atores que farão o tratamento de seus dados, assim como ter o direito de acessar as informações sobre essa operação.

Diversos aplicativos utilizados hoje em dia, desde os mais simples aos com diversas funcionalidades, estão inseridos em um ecossistema de captura de dados. Mesmo que o procedimento seja transparente para o usuário, esse ecossistema engloba centenas de outras empresas que capturam, tratam e vendem dados pessoais. Nessa perspectiva, é possível diferenciar duas modalidades principais de coleta de dados nos aplicativos móveis:

A primeira envolve os dados recolhidos pelo sistema, por exemplo, textos, fotos, vídeos e metadados, são dados sobre outros dados, que o aplicativo usa para o seu próprio funcionamento.

Já a segunda modalidade envolve atividades de recolhimento de dados realizado por terceiros, ou seja, empresas diferentes da empresa que oferece o aplicativo ou serviço. Essa última modalidade é chamada de “third party tracking”. Essas empresas oferecem ferramentas para integrar os seus serviços aos ‘softwares’ desenvolvidos por seus clientes,

A coleta de dados nessa segunda modalidade é vasta, podendo abranger todos os meios digitais (notebooks, celulares, etc. . .) interligados para fornecerem dados às empresas de *tracking*. Com os dados em mãos as empresas podem fazer os mais diversos usos do referido dado.

O exemplo mais rotineiro é quando uma empresa traça um perfil do usuário com fins comerciais e, por exemplo, direciona uma determinada propaganda on-line ao mesmo. Faz isso com base no conjunto de sites/conteúdo que este usuário acessou nos últimos dias.

Diante das ideias vistas anteriormente, essa parte do estudo irá analisar se os

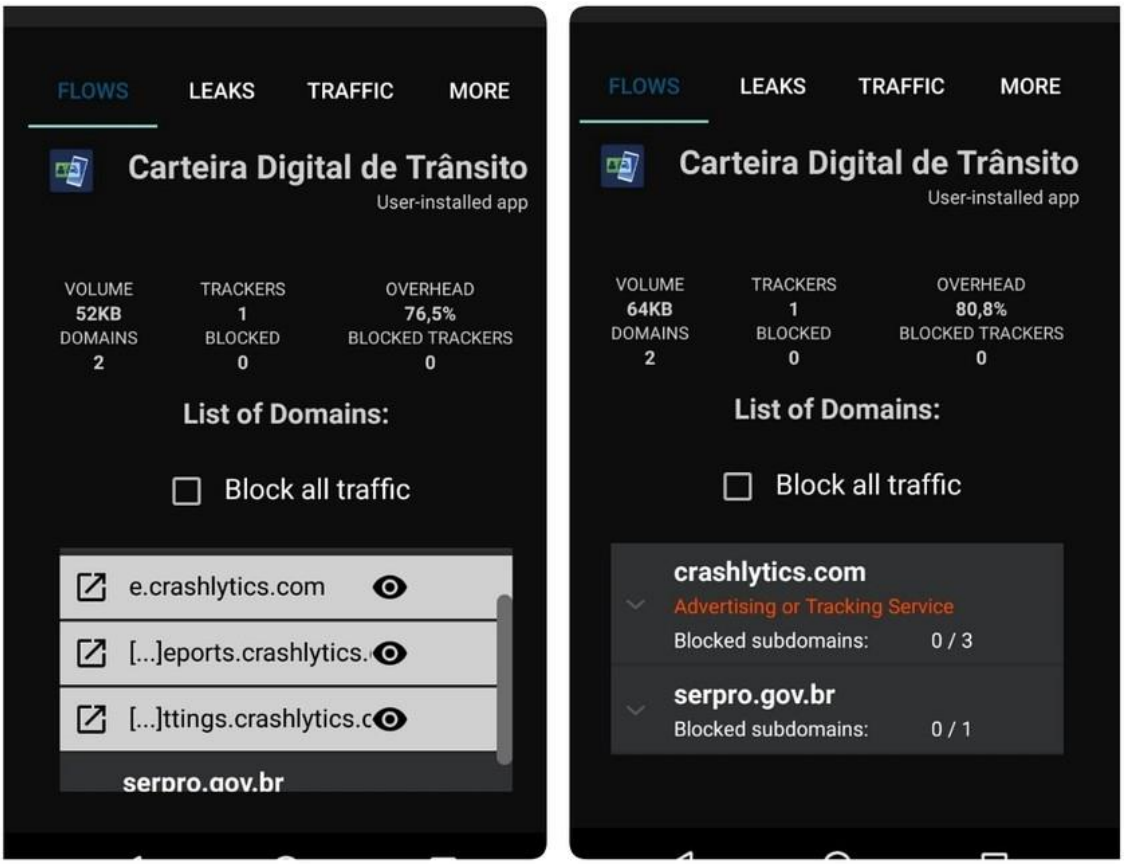
aplicativos móveis do governo possuem algum vazamento de informação. Para executar esse procedimento, utilizarei mais uma vez o aplicativo Lumen Privacy Monitor, para analisar o tráfego de dados dos aplicativos utilizados no dispositivo no qual ele é instalado e identificar “vazamentos” de dados pessoais.

