Os impactos de privacidade em redes wifi e implicações penais no Brasil do caso Google Street View

Líssia Melo, Fernando Veras Bezerra
Centro de Ciências Jurídicas – Bacharelado em Direito
Universidade de Fortaleza (UNIFOR)
Fortaleza, Brasil
lissiamelo@yahoo.com.br, bezerra_fernando@hotmail.com

Pablo Ximenes, André dos Santos
Information Security Research Team (INSERT)
Universidade Estadual do Ceará(UECE)
Fortaleza, Brasil
pablo@ximen.es, andre@dossantos.org

Jairo Ponte
Faculdade de Direito – PPGD
Universidade |Federal de Pernambuco (UFPE)
Recife, Brasil
jairoponte@gmail.com

Resumo—**Através do levantamento das condições de segurança da malha de redes wifi de uma grande capital brasileira, este artigo procura consubstanciar as implicações jurídico-penais e de desrespeito à privacidade decorridas das atividades de coleta de dados do Google Street View no Brasil, bem como trazer à tona o estado atual da segurança das redes sem fio brasileiras.**

Palavras-chave-direito penal, informática, segurançaa da informação, google streetview, tipicidade conglobante, forense computacional

I. Introdução

Em maio de 2010 a Google admitiu, em seu blog oficial, que seu mecanismo de coleta de informações para o serviço Street View também interceptava ilegalmente dados transmitidos por redes wifi [GGL01]. A confissão de maio estipulou que além de fotos e dados para geo-referência, as transmissões de redes sem fio que estivessem presentes nas vizinhanças também eram capturadas. Esse desrespeito à privacidade realizado pela Google desencadeou diversas litigâncias na esfera cível e penal em diversos países do mundo [DEL01][SCM01][THL01]. Contudo, nenhuma menção sobre a fiscalização dessa prática tem sido suscitada no Brasil, que tem sido palco desde o início do ano de 2010, de uma campanha massiva de coleta de dados para o Street View, fomentado pelo advento da copa do mundo de 2014 [GLB01]. Ademais, nenhum estudo tem sido feito acerca de como esse tipo de prática se relaciona com as leis brasileiras e qual o impacto na segurança e privacidade nas malhas metropolitanas de redes sem fio do Brasil.

Dessa forma, este trabalho trata-se de um estudo do impacto das ações de coleta de dados do Google Street View em sua perspectiva legal e de comprometimento à privacidade nas malhas metropolitanas de redes wifi brasileiras. Nesse âmbito, fazemos um levantamento da malha de redes sem fio de uma grande capital brasileira como base de referência, onde coletamos dados de pontos de acesso sem fio, suas respectivas configurações de segurança e analisamos sua vulnerabilidade contra o tipo de prática realizada pela Google no tocante ao Street View. Em suma, procura-se responder à pergunta: "Quão vulneráveis estão as redes sem fio brasileiras e como isso se consubstancia em relação às implicações penais das atividades de coletada de dados do Google Street View?". Assim, procuramos apresentar um levantamento empírico da segurança das redes sem fio Brasileiras com critérios suficientes para demonstrar a amplitude da violação penal que gira em torno do caso e afastar qualquer eventual argumentação de fuga do tipo, mesmo sob a ótica da tipicidade conglobante, que é a forma de análise de maior rigor pró-agente encontrada no ordenamento jurídico brasileiro para tipificação penal.

Este artigo é organizado da seguinte forma. A segunda seção discute o caso Google Street View e como ele se estende ao Brasil. A terceira parte discorre sobre as questões jurídicas acerca do ocorrido, evidenciando com clareza o desrespeito penal do fato, em especial analisando o ocorrigo sob a ótica da tipicidade conglobante. A seção 4 mostra o levantamento realizado sobre a malha de redes sem fio de uma grande capital brasileira com o objetivo de substanciar o impacto das observações jurídicas trazidas à tona na seção 3, analisando o nível de vulnerabilidade da malha investigada. Por fim, a seção 5 traz algumas observações e conclusões acerca dos dados levantados pela pesquisa.

II. O Caso Google Street View

Em 14 de maio de 2010, em resposta a uma investigação das autoridades públicas alemãs, a Google admitiu que seu

veículo de coleta de dados para o serviço *Google Street View* interceptava os dados de comunicação (*payload*) transmitidos por redes wifi desprovidas de criptografia de enlace que estivessem ao logo do percurso de coleta [GGL01]. Como resposta a essa *mea culpa*, vários processos judiciais sugiram ao redor do mundo [DEL01][SCM01][THL01]. Contudo, nenhuma palavra das autoridades brasileiras tem sido manifestada a respeito, mesmo tendo a prática também sido realizada no Brasil.

Essa seção discute os detalhes do caso Google Street View e usas implicações para o Brasil.

A. O Street View e a Confissão da Google

O Google Street View é o serviço oferecido pela Google como parte de seu sistema de mapas, o Google Maps, que permite uma visão ao nível do solo em 360º da paisagem mapeada. A forma que a Google coleta dados para recriar os cenários em 360º, é através de um carro equipado com uma espécie de dispositivo de captura de dados, conforme o indicado na figura 1.

