

Igor Heidrich

**DESAFIOS À PRIVACIDADE NA ESFERA DAS INVESTIGAÇÕES CRIMINAIS:
O QUE DIZEM AS DECISÕES JUDICIAIS SOBRE AS INFORMAÇÕES PRIVADAS
ARMAZENADAS EM DISPOSITIVOS ELETRÔNICOS?**

Florianópolis

2018



IGOR HEIDRICH

**Desafios à privacidade na esfera das investigações criminais:
O que dizem as decisões judiciais sobre as informações privadas armazenadas em
dispositivos eletrônicos?**

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito, da Universidade Federal de Santa Catarina, como requisito parcial para obtenção do título de Bacharel.

Orientador: Prof. Cláudio Macedo de Souza, Dr.

Florianópolis

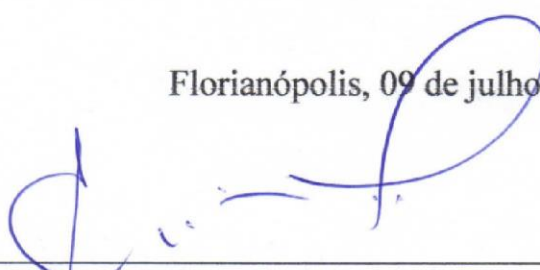
2018

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

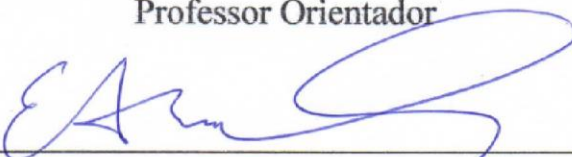
TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado “Desafios à privacidade na esfera das investigações criminais: O que dizem as decisões judiciais sobre as informações privadas armazenadas em dispositivos eletrônicos?”, elaborado pelo acadêmico “**Igor Heidrich**”, defendido em **09/07/2018** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 9.0 (note), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

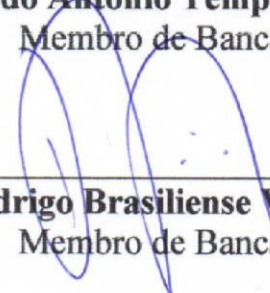
Florianópolis, 09 de julho de 2018



Prof. Cláudio Macedo de Souza, Dr.
Professor Orientador



Prof. Eduardo Antonio Temponi Lebre, Dr.
Membro de Banca



Rodrigo Brasiliense Vieira
Membro de Banca



Universidade Federal de Santa Catarina
Centro de Ciências Jurídicas
COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E
ORIENTAÇÃO IDEOLÓGICA

Aluno: Igor Heidrich
RG: 0248023 SSP/AC
CPF: 483.741.642-04
Matrícula: 13200061

Título do TCC: “Desafios à privacidade na esfera das investigações criminais: O que dizem as decisões judiciais sobre as informações privadas armazenadas em dispositivos eletrônicos?”

Orientador: Prof. Cláudio Macedo de Souza, Dr.

Eu, Igor Heidrich, acima qualificado; venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 09 de julho de 2018.

Assinatura manuscrita em azul de Igor Heidrich.

IGOR HEIDRICH

AGRADECIMENTOS

Obrigado. Para minha mãe Lairce, minha esposa Carol e meus filhos Johann, Mattheus e Philippe. Parece uma pequena palavra, mas sei que foram anos de convívio que doaram a este objetivo que alcançamos juntos.

Obrigado. Aos amigos e professores, que me acolheram e tornaram tanto esforço em algo prazeroso.

Obrigado. Ao meu orientador, professor Cláudio, pelos dias e madrugadas dedicados a tornar esta pesquisa coesa e coerente.

*“ I am a man who walks alone
And when I'm walking in a dark road
At night or strolling through the park*

*When the light begins to change
I sometimes feel a little strange
A little anxious when it's dark*

*Fear of the dark, fear of the dark
I have a constant fear that something's always near
Fear of the dark, fear of the dark
I have a phobia that someone's always there”
(Iron Maiden, Fear of the Dark)*

*“ Every time that I look in the mirror
All these lines in my face gettin' clearer
The past is gone
It went by like dusk to dawn
Isn't that the way?
Everybody's got their dues in life to pay*

*I know, nobody knows
Where it comes and where it goes
I know it's everybody's sin
You got to lose to know how to win*

*Half my life's in books' written pages
Lived and learned from fools and from sages
You know it's true
All the things you do
Come back to you”
(Aerosmith, Dream On)*

*“Existem, durante nossa vida, sempre dois caminhos a seguir: aquele que todo mundo segue e aquele que a nossa imaginação nos leva a seguir. O primeiro pode ser o mais seguro, o mais confiável, o menos crítico, aquele em que você encontrará mais amigos..., mas você será apenas mais um a caminhar. O segundo, com certeza, vai ser o mais difícil, mais solitário, aquele em que você terá maiores críticas. Mas será, também, o mais criativo, o mais original possível. Não importa o que você seja, quem você seja ou o que deseja na vida, a ousadia em ser diferente reflete na sua personalidade, no seu caráter, naquilo que você é. E é assim que as pessoas lembrarão de você um dia.”
(Ayrton Senna)*

