

PRIVACIDADE E SEGURANÇA EM APARELHOS SMARTPHONES

PRIVACY AND SECURITY IN SMARTPHONES

Leonardo Dias Venzo¹, Aléssio Cagliari²

RESUMO: A privacidade de smartphone vem sendo invadida sem a percepção e consentimento de seus usuários. Assim essa pesquisa busca um estudo sobre a viabilidade de criação de um aplicativo para aprimorar os aparelhos para que os mesmos possam oferecer maior segurança aos dados e funções do smartphone. O Objetivo geral desse trabalho é desenvolver um estudo sobre o funcionamento dos apps e sistema dos telefones moveis com o intuito de desenvolver uma solução para que o aparelho móvel se torne mais seguro e com maior privacidade. A metodologia utilizada foi por meio de estudo de caso em empresa que presta assistência técnica de manutenção em aparelhos eletrônicos com ênfase em smartphones, realizando-se uma pesquisa aplicada de abordagem qualitativa, a fim de identificar o custo-benefício de utilização desta nova tecnologia, utilizando-se de pesquisas de informações públicas de custo de desenvolvimento de softwares, realizando assim comparações de custos de desenvolvimento, manutenção do aplicativo e viabilidade de venda ao consumidor. Como resultado, apresenta-se neste trabalho os principais pontos a serem analisados, como também quais os tipos de contratações seriam mais viáveis para o desenvolvimento desse aplicativo. Apresenta-se ainda uma estimativa de gastos e em quanto tempo a empresa levaria para ter o aplicativo desenvolvido para colocar à disposição dos consumidores. Por fim chegou-se à conclusão de que a elaboração do software para a empresa não possui viabilidade financeira para que possa ser executada.

Palavras-chaves: Tecnologia; Celulares; Informações; Inteligência; Artificial; Segurança.

ABSTRACT: the privacy of the smartphone is being cut without the perception or the consent of the user. Knowing that this research seeks to study about the viability of the creation of an app to upgrade the smartphones making them safer for the user. the objective of this paper is to develop a study about how the apps and operational systems work and then develop a solution for the safety and privacy problems. the methodology used was a visit and study in a business that fixes electronic devices, the study was focused in understanding the cost-benefit of the previous mentioned technology and the total cost of the development of said project. This way the study will know the final price of the product for the consumer and the viability of this project. As the result this study presents the priority points as well as presents the professionals that must be involved in the project. Another thing that is shown by this study is the necessary investment of money and time to be spent on the completion of this project.

Keywords: Technology; Cell phones; Information; Artificial Intelligence; Security.

¹ Acadêmico do curso de Gestão em Tecnologia da Informação, Centro Universitário FAI, leovenzo@hotmail.com.

² Mestrando em Ensino Científico e Tecnológico pela Universidade Regional Integrada de Santo Ângelo – RS, URI. Especialista pela Escola Superior Aberta do Brasil - ESAB. Professor do Curso de Gestão da Tecnologia da Informação da UCEFF.; CV: <http://lattes.cnpq.br/3452115034451206> E-mail: alessioic@gmail.com.

1. INTRODUÇÃO

O cientista Charles Darwin criou a teoria da evolução, ideia essa de que as espécies mudam gradualmente de uma geração para outra, por meio de um mecanismo chamado de seleção natural. Este processo faz com que a espécie humana mude e se diversifique ao longo do tempo. Na área tecnológica a evolução também é constante e quando a conectividade chegou, o mundo inteiro pode conversar e trocar experiências, emoções, fotos, histórias, documentos e arquivos, hoje o mundo está na palma da mão, pode-se utilizar a internet do telefone celular para tudo que se deseja, contudo, como explica o muito bem detalhado documentário *The Great Hack*, (2019), “somos um produto de empresas que fazem mais de trilhões de dólares ao ano, todas as nossas atividades são monitoradas em tempo real, como por exemplo: Uso do cartão de crédito, pesquisas, localidades, likes.”

Ao navegar na internet, por diversas vezes são apresentados anúncios e propagandas relacionadas às pesquisas anteriores e conversas com outras pessoas, como se as informações estivessem conectadas a um microfone oculto e repassadas ao seu computador. A sensação de que estamos sendo observados é uma constante e pode ser bem notória com o uso das redes sociais. Exemplificando: Em uma conversa particular pelas redes, há poucos instantes, o comentário é sobre a compra de uma televisão, em sequência ao navegar, se visualiza uma oferta de televisão em uma loja de confiança, seria isso coincidência ou falta de privacidade de dados?

A realidade nos meios de uso da internet é que estamos constantemente passando por análises de comportamento, dando assim previsão de potencialidade, principalmente com vistas à compras, então os anúncios surpreendentemente parecem precisos com aquilo que estamos buscando nos dando a impressão de que estamos sendo monitorados, quando na verdade são exatamente análises de perfil que os próprios usuários autorizam.

Tudo é analisado e ligado a personalidade do usuário, essa possibilidade de cadastro de informações, cria potencialidade de mercado, como uma ferramenta de banco de dados de clientes em potencial, fazendo assim com que o comprador dessas informações, conheça melhor os anseios de cada um, podendo direcionar produtos de acordo com pesquisas feitas na rede, qual é o limite do cliente e o que seria necessário para atravessar esse limite. Humbray (2019) afirma que os dados são o novo petróleo, tem imenso valor, mas que sem refinação não pode ser usado, dados somente podem ser usados quando são analisados. Assim muitas

vezes a opção: “Eu aceito os termos e condições,” possibilita estudo de perfis e criação de banco de dados sem que o usuário perceba que está sendo analisado.