Essa coleta de dados foi explicada em mais detalhes por uma comunicação oficial da Google [GGL02], onde foi informado que o dispositivo de captura coletava apenas:

- Fotografias: necessárias para a reconstrução dos mapas em 360º do Street View.
- Informações de Redes Wifi: coletando apenas dados de SSID e endereços MAC dos Access Points das redes wifi que estivessem no trajeto do carro para uso nos algoritmos de geo-referenciamento.
- Geometria 3D: usando lasers de baixa potência para captura dos detalhes tridimensionais da paisagem.

Contudo, as autoridades alemãs não se contentaram com as declarações da Google e exigiram que lhes fossem fornecidas os dados coletados pelo carro da Google para auditoria. Em face do escrutínio das autoridades alemãs, a Google prontamente revisou sua comunicação a respeito de quais dados eram coletados e confessou que em sua captura de dados de redes wifi, não apenas os dados de SSID e endereços MAC, mas também os dados transmitidos, ou payload, também foram capturados [GGL01]. A partir dessa confissão, diversas iniciativas na esfera civil e penal foram tomadas internacionalmente em retaliação à prática da Google [DEL01] [SCM01][THL01].

A Google, por sua vez, antecipou-se e encomendou uma análise dos códigos e programas utilizados pelo sistema de captura de dados do *Street View* por terceiros [SFR01], que foi realizado pela firma de consultoria Stroz Friedberg. O estudo concluiu que, de fato, a Google coletou e gravou os dados transmitidos (*payload)* em redes sem fio que estivessem desprovidas de criptografia. A Google justificou o ocorrido como sendo um erro de programação dos engenheiros do *Street View*, que teriam deixado não intencionalmente dentro do código de captura de dados uma porção que também fazia a intercepção das comunicações de redes *wifi.* Adicionalmente, a Google alegou que essas intercepções incluíam apenas fragmentos de dados fora de contexto, já o que o veículo estava em movimento [GGL01]. Essas desculpas têm sido contestadas, principalmente depois da descoberta de uma patente da Google que descreve exatamente o mesmo mecanismo de intercepção que tinha sido reputado como um erro não intencional [PAT01] e, com a descoberta por parte da Comissão Nacional de Computação e Liberdade da França de que a intercepção feita pela Google não era apenas de fragmentos de dados, mas de porções completas incluindo até senhas e emails [IWL01]. Como conseqüência das pressões recebidas, a Google decidiu suspender toda e qualquer coleta de dados relacionada a redes sem fio por parte de seus carros do *Street View* [GGL01].

Figure 1. O carro de coleta de dados do Google Street View.

B. A captura de dados wifi e o caso Street View

Em redes sem fio do tipo wifi, as transmissões são codificadas em pequenos pedaços de dados que são enviados por vez, chamados de quadros (do inglês frames). Cada transmissão em uma rede wifi é feita através de um ou vários quadros. Os quadros não existem apenas para transmitir dados, mas também para executar tarefas administrativas da rede, como coordenar as transmissões, permitir ou negar acesso, entre outras. Praticamente todos os tipos de quadros transmitidos em uma rede wifi fazem parte de uma comunicação telemática entre o ponto de acesso (concentrador central da rede sem fio) e uma unidade móvel (ex.: computador notebook) com a exceção de um único tipo que é o quadro conhecido como beacon. O quadro do tipo beacon trata-se de um anúncio público que o ponto de acesso faz periodicamente para todos que estejam nas redondezas com informações sobre hora, SSID, endereço MAC, dentre outras. Esse anúncio público se faz necessário para facilitar o processo de configuração das unidades móveis que desejem se associar a uma rede sem fio. Contudo, esse anúncio pode ser desabilitado caso o administrador da rede assim o deseje, deixando o processo de configuração um pouco mais tortuoso [WIF01].

O equipamento de coleta de dados do Google Street View usou a técnica de captura passiva de pacotes conhecida como

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

sniffing, onde todos os quadros destinados ao ponto de acesso sem fio ou advindos dele eram interceptados. Dessa forma, não somente os quadros beacon, mas todo e qualquer quadro era interceptado e gravado pela Google. Isso incluía inclusive quadros que carregavam dados de usuários, ou os chamados payloads (vídeo, imagens, texto, som, senhas, emails, etc).

É importante salientar que a interceptação de dados supra mencionada foi reputada pela Google como não intencional, mas que, no entanto, existem fortes indícios do contrário. O principal argumento é o registro de patente americana no. 20100020776, feito pela Google em Janeiro de 2010, intitulada "Mecanismo de aproximação de localização baseado em redes sem fio" [PAT01]. Com título auto-explicativo, a patente descreve que "as estimativas de localização podem ser obtidas pela observação/análise de pacotes transmitidos ou recebidos pelo ponto de acesso" da rede sem fio. É importante notar que a patente afirma que inclusive os pacotes destinados ao ponto de acesso devem ser capturados, o que caracteriza a captura de quadros contendo dados de usuário (payload). A patente claramente descreve o mesmo princípio de funcionamennto que tem sido usado pelo carro do Google Street View, que segundo admissão da própria Google, interceptava pacotes com o objetivo de melhorar seus serviços baseados em localização [GGL02]. Ademais, a desculpa de que o código de captura teria passado despercebido é no mínimo ingênua. O grande volume de dados gravados das capturas por si só seria suficiente para se perceber que algo estava errado e se estava capturando mais do que se deveria. A captura de quadros beacon (o que a Google alega ter tido a intenção de capturar) requer bem menos espaço de armazenagem do que a Google de fato usou para guardar suas capturas. Além disso, é improvável que a equipe de engenharia da Google não tenha rotinas de testes que sem dúvida teriam apontado a presença deste tipo de interceptação indevida.