RESUMO

Esta monografia tem como objetivo central investigar julgados penais que, fundamentados na violação do direito à privacidade, excluiu do rol de provas lícitas as informações privadas armazenadas em dispositivos eletrônicos. Cumpre ressaltar que, tais informações são comumente devassadas pela polícia durante a persecução criminal. Ademais, por causa da ausência de autorização judicial, o ato de devassar o conteúdo tem sido considerado indevido e, portanto, prova ilícita. Diante da ilicitude da prova, observou-se que, durante a tramitação processual, juízes têm decidido pelo desentranhamento de documentos nos quais conste o conteúdo das informações. Diante desta constatação a pesquisa apresentou a seguinte indagação: “Quais razões têm sido consideradas pelo Poder Judiciário ao decidir pela exclusão do conteúdo das informações privadas armazenadas em dispositivos eletrônicos dos autos do processo?” Supõe-se que a exclusão deste conteúdo dos autos do processo tenha como motivação a violação do direito à privacidade do investigado como forma de relativizar o interesse público. Para alcançar o objetivo, no primeiro momento, foi realizada investigação teórica mediante técnica de pesquisa bibliográfica. No segundo momento, foi realizado o levantamento e a avaliação de julgados penais a fim de investigar decisões pautadas pelo direito à privacidade, em especial à intimidade. Portanto, a monografia baseou-se na pesquisa quantitativa como forma de abordagem mediante o levantamento de decisões de primeira instância da Justiça Federal na esfera criminal, bem como decisões do STJ que estão formando jurisprudência. Ainda houve o escopo qualitativo com vistas à avaliação do conteúdo das decisões judiciais coletadas. A fase qualitativa foi indispensável para atestar a hipótese de pesquisa. Além de examinar o conceito jurídico de privacidade, debateu-se a relação entre as espécies de comunicação e suas quebras de sigilo com o direito à privacidade a fim de compreender a necessária proteção às informações privadas armazenadas em dispositivos eletrônicos. A partir das decisões judiciais avaliadas, concluiu-se que o direito à privacidade dos investigados está sendo violado devido ao acesso indevido às informações privadas armazenadas nos dispositivos eletrônicos pela polícia judiciária, sem autorização judicial. Também, concluiu-se pela falta de clareza na jurisprudência e pela necessidade de atualização das normas para que seja previsto em quais situações emergenciais a persecução penal poderá acessar as informações privadas armazenadas nos dispositivos eletrônicos encontrados com os investigados.

Palavras-chave: Comunicação. Privacidade. Interesse público. Segurança pública. Prova ilícita.

LISTA DE GRÁFICOS

Gráfico 1 - Percentual nos EUA	28
Gráfico 2 - Percentual no mundo	28
Gráfico 3 - Mapa com os percentuais	28
Gráfico 4 - Dispositivos Portáteis – móveis conectáveis à Internet	32

LISTA DE TEXTOS

Texto 1 – Caso 1: Delegado encaminha mídia ao MP	44
Texto 2 - Caso 1: Remoção parcial, necessidade de autorização.....	47
Texto 3 - Caso AC: Decisão.....	53

LISTA DE FIGURAS

Figura 1 - Tela inicial, com os dados de propriedade e do dispositivo em si	40
Figura 2 - Chamadas pelo WhatsApp e seus metadados	40
Figura 3 - Chat do WhatsApp com mensagens e arquivos anexos	41
Figura 4 - Localizações e sua origem, na seleção uma imagem e suas coordenadas ...	41
Figura 5 - Imagens encontradas e visualização estendida da seleção.....	42
Figura 6 - Lista de informações encontradas	42
Figura 7 - Classes de informação.....	43

SUMÁRIO

1	INTRODUÇÃO	11
2	A PRIVACIDADE NA ORDEM JURÍDICA E NA DOCTRINA	14
2.1	BREVE HISTÓRICO	14
2.2	CONCEITO E FINALIDADE	16
2.2.1	O direito de ser deixado em paz	17
2.2.2	Acesso limitado a si	17
2.2.3	Sigilo	18
2.2.4	Controle sobre as informações pessoais	18
2.2.5	Personalidade	19
2.2.6	Intimidade	19
2.2.7	Considerações sobre a privacidade	20
2.3	FUNDAMENTO CONSTITUCIONAL	20
2.4	DOCTRINA BRASILEIRA	21
2.5	DOCTRINA INTERNACIONAL	26
3	TIPOS DE COMUNICAÇÕES E SEUS AFASTAMENTOS DE SIGILO	31
3.1	TIPOS DE COMUNICAÇÃO	32
3.2	TIPOS DE AFASTAMENTO DE SIGILO	34
3.2.1	Comunicações privadas armazenadas	35
3.2.2	Interceptações de comunicações	37
3.2.3	Busca e apreensão	38
3.3	TIPOS DE VESTÍGIOS ENCONTRADOS	39
4	REMOÇÃO DE DADOS - ESTUDO DE CASOS: ACUSAÇÃO, DEFESA E DECISÕES	43
4.1	CASO SC: (DES)NECESSIDADE DE AUTORIZAÇÃO	44
4.2	CASO AC: ANULAÇÃO E NOVO LAUDO	52
4.3	CASO STJ 2016: RHC 51.531 - RO (2014/0232367-7)	58
4.4	CASO STJ 2017: RHC 89.981 - MG (2017/0250966-3)	62
5	CONCLUSÃO	67
	REFERÊNCIAS	70
	ANEXO A – DESPACHO SOBRE LAUDO DE CELULARES	73
	ANEXO B – MANIFESTAÇÃO DO MP SOBRE QUEBRA DE SIGILO	75
	ANEXO C – RETIFICAÇÃO DA REPRESENTAÇÃO INICIAL	79