2. REVISÃO TEÓRICA

2.1 SISTEMA DE SEGURANÇA E PRIVACIDADE

Hoje existem vários sistemas de segurança para proteger os dados de seu aparelho móvel, esses aplicativos servem para aumentar a segurança do seu dispositivo e dos aplicativos nele instalados, pois alguns programas podem ter um elemento duvidoso que podem fornecer mensagem com o código de ativação para roubar dados da conta do usuário. (ROHR, LAVADO, 2019)

O celular se tornou um instrumento essencial na vida das pessoas, pois com o avanço tecnológico através dele o usuário pode ter acesso a há diversas ferramentas que atendem a sua necessidade básica que vai desde da socialização com os amigos até uma simples transação bancária.

“O celular é um dos instrumentos viabilizadores da comunicação, principalmente privada. A privacidade na comunicação é maculada quando, sem o desejo ou o consentimento do dono, terceiros acabam acessando o conteúdo existente no aparelho, ainda que no exercício do dever constitucional da segurança pública pelas autoridades policiais (CF/88, art. 144 da CF/88), que compreende a atividade persecutória estatal pela Polícia. Desta forma, há um potencial conflito de direitos, de um lado, o direito fundamental à privacidade (art. 5º, X e XII, da CF/88), incidente nos instrumentos que viabilizam a comunicação, e de outro, o direito social à segurança pública (arts. 6º e 144 da CF/88), no qual se insere a persecução criminal.” (SILVA, 2018)

Para Richard Stallman os smartphones tem um sistema que localizar o usuário e só permitem a instalação de programas que possuam essa função. O Richard foi o criador do primeiro sistema operacional livre, onde o usuário pode utilizar sem precisar fazer o seu cadastro e o sistema não têm como verificação a sua localização e nem saber sobre a sua localização. Atualmente a sociedade em boa parte do mundo está sendo monitorada 24 horas por dia, através de câmeras e aplicativo instalados no dispositivo de localização. Dessa forma as empresas tem todos os dados do usuário e sabe de suas necessidades antes mesmo do portador do aparelho. Tudo isso só é possível através do controle da conta. (RIBEIRO, 2019)

Há várias maneiras de proteger seu dispositivo através de um sistema que cria senhas para os aplicativos e algumas precauções que usuário precisa ter, evitando abrir mensagens de

pessoas desconhecidas e de entrar em sites de origem duvidosa, como também está com o antivírus sempre atualizado. (RINALDI, 2019)

A privacidade de um aparelho de celular tem o seu limite, em caso que o aparelho possa ser uma das provas de um ato ilícito, essa privacidade pode ser invadida por ordem judicial. Também em caso de emergência, nesse caso não é necessário que se tenha uma ordem judicial, para a invasão do aparelho. (SILVA, 2018)

O problema que envolve a segurança e privacidade do usuário, não envolve apenas dispositivos móveis, como: celular, smartphone, iphone, ipad, entre outros, mas também outros, como: computadores e notebooks e também dispositivos bancários, para evitar essas exposição, também foram criados sistemas de segurança, pois a maioria dos estabelecimentos bancários já disponibiliza aplicativo para que seja feita as transações bancárias dos correntistas pelo aparelho de celular. Para que isso ocorra com segurança é relevante que o usuário baixe o aplicativo do site seguro das instituições bancárias e que tenha certa cautela quando for utilizar.

2.2 INTELIGÊNCIA ARTIFICIAL

O projeto de pesquisa para a criação da AI³, ocorreu no ano de 1956 e contou com ajuda de 10 cientistas, que foram organizados por John McCarthy. Esse projeto na época, foi intitulado de *Dartmouth Summer Research Project on Artificial intelligence*. O intuito era criar uma inteligência que tivesse algumas das características da inteligência humana, onde fosse possível: calcular, a utilização de idiomas e de neurônios e que também fosse capaz de manipular as palavras. (McCARTHY, 1955 apud PIMENTEL, OLIVEIRA, SILVA, 2018)

A inteligência artificial até hoje não tem uma definição concreta entre os grandes pesquisadores, pois para isso seria necessário primeiro definir o que seria inteligência humana e estabelecer uma ligação entre ambas, através de alguns pontos que são considerados relevantes. De acordo com o físico Alan Turing, inteligência é a habilidade de executar tarefas cognitivas onde fosse possível enganar um interrogador. O teste seria feito para medir a capacidade do computador de se comunicar como um ser humano, de armazenamento de informações colhidas no interrogatório, de usar as informações para responder as perguntas feitas no interrogatório e de aprender ou superar os padrões, porém ainda não foi inventada uma máquina que tivesse criatividade ou que tivesse o lado emocional, o que de acordo com

³ AI Inteligência Artificial

uceff.edu.br

Centro Universitário FAI • |49| 3678.8700
Rua Carlos Kummer, 100
Bairro Universitário
Itapiranga - SC • 89896-000

Centro Politécnico • |49| 3319.3800
Av. Irineu Bornhausen, 2045 E
Bairro Quedas do Palmital
Chapecó - SC • 89814-650

