



Estado do Tocantins
Tribunal de Justiça
3ª Vara Criminal de Palmas

Processo nº 0009855-73.2019.827.2729

DECISÃO

Cuida-se de representação formulada pela delegada de polícia **Milena Santana de Araújo Lima**, da Delegacia de Repressão a Crimes Cibernéticos - DRCC, no bojo de investigação encetada para apurar a suposta prática de **furto qualificado**, ocorrido mediante invasão de conta bancária de titularidade do Conselho Regional de Odontologia do Tocantins, fato ocorrido no dia 27/10/2017.

O Ministério Público opinou pelo deferimento.

Destaco que o fato está sendo investigado no Inquérito Policial nº **0007206-38.2019.827.2729/TO**, ao qual esta representação está relacionada.

Eis a síntese dos fatos, de acordo com o que foi descrito pela autoridade policial na petição inicial:

"Foi instaurado o Inquérito Policial nº023/2019, nesta Especializada, após ter sido declinada a competência da Justiça Federal para a Justiça Estadual, dando continuidade às investigação, iniciada pela Polícia Federal (Inquérito Policial nº 30/2018-SR/DPF/TO), para apurar a prática de furto qualificado, ocorrido mediante invasão de conta bancária [REDACTED] de titularidade do [REDACTED], fato ocorrido no dia 27/10/2017.

Após burlar o sistema de segurança do Banco do Brasil S.A., o suspeito efetuou o pagamento de imposto (SEFAZ ARREC ICMS/IPVA), no valor de R\$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), configurando o crime capitulado no Art. 155, § 4.º,II, do Código Penal.

Conforme relato de [REDACTED], secretária do [REDACTED], a prática delitiva se iniciou no dia anterior, com ligação telefônica de funcionário de suposta empresa de telefonia, conforme abaixo:

"(...) 26/10/2017, por volta das 12 horas e 40 minutos, onde o interlocutor se fez passar por um funcionário de uma empresa de telefonia, alegando que precisava que fosse encaminhado um comprovante de pagamento, pelo que, teria sido encaminhado um e-mail, sendo a declarante orientada para que acessasse o link encaminhado em anexo; QUE esse anexo corresponderia a um documento que deveria ser assinado pela declarante; QUE ao abrir o anexo, o documento não correspondia ao descrito na ligação; QUE verificou que na verdade, o documento baixado correspondia a um documento de nome — Autorização de Figuração", similar a um contrato,(...) QUE não possui registro do terminal de telefone responsável pelo contato fraudulento se passando pela empresa de



Documento assinado eletronicamente por **RAFAEL GONCALVES DE PAULA**, Matrícula **78047**
Para confirmar a validade deste documento, acesse: https://eproc1.tjto.jus.br/eprocV2_prod_1grau/externo_controlador.php?acao=valida_documento_consultar e digite o Código Verificador [REDACTED]

telefonía, pois o conselho não possui bina no telefone que recebeu a ligação; QUE as possíveis linhas que receberam a ligação foram 63 3 [REDACTED] /321 [REDACTED] 914".

Para fins de instruir o feito, foi juntado aos autos a cópia do email enviado do endereço virtual ater [REDACTED] @gmail.com e tendo como destinatário a caixa eletrônica do Conselho de Odontologia, contendo um provável malware (programa malicioso) que viabilizou a técnica de phishing (furto de dados), bem como expediente da Instituição Bancária informando ter restituído a vítima, assumindo integralmente o prejuízo financeiro, motivo que ensejou a declinação da competência".

Essa narrativa encontra respaldo no inquérito policial referido, donde constam a mesmas declarações acima, que demonstram que a secretária do CRO/TO foi aparentemente induzida a instalar um programa espião em um dos computadores da entidade, por meio do qual se obtiveram os dados da conta bancária desta.

Comprovou-se ainda a realização de pagamento de boleto bancário no valor de R\$ 5.235,45, pagamento que, segundo informado, foi efetuado indevidamente, provavelmente mediante a utilização dos dados furtivamente obtidos.

