Solução de Inteligência em Fontes abertas, Mídias Sociais, Deep e Dark Web: entendendo as reais ameaças contidas nesta aquisição do Ministério da Justiça

O pregão eletrônico (Nº 3/2021, PROCESSO Nº 08000.000865/2020-30), realizado pelo Ministério da Justiça para aquisição de solução de Inteligência em *Fontes abertas*, *Mídias Sociais*, *Deep* e *Dark Web* apresenta uma série de questões a serem observadas cuidadosamente, a partir da análise do seu edital.

Todavia, antes de fazê-lo, cabe observar o pressuposto de que existe legislação que determina autorização judicial para a quebra dos sigilos de comunicação telefônica e telemática, quando necessárias as investigações policiais. Tais demandas devem ser apresentadas exclusivamente pela Polícia Judiciária, tendo como lastro inquéritos policiais e processos de investigações criminais, ou pelo Ministério Público, mediante peticionamento ao juiz do referido processo.

Excetuando os casos acima descritos, inexiste no repertório legal brasileiro permissão para que qualquer agência de inteligência, força armada, órgão público, ou polícia ostensiva(militar), tenham acesso ao conteúdo das comunicações de qualquer cidadão brasileiro. Não existindo, portanto, formula legal para tal.

Neste sentido, tal qual um cidadão não tem permissão para adquirir um blindado militar ou um caça, uma vez que não teria permissão para utilizá-los, igualmente um órgão ou instituição de Estado não pode adquirir ferramentas as quais não tem autorização legal para fazer uso. Um sistema de interceptação de comunicações telemáticas, por exemplo, que monitore trocas de mensagens textuais, e comunicações por voz, está claramente sob a cobertura legal da legislação acima descrita, que rege as condições para quebra do sigilo de comunicações. O mesmo se daria quanto a ferramentas que permitam o acesso aos aparelhos celulares dos cidadãos brasileiros ou estrangeiros. Ou seja, sua aquisição seria restrita as instituições que podem empregar tais recursos: Polícia Judiciária e Ministério Público.

Cabe ressaltar ainda, que o Ministério da Justiça, ou seu órgão de inteligência, não são instituições policiais, não podendo, deste modo, demandarem ao poder judiciário quaisquer quebras de sigilo de comunicações telefônicas ou telemáticas. Compete ressaltar ainda, que nos quadros do MJ existem policiais civis, militares ou federais, cedidos por suas instituições, estando deslocados de suas missões originais. Todavia, o policial (civil e federal) não carrega consigo a prerrogativa do exercício da investigação com quebra de sigilos, vez que esteja no exercício de outra função que não a de policial. Igualmente estão proibidas de atentar contra o sigilo das comunicações a Agência Brasileira de Inteligência (Abin), os órgãos de inteligência das Forças Armadas, a Polícia Rodoviária Federal (PRF), ou as Polícias Militares nos estados. Muito menos órgãos como a Receita Federal e suas congêneres estaduais, ou órgãos de fiscalização ambiental, dentre outros.

Igualmente vale observar a Lei Geral de Proteção de Dados Pessoais, que prevê a proteção de dados dos indivíduos, e que tão pouco permite qualquer acesso aos órgão de inteligência de Estado ou de polícia ostensiva, e muito menos de instâncias ministeriais.

Por fim, cabe notar que, ao contrário do senso comum, agências de espionagem como a *National Security Agency* (NSA), fundada em 1952, sofrem diversos limites legais em suas atividades. Não somente existe legislação regulando a interceptação de estrangeiros ou suspeitos de espionagem em território norte-americano, como existe um setor no judiciário para autorizar, ou não, tais violações de sigilo, no tocante a inteligência de Estado. A *United States Foreign Intelligence Surveillance Court* (FISC, ou *FISA Court*) foi estabelecida desde o marco legal criado pelo *Foreign Intelligence Surveillance Act* de 1978. Nos Estados Unidos, por exemplo, não existem exigências legais somente para a interceptação realizada sobre estrangeiros residentes fora do país. Mesmo assim, as atribuições de espionagem sobre o exterior estão claramente atribuídas sob o prisma legal deste Estado, desde a origem da CIA e da NSA.

Aqui cabe uma pequena ressalva de que a ausência de regulação do tema no país, provavelmente daria margem para as atuações pouco republicanas, em detrimento das reais necessidades de proteção do Estado e da sociedade ante as ameaças externas, como é o caso da própria NSA.