ANEXO D – MP: PEDIDO DE ACESSO AOS DADOS TELEFÔNICOS.....80

1 INTRODUÇÃO

Esta monografia tem como objetivo central investigar julgados penais que, fundamentados na violação do direito à privacidade, excluiu do rol de provas lícitas documentos nos quais conste conteúdo das comunicações privadas armazenadas em dispositivos eletrônicos. Ou seja, decisões judiciais, relacionadas ao sigilo de dados em dispositivos móveis no âmbito das investigações, em especial aquelas sobre a exclusão dos conteúdos, serão avaliadas. Nesse contexto, será avaliado também o estrito cumprimento do dever legal exercido pelos agentes públicos que, durante a persecução penal, juntaram aos autos da investigação documentos com conteúdo de informações devassado indevidamente.

Uma importante justificativa para esta monografia reside em que tais dispositivos, em especial os celulares com recursos integrados à Internet, aqueles chamados de *smartphones*, alcançam atualmente mais da metade da população brasileira e que em quantidade já supera a população nacional.

A delimitação do tema teve como base o artigo 5º, inciso XII, da Constituição da República Federativa do Brasil (CRFB), que não vem sendo interpretado de maneira uniforme, nem em âmbito doutrinário e tampouco no meio jurisprudencial, principalmente quando utilizado em conjunto com a Lei nº 9.296 de 1996 das interceptações telefônicas, a qual requer atualização.

Uma das justificativas dessa monografia reside na imensa confusão gerada pelos diferentes conceitos abordados, tanto sobre os tipos de privacidade quanto de tecnologias de comunicação envolvidas. Novas definições estão surgindo nas decisões judiciais que trazem como fundamento a Lei nº 12.965 de 2014, o Marco Civil da Internet, como forma de garantir o direito à privacidade não só no fluxo da Internet, mas de todos os dispositivos que tenham capacidade para acessá-la e armazenar suas comunicações privadas mesmo que apenas seus metadados.

Diante desta observação a pesquisa apresentou a seguinte indagação: “Quais razões têm sido consideradas pelo poder judiciário ao decidir pela exclusão do conteúdo das informações armazenadas em dispositivos eletrônicos dos autos do processo?”

Supõe-se que a exclusão do conteúdo das informações armazenadas dos dispositivos eletrônicos dos autos do processo tenha como motivação a violação do direito à privacidade do investigado como forma de relativizar o interesse público.

Para alcançar o objetivo, no primeiro momento, foi realizada investigação teórica mediante técnica de pesquisa bibliográfica. No segundo momento, foi realizado o levantamento

e a avaliação de julgados penais a fim de investigar decisões pautadas pelo direito à privacidade, em especial à intimidade. Portanto, a monografia baseou-se na pesquisa quantitativa como forma de abordagem mediante o levantamento de decisões de primeira instância da Justiça Federal na esfera criminal. Ainda houve o escopo qualitativo com vistas à avaliação do conteúdo das decisões judiciais coletadas. A fase qualitativa foi indispensável para atestar a hipótese de pesquisa.

A monografia está dividida em três capítulos. No primeiro capítulo foi examinado o conceito jurídico de privacidade com base na Constituição Federal, na legislação infraconstitucional e na doutrina nacional. Devido à rapidez das transformações ocorridas no suporte das informações a serem protegidas, também, foi preciso inserir à monografia o conceito de privacidade construído em outros países, que também vivenciam os mesmos desafios.

O segundo capítulo debateu a relação entre as diversas espécies de quebra de sigilo com o direito à privacidade a fim compreender em que momento estaríamos a proteger a privacidade, na presente monografia, no âmbito das informações e comunicações privadas armazenadas em dispositivos eletrônicos. Para isso precisamos estudar quais os tipos de comunicação e quais as formas de afastamento do sigilo existentes no nosso ordenamento, bem como os tipos de informações que podem ser extraídas, qual o nível de comprometimento da intimidade de um indivíduo contida nos registros armazenados em um dispositivo tão pequeno quanto um celular.

No terceiro capítulo, foram avaliadas decisões judiciais da 1ª instância da Justiça Federal relacionadas com casos que envolvem apreensão de dispositivos eletrônicos. Bem como analisaremos casos que estão formando jurisprudência no Superior Tribunal de Justiça. Neste capítulo, a qualidade das decisões foi fator que gerou discussões em várias instâncias, onde ficou latente a importância do conteúdo abordado nos capítulos anteriores. Nos casos estudados, houve interpretações que confundiram a extração dos dados com interceptação telefônica, e que utilizaram leis, termos e referências jurisprudenciais que não se subsumiam aos casos fáticos. Como adicional aos casos primeiramente analisados e que são provenientes da primeira instância federal, foi necessária, devido à recente divulgação dos novos desafios da jurisprudência pelo STJ, profunda análise dos casos divulgados pelo Tribunal.

Por fim, este trabalho concluiu que se faz necessária uma ampla divulgação da nova jurisprudência junto aos *players* da persecução penal, pois as decisões judiciais escolhidas e as violações que as geraram, estão se repetindo, sob os mesmos fundamentos. Principalmente pelos policiais que devem buscar resguardar os vestígios, mas também pelos juízes que devem

decidir, ponderando o direito à privacidade de um indivíduo com o interesse público na resolução dos crimes investigados.