Unidade Central • |49| 3319.3838
Rua Lauro Müller - 767 E
Bairro Santa Maria
Chapecó - SC • 89812-214

os pesquisadores isso ainda estaria longe de acontecer. (FILHO, ALCOFORADO, LIRA, 2018)

Mesmo com a relevância que tomou o tema recentemente, os estudos vêm de longo tempo. O homem sempre teve interesse de criar uma máquina parecida com o humano, mesmo através de pequenas descobertas, porém no último século alguns nomes se destacaram no auxílio da concretização da tão sonhada criação, como no campo da computação lógica, da matemática e da neurociência. (COELHO, 2017)

Quando se refere a inteligência artificial, algumas pessoas acreditam que é algo ainda distante da realidade que vivemos, resumido apenas aos filmes de ficção científica. Mark Twain dizia, e tinha razão, que a diferença entre a realidade e a ficção, é que a ficção tinha que mostrar uma credibilidade para o público, enquanto que a realidade já a possuía. Mas se observamos ao nosso redor já a utilizamos e nosso cotidiano e nem percebemos. O primeiro tipo de AI utilizado foi o uso de algoritmos inteligentes utilizados para solucionar problemas, que o homem levaria um certo tempo para resolve-lo e com uma enorme margem de erros. (JUNIOR, 2017)

Os anos de ouro para a AI foram entre os anos de 1950 e 1970, onde ocorreram enormes avanços na área. Foram estudadas as Redes Neurais, tiveram avanço nos algoritmos e a inteligência passou a ser utilizada em jogos. Então especificamente no ano de 1956, o sistema passou formalmente a se chamar de Inteligência Artificial.

Nesse período se viu a possibilidade de a AI ser utilizada na área de direito. No entanto foi na década de 70 que a sua inclusão passou a ser realidade, com os projetos LEGOL 19 e TAXMAN. Nas décadas seguintes passou-se a debate sobre a viabilidade de sua aplicação no jurídico. (COELHO, 2017)

Conforme foi abordado, na década dos anos 50, pesquisadores estavam convencidos de que I.A. seria relevante nos próximos anos. Contudo, os inúmeros anos dedicados a pesquisa promoveram pequenos avanços. Diante do desafio, muitos achavam que nunca seria possível criar máquina capaz de simular a função humana. A complexidade da tecnologia é tal que mesmo em face dos modernos avanços não se imaginava que seria alcançada em futuro próximo. Hoje poucos pesquisadores são ativos na área; projetos são diversos e geralmente pioneiros em natureza. (COELHO, 2017)

Na Inteligência artificial está inserida:

“Machine Learning é caracterizado como estudo e desenvolvimento de algoritmos capazes de aprender e fazer previsões a partir de dados, superando programações estritas e limitadas a escopos iniciais e concedendo

a computadores a capacidade de “aprender sem serem expressamente programados”. São aplicados em tarefas computacionais nas quais a programação de algoritmos específicos se revela difícil ou inviável, como visão computacional e tradução de textos. (COELHO, 2017, p. 21)

Redes Neurais consistem em uma família de modelos de Machine Learning baseada na estrutura neural biológica observada no cérebro humano. O modelo está compreendido na abordagem conexionista de estudos de I.A., iniciada na década de 40. Apesar de ser hoje o arquétipo mais adotado no campo, não recebera devida atenção até o início dos anos 80. (COELHO, 2017, p. 23)

As redes artificiais são estruturadas em três camadas básicas: (i) camada de entrada (input layer), que recebem estímulos externos à rede, (ii) camada de saída (output layer), que transmitem estímulos para fora da rede, e (iii) camada(s) intermediária(s) ou oculta(s) (hidden layers), responsável pelo processo de aprendizagem da rede e comunicação entre as demais. As camadas podem possuir número variável de neurônios, a depender da arquitetura adotada para o modelo.” (COELHO, 2017, p. 26)

Não foi só no judiciário que ela ganhou destaque, mas também nas previsões de quem será o próximo presidente, as regiões que existem maior probabilidade de propagar alguma doença viral, onde será o próximo abalo sísmico, se será possível a existência de uma crise econômica nos próximos anos, o percentual de reincidência de um criminoso ou a credibilidade de uma pessoa se tornar um futuro devedor na linha de crédito. Esses são alguns exemplos da utilidade da AI (DONEDA, 2018).

Podemos observar que a inteligência artificial vem sendo utilizada como recurso de captura de informações de usuários de redes sociais, não há necessariamente um monitoramento realizado por pessoas e sim com o uso de programas que monitoram palavras chave em conversas, utilizando a captura de áudio e pesquisas feitas no computador. Assim com o recolhimento das palavras chave é possível criar um perfil de consumo, tornando possível a propagando para sites de vendas direcionado para o público alvo.