Como se vê nos autos do procedimento investigatório, há indícios da existência do crime, por isso a autoridade policial pretende obter dados que levem à identificação dos autores.

Neste caso, exige-se a continuidade das investigações do que foi noticiado pela autoridade policial, ainda mais que há possibilidade de que as ações venham se repetindo, com novas vítimas ainda não identificadas. Neste aspecto, as medidas postuladas são de fundamental importância, pois sem elas a autoridade policial dificilmente terá condição de aprofundar na apuração do fato e muito menos desvendar a autoria.

Neste tipo de crime, em que se usa a rede mundial de computadores para o enriquecimento ilícito, a investigação torna-se virtualmente impossível, caso se utilizem apenas os meios tradicionais de investigação. Afinal, as pessoas envolvidas nas práticas criminosas podem estar em qualquer lugar do globo terrestre, o que dificulta sobremaneira sua localização.

Como bem salientado na petição inicial, **"as medidas administrativas possíveis pela Autoridade Policial que iniciou a investigação, não foram o suficiente para individualizar a Autoria e participação dos envolvidos, o que somente será possível após o afastamento do sigilo telefônico, telemático e bancário que se propõe com a presente representação".**

Desta forma, no tocante à quebra dos sigilos, o deferimento da representação é medida que se impõe para viabilizar a atuação policial. Ressalto que a tutela jurisdicional ora prestada assegurará que sejam respeitados os direitos individuais dos usuários das redes sociais e dos terminais telefônicos usados para a consecução dos crimes, assim como dos titulares das contas bancárias envolvidas.

Diante do exposto, defiro a representação e concedo autorização para que a autoridade policial obtenha as seguintes informações das pessoas jurídicas indicadas a seguir:

a) da **Brasil Telecom S.A. (Oi Fixa)**, por meio de seus representantes no Brasil: o histórico de chamadas recebidas no dia 26/10/2017, das linhas telefônicas abaixo (número chamado), bem como, se possível, os números telefônicos, IMEI, dados cadastrais e ERB do número chamador:



(63) 3 [REDACTED]
(63) 3 [REDACTED]
(63) 3 [REDACTED]

b) do *Google Brasil Internet Ltda*, por meio de seus representantes no Brasil:

b.1) os registros de criação do email [aten\[REDACTED\]@gmail.com](mailto:aten[REDACTED]@gmail.com), contendo números de IP, data, hora, fuso horário, portas de origem, eventual email de recuperação e telefones, bem assim os acessos ao referido endereço eletrônico nos dias 25/10/2017 a 28/10/2017, bem como dos últimos 60 dias a contar do recebimento desta decisão, dentre outros elementos de prova que possam colaborar com a investigação;

b.2) cópia dos dados armazenados no endereço eletrônico [aten\[REDACTED\]@gmail.com](mailto:aten[REDACTED]@gmail.com) e IMEI atrelado a ele, devendo conter:

b.2.1) acesso a todo o conteúdo do Google Drive;

b.2.2) acesso a todo o conteúdo da ferramenta Maps (Seus lugares, Suas contribuições, Sua linha do tempo, etc);

b.2.3) acesso ao conteúdo do Google Docs e outros serviços da Google;

b.2.4) acesso a todos os aplicativos do Google Play Store instalados no aparelho;

b.2.5) acesso ao histórico de mensagens do aplicativo Hangouts (Google Talk);

b.2.6) acesso ao histórico de localização (Location History), disponibilizando o trajeto efetuado pelo alvo;

b.2.7) acesso ao conteúdo da ferramenta de backup de Fotos (Google Fotos).