O uso generalizado de *smartphones* e suas diversas tecnologias, com a consequente apreensão destes dispositivos devido à quantidade de conhecimento passível de ser adicionado à investigação, geram uma situação onde os magistrados estão sendo instados a decidir sobre a devassa que está ocorrendo, sem nenhuma espécie de autorização, e que viola a vida íntima e a privacidade dos investigados.

Entretanto, a falta de clareza nos fundamentos das decisões torna a situação mais crítica do que a imaginada, pois as determinações do STJ pelo desentranhamento estão sendo revertidas em primeira instância através da exclusão e posterior decisão pela renovação das provas, claramente convalidando as provas ilicitamente colhidas na investigação.

Com o levantamento efetuado, percebeu-se que a jurisprudência está fragilizada, necessitando de uma padronização de termos e referências, mas principalmente, recomenda-se alteração imediata das normas, a fim de prever em quais situações emergenciais a persecução penal pode realizar acesso aos dados privados armazenados, não só nos dispositivos eletrônicos encontrados com os investigados, mas também aos dados de terceiros que fornecem os meios para a comunicação entre as partes, de forma a serem proporcionais e posteriormente justificados e auditados.

E nos demais casos, onde a obrigatória, prévia e justificada concessão de afastamento de sigilo, autorizada por juiz competente, o Estado deverá buscar formas para que a ordem judicial para acesso aos dados privados armazenados, tenha agilidade, mas que tenha parâmetros a serem respeitados, para que não se torne mera autorização irrestrita, preservando assim a intimidade dos investigados, mas sem conceder permissão ao crime e à impunidade.

2 A PRIVACIDADE NA ORDEM JURÍDICA E NA DOUTRINA

Este capítulo objetiva examinar a privacidade, em especial sua previsão e proteção na ordem jurídica brasileira e na doutrina.

Entre os direitos mais questionados em uma sociedade onde a informação e a exposição pessoal permeiam nossos dias, a privacidade faz-se necessária para impedir que nos tornemos reféns de nossa intimidade. Atualmente nos parece que cada atitude, cada fotografia, cada lugar que visitamos, cada assunto que “curtimos” ou buscamos nos coloca ou como algo a ser comercializado, ou a ser investigado.

2.1 BREVE HISTÓRICO

Não se sabe ao certo quando as garantias fundamentais surgiram. Podemos ter uma noção do nascimento, ainda que primitivo, dos direitos e deveres do homem. Nas civilizações mais antigas como Egito e Mesopotâmia, já se vislumbravam algumas proteções individuais, entre outras, contra a vida, a honra e a dignidade.

Diversas menções à privacidade podem ser encontradas na Bíblia, em textos gregos clássicos e mesmo da china antiga, enfocando basicamente o direito, ou então a necessidade da solidão. Na Inglaterra do século XVII estabeleceu-se o princípio da inviolabilidade de domicílio – *man's house is his castle*, que iria dar origem à tutela de alguns aspectos da vida privada do homem. Ainda na época feudal, a casa da família passou a representar um espaço de intimidade, proporcionado a separação da vida da comuna e indo ao encontro de interesses pessoais – a intimidade do sono, do almoço, do ritual religioso, talvez até do pensamento; e com a família burguesa a ideia do ensinamento em casa e de cada indivíduo em seu quarto passou a ser vista como condição de habitabilidade. Mesmo assim não foi o homem do medievo, por demais integrado a uma vida cotidiana de caráter coletivista, que desejou o isolamento. No outono da Idade Média surgia o homem burguês que, juntamente com sua necessidade da propriedade privada, precisava também de uma vida privada. O burguês passou a se isolar dentro de sua própria classe, dentro de sua própria casa – dentro de sua propriedade. (MORAES, 2000, p. 24)

Apesar do fato de que a privacidade só se tornou um direito geralmente aceito no século XIX-XX, a privacidade existia muito antes dessa era. A privacidade tem uma longa história, com origens nas sociedades antigas. Até a Bíblia tem algumas passagens onde a violação da privacidade apareceu em sua forma inicial, onde a vergonha e raiva seguiu-se à intrusão à vida privada. É justo pensar que Adão e Eva começaram a cobrir seus corpos com folhas a fim de preservar sua privacidade. Do ponto de vista legal, o Código de Hamurabi continha um parágrafo contra a intrusão na casa de um homem, a lei romana também regulamentou a mesma

questão. A ideia de privacidade tradicionalmente vem da diferença entre “privado” e “público”, distinção que vem da necessidade natural - tão antiga quanto a humanidade - do indivíduo para fazer uma distinção entre ele próprio e o mundo exterior (KONVITZ, 1966, p. 274).

Apenas destacando algumas das mais importantes eras da história: Nas sociedades da antiguidade, as pessoas tinham uma possibilidade relativamente limitada de como suas vidas (privadas) sofriam influência pelo estado. Platão ilustra esse fenômeno em seu diálogo *Leis*, onde a vida completa do indivíduo era determinada pelo Estado e seus objetivos, não havia lugar para liberdade e autonomia individual.

No medievo, não havia uma privacidade como valor social no sentido de hoje, o indivíduo existia como um membro de uma comunidade, então sua vida privada era afetada pelo constante “monitoramento” por outros membros. O aparecimento da privacidade “real” está relacionado à transformação dessas pequenas comunidades: o aparecimento das cidades.