Dos noves aplicativos analisados pelo Lumen, em cinco apps foi identificado a comunicação externa com terceiros. Os apps foram: SNE, Sigepe, CNH Digital, Meu Digi SUS e Nota Legal.

A análise dinâmica que monitora o tráfego de rede identificou que dados de alguns aplicativos estavam sendo vazados para outros domínios diferentes do original da aplicação.

O relatório demonstrado pela funcionalidade FLOWS do aplicativo Lumen relata que a aplicação CNH Digital, por exemplo, troca informações com os domínios crashlytcs.com e reports.crashlytics.com.

Figura 10 – Vazamento de informações da aplicação CNH Digital



Fonte: Cópia de Tela do aplicativo Lumen Privacy Monitor com as descrições das conexões do sistema CNH Digita com domínio externos.

Foi identificado que crashlytics é uma ferramenta de relatório de falha em tempo

real da Google. Em consulta à política de privacidade dessa ferramenta foi encontrado a seguinte informação:

> [.;.] As informações de relatório consistem no tipo de dispositivo, na versão do sistema operacional e em determinadas informações de hardware sobre o dispositivo móvel, bem como a hora da falha, o estado do aplicativo no momento da falha e os rastreamentos de pilha. As informações não incluem o endereço IP ou qualquer outra informação que possa ser usada para identificar o usuário ou seu dispositivo móvel individualmente e não inclui nenhuma outra informação do seu dispositivo [.;.]

No entanto, ao verificar a política de privacidade do CNH Digital não é encontrada nenhuma informação sobre essa ferramenta de relatório ou como funciona a comunicação com a mesma.

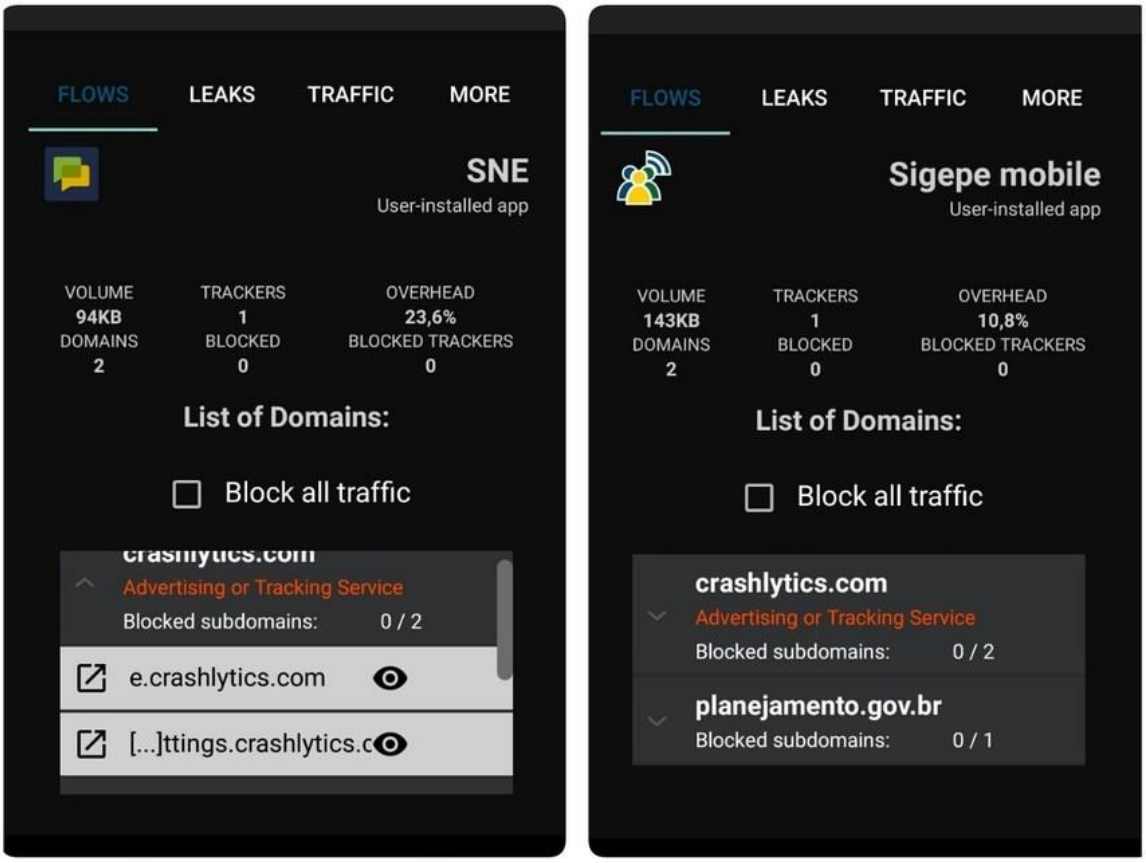
Vale destacar a seguinte informação da política de privacidade do CNH Digital:

> “Respeitadas as exceções legais, o Serpro e o Denatran não repassarão a terceiros informação de nível individual que por você seja cedida com este aplicativo.”