A empresa deverá ainda preservar os registros de acesso/conexão pelo prazo que durar a investigação;

c) do *Banco do Brasil S.A.*, por meio de seus representantes:

c.1) os dados referentes ao pagamento do imposto no valor de R\$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), após acesso não autorizado à conta [REDACTED] do Banco do Brasil) de titularidade do [REDACTED], fato ocorrido no dia 27/10/2017, especificando o código de barras e possível beneficiário;

c.2) os registros de conexões referentes à mencionada operação, bem como de eventuais outras transações realizadas por meio de internet banking na referida conta entre o dia 26/10/2017 a 28/10/2017, fornecendo número de IP, data, hora, fuso horário, porta lógica, número MAC, entre outros dados que possam corroborar com a investigação;

c.3) informação sobre se o número de IP eventualmente descoberto está associado a outras invasões bancárias ocorridas no mesmo período.

Esta decisão servirá como ofício requisitório endereçado a todas as pessoas jurídicas acima referidas, com as seguintes observações:

a) as respostas deverão ser apresentadas no prazo de 15 dias, a contar da data de recebimento por elas;

b) as respostas deverão ser encaminhadas diretamente à autoridade policial por meio do endereço eletrônico drcc@ssp.to.gov.br, com expressa referência ao número do processo, podendo ainda ser disponibilizado link, com login e senha para download;

c) alternativamente, as respostas poderão ser encaminhadas a este juízo por meio do endereço eletrônico criminal3palmas@tjto.jus.br, com expressa referência ao número do processo;

d) o sigilo da investigação deve ser preservado, portanto as empresas devem abster-se de informar aos



Documento assinado eletronicamente por **RAFAEL GONCALVES DE PAULA**, Matrícula **78047**
Para confirmar a validade deste documento, acesse: https://eproc1.tjto.jus.br/eprocV2_prod_1grau/externo_controlador.php?acao=valida_documento_consultar e digite o Código Verificador [REDACTED]

usuários e correntistas o fornecimento dos dados acima.

A entrega da decisão/ofício às empresas destinatárias será feita pela autoridade policial, que, para tanto, poderá valer-se de qualquer meio, inclusive eletrônico.

Intimo o Ministério Público e a autoridade policial.

Palmas/TO, 14 de março de 2019.

Rafael Gonçalves de Paula

Juiz de direito



Documento assinado eletronicamente por **RAFAEL GONCALVES DE PAULA**, Matrícula **78047**
Para confirmar a validade deste documento, acesse: https://eproc1.tjto.jus.br/eprocV2_prod_1grau/externo_controlador.php?acao=valida_documento_consultar e digite o Código Verificador [REDACTED]



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

EXCELENTÍSSIMO(A) SENHOR(A) JUIZ(A) DA 3ª VARA CRIMINAL DA COMARCA DE PALMAS - TO.

Inquérito Policial nº: 023/2019

Eproc: 0007206-38.2019.827.2729

QUEBRA DE SIGILO DE DADOS

Exmos(a). Srs(a). Juiz(a) e Promotor(a) de Justiça,

A Polícia Civil do Tocantins, por intermédio da Delegada de Polícia Civil, **Milena Santana de Araújo Lima**, que ao final subscreve, responsável pela Delegacia de Repressão a Crimes Cibernéticos-DRCC, no uso de suas atribuições legais e constitucionais, vem informar para ao final requerer:

Foi instaurado o Inquérito Policial nº023/2019, nesta Especializada, após ter sido declinada a competência da Justiça Federal para a Justiça Estadual, dando continuidade às investigação, iniciada pela Polícia Federal (Inquérito Policial nº 30/2018-SR/DPF/TO), para apurar a **prática de furto qualificado**, ocorrido mediante invasão de conta bancária [REDACTED] de titularidade do [REDACTED], fato ocorrido no dia 27/10/2017.

Após burlar o sistema de segurança do Banco do Brasil S.A., o suspeito efetuou o pagamento de imposto (SEFAZ ARREC ICMS/IPVA), no valor de R\$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), configurando o crime capitulado no Art. 155, §4.º,II, do Código Penal.

