# A obsolescência da interceptação telefônica na era pós-internet

A interceptação telefônica lançou, por muito tempo, um brilho peculiar sobre os demais meios de obtenção de prova no processo penal. Se a *confissão* alçou o malfadado posto de *rainha das provas* em sua herança inquisitorial, à interceptação telefônica — no período que sucedeu à II Guerra Mundial, em especial pelo fomento às atividades de inteligência, contrainteligência e espionagem da Guerra Fria — poderia também ser atribuído pronome de tratamento de autoridade, especialmente pela sua relevância à finalidade acusatória.

A interceptação, entretanto, já não é mais o mesmo meio (de obtenção) de prova que costumava ser antes da expansão das redes de comunicação de dados e da *internet*. É claro que o *papel* ou a *voz*, como mecanismos intercomunicativos na era *pós-internet*, ainda possuem eficácia probatória, mas estão sendo diariamente mitigados pelo crescente uso de outras formas de comunicação. O encolhimento da telefonia fixa e móvel (especialmente do uso tradicional) é fato notório, especialmente quando analisamos a expansão dos aplicativos que os *smartphones* e a *internet* garantem, não raras vezes, com maior segurança, privacidade, rapidez, qualidade e clareza da voz e menores custos.

A relevância da criptografia dos dados transmitidos, neste tipo de transmissão, é mitigada, pois a comunicação entre interlocutores A e B é feita por canal dedicado e por meio de rede de transmissão de acesso exclusivo das operadoras. Logo, ao menos que haja um terceiro não autorizado acessando a rede pública de telefonia (*man in the middle*), a interceptação, indesejada e não autorizada, se não improvável, será no mínimo, dificultosa. Por outro lado, mesmo que criptografada a *voz digital*, possivelmente, sua implementação será feita no âmbito *server side*, ou seja, as ações de criptografar e descriptografar os dados da voz digitalizada seriam controladas pela concessionária ou autorizada com o emprego de uma chave criptográfica de seu domínio — ao contrário do modelo *end to end*, ou P2P (*peer to peer*, ponto a ponto), em que remetente e destinatário compartilham de uma mesma chave criptográfica sem que o servidor, quem transporta a informação, possa decifrá-la.

Na *comunicação por dados na internet*, ao contrário, a *voz*, em formato *digital*, trafega pela rede mundial, descentralizada e rizomática em sua essência, sem que haja exclusividade ou canal dedicado entre os interlocutores. A digitalização do sinal analógico vocal, e o processo interpretativo inverso, é realizada não por quem provê o acesso à *internet* (provedor de conexão), mas, sim, pelo próprio dispositivo eletrônico (*gadget*) dos participantes. Logo, o processo de *sampling*, *quantization*, *encoding* e *compression* é feito no âmbito dos clientes (*client side*).

Em razão dos riscos decorrentes da abundância no número de usuários e da iminente suscetibilidade de interceptação na comunicação realizada pela *internet*, eis que, como dito, inexistente canal dedicado, a criptografia, nesta via comunicativa, será, em favor da segurança da informação e privacidade, indiscutivelmente, necessária.

O processo de criptografia na *comunicação por dados na internet* com o uso de dispositivos telefônicos ( *smartphones*) será implementando na espécie P2P (*peer to peer*). Cada interlocutor compartilhará de uma mesma chave criptográfica, empregada no mesmo *software* (app), em dispositivos distintos. O provedor de acesso à internet (provedor de conexão) e o provedor de conteúdo (servidor ao qual será

estabelecida uma conexão a partir do uso do *software*) poderão, eventualmente, ter acesso ao conteúdo cifrado. Os dados criptografados, entretanto, só poderão ser decifrados por seus interlocutores, já que compartilham de uma mesma chave e interface de comunicação (*software*). Logo, um terceiro interceptador, com ou sem (MITM) autorização judicial, poderá ter acesso à informação transmitida, porém, ela não será interpretável sem o uso da chave criptográfica.

É exatamente neste último ponto que reside o principal fundamento detrás da defasagem da interceptação telefônica enquanto meio de obtenção de prova.

É que se há uma perceptível migração comunicativa da *telefonia convencional, fixa* e *celular*, para a *comunicação (por dados) pela internet*, mesmo que se possa cogitar sobre a possível interceptação e armazenamento do conteúdo transmitido por esse último meio, sem que se tenha acesso à chave criptográfica não se poderá interpretar o teor da conversação (interceptada e armazenada).

A chave do problema parece estar na chave criptográfica compartilhada entre os interlocutores. Logo, para que se possa decifrar o conteúdo cifrado interceptado ou armazenado, é preciso, em primeiro lugar, que se capture a chave criptográfica. É preciso ter domínio da chave criptográfica e também acesso ao conteúdo que se pretende decifrar. Ademais, existe uma dificuldade extra: o formato da informação transmitida, ou seja, se armazenável (como imagens, texto simples e áudios) ou não (como a efêmera *voz* contida em um diálogo por *app*, tal qual o *Whatsapp* e o *Telegram*).