Os aplicativos SNE e Sigepe possuem o mesmo comportamento do software CNH Digital. Eles possuem comunicação com o domínio crashlytics

.

Figura 11 – Vazamento de informações da aplicação Sigepe



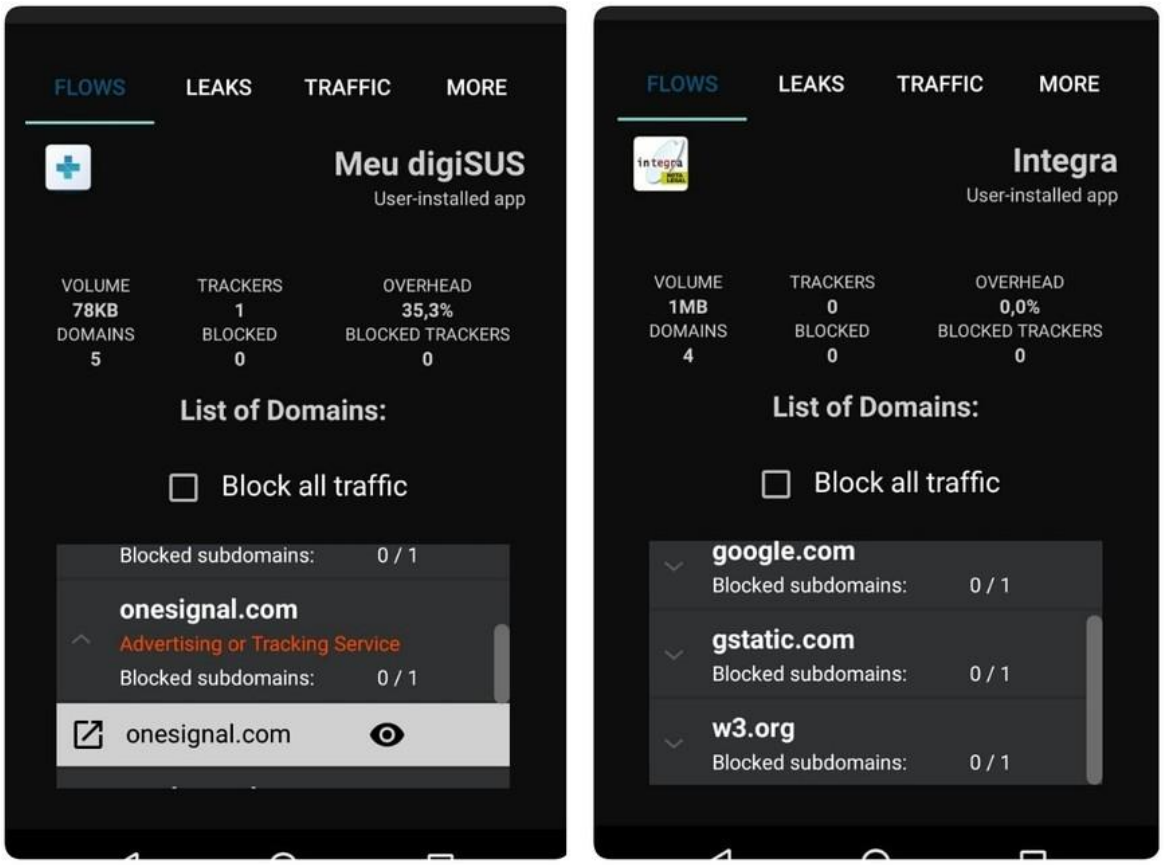
Fonte: Cópia de Tela do aplicativo Lumen Privacy Monitor com as descrições das conexões do sistema Sigepe com domínios externos.

Os softwares Meu digiSUS e Nota Legal também possuem comunicação com terceiros. Ao analisar esses dois apps, foi encontrado as seguintes Hipóteses:

O meu *digiSUS* possui conexão com o domínio onesignal.com. OneSignal é uma ferramenta para envio de notificações em massa. O meu digiSUS deve utilizar essa ferramenta para envio de mensagens ou p*oups* para os usuários.