2.3 A SOCIEDADE DIANTE DA NOVA TECNOLOGIA

As pesquisas no meio científico esteve sempre voltada para a criação de um homem que superasse as suas limitações, sem se preocupar muito com o seu bem-estar, porém essas limitações com o decorrer da história nunca foi superada, então surgiu a possibilidade da criação de uma máquina que tivesse as características do ser humano e com o tempo, fosse sendo aperfeiçoada para superar algumas limitações. Com esse objetivo foi criado o

computador “Deep Blue”, que em 1977, conseguiu vencer no jogo de xadrez, Gary Kasparov, o campeão mundial da categoria. (JUNIOR, 2017)

Pela revolução na informática ocorrendo de uma maneira bastante acelerada, onde, principalmente há trocas de informações, sentiu-se a necessidade de ser revisto a segurança em relação a identidade e privacidade desses dados. Com esse objetivo o Parlamento Europeu – *The European Parliament*, no ano de 2016, passou algumas recomendações à Comissão sobre disposições de Direitos Civil sobre a Robótica, para evitar problemas futuros com o desenvolvimento da Inteligência Artificial. (AFFAIRS, 2016, p.4 apud (PIMENTEL, OLIVEIRA, SILVA, 2018)

2.4 O DIREITO CIVIL E A TECNOLOGIA

O direito, com o desenvolvimento de novas tecnologias, está formando nova leis onde envolve não só as pessoas, nas relações sociais e comerciais, nem tão somente o Estado, mais também ao novo sistema que está sendo implantado na sociedade através de estudos com AI. Para que se tenha uma convivência equilibrada entre pessoas e máquinas, é relevante que seja elaborada regras ao uso e a responsabilidade de caso haja uma falha no sistema, como exemplo podemos citar, problemas com o reconhecimento do responsável por um acidente causado por um carro autônomo ou de robô utilizado em serviços domésticos? (JUNIOR, 2017)

Essa questão foi levantada por Ryan Calo (2015, p. 513-515) ao abordar as três características que o robô humanoide passa a possuir, que são: materialidade, que é o seu formato de humano, comportamento emergente que está relacionado a sua autonomia na execução de certas atividades e o de valor social, por despertar no humano um envolvimento diferente em relação ao robô. Por essas características volta-se a levantar questão sobre que seria o responsável por algum dano causado por algumas dessas máquinas ou de quem seria a responsabilidade se a máquina tivesse um comportamento imprevisível diante de uma situação? (DONEDA, 2018)

Antes para se ter direito dentro de uma sociedade, primeiramente era necessário que seja classificado como pessoa. Onde nesse perfil só se incluiria o homem, porém com o Código Civil Brasileiro de 2002, passou a incluir a mulher, para não haver discriminação de sexo e a pessoa jurídica passou a ser as empresas que são representadas por pessoas, que tem direitos e deveres. Com o avanço da tecnologia, essa visão tende a mudar por causa da

inclusão e desenvolvimento da AI, que passou a fazer parte do cotidiano da sociedade. (FILHO, ALCOFORADO, LIRA, 2018).

3. METODOLOGIA

Este artigo tem a finalidade de apresentar a vulnerabilidade de dados pessoais que são transmitidos em smartphones e como aplicativos tomam dados de usuários sem o seu consentimento.

Quanto aos objetivos a pesquisa será descritiva, que como segundo Rampazzo e Corrêa (2008, p. 73) consiste em “observar, registrar, analisar e correlacionar fatos ou fenômenos (variáveis) sem manipula-los; estabelecer relações e conexões entre variáveis; utilizar técnicas padronizadas na coleta de dados”. Desta forma se obtém um embasamento melhor sobre o assunto.

Sua abordagem será qualitativa, ou seja, depois que os fatos forem coletados e estudados serão avaliados como um todo, para ajuda na tomada de decisões sobre a sua implementação. Rampazzo e Corrêa (2008, p. 71) afirmam que “na pesquisa qualitativa todos os fenômenos são importantes, a consistência, a interrupção, a fala e o silêncio. Buscar compreender o que a eles subjaz.”

Este artigo se caracteriza como sendo uma pesquisa bibliográfica, que foi o método utilizado para obtenção do referencial teórico que embasa o tema proposto que é privacidade e segurança em aparelhos celulares. Para a melhor formação e segurança do projeto será consultado e utilizado material

Bibliográfico de diferentes fontes, juntamente com a análise do processo de implementação do estudo. Quanto a pesquisas bibliográficas, Rampazzo e Corrêa (2008) afirmam que as pesquisas bibliográficas procuram esclarecer um problema a partir de referências teóricas feitas em documentos. Que são pesquisas produzidas exclusivamente a partir de materiais que já foram produzidos como livros, jornais, revistas enciclopédias.

4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

A análise feita foi realizada em empresa de manutenção de smartphones e aparelhos eletrônicos, como tablets e notebooks entre outros assemelhados. Localizada na cidade de

Tenente Portela, pertencente a Região Celeiro do Rio Grande do Sul que abrange 21 municípios, a empresa é do ramo de franquias e possui pequeno porte, tendo 2 funcionários no seu quadro de pessoal, sendo um cargo de atendente e um técnico exercido pelo proprietário que possui formação em Ciências da Computação, e que atende diariamente 20 pessoas para análise de serviço e orçamentos e em torno de 3 ordem de serviços - OS diárias.

O processo de trabalho consiste em cadastramento de clientes pelo atendente, o qual faz a primeira avaliação, sendo que posteriormente faz o recebimento do aparelho e encaminha para análise do técnico, o qual faz observações sobre o estado do aparelho, sob a viabilidade de conserto e apresenta o orçamento. Após o retorno do cliente autorizando o reparo, é emitida ordem de serviço - OS para execução do trabalho, que podem ser como exemplo, troca de tela, troca de microfone, troca de carcaça, limpeza de aparelhos, atualização de software, reinstalação de software, limpeza de software, desoxidação de aparelhos, reparo de placas entre outros serviços de manutenção.