Mensagens de textos simples, imagens e arquivos, em geral, são obtidos com maior facilidade por meio de cautelares de busca e apreensão ou, ainda, em apreensão decorrente da prisão em flagrante do agente investigado (por exemplo, em flagrantes diferidos em ação controlada da Lei 11.343/06).

Mesmo que o investigado alvo da apreensão resolva excluir o *app* ou o conteúdo de tais informações (mensagens, imagens e arquivo), é possível que remanesçam intactos *backups* contidos no armazenamento em *cloud computing* (na *nuvem*) (como por exemplo os *backups* diários automatizados, por alguns *iPhones*, no *iCloud*, por exemplo) ou em dispositivos sincronizados (como no uso do *Whatsapp Desktop* ou *Whatsapp Web* em desktops, *notebooks* e *tablets*).

O que se tem visto, na prática, são decisões de busca e apreensão já instruídas com o comando e a autorização, automática, da devassa (quebra do sigilo) das conversas armazenadas nos aplicativos de intercomunicação[1]. Sob o ponto de vista instrumental, a coleta dos elementos de prova por este meio (cautelar busca + apreensão + devassa) mostra-se tão eficaz, se não mais, quanto a interceptação telemática que era decretada sobre a telefonia convencional (em que almejava-se, por exemplo, a interceptação de mensagens SMS, hoje em dia, absolutamente obsoletas).

Mas surge um novo problema: a interceptação e coleta da conversa —ligação, não armazenada, e, portanto, caracterizada pela efemeridade — efetuada *por dados pela internet*, tal qual aquelas realizadas por *Whatsapp* e *Telegram*.

Como o conteúdo da conversa é efêmero, ou seja, se não armazenado, esvanece-se, e como a interceptação de dados criptografados, como visto, é ineficaz, o maior desafio está na escolha do meio e técnica — processualmente válidas — para se coletar, armazenar e decifrar o teor da conversa mantida.

A tarefa é ainda mais difícil quando se constata que a criptografia, em alguns aplicativos, além de P2P ( *peer to peer*), é, também ela, efêmera. Isto é, a cada mensagem enviada e a cada ligação efetuada uma nova chave é gerada entre os interlocutores. De tal modo, a interceptação, para dispor de eficácia em sua finalidade probatória, teria que, instantânea e remotamente, dispor da chave e do conteúdo criptografado — o que é descartado de plano.

Uma das respostas, muitas vezes sugeridas, para esta incontornável situação — como coletar o elemento de prova contido em ligações de aplicativos da *internet* — seria o acesso não autorizado ao celular de um dos interlocutores mediante a obtenção de privilégio de usuário administrador a partir da exploração de falha ou vulnerabilidade do sistema operacional do celular.

Outra hipótese, para além da mencionada, seria a clonagem do *chip* telefônico com a instalação, em outro celular com o chip clonado, do aplicativo no qual se pretenderia colher o elemento de prova.

Por fim, poderia se cogitar sobre a atuação de agentes infiltrados, com amparo na recente Lei 13.441/17 e na Lei 11.343/06, ou, ainda, o *hacking* do celular em que se pretende colher a prova a partir da instalação de *backdoors* ou *malwares* de *logging* e, finalmente, a análise de metadados do tráfego gerado na rede pelos dispositivos e IPs dos interlocutores.

O uso de alguns de tais meios, porém, não justificariam os fins. Sob o ponto de vista processual, caracterizariam não só o abuso de direito da acusação em desfavor do investigado como também a instrumentalização de técnicas ilegais que resultariam em prova ilícita originária e ilícitas por derivação. Também não se pode atropelar o direito de não autoincriminação, de modo que o imputado não está obrigado a franquear o acesso aos aplicativos ou mesmo ao smartphone.

O desafio para as autoridades e protagonistas judiciais, pela questão apresentada, certamente, é grande. A migração do sistema convencional de comunicação para o modelo globalizado de interconexão além de demonstrar a incapacidade do ser humano em se adaptar à velocidade do progresso tecnológico, põe em xeque a *rainha* contemporânea dos meio de obtenção de provas, a interceptação telefônica. Novas soluções, processualmente válidas e que respeitem as regras do jogo, precisarão ser repensadas no processo penal do momento *pós-internet*.

---

[1] A ausência de autorização judicial para a devassa, inclusive, já foi objeto de enfrentamento pelo STJ e resultou na nulidade da prova obtida em caso emblemático: PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. TRÁFICO DE DROGAS. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO. 1. Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial. 2. Recurso ordinário em habeas corpus provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.

(RHC 51.531/RO, Rel. Ministro NEFI CORDEIRO, SEXTA TURMA, julgado em 19/04/2016, DJe 09/05/2016).

**Date Created**
16/06/2017