C. *O Google Street View no Brasil*

Desde o início de janeiro de 2010 a Google intensificou a coleta de dados para o serviço *Street View* no Brasil, iniciando o mapeando das cidades de São Paulo e do Rio de Janeiro. Anteriormente, esse mapeamento já havia sido feito na cidade de Belo Horizonte, sede do centro de engenharia da Google no Brasil [GLB01]. A estimativa é que a captura de dados em São Paulo e no Rio de Janeiro levaria aproximadamente 4 (quatro) meses, estando completa em abril de 2010. Dessa forma, o desrespeito à privacidade de comunicações em redes sem fio realizado pela Google também se estendeu ao Brasil, já que três das maiores cidades brasileiras foram escrutinadas pelo sistema de coleta de dados da Google, antes que essa tivesse suspendido a captura de dados de redes sem fio, o que ocorreu apenas na segunda metade de maio do mesmo ano.

Apesar do fato de que o carro de coleta do *Google Stree View* mapeou três de nossos maiores centros urbanos da mesma forma que fez no resto do mundo, nenhuma menção foi feita pelas autoridades brasileiras a respeito do despeito à privacidade decorrido do fato. Dessa forma, a seção seguinte discorre sobre as razões pelas quais essa inércia deveria ser rompida.

III. Implicações criminais do caso Google Street View no Brasil

Considerando as informações colhidas no tocante ao caso do Google Street View, buscamos esclarecer até que ponto essas condutas violam o direito penal brasileiro.

A. *Da Interceptação Telemática na ótica do Direito Penal*

O ordenamento jurídico brasileiro oferece garantias constitucionais rígidas contra a violação da privacidade de comunicações em geral. O artigo 5º de nossa carta magna, em seu inciso XII é claro e objetivo ao afirmar:

"*Art. 5º, inc. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;*"

O texto constitucional, porém, não prescreve punições específicas contra o desrespeito desta proteção. Esta função é da lei ordinária infraconstitucional. A Lei Federal 9.296/96 foi criada com o objetivo expresso de regulamentar especificamente a parte final deste dispositivo constitucional, disciplinando a possibilidade de autorização judicial para de interceptação de comunicações telefônicas e de dados. Ao final a lei 9.296/96 apresenta o seguinte tipo penal:

"Art. 10 – Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de dois a quatro anos, e multa."

Vale comentar brevemente que este tipo penal não serve para proteger toda e qualquer violação ao disposto no inciso XII do art. 5º da CF/88. É que o texto constitucional fala primariamente de inviolabilidade de sigilos, dizendo respeito tanto ao sigilo na circulação (comunicação) de dados como ao sigilo dos dados em si. Já o crime previsto na lei trata principalmente da conduta de interceptar comunicações, fazendo referência apenas ao sigilo de Justiça, o que deixa sem proteção o sigilo dos dados armazenados de qualquer forma que não seja afetos à atividade de Justiça. Diante disso, a primeira questão que surge para a correta aplicação desta tipificação penal é identificar se efetivamente ocorreu interceptação de comunicações telemática no caso do *Gooogle Street View*.

O mecanismo de captura de dados que a Google assumiu utilizar, capturou e gravou dados que circulavam por meio de redes sem fio, não apenas os quadros *beacon*, mas também os quadros contendo dados de usuário, configurando claramente a interceptação de comunicação telemática. Não há dúvida sobre a materialidade do delito, ou seja, que a conduta prevista na lei como crime efetivamente ocorreu.

Outro aspecto que precisa ser esclarecido para a configuração da responsabilidade criminal, além da materialidade, é a autoria. Este assunto é um pouco mais complexo que o tema anterior, pois não basta indicar quem realizou conduta, mas também se o agente sabia que praticava algo ilícito e queria o resultado. A mais, o resultado (interceptação de comunicações) é fruto de várias etapas,

Identify applicable sponsor/s here. If no sponsors, delete this text box. (sponsors)

desde a confecção do programa e do equipamento, até a sua efetiva aplicação em campo.

É necessário fazer um recorte. Tendo em vista as informações disponíveis, não parece viável discutir com a profundidade devida a responsabilidade dos escalões mais baixo da Google, aqueles encarregados de atividades operacionais. Não há informação suficiente que permita discutir se tais funcionários conheciam os detalhes do programa que esta sendo utilizado para interceptação de comunicações. Por outro lado, contudo, todos os atos que desembocaram na realização do resultado, estavam sob o controle real ou potencial dos setores dirigentes da empresa. Da mesma forma, já existem informações veiculadas pela imprensa internacional que dão conta das explicações dadas pela empresa através de seus setores dirigentes, o que nos permite tecer comentários sobre a consistência de tais explicações a luz do regulamento penal brasileiro.

Vale advertir que, embora este recorte reduza a complexidade da análise, ele não é suficiente para uma efetiva responsabilização penal. Seria necessária a indicação de condutas especificas e de forma individualizada. Isso só parece possível mediante uma investigação criminal. De qualquer forma, mesmo considerando esta ressalva, não parece possível negar o nexo de causalidade entre o resultado (interceptação telemática) e as condutas da Google. Logo, ainda que de forma preliminar, a autoria parece estar configurada.