Aproveitando-se do caos das mudanças tecnológicas

Interessante notar que o termo *inteligência de fontes abertas*, que recebe o acrônimo anglo-saxão de *Osint* (*Open source intelligence*), até algumas décadas atrás representava quase tão somente a coleta de dados disponibilizados espontaneamente. Ou seja, o conteúdo de periódicos, jornais, livros, filmes, arquivos públicos, repositórios de patentes, publicações científicas, pesquisas acadêmicas, dentre outros. Como se pode inferir, tais fontes, mesmo mediante o acesso pago, estão à disposição do público. Com a evolução tecnológica, em anos recentes, seu suporte físico sofreu modificações, se digitalizando. Quase todos estes citados recursos se tornaram disponíveis a partir da Internet, e seu acesso continua “público”, mesmo que remunerado.

No entanto, ao mesmo tempo, surgiram integradas neste mesmo ambiente digital as denominadas redes sociais como o *Facebook*, *Instagram*, *WhatsApp* e *Signal*. Parte destas ferramentas permitem o acesso público para algumas informações, como é o caso do *Facebook*. Mas ao mesmo tempo restringem o acesso de dados pessoais, bem como disponibilizam meios de comunicação inteiramente privados, como o Facebook com o *Messenger*. Paralelamente existem os aplicativos estritamente de comunicação, tais quais o *WhatsApp, Telegram* e *Signal*, que concorrem claramente com os serviços clássicos, ofertados pelas empresas de telefonia fixa e celular, não permitindo qualquer tipo de vínculo com o que seria conhecido originariamente como “fontes abertas”.

De natureza igualmente restrita são as redes corporativas de empresas, partidos, sindicatos ou governos, e que se conectam a internet. Também restritos são os webmails, e-mails institucionais, salas virtuais de conversação, bem como os repositórios para armazenamento de dados privados. Embora todos estes recursos estejam conectados à internet, não são indexados pelo google, e demais buscadores, por serem privados. Por decorrência são definidos como deep web, ou web profunda. Grande parte destes novos canais de informação não são fontes abertas, muito antes pelo contrário, abrigam segredos industriais, conversas políticas reservadas ou mesmo a simples intimidade dos indivíduos. Estão, portanto, plenamente resguardados pela legislação que protege dados e comunicações, bem como a que regula as investigações policiais.

Outro termo empregado, *Dark Web*, ou Web escura, tem em sua nomenclatura o simbolismo de crime e transações duvidosas. Na verdade, este conceito faz referência a sites que existem atrás de diversas camadas de criptografia, não podendo, deste modo, serem encontrados mediante as ferramentas de busca tradicionais, como o Google, ou visitados com navegadores da web clássicos, como o Google Chrome ou o Firefox. A ampla maioria dos sites na denominada *Dark Web* escondem sua identidade com o emprego da ferramenta de criptografia Tor, sendo este também um navegador que permite o acesso a tais sites. Como não existem buscadores, somente se acessa a maioria dos sites conhecendo o seu endereço. Por esta capacidade de prover privacidade e segurança, este ambiente atrai pessoas e grupos necessitando privacidade para sobreviverem, a exemplo de sites de encontros LGBTQ, movimentos de mulheres em países islâmicos, ou grupos pela democracia em nações totalitárias. No entanto, de fato, este mesmo ambiente abriga mercados de drogas ilícitas, trafego de mulheres, venda de órgãos humanos, ou tramas nazifascistas.

Figura 1. Mídias Sociais, Deep e Dark Web

Desta forma, adentramos no uso proposital de termos e denominações cujo real significado provoca dubiedade, com o possível propósito de desrespeitar a lei. No tocante as compras tecnológicas do pregão em debate, ao ser genérica na descrição do que sejam *mídias sociais, deep e dark web*, a licitação em questão permitiria a aquisição de ferramentas como o spyware "Pegasus", da empresa israelense NGO Group. Este tipo de empresa tenta descobrir permanentemente, inclusive pagando por descobertas de terceiros, novas falhas em sistemas operacionais como o Android ou o iOS. Uma vez encontrada a abertura, conseguem instalar sub-repticiamente seu spyware, ou a partir de mensagens que sirvam como isca. Como resultado, passam a monitorar textos, conversas por voz e a localização permanente do usuário. Também conseguem ativar a câmera e o microfone do aparelho. Tudo isso realizado até mesmo quando o smartphone está desligado.

Interessante notar que empresas israelenses, como a NGO Group, tem seus fundadores (Shalev Hulio, Omri Lavie), como via de regra originários da Unidade 8200. Essa unidade é responsável pela interceptação de comunicações para o exército Israelense, e parceira estratégica da NSA norte-americana, para além de ser considerada uma escola de empreendedorismo tecnológico. Desta maneira, a probabilidade de os dados coletados serem disponibilizados à inteligência israelense, e em seguida as agências norte-americanas, é um risco a ser considerado. Ao contrário do que muitos brasileiros avaliam, as agências de espionagem não operam comprometidas com as normas, tratados e acordos internacionais, ou sob um código de moralidade quanto as informações que podem obter.