Durante o século 19 as novas mudanças na economia e na sociedade levaram à transformação da maneira como as pessoas viviam e essas mudanças tiveram consequências para a privacidade também, já que a privacidade física e mental foi separada e evoluíram de duas maneiras diferentes. Devido à urbanização, a população das cidades começou a crescer e isso levou à perda física de privacidade, já que as pessoas nas cidades tinham que morar em lugares lotados.

Por outro lado, os cidadãos poderiam experimentar um novo “tipo” de privacidade, uma vez que deixavam de viver sob os sempre atentos olhos de seus vizinhos da aldeia e o constante controle moral estabelecido por eles.

Para Alexandre de Moraes, a Constituição norte-americana e suas dez primeiras emendas, com o objetivo de limitar o poder do Estado, determinaram a separação dos poderes estatais e inúmeros direitos humanos fundamentais. Mas em 1789, com a Declaração dos Direitos do Homem e do Cidadão deu-se o marco histórico das garantias fundamentais.

Outra mudança muito importante foi o surgimento e crescimento de jornais (tabloides), que eram uma área fértil para fofoca e fotojornalismo. Foi Samuel D. Warren e Louis D. Brandeis, que reconheceram pela primeira vez as ameaças à privacidade causadas pelo desenvolvimento social em seu famoso artigo *O Direito à Privacidade* em 1890.

No Brasil, veio a ser consagrado na nossa Constituição Federal de 1988, que traz como fundamentos da República Federativa do Brasil e conseqüentemente, do Estado Democrático de Direito, a dignidade da pessoa humana.

É o que dispõe o art. 1º, III da Constituição Federal:

A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

III – a dignidade da pessoa humana. (BRASIL, 1988)

Da noção primordial da dignidade de um indivíduo, nascem inúmeros conceitos que milênios depois, com a evolução do pensamento humano, em especial nos últimos dois séculos com o advento do Iluminismo, chegam às chamadas garantias fundamentais e aos direitos humanos, que reconhecidamente foram a base da assim chamada Constituição Cidadã de 1988.

2.2 CONCEITO E FINALIDADE

Segundo Alexandre de Moraes:

Os direitos à intimidade e à própria imagem formam a proteção constitucional à vida privada, salvaguardando um espaço íntimo intransponível por intromissões ilícitas externas. A proteção constitucional consagrada no inciso X do art. 5.º refere-se tanto a pessoa física quanto a pessoas jurídicas, abrangendo, inclusive, à proteção à própria imagem frente aos meios de comunicação em massa. (MORAES, 2009, p. 53)

O artigo 11 do Pacto de San José da Costa Rica, recepcionado no Brasil pelo Decreto 678 de 1992, assegura a Proteção da honra e da dignidade:

1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (AMERICANOS, ORGANIZAÇÃO DOS ESTADOS, 1969)

Ao analisarmos a composição da nossa privacidade, temos nossa intimidade, honra, imagem, nosso domicílio, correspondências e comunicações telegráficas, de dados das comunicações telefônicas e na atualidade, muitas dessas informações se confundem com os serviços prestados por empresas.

Cabe diferenciar então a vida íntima da vida privada, visto a primeira estar inserida na segunda, pois a intimidade são as informações da vida pessoal do indivíduo, hábitos, vícios, segredos desconhecidos até mesmo da própria família, as preferências sexuais, dentre outros, ao passo que a vida privada está assentada no que acontece nas relações familiares e com

terceiros, como interferir em empréstimo feito junto aos seus familiares ou obter informações sobre o saldo bancário do empregado, devendo ser preservado no anonimato o que ali ocorre.

Portanto, a proteção à intimidade e à vida privada se fundamenta na proteção à dignidade da pessoa humana, da qual emana toda e qualquer proteção ao indivíduo.

O início da discussão teórica a respeito do direito à intimidade começou em 1890 com a publicação do artigo de Warren e Brandeis, intitulado “The right of privacy”, cuja finalidade era dificultar a intromissão da imprensa na vida e na honra das pessoas. Tendo como base esse artigo, Daniel J. Solove, um dos maiores especialistas em privacidade do mundo, enxergou seis tipos de privacidade (SOLOVE, 2002, p. 1094):

- a) O direito de ser deixado em paz – direito ao isolamento;
- b) Acesso limitado a si - a capacidade de proteger-se do acesso indesejado por outros;
- c) Sigilo – a ocultação de certos assuntos de outros;
- d) Controle sobre as informações pessoais - a capacidade de exercer controle sobre as suas informações;
- e) Personalidade - a proteção da personalidade, individualidade e dignidade de uma pessoa;
- f) Intimidade - controle ou acesso limitado a relacionamentos íntimos ou aspectos de sua vida.

2.2.1 O direito de ser deixado em paz

Este conceito reconhece o “direito do indivíduo ao isolamento e viver separado dos demais” (WARREN e BRANDEIS, 1890, p. 193). É a forma da privacidade como um tipo de isolamento ou reclusão. Tal conceito, cerne do artigo de Warren e Brandeis, responde ao crescimento de uma imprensa cada vez mais invasiva e veloz, procurando demonstrar como os delitos tradicionais do *common law* poderiam ser racionalmente estendidos para cobrir essa nova situação, sem introduzir conceitos radicalmente novos.