A Google tenta explicar o incidente indicando que se tratou de um engano de sua equipe de engenharia que incluiu equivocadamente no programa de captura das informações licitas das redes *wifi*, um código feito um ano antes que tinha a finalidade de capturar todos os tipos de quadros, o que levou a ocorrência de interceptação ilegal. Com esta explicação a Google tenta qualificar sua conduta como culposa, em vez de dolosa, na forma do código penal brasileiro:

Art. 18 - Diz-se o crime:

I - doloso, quando o agente quis o resultado ou assumiu o risco de produzi-lo;

II - culposo, quando o agente deu causa ao resultado por imprudência, negligência ou imperícia.

Essa qualificação serviria para desclassificar a conduta como criminosa, visto que só se considera crime quando o resultado decorre de conduta dolosa, salvo em caso de previsão expressa de lei, como manda do parágrafo único do art. 18.

Art. 18 (...)

Parágrafo único - Salvo os casos expressos em lei, ninguém pode ser punido por fato previsto como crime, senão quando o pratica dolosamente.

Contudo, uma observação atenta revela que esta versão da Google não se sustenta. Se ocorreu da forma como a Google afirma, então um código, apto a realizar uma interceptação proibida foi produzido por um de seus engenheiros. Este código, como todos os demais produzidos dentro das atividades da empresa, foram produzidos sob ordem e/ou orientação superior. Mais que isso, o relatório encomendado pela própria Google feito pela empresa Stroz Friedberg, é contundente em afirmar que o *software* de captura usado nos carros da Google realizou as interceptações ilegais não pela mera inclusão de um código, mas porque este código estava ativo e configurado para tanto. Em outras palavras, o código de captura é configurável, deixando a critério do operador/configurador do sistema a opção de deixá-lo na forma de captura ilegal ou não. [SFR01]

Tudo isso indica que a Google queria produzir o resultado (interceptação ilegal) ou, ao menos, assumiu o risco, uma vez que determinou a realização de todos os atos necessários à produção do resultado. Novamente aqui seria necessária uma investigação policial para esclarecer detalhadamente o que ocorreu. Contudo, as informações colhidas já são suficientes ao menos como indícios de autoria e materialidade, indícios fortes, diga-se de passagem.

B. A Tipicidade Conglobante no caso Google Street View

Ds Expostos os elementos da conduta, é aparentemente incompreensível a passividade das autoridades policiais e do ministério público brasileiro em apurar o caso Google Street View. O único aspecto que justificaria tal complacência e que precisa ser esclarecido diz respeito a elementos da tipicidade vistos de uma forma mais global, onde algum atenuante material do tipo esteja presente. Para tanto, se lança mão da teoria da tipicidade conglobante, que tem em Raul Zaffaroni a principal referência. De acordo com Zaffaroni:

> *"O tipo objetivo não se esgota na correspondência com qualquer pragma, mas tão somente com um pragma conflitivo; constatar tal conflitividade constitui passo indispensável para a verificação da tipicidade objetiva. O pragma típico se determina desde logo pela função sistemática, que importa um âmbito máximo de antinormatividade, porém só se confirma com a simultânea constatação de sua conflitividade, procedimento que pode culminar em sua exclusão ou redução, sem jamais ultrapassar o máximo rudimentar estabelecido pela tipicidade objetiva sistemática. Por isso, pela necessidade de constatar a conflitividade, imposta pela requisição jurídica geral da alteridade e pelo objetivo político redutor da construção, cabe distinguir dentro do tipo objetivo um tipo que dê conta de tal objetivo: o tipo conglobante."* [ZAF10]

Dessa forma, o tipo conglobante é nada mais que o tipo penal no caso concreto, onde a letra da lei deixa de imperar isolada e passa a se relacionar com elementos da realidade que possam descaracterizar a conduta como típica. Exemplo disso é o caso do lutador de box que produz lesão corporal no exercício de seu esporte, mas não é apenado por isso. Assim diz o Art. 129 do Código Penal Brasileiro: *"Ofender a integridade corporal ou a saúde de outrem: Pena - detenção, de três meses a um ano"*.

Ora, o tipo penal de lesão corporal é claro, contudo porque o lutador de box não é julgado por isso? Isso se deve ao fato da existência de um contrato social que desconsidera como criminosa tal conduta, mesmo que formalmente definida como crime. Durante a luta, os dois lutadores aquiescem em sofrer lesão corporal, abdicando do direito do qual são titulares. Ainda nas palavras de Zaffaroni:

"A tipicidade conglobante cumpre sua função redutora constatando a existência de um conflito (conflitividade) [...] Não existe conflitividade quando a ação não ofende a ninguém" [ZAF10]. Ora, a conduta da Google no caso da coleta de dados de redes sem fio, ainda que definida formalmente no tipo penal de interceptação telemática ilegal, poderia ter uma avaliação que a considere atípica no caso concreto sob a teoria da tipicidade conglobante caso não seja encontrada a conflitividade. A inexistência da conflitividade justificaria a falta de ação da autoridade pública no caso estudado. Dessa forma, vemos que a tipicidade conglobante não apenas se trata de uma abordagem mais completa do fenômeno da tipicidade, mas é também uma tese de matriz profundamente democrática e despenalizante. Assim, ao analisar a tipicidade das condutas relacionada ao caso Google Street View sob a luz de uma teoria penal crítica, buscando a abordagem mais favorável ao agente, estabelece-se um teste rigoroso: se mesmo com uma teoria despenalizante, as condutas da Google ainda podem ser consideradas típicas, não existe outra conclusão viável a não ser a de que as autoridades falharam em indiciar e investigar o caso revelando a clara existência da seletividade caracterizada nos capítulos anteriores.