Conforme relato de [REDACTED], secretária do [REDACTED] a prática delitiva se iniciou no dia anterior, com ligação telefônica de funcionário de suposta empresa de telefonia, conforme abaixo:



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

“(…) 26/10/2017, por volta das 12 horas e 40 minutos, onde o interlocutor se fez passar por um funcionário de uma empresa de telefonia, alegando que precisava que fosse encaminhado um comprovante de pagamento, pelo que, teria sido encaminhado um e-mail, sendo a declarante orientada para que acessasse o link encaminhado em anexo; QUE esse anexo corresponderia a um documento que deveria ser assinado pela declarante; QUE ao abrir o anexo, o documento não correspondia ao descrito na ligação; QUE verificou que na verdade, o documento baixado correspondia a um documento de nome — Autorização de Figuração”, similar a um contrato,(…) QUE não possui registro do terminal de telefone responsável pelo contato fraudulento se passando pela empresa de telefonia, pois o conselho não possui bina no telefone que recebeu a ligação; QUE as possíveis linhas que receberam a ligação foram 63 3 [REDACTED] 321 [REDACTED] 914”

Para fins de instruir o feito, foi juntado aos autos a cópia do email enviado do endereço virtual [ater\[REDACTED\]@gmail.com](mailto:ater[REDACTED]@gmail.com) e tendo como destinatário a caixa eletrônica do [REDACTED] [REDACTED] contendo um provável *malware*(programa malicioso) que viabilizou a técnica de *phishing*(furto de dados), bem como expediente da Instituição Bancária informando ter restituído a vítima, assumindo integralmente o prejuízo financeiro, motivo que ensejou a declinação da competência.

Salvo melhor juízo, ainda não é possível afirmar exatamente qual a técnica utilizada, se houve acesso remoto (no qual aparecerá os dados de conexão da própria vítima) capturando-se os dados armazenados/digitados na máquina da vítima ou se os dados capturados foram remetidos para um banco de dados e posteriormente utilizado em conexão própria à invasão bancária.

Não há dúvidas que se trata de investigação de alta complexidade, possivelmente praticado por ASSOCIAÇÃO ou ORGANIZAÇÃO CRIMINOSA, cuja engenharia delitiva conta com a atuação de diversas pessoas, na função de autores ou partícipes, envolvendo diversas etapas:

Etapas 1: o *malware* e possíveis páginas falsas são desenvolvidas por uma pessoa ou mais pessoas com avançados conhecimentos na área de informática, sendo posteriormente vendido para que terceiro pratique a fraude de maneira independente ou compartilhado um co-autor, que geralmente é quem executa os furtos, rateando percentuais de lucros;



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

Etapa 2: este co-autor, em regra já recebe em um banco de dados o login e senha da vítima capturados seja através de vírus, página falsa ou outra técnica, acessando a conta da vítima para subtrair valores;

Etapa 3: por fim, após a invasão da conta bancária, os valores serão transferidos para conta de “laranjas” ou utilizado para pagamentos de boletos bancários “com descontos” de clientes que procuram esse tipo de serviço; Em regra, esses clientes não conhecem ou mantêm contato com o criador do programa e nem com o operador do sistema, mas sim com um terceiro que faz o papel de intermediário e captador de clientes e “laranjas”;

As medidas administrativas possíveis pela Autoridade Policial que iniciou a investigação, não foram o suficiente para individualizar a autoria e participação dos envolvidos, o que somente será possível após o afastamento do **sigilo telefônico, telemático e bancário** que se propõe com a presente representação.

Quanto aos dados de telefonia, faz necessária também para fins de obtenção do histórico de chamadas recebidas pelos números telefônicos da vítima (63 3 [REDACTED]/321 [REDACTED] 914), considerando que a prática da fraude se iniciou com ligação no dia anterior, 26/10/2017, para um dos referidos números. A medida poderia e deveria ser fornecida mediante requisição policial, pois não se confunde com interceptação telefônica, a qual necessariamente depende de autorização judicial, conforme melhor tratado abaixo. Entretanto, as empresas de telefonia não as fornecem.