Já o Nota Legal se comunica com o domínio gstatic.com e *google*. com. Foi verificado que o *gstastic* é um *coockie* pequenos arquivos gravados pelos navegadores de internet no computador dos usuários, que usa esse domínio para descarregar conteúdo estático (código JavaScript, imagens e CSS) para um nome de domínio diferente, em um esforço para reduzir o uso de largura de banda e aumentar o desempenho da rede para o usuário final.

Figura 12 – vazamento de informações da aplicação Meu digiSUS



Fonte: Cópia de Tela do aplicativo Lumen Privacy Monitor com as descrições das conexões do sistema Meu digiSUS com domínio externos.

Embora se comprove a ligação dos aplicativos analisados com serviços de terceiros, não foi encontrado nenhuma publicidade nessas aplicações. No entanto, é evidente que a política de privacidade desses 'softwares' não é transparente para o usuário. Visto que alguns apps, como o SNE e CNH Digital, por exemplo, não possuem uma política específica para o seu serviço e não são transparente quanto ao tratamento e compartilhamento de informações pessoais dos usuários.

5 Conclusão

Diante das informações levantadas neste estudo, podemos observar alguns pontos que precisam de melhoria sobre o tratamento de dados pessoais nas aplicações móveis do governo. Pois para se adequarem as novas exigências da lei de proteção de dados, Lei nº 13.709/2018, será necessárias algumas adequações.

Um dos pontos de adequação seria referente a política de privacidade, onde é preciso desenvolver uma política com informações mais claras e de fácil acesso pelo usuário. De forma a deixar evidente sobre qual será o período de armazenamento dos dados e qual o procedimento para requerer a exclusão dessas informações, visto que nenhuma das políticas de privacidade analisada possuem essas informações.

Outro ponto é que precisa ser adequado são os graus de consentimento, visto que trata da principal fase do processo de tratamento de dados pessoais, e o usuário deve ter a ciência sobre como serão tratadas as suas informações pessoais e as implicações do tratamento.

O consentimento do titular para compartilhamento de dados com terceiros também deve ser evidente, pois é vital que no momento de apresentar a sua autorização, o titular do dado seja informado, de forma objetiva, sobre as ações de compartilha- mento de seus dados a terceiros e as possíveis consequências.

Acrescenta-se também a técnica de anonimizarão dos dados, onde é um dos procedimentos recomendados pela LGPD para assegurar e proteger os dados pessoais. O trecho abaixo explica bem o conceito de anonimização de dados:

LEMOS (05/2018, A anonimização é a forma mais rígida de proteção de dados pessoais. Através de “chave” criptográfica, os dados são anonimizados, e, por consequência, podem perder sua característica de “dados pessoais” e, desse modo, ser processados, armazenados e compartilhados sem risco de identificação de seus titulares. O objetivo imediato é, portanto, assegurar que os dados armazenados não permitam a identificação dos cidadãos, escondendo de forma permanente informações que os individualizem. Ainda, o uso de criptografia para a codificação de dados evitaria que atores mal-intencionados tenham acesso a informações coletadas por meio de soluções IoT, de forma a resguardar a identidade do titular de dados.)

Nesse sentindo, esse procedimento deve ser utilizado sempre que possível, como no caso de estudos em saúde pública e por órgãos de pesquisa. É, também, um dos direitos assegurados ao titular, ao identificar que seus dados estão sendo

utilizados de forma desnecessária, excessiva ou em desconformidade com a lei.

O aplicativo meu digiSUS se enquadra nesse caso, uma vez que trata diversos dados sensíveis, como medicamentos, exames de sangue, vacinas e transplantes.

Como o ministério da saúde possui um banco de dados muito rico em informações, seria interessante aplicar essa técnica de anonimização de dados antes de interligar base de dados entre entidades do governo ou se prevenir de um possível vazamento de informações.

Por fim, a legislação sobre proteção de dados deve implementar uma série de garantias aos cidadãos. Entre elas, deve constar o consentimento, o princípio de legítimo interesse que é capaz de mitiga-lo quando necessário, o princípio da finalidade, da transparência, além do princípio da necessidade e proporcionalidade.

Referências

BRASIL, Casa Civil. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www. planalto. gov. br/ccivil_03/_ato2011-2014/2014/lei/l12965. htm. Acesso em

COELHO, Gabriela. MP-DF acusa empresa pública de vender dados pessoais de brasileiros. **Consultor Jurídico.** 31 de maio de 2018. Disponível em: https://www.conjur.com.br/2018-mai- 31/mp-df-acusa-empresa-publica-vender-dados-brasileiros. Acesso em: 28/12/2018. Citado na página 18.

LEMOS, R.; ADAMI, M.P.; SUNDFELD, P. Proteção de dados na Administração Pública. **Jota.** 14 de maio de 2018. Online. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados- administracao-publica-14052018#sdfootnote3anc . Acesso em: 02/02/2019.