- Para que seja determinada a existência de conflitividade, e assim a caracterização da tipicidade conglobante, Zaffaroni nos ensina que quatro elementos básicos devem ser avaliados: a) se a ação foi fomentada pelo direito; b) se a ação se tratou do cumprimento de um dever jurídico; c) se a ação se realizou por aquiescência do titular do bem jurídico; e d) se a afetação ao bem jurídico é insignificante ou não. [ZAF10].
- O fomento jurídico da ação realizada pela Google está claramente descaracterizado, já que não existe nenhuma normatização que enseje a conduta. Para Zaffaroni, o fomento surge quando a normatização jurídica "inspira políticas públicas amplamente discutidas: assim, as atividades educacionais, sanitárias, desportivas, de investigação científica, produtivas etc" [ZAF10]. No caso da Google, a ação não se tratou de algo equiparável, já que coletar dados de redes sem fio não se relaciona com nenhuma política pública conhecida. Também é evidente que o caso estudado não se deu devido ao cumprimento de um dever jurídico. Segundo Zaffaroni, este caso se perfaz quando a norma jurídica é conflitante quando *"a norma jurídica dedutível do tipo legal proíbe fazer aquilo que outra norma jurídica de idêntica hierarquia proíbe omitir"* [ZAF10]. Mais detalhadamente temos:
- *"O cumprimento de um dever jurídico é um fenômeno que ocorre quando um mandado recorta uma norma proibitiva, prevalecendo sobre ele. O meirinho que arrecada um bem penhorado não pratica furto, o policial que efetua uma prisão em flagrante não comete constrangimento ilegal, a autoridade sanitária que ingressa numa casa para extinguir um foco de epidemia nela constatado não incorre em violação de domicílio, o soldado que em combate fere o inimigo não perpetra lesões corporais etc."*

Dessa forma é inconcebível interpretar as atividades da Google no caso estudado como cumprimento de qualquer dever legal, visto o fato de que nenhuma ordem judicial existia para tanto e que seu papel social não a incube de nada assemelhado. Com relação à aquiescência do titular do bem jurídico, é evidente que não existia. Seria inviável, pelo estilo usado na interceptação, conseguir consentimentos expressos de todos os titulares do bem jurídico vilipediado pela Google. Contudo, nos conta Zaffaroni que o consentimento expresso só é necessário como excludente de antijuridicidade, servindo de elemento justificante da conduta. Em se tratando da discussão de tipicidade, seria garantida a atipicidade apenas pela existência, mesmo que não exteriorizada, do consentimento. [ZAF10]. Dessa forma, mesmo que a Google não tenha levantado documentos assinados pelos titulares do bem jurídico lesado neste caso especificando claramente a sua aquiescência, a mera indicação da existência desta aquiescência seria elemento excludente desta tipicidade. Para que seja analisada se existe tal aquiescência é imperativo tomemos em consideração quantos foram os titulares do bem jurídico lesado. É possível se esperar que um conjunto de 10 pessoas entre em acordo unânime em consentir com tais ações, porém um grupo de 1000 pessoas já seria bem menos inclinado a entrar em consenso, onde um percentual do grupo negaria tacitamente a presença de qualquer aquiescência. Ademais, no caso das comunicações telemáticas das redes sem fio interceptadas pela Google, os titulares do bem jurídico não se limitam aos que diretamente se conectavam às redes interceptadas, visto que a comunicação é uma via de mão dupla e tais redes darem acesso à Internet. Dessa forma, cada uma das comunicações interceptada servia de ponte entre um usuário diretamente conectado à rede sem fio violada e outro em alguma outra parte do mundo, via Internet. Dessa forma, os titulares do direito violado se multiplicam exponencialmente na proporção direta do número de conexões de internet dos usuários conectados diretamente às redes sem fio em questão. Por fim, temos análise da questão da significância da ofensa ao bem jurídico tutelado. Relembramos que o bem jurídico neste caso trata-se da inviolabilidade das comunicações telemáticas, onde os titulares são os participantes da comunicação. Para tanto é importante compreender como se manifesta no caso concreto o quesito da insignificância levantado por Zaffaroni et al [ZAF10]:

"Os casos de lesões insignificantes a bens jurídicos foram tratados como atípicos por Welzel, dentro de sua teoria da adequação social da conduta. Mais tarde, o velho princípio mínima non curat Praetor serviu de fundamento para o moderno enunciado do princípio da insignificância ou da bagatela, segundo o qual as afetações diminutas do bem jurídico não constituem lesão relevante para os fins da tipicidade objetiva."