Embora pareça enfatizar a não-interferência, na verdade, ela geralmente consiste em “uma alegação de interferência do estado na forma de proteção legal contra outros indivíduos”. Em muitos aspectos, especialmente quando articulado para lidar com a situação do jornalismo invasivo.

2.2.2 Acesso limitado a si

O ponto dessa visão de privacidade - estreitamente relacionada com o anterior - é permitir que “todo homem guarde para si seus assuntos” e reconheça o desejo do indivíduo por

ocultação e por estar separado dos outros, mas não é equivalente a solidão, nem de afastamento de outros indivíduos. Conceitualmente, uma falha nesta visão é que ela fornece pouca orientação quanto ao grau de acesso necessário para constituir uma violação de privacidade. Também não indica claramente quem decide: é sobre eu decidir qual acesso os outros têm para mim? Ou existe uma espécie de padrão absoluto ou universal que pode ser colocado em jogo?

2.2.3 Sigilo

Solove chamou isso de "ocultação de informações" ou "direito de um indivíduo de ocultar fatos desonrosos sobre si mesmo". Solove descreve o sigilo "como um subconjunto de acesso limitado ao eu", mas em apenas uma dimensão: "a ocultação de fatos pessoais". De acordo com Solove, essa concepção sustenta o direito constitucional à privacidade da informação. É também o aspecto da privacidade que identificou mais firmemente com um direito constitucional americano claro: o direito da Quarta Emenda de ser livre de "buscas e apreensões irracionais".

Legalmente, uma abordagem de privacidade como sigilo geralmente significa que, quando um fato vaza, "não pode mais permanecer privado". Assim, a Jurisprudência sobre a Quarta Emenda "sustenta que as questões que não possuem sigilo total não são privadas". Isso, o lixo não recebe proteção porque está conscientemente exposto ao público, uma vez que é prontamente acessível. A vigilância das aeronaves não implica a Quarta Emenda, uma vez que "a vigilância foi idealizada a partir do ponto de vista da supremacia do interesse público".

Mas tais caracterizações de privacidade como segredo perdem um desejo de confidencialidade: "compartilhar a informação com um seletivo grupo de pessoas de confiança". Proteger a confidencialidade, que identifico como uma preocupação do século XIX - é uma forma crítica de privacidade para muitas pessoas, especialmente no contexto médico. Assim, entender a privacidade como sigilo é muito restritivo e muito limitado.

2.2.4 Controle sobre as informações pessoais

De acordo com Solove, a privacidade é "a reivindicação de um indivíduo de controlar os termos sob os quais informações pessoais - informações identificáveis para o indivíduo - são adquiridas, divulgadas e usadas".

Esta é também a concepção que as leis de saúde relacionadas à privacidade usam. Mas, novamente, essa concepção é excessivamente restrita, já que exclui aspectos não informativos da privacidade, "como o direito de tomar certas decisões fundamentais sobre o corpo, a

reprodução ou a criação de seus filhos”. Geralmente também não define o que significa “controle” e geralmente falha em definir efetivamente o escopo do que é protegido.

Outra abordagem relacionada ao controle de informações pessoais torna as informações em propriedade. Essa abordagem *lockeana* é a espinha dorsal da lei da propriedade intelectual americana, que deriva grande parte de sua justificativa da noção “autor romântico” de criação autoral (ou inventiva) individual: “se ganha um direito de propriedade em algo quando emana de si mesmo”. O delito de apropriação e o direito conexo de publicidade, protege as pessoas contra outros usando sua imagem ou aparência para obter ganhos comerciais.

Mas essa concepção também tem problemas. A informação pessoal é “tanto uma expressão do eu como um conjunto de fatos - um registro histórico do comportamento de alguém”. Negar aos jornalistas o direito de apresentar esses fatos fere a liberdade de expressão, entre outras questões. Assim, a verdade é uma defesa contra a difamação, que por si só é um delito relacionado à privacidade.

Além disso, informações pessoais são frequentemente formadas através de relacionamentos, e não pelo “eu” de um único indivíduo. Assim, uma pessoa relatando sua própria história pode implicar a história de outra pessoa – deverão se limitar em não o fazer porque infringe a privacidade da outra pessoa?

2.2.5 Personalidade

O conceito aqui é a proteção da integridade da personalidade e muitas vezes é usada em conjunto com outras teorias. Solove descreve isso como a teoria que envolve “escolhas centrais para a dignidade e autonomia pessoal”. Alguns identificam esse direito como mais ligado à liberdade e à autonomia do que à privacidade, mas outros sugerem que existe uma noção intuitiva de privacidade invocada nos casos de privacidade constitucional. Segundo Nelson, a “personalidade” é muito vaga para ser útil, e que pensa-la em termos de autonomia é mais esclarecedor do que conceituá-la como privacidade.

2.2.6 Intimidade

Essa perspectiva conecta a privacidade às relações humanas pessoais, bem como à “autocriação individual”. Pode ser difícil definir exatamente o que é “íntimo”, exceto em termos do que os indivíduos querem revelar apenas para algumas outras pessoas ou definições semelhantes na prática. No entanto, ajuda a unificar certas concepções de privacidade com autonomia: o aborto é uma decisão privada porque é “íntimo”.