Quanto aos dados telemáticos, essas informações se referem aos dados cadastrais e números de endereços IP armazenados nos servidores do provedor de aplicação de onde partiu o email contendo documento e possível link malicioso ([ate \[REDACTED\]@gmail.com](#)), bem como os logs de acesso ao *internet banking* da empresa.

Embora as próprias vítimas, Conselho Regional de Odontologia do Tocantins e Banco do Brasil, possuam legitimidade para terem acessos aos registros de conexão e/ou apresentarem como elementos de prova, assim não o fizeram, sendo necessário, portanto, a autorização judicial a quebra de sigilo.

Cumpra esclarecer que o Marco Civil da Internet prevê que elas somente podem ser obrigadas a fornecê-los mediante ordem judicial, nos termos do Art. 15, §3º, da Lei nº 12.965/2014, cujo *caput* também trata da guarda desses registros pelo prazo de 6 meses.



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

Por oportuno, esclareço que os dados cadastrais são aqueles dados voluntariamente informados pelo usuário do serviço, a exemplo de nome, email, telefone, entre outros, podendo ser verdadeiros ou falsos. Por sua vez, o número de endereço de IP (*Internet Protocol*) equivale a placa de um carro ou até mesmo um número telefônico, sendo, em regra, visualizável ao trafegar pela rede mundial de computadores. Sua natureza também é de dados, e não conteúdo, motivo pelo qual seu fornecimento não poderia ter sido condicionado à reserva de jurisdição.

Em verdade, ao se obter um número IP, associados à data de hora, ou a relação contendo registros de acesso/ conexões (diversos números IP associados à datas e horas), além de não revelar conteúdo, sequer informar quem é o titular do serviço de conexão, sendo ainda necessário buscar perante o provedor de conexão os dados cadastrais do cliente.

Com efeito, ao tratar da matéria, assim ressaltou apenas o fluxo de comunicações telefônicas à reserva de jurisdição:

CF/1988. Art. 5º.(...)

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; (Vide Lei nº 9.296, de 1996)
(http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm)

Não por outro motivo, a Lei das Interceptações Telefônicas (Lei nº 9296/ 96) não traça uma linha sequer sobre os dados telefônicos, tratando exclusivamente do **fluxo de comunicações**, em consonância com o raciocínio ora compartilhado. Todas as informações tratadas pelo Art.5º, XII, da CF, já estão protegidas pelo sigilo, porém condicioná-las à ordem judicial não somente desacelera a investigação policial, como provoca um aumento desnecessário de demandas judiciais. Não se pode confundir sigilo com reserva de jurisdição.

Por fim, quanto aos dados bancários, o pedido encontra-se amparado na Lei Complementar 105/2001, cujas informações são essenciais para definição da competência e individualização da autoria.



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

Diante do exposto, não havendo outro meio de avançar nas investigações, demonstrado o *fumus comissi delicti* e *periculum in mora*, solicito a Vossa Excelência, **AUTORIZAÇÃO JUDICIAL**, com supedâneo no Art. 22, da Lei nº12.965/2014 e Lei Complementar 105/2001, para que as pessoas jurídicas abaixo:

1) BRASIL TELECOM S.A.(OI FIXA), por meio de seus representantes no Brasil, forneça:

a) Forneça o histórico de chamadas recebidas no dia 26/10/2017, das linhas telefônicas abaixo(número chamado), bem como se possível for, especificando os números telefônicos, IMEI, dados cadastrais e ERB do número chamador:

- (63) 3 [REDACTED]
- (63)3 [REDACTED]
- (63)3 [REDACTED]

b)Encaminhe as respostas para o email, drcc@ssp.to.gov.br, independente de remessa postal, objetivando otimizar e acelerar à análise dos dados, independente de remessa postal;