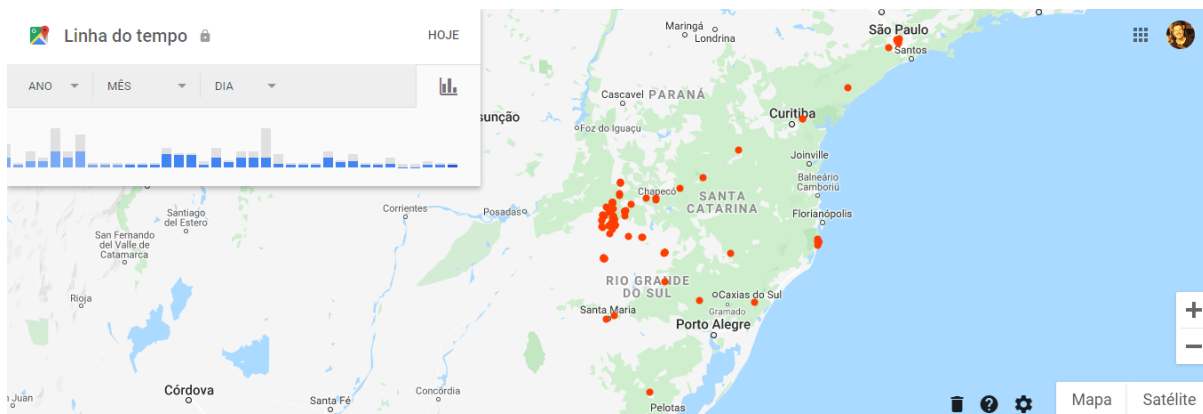
Após o término do serviço tendo o aparelho, “com solução”, é comunicado ao cliente para efetuar o pagamento e posterior retirada. Quando o aparelho é entregue, “sem solução”, o cliente paga somente a taxa de análise e serviço, e o mesmo é devolvido ao seu dono.

Foram observados, que após a realização dos serviços de manutenção de softwares em smartphones, que há fragilidade nos dados pessoais dos clientes, pois os mesmos muitas vezes dependiam apenas da ética do profissional que realiza a manutenção, o que na empresa pode ser constatado existir, já que além do caráter pessoal do técnico, ainda há zelo por fazer parte de franquias o que repassa aos clientes o sentimento de confiabilidade em entregar seus aparelhos onde estão armazenados os dados particulares de cada um.

Porém somente a ética dos técnicos não garante a privacidade de dados, pois ao aceitar os Termos e Condições de uso de redes sociais, e alguns aplicativos o usuário do smartphone permite que esses acessem todo o conteúdo e funções do telefone, podem oportunizar-se dessas informações como por exemplo o direcionamento de páginas de compras após um aplicativo de rede social reconhecer uma palavra chave e assim oferecer um produto relacionado a essa palavra.

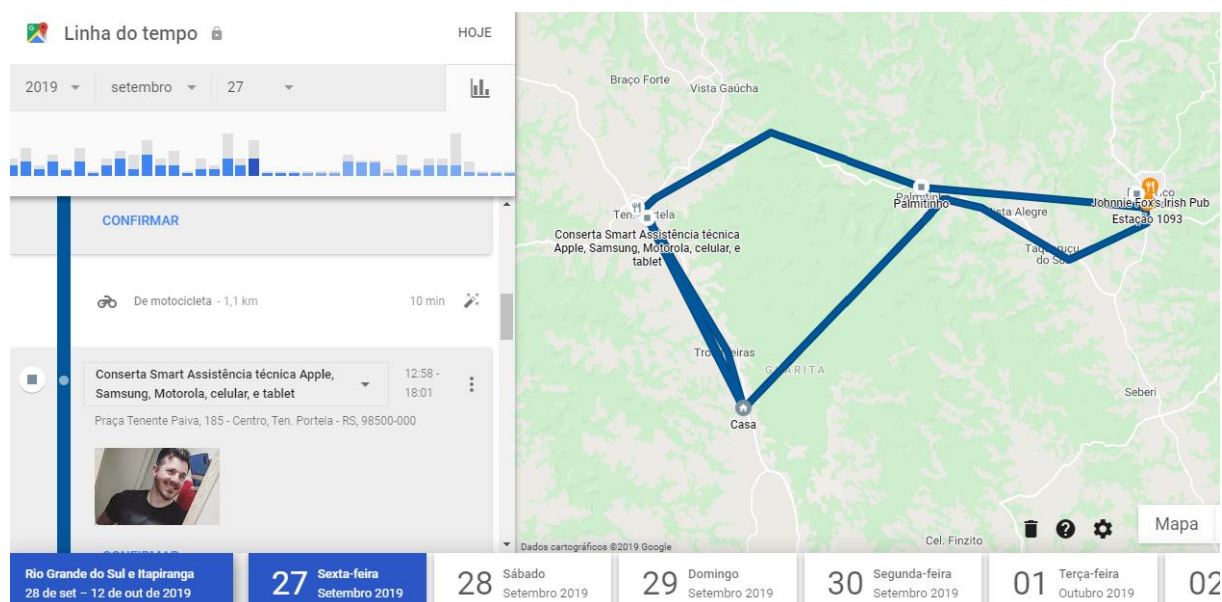
Destaca-se ainda que aplicativos que usam o GPS, podem traçar seu perfil de consumo pelos lugares mais frequentados pelo portador do aparelho smartphone, mostrando assim sugestões de lugares os quais o usuário tem potencialidade de frequentar, assim como pede avaliações de locais mesmo sem ser realizado checkin pelo portador do smartphone.