Essas definições tendem a ser muito amplas no escopo. Em muitos aspectos, não é muito mais útil do que o termo “privacidade” em si. Ao mesmo tempo, é excessivamente limitante como uma teoria geral, porque está excessivamente focado apenas nas relações interpessoais.

2.2.7 Considerações sobre a privacidade

Solove afirma que as concepções teóricas acima “falham em seus próprios termos” e “nunca atingem o objetivo de encontrar o denominador comum”. Então, o que devemos fazer então? Sua proposta é dispensar a filosofia *top-down* e, em vez disso, focar nos problemas que enfrentamos em quatro dimensões: método, generalidade, variabilidade e foco.

Seu método é pluralista, para ele: “a privacidade não é uma coisa, mas um conjunto de muitas coisas distintas, mas ainda assim relacionadas”, escreve Solove. Por generalidade, ele quer dizer que ele escolherá um nível útil de generalidade, que é contextual e prático, e não filosófico. Ele também reconhece a variabilidade da privacidade e sua contingência histórica e cultural. Ele não procura fornecer uma base fixa para a privacidade, mas sente que “ainda pode ter estabilidade suficiente enquanto acomoda a variabilidade”. Finalmente, limita seu foco do tema privacidade nos problemas de privacidade. Mais uma vez, ele procura evitar o abstrato e filosófico e ficar com o particular e específico.

A cada texto sobre o assunto, confrontado com a incansável evolução tecnológica, em especial a auto exposição mundialmente crescente, nos aproximamos do profético-visionário futuro de Arthur Miller:

"O computador, com sua insaciável sede de informação, com sua imagem de infalibilidade, com sua incapacidade de esquecer o que armazena, chegará a ser o centro de um sistema de vigilância permanente que converterá a sociedade em que vivemos num mundo transparente, em que nossa casa, nossas finanças, nossas associações e instituições, nossa condição física e mental aparecerá una a qualquer observador" (MILLER, TEIXEIRA e MENDES, 1996, p. 161)

2.3 FUNDAMENTO CONSTITUCIONAL

Alguns são os fundamentos historicamente ligados à privacidade. Na Constituição Cidadã temos o já citado inciso III do artigo 1º que traz como fundamento da República a dignidade da pessoa humana.

Dentro do conceito de dignidade, temos a vida íntima, o direito à privacidade. No ordenamento temos um crescente detalhamento da forma de proteção desta no art. 5º, que diz: “X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado

o direito a indenização pelo dano material ou moral decorrente de sua violação; ” (BRASIL, 1988)

Aqui começamos a perceber que a dignidade possui diversas dimensões, dentre elas temos o direito à privacidade e dentro deste, como temos muitas formas de exposição nos dias atuais, inúmeros serão os tipos de proteção a serem guarnecidos ao cidadão.

Nossa constituição, ao tratar do tema, em que pese a já datada edição da mesma, sofre de uma atecnia amplamente divulgada, e obviamente explorada, para decidir quando se deseja para qualquer lado. Temos então o inciso XII do artigo 5º, que diz:

XII - e 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)

2.4 DOCTRINA BRASILEIRA

Zavala de González, sob o ponto de vista filosófico, nos diz que “a intimidade constitui uma condição essencial do homem que lhe permite viver dentro de si mesmo e projetar-se no mundo exterior a partir dele mesmo, como único ser capaz de dar-se conta de si e de fazer de si o centro do universo” (ZAVALA DE GONZÁLEZ, 1982, p. 175).

Já há algum tempo, a doutrina vem conceituando o direito à intimidade como aquele que busca defender as pessoas dos olhares alheios e da interferência na sua esfera íntima, por meio de espionagem e divulgação de fatos obtidos ilicitamente. O fundamento de tal garantia estaria pautado no direito “de fazer e de não fazer” (PONTES DE MIRANDA, 1983, p. 124) - é o “direito de ser deixado em paz”, vale dizer, de não ser importunado pela curiosidade ou pela indiscrição alheia, como defendido pelo magistrado americano Cooley, no ano de 1873.

No âmbito civilista, o direito à intimidade é tipificado como direito da personalidade, inerente, pois, ao próprio homem, tendo por objetivo resguardar a dignidade e integridade da pessoa humana, sendo, ainda, caracterizado como um direito subjetivo absoluto, uma vez que exercitável e oponível *erga omnes*.

O novo Código Civil (BRASIL, 2002) traz a proteção da vida privada no seu artigo 21: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

O STF tem adotado raciocínios conflitantes, conforme se depreende do o voto do Ministro Nelson Jobim, proferido no julgamento do RE 219.780/PE, que assim dispõe, *in verbis*:

Passa-se, aqui, que o inciso XII não está tornando inviolável o dado da correspondência, da comunicação, do telegrama. Ele está proibindo a interceptação da comunicação dos dados, não dos resultados. Essa é a razão pela qual a única interceptação que se permite é a telefônica, pois é a única a não deixar vestígios, ao passo que nas comunicações por correspondência telegráfica e de dados é proibida a interceptação porque os dados remanescem; eles não são rigorosamente sigilosos, dependem da interpretação infraconstitucional para poderem ser abertos. O que é vedado de forma absoluta é a interceptação da comunicação da correspondência, do telegrama. Por que a Constituição permitiu a interceptação da comunicação telefônica? Para manter os dados, já que é a única em que, esgotando-se a comunicação, desaparecem os dados. Nas demais, não se permite porque os dados remanescem, ficam no computador, nas correspondências etc. (RE 219.780/PE, Rel. Min. Carlos Velloso, DJ de 10.09.99, p. 23).