Apesar da simplicidade do conceito, a sua aplicação no cenário jurídico brasileiro ainda é confusa, pois não são claros os critérios de sua aplicabilidade visto o fato de este não ser um princípio legislado expressamente. É sobre isto que relata Gomes [GOM10]:

- *"O ponto complicado da referida decisão diz respeito aos critérios de aplicabilidade do princípio da insignificância. Sendo um princípio não legislado expressamente no Direito penal comum, mais do que natural é a dificuldade de se encontrar sua base de apoio, isto é, seus vetores ou critérios de razoabilidade. Direito, aliás, é razoabilidade. Não estamos nos referindo, portanto, aos fundamentos do próprio princípio da insignificância, que encontra eco no princípio maior da intervenção mínimae mais especificamente nos seu aspecto de fragmentariedade. A questão é outra: de quais critérios deve o juiz se valer para reconhecer o princípio da insignificância? Deve considerar só a conduta (o desvalor da conduta) ou também deve levar em conta o resultado (o desvalor do resultado)? Ou ainda seria o caso de também se dar relevância ao desvalor da culpabilidade (bons antecedentes, primariedade, personalidade etc.). A jurisprudência brasileira, em geral, já não tem dúvida em admitir o princípio da insignificância. Mas no que concerne aos seus fundamentos o tema continua complicado."*
- Levando-se em conta que, segundo a conduta admitida pela Google, o que houve foram interceptações curtas de redes sem fio ao longo do trajeto de seu veículo de coleta de dados, onde a interceptação só se perfazia no caso de redes sem fio desprovidas de criptografia, faz-se novamente necessária a análise do caso concreto para se verificar a lesividade ao bem jurídico resultante das ações da Google. Neste aspecto é importante compreender a dimensão da ofensa jurídica. Quantas redes foram afetadas? Qual a média de usuários por rede sem fio? Sabemos que o princípio da insignificância é de fundamentação complexa no direito brasileiro, porém podemos descartar tal princípio caso a dimensão da ofensa seja notadamente grande.
- Como vimos, dois dos elementos da tipicidade conglobante, a saber: a insignificância e a aquiescência, precisariam de uma análise dos elementos materiais de como se deu a ofensa. Em última análise, precisaríamos estabelecer qual foi o impacto quantitativo das ações da Google em termos de interceptação telemática em redes em fio. Para responder a esse questionamento precisamos levantar, mesmo que aproximadamente, a quantidade de redes sem fio afetadas e que percentual delas funcionam sem criptografia. A seção seguinte trata justamente desse ponto

IV. Análise de Segurança da Malha Metropolitana de Redes Wifi

Essa seção descreve o levantamento realizado do nível de segurança da malha de redes *wifi* da cidade de Fortaleza – Ceará. O objetivo do levantamento é compreender o quão as redes brasileiras estão suscetíveis às práticas realizadas pela Google no caso do levantamento de dados para o serviço *Street View* e usar essas informações como parâmetro para afastar o princípio da insignificância penal no caso Google *Street View*.

O levantamento consistiu de uma incursão de captura de dados de redes sem fio em regiões selecionadas da cidade de Fortaleza, em um formato semelhante ao trabalho encontrado em [SSW01]. A escolha de se fazer o estudo na cidade de Fortaleza e não em alguma das três capitais realmente afetadas pelo problema foi devida a limitações do grupo de investigação que, sediado em Fortaleza, não possuiu recursos para investigar as capitais mencionadas. Contudo, os dados obtidos em Fortaleza são extrapolados de forma a garantir minimamente os critérios desejados para o afastamento do princípio da insignificância penal. Diferentemente da Google, os dados coletados por nosso experimento se restringiram apenas a informações anunciadas publicamente pelos pontos de acesso das redes sem fio estudadas (e.x.: SSID, etc), sem incluir nenhum dado de usuário (*payload*).

A. Metodologia

O objetivo do levantamento foi avaliar a criticidade do nível de vulnerabilidade das redes sem fio de Fortaleza a um ataque semelhante à prática da Google no tocante ao *Street View*. Dessa forma, foram selecionadas regiões específicas da cidade de Fortaleza, representadas pelos bairros Aldeota, Meireles, Joaquim Távora, Alto da Balança e Serrinha. A escolha dos bairros se deu baseada nas condições sócio-econômicas, bem como nas características populacionais de cada bairro. A tabela 1 mostra as principais características de cada bairro escolhido.

TABLE I. Bairros Selecionados

Bairro	População	Classe	Status Comercial
Aldeota	38.636	A	Alta Presença
Meireles	30.397	A	Média Presença
Joaquim Távora	23.051	A/B	Média Presença
Serrinha	25.682	C/D	Baixa Presença
Alto da Balança	13.229	C/D	Baixa Presença

Características dos Bairros selecionados

Dessa forma, realizamos o levantamento nos bairros selecionados através de trajeto percorrido com um carro utilizando um dispositivo móvel de captura *wifi* munido de GPS. Assim, pudemos levantar os seguintes tipos de dados dos pontos de acesso das redes *wifi* da regiões investigadas:

- SSID: o nome da rede sem fio;
- MAC: endereço de hardware do ponto de acesso sem fio;
- tipo de criptografia: tipo de criptografia de enlace utilizada pela rede;
- freqüência: freqüência utilizada pela rede;
- nível de sinal: o nível de atenuação de sinal no momento da captura;
- data e hora: data e hora do instante da captura;

- latitude e longitude : uma derivação do posicionamento do ponto de acesso sem fio feito a partir da informações provenientes do sistema de GPS utilizado.