Figura 1 – Exemplo do uso do GPS no smartphone. Timeline do google maps, todos usuários do sistema operacional Android tem toda sua atividade e locais que frequenta quando estava portando o seu smartphone.



Fonte: Pagina Google Timeline (2019).

Figura 2 – Figura demonstrando de forma mais detalhada como funciona o registro do timeline, o sistema registra como você chegou em seu destino, o tempo que levou, os locais em que parou, fotos que tirou no processo, data e hora.



Fonte: Pagina Google Timeline (2019).

Analisando os dados apresentados, visualizou-se a necessidade de criação de bloqueadores para uso de informações, mas que ao mesmo tempo permita que a pessoa

continue usando as redes sociais, sites de busca, GPS e outros, pois alguns são utilizados como ferramenta de trabalho e tornam-se indispensáveis ao mundo atual.

A criação de um aplicativo que refinaria as autorizações de uso para que apenas o que estivesse expressamente escrito fosse autorizado, pois o simples “eu aceito” não permite questionamentos por parte do usuário, tornando-se semelhante a contratos de adesão onde as cláusulas não podem ser modificadas ou personalizadas, o que desfavorece uma relação de consumo onde se tem a “oferta” de um produto e a “compra”.

Como não existe atualmente nenhuma possibilidade de personalização dos - Termos e Condições de uso - e sem essa concordância não há possibilidade de utilização dos aplicativos em questão, a solução que se apresenta é o desenvolvimento de aplicativo bloqueador/inibidor de uso de microfones, câmeras e dados restritos, e que emita alerta ao usuário sempre que essas funções forem ativadas remotamente, ou seja não por solicitação do portador.

Os recursos necessários para a implementação dessa tecnologia são uma equipe de programação, desenvolvimento, gerenciamento de tarefas, computadores para o design e programação, um servidor para manter o aplicativo online e atualizado já que como os aplicativos atualizam seus termos e condições também mantendo o banco de dados do aplicativo, a equipe de programação deverá atualizar também os do aplicativo, um SDK (Software development kit) que se trata de um pacote de desenvolvimento de software.

O aplicativo seria lançado para Apple Store (Sistema operacional para telefone quem tem sistema operacional IOS, Iphone), Google play (Sistema operacional de quem usa Android), o mesmo fica instalado no celular de quem o baixar, pois é um software. Assim quando o usuário faz uma ação o aplicativo apenas se conecta ao banco de dados para buscar e transmitir informações.

A equipe de profissionais que é necessária seria formada dos seguintes profissionais com preços médios de serviços, disponíveis em sites de busca da internet em torno do descrito abaixo:

Designer que se encarregaria de toda a parte do front end (parte visual de um aplicativo) como botões, aparência, cores, interfaces e principalmente usabilidade. 30R\$ por hora 180 horas por mês (20 dias úteis por mês) salário R\$5.400 (cinco mil e quatrocentos reais).

Web design o que aplica todo o layout projetado pelo designer, ajuda na parte back end (Parte de código não visível para o usuário). R\$4.000,00 (quatro mil reais). Sendo assim, uma hora de trabalho de um webdesigner seria de aproximadamente R\$23,00 (vinte e três reais).

Analista de sistemas que é o profissional que vai entender a necessidade do aplicativo especificando por escrito tudo o que o software deve fazer. Um analista de sistemas, de acordo com a Tabela, ganha entre R\$2.500,00 (dois mil e quinhentos reais) e R\$17.000,00 (dezessete mil reais).

Arquiteto de softwares analisa as necessidades de todo o projeto, define a arquitetura que melhor se encaixa ao aplicativo. ganhando R\$7.572,00 (sete mil quinhentos e setenta e dois reais) de salário e pode vir a ganhar até R\$12.105,00 (doze mil cento e cinco mil reais);

Programador ou desenvolvedor o responsável por transformar todas as especificações do software em um código, seguindo rigorosamente a análise funcional do analista e as diretrizes do arquiteto. Também o código que faz ponte com a conexão do banco de dados, parte visual, leitura e gravação de informações. Essa parte representa cerca de 50% de um projeto. A hora técnica de um bom programador pode custar de R\$161,00 (cento e sessenta e um reais) até R\$404,00 (quatrocentos e quatro reais) / hora, dependendo do nível de programação e dificuldade no projeto.

Analista de banco de dados (DBA) o responsável por criar a arquitetura responsável pela manipulação de dados gerados no aplicativo. Analista de Banco de Dados ganha em média um salário de R\$ 3.756,00 (três mil setecentos e cinquenta e seis mil reais).

Analista de testes o responsável pela validação do aplicativo testando o mesmo fazendo com que todas as abas, botões e funções estejam realmente funcionando. A média salarial para Analista de Testes no Brasil é de R\$ 3.407,00 (três mil quatrocentos e sete reais).

Gerente de projeto o profissional que irá administrar o trabalho e andamento das atividades de toda a equipe. Gerente de Projeto de Pesquisa em todo o Brasil é de R\$ 6.000,00 (seis mil reais).