Por atuarem predominantemente no exterior, buscam ganhos para o próprio país, e para isso roubam informações econômicas, obtém decisões governamentais ou empresariais importantes, pesquisas tecnológicas, projetos de patentes, e até mesmo pornografia ou situações vexatórias e de infidelidade conjugal, que possam ser posteriormente empregadas para chantagear personalidades em posições relevantes. Também existem programas oficiais de assassinatos no exterior, realizados por Israel ou pelos Estados Unidos, por exemplo, que são autorizados ao Mossad/CIA pelos principais mandatários de seus respectivos países. A localização geográfica dos alvos é um grande facilitador.

A licitação

A *Diretoria de Inteligência* da *Secretaria de Operações Integradas* (DINT/SEOPI), do Ministério da Justiça, possui como finalidade central a integração da gestão de alto nível do sistema de inteligência de segurança pública, a análise de cunho estratégico e a coleta de dados que subsidiem tal processo. A priori, conforme extensamente observado, o próprio *Ministério da Justiça* não poderia investigar indivíduos mediante a quebra de qualquer dos sigilos governados pela lei. O mesmo vale para os serviços de inteligência como a Abin. Ou seja, pela lógica de que a posse se fundamenta na possibilidade do emprego, somente as polícias judiciárias e os Ministérios Públicos poderiam possuir ferramentas que permitam o monitoramento de comunicações privadas a partir de redes sociais ou da deep web e dark web. Mesmo assim, a sua utilização exige autorização judicial. Todavia, o edital em questão, conforme igualmente observado, tem como objetivo abrangente monitorar: “mídias sociais, deep e dark Web”.

Para além de qualquer dúvida eventual sobre o real significado dos termos, ao se efetuar uma análise do resultado provisório do pregão tais questões são dirimidas. Em que pese a maioria das empresas serem bastante sintéticas sobre os detalhes dos serviços e produtos a serem fornecidos, a ferramenta *Orbis*, representante da Cognyte, adentrou um pouco mais em detalhes em seu prospecto, constante na relação de anexos apresentados pela empresa (*ORBIS Plus Cognyte - RFQ SEOPI v1.2 Mar_2021 (1).pdf*). A imagem abaixo é bastante emblemática sobre as possibilidades do software, (página 18).

Figura 2. Camadas da Web alcançadas pelo Orbis

No texto descritivo da *Cognyte* são asseguradas as capacidades de acessar histórico de navegação, "contas de mídia social que geralmente são bloqueadas para acesso geral", "áreas da web que são intencionalmente ocultas", "contas privadas seguras", "ferramentas de rastreamento", dentre outras. Vale observar que a *Cognyte* tem origem israelense, tendo sido adquirida pela norte-americana *Verint*, mas permanecendo com sua principal base de desenvolvimento em *Herzliya*, *Israel*. Possui cinquenta e três subsidiárias pelo mundo, e mais de cem parcerias, sendo uma gigante do setor. Evidentemente, também possui em seus quadros um grande número de egressos da *Unidade 8200* de inteligência de sinais, sendo um critério e padrão de recrutamento da própria empresa.

Questões

Ante os pressupostos acima, caberiam alguns questionamentos ao Ministério da Justiça:

1. Ferramentas de relacionamento como o *Facebook* ou *Instagram*, mesmo que com perfil de acesso restrito, serão monitoráveis pela ferramenta?

2. Mídias para troca de mensagens e comunicações por voz, como o *WhatsApp*, *Telegram* poderão ser monitoradas?

3. *Correios eletrônicos* corporativos e *webmails* poderão ser monitorados?

4. A localização geográfica dos "alvos" será passível de monitoramento?

5. Redes corporativas ou institucionais de empresas, ONGs ou partidos políticos são consideradas como *deep web* ou *dark web*?

6. O sistema a ser contratado prevê a captação ambiental de comunicações? Terá capacidade de empregar um aparelho celular como meio de captação ambiente?

7. Aparentemente a solução contratada será em nuvem. Qual a segurança física dos dados? O que impedirá o extravio ou venda daquilo que for coletado para agências de espionagem estrangeira?

8. Visto que a legislação de interceptação telefônica e telemática (Lei: 9296/1996) prevê em seu terceiro artigo que somente "*a autoridade policial, na investigação criminal*", e "*o representante do Ministério Público, na investigação criminal e na instrução processual penal*" possam peticionar pela quebra das comunicações ao poder judiciário, qual a constitucionalidade da interceptação de comunicações por parte de uma instância de inteligência no Ministério da Justiça?

9. Existiu alguma consulta prévia ao poder judiciário ou ao Ministério público sobre a competência do Ministério da Justiça de adquirir este tipo de equipamento para si mesmo?

9. Atualmente o Ministério da Justiça ou a Abin monitoram comunicações a partir de redes sociais?