B. Equipamento Utilizado

Para o levantamento de dados utilizamos um *smartphone* municiado de suporte a *wifi* A-GPS. Mais especificamente, utilizamos o modelo Motorola Milestone A853, equipado com o sistema operacional Android. Nenhuma antena especial foi utilizada, apenas a antena interna do telefone. O veículo utilizado foi um sedan nacional, onde o telefone foi posicionado no painel dianteiro e conectado ao acendedor de isqueiro para manter o nível da bateria.

O software de captura de dados utilizado foi WarDriving App [WDA01] disponível no Android Market (repositório de programas para a plataforma Android). Vale salientar que o WarDriving App registra apenas os pacotes do tipo *beacon*.

C. Dados Levantados

O experimento realizado levantou um total de 2.203 pontos de acesso na região especificada. Podemos ver na figura 2 uma distribuição geral de como os pontos de acesso levantados estão distribuídos geograficamente. É importante notar a imprecisão da geo-referência no posicionamento dos pontos de acesso, já que para tanto o software de coleta realiza um cálculo baseado na posição GPS do coletor juntamente com a atenuação de sinal do ponto de acesso, gerando um raio de cobertura da posição provável do ponto de acesso.

Figure 2. Mapa dos pontos de acesso coletados

Compreendemos que devido à insuficiência de potência do equipamento utilizado, é provável que os pontos de acesso das regiões escolhidas não tenham sido completamente mapeados. Contudo, o objetivo da investigação não está pautado em mapear todo e qualquer ponto de acesso, mas somente aqueles que estariam visíveis em uma situação equivalente à nossa, como no caso da coleta feita pelo carro do *Google Street View*.

Do total coletado 10.48% foram de redes sem nenhum tipo de criptografia de enlace; 44.39% usavam exclusivamente o padrão WEP; enquanto o restante usava os padrões WPA e WPA2.

A figura 3 sumariza os dados de criptografia de enlace das redes analisadas. É importante notar que algumas das redes analisadas ofereciam simultaneamente os padrões WPA e WPA2 razão pela quais a porcentagem total é maior que 100.

No entanto, as redes WEP e abertas usavam apenas um padrão.

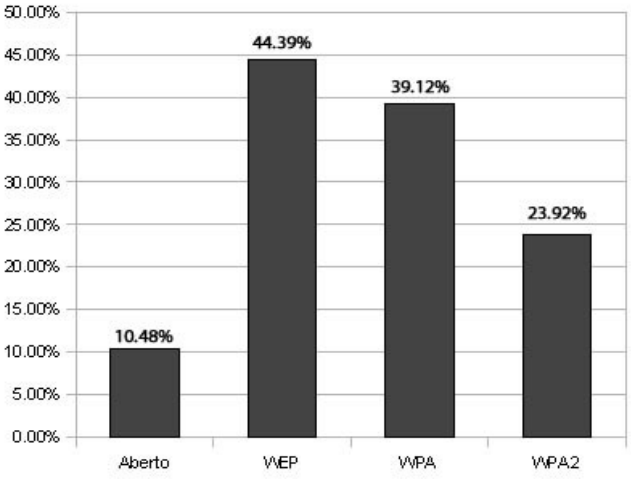

Figure 3. Estatísticas de uso de criptografia nas redes sem fio coletadas

O que nos mais chamou a atenção, além dos 10.48% de redes sem nenhum tipo de criptografia de enlace, foi o fato de quase metade de todas as redes sem fio estarem usando WEP, um protocolo de segurança defasado e sem garantias.

Os dados coletados apontaram também para uma predominância do uso da freqüência 2.437GHz, representando 47.60% de todas as redes coletadas.

A figura 4 sintetiza o apanhado de informações sobre uso de freqüência das redes analisadas.

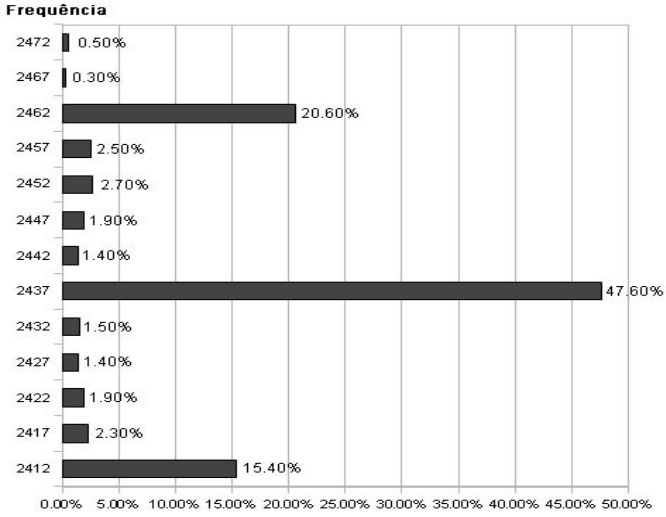

Figure 4. Estatísticas de uso de freqüência

D. *Análise*

Se tomarmos o contingente populacional das regiões de Fortaleza analisadas teremos um total de 130.995 habitantes para a região total analisada. Dessa forma, podemos derivar que nosso levantamento encontrou uma densidade de pontos de acesso equivalente a aproximadamente um ponto de acesso para cara 59 habitantes. Levando-se em conta que do total coletado por nosso levantamento, 10.48% são de redes abertas, chegamos à densidade de aproximadamente 567 habitantes por ponto de acesso aberto.