O custo de uma equipe completa, abrangendo todos os profissionais acima descritos seria de 25 à 80 mil reais e um tempo médio de 2 à 4 meses de desenvolvimento.

Com essas informações pode se observar que há três formas para o aplicativo ser produzido. Através da contratação de uma equipe, de freelancers ou empresa. Todas possuem seus pontos fortes e fracos como por exemplo:

Opção Equipe: Quando uma equipe é contratada, a mesma faz seu trabalho na empresa e o desenvolvimento se dá in-house.

Vantagens: Profissionais passam a fazer parte da equipe da empresa, ou seja, irão se familiarizar com o projeto, e sempre estarão disponíveis para uma atualização ou problema gerado pelo aplicativo.

Desvantagens: A contratação deve ser de uma equipe com experiência e seu custo é de grande valor. Dados retirados do site www.glassdoor.com.br:

Profissional	Horas	Valores médios		Tempo médio	TOTAL
Programador Android	130	R\$ 3.980	R\$ 2.100	1 mês	R\$ 6.080
Programador iOS	130	R\$ 5.000	R\$ 2.644	1 mês	R\$ 7.644
Gerente de Projetos	26	R\$ 8.972	R\$ 4.745	1/6 mês	R\$ 2.286
Designer	39	R\$ 3.009	R\$ 1.600	1/4 mês	R\$ 1.152
Desenvolvedor Web	13	R\$ 2.801	R\$ 1.480	1/8 mês	R\$ 535
Desenvolvedor Backend	33	R\$ 2.500	R\$ 1.322	1/4 mês	R\$ 955
Custos de rescisão contratual aproximadamente					R\$ 7.100.
Total do projeto:					R\$18.663,00/ mês
Subtotal: R\$ 37.326 + R\$ 7.100					Subtotal: R\$ 37.326 + R\$ 7.100
Total Estimado:					R\$ 44.426,00

Opção freelancers: Freelancers são os profissionais contratados para apenas um serviço que depois de completo são dispensados.

Vantagem: A alternativa mais econômica e profissionais flexíveis com experiência em diversos projetos.

Desvantagens: Como o profissional executa muitos projetos, não possui disponibilidade exclusiva, ou seja, quando a empresa o solicitar novamente o mesmo pode

estar executando outro serviço e não ter carga horaria disponível. Também há risco quando um código ou tarefa não é bem documentada o que se pode tornar um grande problema para manutenções futuras. Segue abaixo as informações de preços médios fornecidas no site www.freelancer.com:

Profissional	Quantidade de Horas	Valor/Hora	Total
Programador Android	100	75	R\$ 7.500
Programador iOS	100	80	R\$ 8.000
Gerente de Projetos	20	100	R\$ 2.000
Designer	30	35	R\$ 1.050
Desenvolvedor Web	10	50	R\$ 500
Desenvolvedor Backend	25	40	R\$ 1.000
Total do projeto:			R\$ 20.050,00

Opção empresa: A Contratação de desenvolvimento por meio de empresas especializadas são a forma mais profissional e garantida de desenvolvimento de um bom software, eis que as mesmas tem experiência com a produção de muito projetos e já possuem profissionais experientes e capacitados.

Vantagem: Qualidade e profissionalismo do aplicativo, tempo reduzido e uma melhor orientação de como o aplicativo deve ser feito.

Desvantagens: Preço elevado, e menos flexibilidade não podem realizar tantas modificações durante seu desenvolvimento.

A informações de preço médio foram extraídas do site: www.mobimais.com.br.

Empresa	Região	Valor
Empresa A	SP	R\$ 55.400
Empresa B	RS	R\$ 32.900
Empresa C	PR	R\$ 40.400
<i>Prazo médio 2 meses</i>		
Valor estimado do projeto		R\$ 42.900

As opções de contratação apresentadas acima deverão ser analisadas para cada caso específico, no estudo de viabilidade para a empresa em foco a opção mais vantajosa seria a contratação de empresa desenvolvedora eis que há a necessidade de constante atualização, já que os aplicativos a cada atualização poderão modificar Termos de Uso e Condições havendo a necessidade de acompanhamento constante.

5. CONCLUSÕES E CONSIDERAÇÕES FINAIS

Percebe-se a partir dos resultados apresentados que a necessidade de desenvolvimento de aplicativo para inibir o uso de dados e recursos do smartphone é iminente, porém o custo de desenvolvimento é elevado eis que haveria necessidade de atualização permanente, pois só o desenvolvimento sem o acompanhamento das atualizações dos diversos Termos e Condições de uso tornaria o aplicativo incompatível.

Assim, este estudo pode concluir que apesar da necessidade comprovada de haver um aplicativo para bloqueio de acesso a dados privados de usuários, o alto custo de desenvolvimento para a empresa não é viável, já que seu maior foco é manutenção de smartphones e não a produção de venda de aplicativos para o cliente.

Nesse sentido, responde-se que a invasão de privacidade em smartphones existe de fato e que os próprios usuários autorizaram essa invasão mesmo que implicitamente, porém a alternativa encontrada para dar suporte aos clientes da empresa estudada não possui viabilidade financeira para execução do desenvolvimento de aplicativo específico para esse fim.