2) GOOGLE BRASIL INTERNET LTDA, por meio de seus representantes no Brasil, forneça:

a) Os registros de criação e acesso acessos dos dias 25/10/2017 à 28/10/2017, bem como dos últimos 60 dias, contendo números de IP, data, hora, fuso horário, portas de origem, eventual email de recuperação, telefones, atrelados ao email [ate\[REDACTED\]@gmail.com](mailto:ate[REDACTED]@gmail.com) entre outros elementos de prova que possam colaborar com a investigação;

b) Forneça cópia dos dados armazenados no referido endereço eletrônico [ater\[REDACTED\]@gmail.com](mailto:ater[REDACTED]@gmail.com) e IMEI atrelado a ela, devendo conter:

- Acesso a todo o conteúdo do **Google Drive**;
- Acesso a todo o conteúdo da ferramenta **Maps**(Seus lugares, Suas contribuições, Sua linha do tempo, etc);
- Acesso ao conteúdo do **Google Docs** e outros serviços da Google;
- Acesso a todos os aplicativos do **Google Play Store** instalados no aparelho;
- Acesso ao histórico de mensagens do aplicativo **Hangouts (Google Talk)**;
- Acesso ao histórico de localização(**Location History**), disponibilizando o trajeto efetuado pelo alvo;
- Acesso ao conteúdo da ferramenta de backup de **Fotos (Google Fotos)**;



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS – DRCC

- Acesso ao conteúdo do **Gmail**(enviados, recebidos, deletados, rascunhados, etc);
- Acesso à **Agenda de Contatos**;

c) Preserve os registros de acesso/conexão pelo prazo que durar a investigação;

d) Encaminhe as respostas para o email, drcc@ssp.to.gov.br, ou link criado para esse fim, independente de remessa postal, objetivando otimizar e acelerar à análise dos dados, independente de remessa postal;

3) BANCO DO BRASIL S.A, por meio de seus representantes, forneça:

a) Os dados referentes ao pagamento do imposto no valor de R\$ 5.235,45 (cinco mil, duzentos e trinta e cinco reais, quarenta e cinco centavos), após acesso não autorizado [REDACTED] [REDACTED] de titularidade do Conselho Regional de Odontologia do Tocantins, fato ocorrido no dia 27/10/2017, especificando o código de barras e possível beneficiário.

b) Forneças os registros de conexões referentes a citada operação não autorizada, bem como de eventuais outras transações realizadas por meio de internet banking entre o dia 26/10/2017 à 28/10/2017, fornecendo número de IP, data, hora, fuso horário, porta lógica, número MAC, entre outros dados que possam corroborar com a investigação;

c) Informe se o referido número de IP está associado a outras invasões bancárias ocorridas no mesmo período;

d) Que as informações solicitadas no presente pedido sejam encaminhadas para o email institucional drcc@ssp.to.gov.br ou disponibilizando link, com login e senha para download, independente de remessa postal;

Nestes termos,
Pede deferimento.

Palmas/TO, 10 de março de 2019.

Milena Santana de Araújo Lima
Delegada de Polícia Civil



POLÍCIA CIVIL DO ESTADO DO TOCANTINS
DELEGACIA DE REPRESSÃO A CRIMES CIBERNÉTICOS - DRCC

OFÍCIO/DRCC/SSP/Nº483/2019

Palmas, 02 de julho de 2019.

SIGILOSO

Ilustríssimo(a) Senhor(a)
Representante Legal
Google Brasil Internet

Assunto: Cumprimento de decisão judicial

Ref.: IP 023/2019 (Processo nº 0009855-73.2019.827.2729)

Senhor(a) Representante,

Cumprimentando-o cordialmente, encaminho a Vossa Senhoria **Decisão Judicial** expedida pela 3ª Vara Criminal da Comarca de Palmas/TO, assinada digitalmente pelo MM. Juiz de Direito, Rafael Gonçalves de Paula, nos autos do processo em epígrafe, **para cumprimento em 15 (quinze) dias.**

Ressalto que as informações requisitadas deverão ser encaminhadas para o e-mail institucional **drcc@ssp.to.gov.br**, independentemente da remessa postal e com a maior brevidade possível.

Atenciosamente,


Cinthia Paula de Lima
Delegada de Polícia Civil