Podemos usar essa proporção de habitantes por redes abertas para vislumbrar as realidades das cidades percorridas pelo carro do Google *Street View* no Brasil. Aplicando a mesma proporção à São Paulo (19.223.897 habitantes) teremos um total de 33.904 pontos de acesso abertos. Se aplicarmos à realidade do Rio de Janeiro (6.186.710 habitantes) teremos como resultado 10.911 pontos de acesso sem nenhuma criptografia de enlace. Por fim, aplicando a mesma proporção à cidade de Belo Horizonte (2.452.617 habitantes), chegamos a um total de 4.325 pontos de acesso sem proteção nenhuma.

Como podemos ver por nossa estimativa, quase 50 mil redes sem fio tiveram suas comunicações interceptadas pela Google no Brasil. Apesar de se tratar de uma projeção rudimentar, a evidência técnica trazida pela estimativa já é suficiente para descartar a insignificância penal do ocorrido, já que o volume de comunicações telemáticas interceptadas é notadamente elevado.

Conclusão

Este trabalho demonstrou que existem indícios suficientes de autoria e materialidade do crime de interceptação ilegal de comunicações telemáticas da forma tipificada pelo artigo 10, da lei 9692/96 como resultado das ações de coleta de dados para o serviço *Google Street View* no Brasil. Ademais, o trabalho apresentou um levantamento empírico da segurança das redes sem fio Brasileiras com critérios suficientes para demonstrar a amplitude da violação supra-mencionada e afastar qualquer eventual argumentação de fuga do tipo, mesmo sob a ótica da tipicidade conglobante, que é a forma de análise de maior rigor pró-agente encontrada no ordenamento jurídico brasileiro para tipificação penal. Diante desta realidade, nem a autoridade policial competente nem o ministério público podem se esquivar de instaurar o adequado procedimento investigatório acerca dessas condutas da Google no Brasil, fato que não ocorreu até o momento. Espera-se que este trabalho sirva de alerta e protesto contra tal passividade de nossas autoridades.

Referências

[GGL01] Alan Eustace (2010); "WiFi data collection: An update"; Google's Oficial Blog; Disponível em: http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html

[GLB01] Gustavo Petró (2010); "Google foca em mapear cidades-sede da Copa de 2014 para o Street View"; Caderno de Tecnologia, Globo.com; Disponível em: http://g1.globo.com/Noticias/Tecnologia/0,,MUL1439464-6174,00-GOOGLE+FOCA+EM+MAPEAR+CIDADESSEDE+DA+COPA+DE+PARA+O+STREET+VIEW.html

[GGL02] Peter Fleischer (2010); "Data collected by Google cars"; Google's European Public Policy Blog; Disponível em: http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html

[DEL01] Renai LeMay (2010); "Attorney-General refers Google Wi-Fi issue to AFP"; Delimiter News; Disponível em: http://delimiter.com.au/2010/06/06/attorney-general-refers-google-wi-fi-issue-to-afp/

[SCM01] Angela Moscaritolo (2010); "Google sued for data collection via Wi-Fi"; SC Magazine; Disponível em: http://www.scmagazineus.com/google-sued-for-data-collection-via-wi-fi/article/171089/

[THL01] Gautham Nagesh (2010); "Watchdog group wants federal investigation of Google Street View flap"; The Hill News; Disponível em: http://thehill.com/blogs/hillicon-valley/technology/99457-epic-wants-investigation-of-google-street-view-flap

[PAT01] Adel Amin Youssef et al. (2010); "Wireless network-based location approximation"; US Patent Application # 20100020776; Assignee: Google Inc, Mountain View, CA

[SFR01] STROZ FRIEDBERG (2010); "Source Code Analysis of gstumbler"; Prepared for Google and Perkins Coie; Disponível em: http://www.google.com/googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf

[IW01] Peter Sayer (2010); "Google's Street View Wi-Fi data included passwords, email"; IDG News Service/Infoworld; Disponível em: http://infoworld.com/d/networking/googles-street-view-wi-fi-data-included-passwords-email-679

[WIF01] Bruce Potter e Bob Fleck (2002); "802.11 Security"; O'Reilly & Associates, Inc.

[SSW01] A. Vindašius (2006); "Security State of Wireless Networks"; ISSN 1392 – 1215 2006. Nr. 7(71) ELEKTRONIKA IR ELEKTROTECHNIKA; Finlândia

[WDA01] Raffaele Ragni (2010); "wardrive-android: wardrive Android Application"; Disponível em: http://code.google.com/p/wardrive-android/

[SIL04]: SILVA, Ivan Luiz da. Princípio da insignificância no direito penal. Curitiba: Juruá, 2004

[GOM10] GOMES, Luiz Flávio. Princípio da Insignificância e outras Excludentes de Tipicidade. 2ª edição. vol.1. São Paulo: Revista dos Tribunais. Ano 2010

[ZAF10] ZAFFARONI, Eugenio Raúl; BATISTA, Nilo; ALAGIA, Alejandro; SLOKAR, Alejandro; **Direito Penal Brasileiro.** Rio de Janeiro: Revan, 2010.v.2.