Após a análise desse estudo constatou-se que os avanços tecnológicos vieram facilitar a dinâmica da vida em sociedade, porém trouxeram consigo algumas desvantagens ocasionadas pelo próprio sistema, pois apesar de a informática promover disponibilidade de acesso a várias atividades com apenas um toque no dispositivo móvel que esteja conectado a um provedor de internet, deixou o usuário, em parte vulnerável com relação a sua privacidade.

No intuito de inibir as práticas de invasão de privacidade no uso de Smartphones se vê inclusive a criação de leis para inibir esse tipo de ato ilícito, porém, ainda há muito para ser feito e o que resta ao usuário para preservar os seus dados é a utilização de aplicativos de segurança disponibilizado pelos fornecedores dos produtos de informática e dispositivo móvel.

Porém, foram avaliados nesse estudo a vulnerabilidade da privacidade dos usuários de aparelhos smartphones por meio de autorização de “Termos e Condições”, pois algumas

autorizações ficam implícitas como por exemplo o uso de microfones, câmeras e localização. Foi verificado que não há aplicativo existente que bloqueie o acesso a dados ou funções privadas, ou que envie notificações cada vez que o microfone ou câmera for acionada remotamente.

Assim, verificou-se que os usuários de Smartphones podem ser considerados vulneráveis perante o uso de redes sociais e alguns aplicativos, porém que o desenvolvimento do software para criação de aplicativo para esse fim teria alto custo não só de desenvolvimento, bem como, de manutenção.

Conclui-se então que a privacidade de dados de clientes em lojas de manutenção de aparelhos existe, pois há uma responsabilização individual de quem está fazendo o serviço no aparelho, porém essa privacidade não é respeitada com a utilização de redes sociais e aplicativos que ativam ferramentas e componente do telefone sem que o usuário saiba que está sendo monitorado, e direcionando frequentemente os usuários para sites de vendas, ou estabelecimento comerciais que possam ser de interesse a levar a consumo.

Ao realizar a pesquisa, o acompanhamento da rotina do trabalho executado foi um agregador de conhecimento, pois além do conhecimento do técnico de manutenção, pode-se analisar a rotina de atendimento a clientes, as dificuldades de usuários, bem como, a empresa pode ter traçado um perfil e ter uma avaliação de funcionalidade através dessa pesquisa, sendo inclusive avaliada para um possível desenvolvimento de software.

6. REFERÊNCIAS

COELHO, J. V. A. B. R. **Aplicações e implicações da inteligência artificial no direito**. 2017. 61fls. Monografia - Universidade de Brasília, Brasília, 2017.

DONEDA, D. C. M. et al. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal**. Pensar, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

FILHO, J. L. S. M; ALCOFORADO, A. R. P.; LIRA, A. A. G. P. R. **A proximidade da realidade cyberpunk e os direitos da personalidade de inteligências artificiais**. Página 96 de 110. Direito, arte, tecnologia e ficção (Vol. II) / Organizadores: Adriano Marteleto Godinho; Marcílio Toscano Franca Filho; Alfredo Rangel Ribeiro; Felipe Negreiros Deodato – João Pessoa: IDCC, 2018.

HUMBY, Clive. Big Data and AI is not a panacea. 2019. Disponível em: <<https://www.linkedin.com/pulse/big-data-ai-panacea-clive-humby-obe/>>. Acesso em: 4 jul. 2019.

JUNIOR, E. Q. O. **A inteligência Artificial e o Direito.** 2017. Disponível em:< <https://eudesquintino.jusbrasil.com.br/artigos/507840893/a-inteligencia-artificial-e-o-direito>>. Acesso em: 09 out. 2019.

PIMENTEL, A. E.; OLIVEIRA, J. R; SILVA, Z. M. **A inteligência artificial e a profissão jurídica.** 2018. 10fls. Artigo - FSG Centro Universitário, Serra Gaúcha, 2018.

RAMPAZZO, S. E; CORRÊA, F. Z. M. **Desmitificando a metodologia científica: guia prático de produção de trabalhos acadêmicos.** Erechim: Habilis (2008).

RIBEIRO, F. R. **Stallman – Celulares são vilões na privacidade, mas GDPR é um bom caminho.** 2019. Disponível em:< <https://canaltech.com.br/seguranca/richard-stallman-celulares-sao-viloes-na-privacidade-mas-gdpr-e-um-bom-caminho-134135/>>. Acesso em: 07 out 2019.

RINALDI, C. **Olhar Digital: 3 dicas simples para proteger a sua privacidade digital.** 2019. Disponível em:< https://olhardigital.com.br/fique_seguro/noticia/3-dicas-simples-para-proteger-a-sua-privacidade-digital/86949>. Acesso em: 08 out. 2019.

ROHR, A.; LAVADO, T. **Saiba como aumentar a segurança do celular e dos aplicativos de mensagens.** 2019. Disponível em:< <https://g1.globo.com/economia/tecnologia/noticia/2019/06/12/saiba-aumentar-a-seguranca-do-celular-e-dos-aplicativos-de-mensagens.ghtml>>. Acesso em: 04 out. 2019.

SILVA, B. H. S. **Privacidade versus segurança pública: o acesso ao conteúdo de celular pela autoridade policial.** Quaestio Iuris, Rio de Janeiro, vol. 11, nº. 04, p. 3220-3241, 2018. THE Great Hack. Direção e produção de Karim Amer. Roteiro: Karim Amer. Eua: Netflix, 2019. P&B.