Ao se examinar a Lei Nº 9.296/96, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal, temos que mesmo esta, possui amarras tecnológicas em seus termos, o que em uma visão garantista, pode levar a impunidade, vejamos:

Art. 1º A interceptação de **comunicações telefônicas**, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em **sistemas de informática e telemática**. (BRASIL, 1996, grifo nosso)

Pode parecer em um primeiro momento um certo preciosismo deste graduando, mas atualmente existe um embate sobre o fornecimento por parte de empresas que, prestam serviço de comunicação, utilizando sistemas de informática e que não cumprem esta norma alegando que o aplicativo WhatsApp, por exemplo, não é uma ferramenta de comunicação telefônica e sim um aplicativo que presta um serviço de valor agregado, o que quer que isso possa significar.

Com essa alegação, se privam também de obedecer a Lei Nº 12.965/14, o tão aguardado Marco Civil da Internet, este sim traz uma maior compatibilidade entre os termos técnicos e legais.

No Marco Civil, em seu Capítulo II, dispõe sobre os direitos e garantias dos usuários da Internet, no qual entendemos como os direitos mais importantes ao presente trabalho:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

[...]

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

[...]

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

[...]. (BRASIL, 2014)

O Superior Tribunal de Justiça enfrentou a questão na apreciação do RHC nº 51.531 (a ser apresentado na seção 4.3), em caso que pleiteava a imprescindibilidade de autorização judicial prévia para o acesso ao conteúdo das conversas armazenadas em telefone celular, firmando entendimento de que ilícito o acesso aos dados e conversas de mensageiros instantâneos, obtidos diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial.

A decisão do STJ, pode ser exemplificada na manifestação do Exmo. Ministro do STJ ROGÉRIO SCHIETTI CRUZ, que firmou o seguinte entendimento:

Não desconheço o julgamento pelo Supremo Tribunal Federal do HC n. 91.867/PA, da relatoria do Ministro Gilmar Mendes, em que a Segunda Turma do Excelso Pretório entendeu pela inexistência de coação ilegal na hipótese em que, após a prisão em flagrante, os policiais, ao apreenderem dois aparelhos de celular, procederam à análise dos registros telefônicos.

[...]

Como se vê, o Ministro Gilmar Mendes relata que "as autoridades policiais não tiveram, em nenhum momento, acesso às conversas mantidas entre os pacientes e o executor do crime e, ao apossarem-se do aparelho, tão somente procuraram obter do objeto apreendido, porquanto razoável obtê-los, os elementos de informação necessários à elucidação da infração penal e da autoria, a teor do disposto no art. 6º do CPP.

[...]

Os fatos narrados nesse writ são de 2004, período em que os telefones celulares sabidamente não eram conectados à internet de banda larga como o são já há algum tempo – os chamados *smartphones*, dotados de aplicativos de comunicação em tempo real –, motivo pelo qual o acesso que os policiais teriam àquela época seria necessariamente menos intrusivo que o seria hoje. (BRASIL, 2016)

Com o exposto, fica cristalino que o uso da doutrina até então adotada está em descompasso com a realidade fática, restando ao ministro passar a cotejar, mesmo que precariamente, as diferentes realidades.

Atualmente, o acesso a aparelho de telefonia celular de pessoa presa em flagrante possibilita, à autoridade policial, o acesso à inúmeros aplicativos de comunicação em tempo real, tais como WhatsApp, Viber, Line, Wechat, Telegram, BBM, SnapChat, etc. Todos eles com as mesmas funcionalidades de envio e recebimento de mensagens, fotos, vídeos e documentos em tempo real. Após baixados automaticamente no aparelho celular, tais arquivos ficam armazenados na memória do telefone, cabendo ressaltar que a maioria das empresas que disponibilizam tais funcionalidades não guardam os referidos arquivos em seus servidores.

Daí a constatação de que existem dois tipos de dados protegidos na situação dos autos: os dados gravados no aparelho acessados pela polícia ao manusear o aparelho e os dados eventualmente interceptados pela polícia no Documento: 1497056 - Inteiro Teor do Acórdão - Site certificado - DJe: 09/05/2016 Página 16 de 29 Superior Tribunal de Justiça momento em que ela acessa aplicativos de comunicação instantânea. (BRASIL, 2016)

O voto passa a citar o que a doutrina nomeia como direito probatório de terceira geração, que versa sobre "provas invasivas, altamente tecnológicas, que permitem alcançar conhecimentos e resultados inatingíveis pelos sentidos e pelas técnicas tradicionais":

[...]

A menção a elementos tangíveis tendeu, por longa data, a condicionar a teoria e prática jurídicas. Contudo, a penetração do mundo virtual como nova realidade, demonstra claramente que tais elementos vinculados à propriedade longe está de abarcar todo o âmbito de incidência de buscas e apreensões, que, de ordinário, exigiriam mandado judicial, impondo reinterpretar o que são "coisas" ou "qualquer elemento de convicção", para abranger todos os elementos que hoje contém dados informacionais.

Nesse sentido, tome-se o exemplo de um *smartphone*: ali, estão e-mails, mensagens, informações sobre usos e costumes do usuário, enfim, um conjunto extenso de informações que extrapolam em muito o conceito de coisa ou de telefone.

Supondo-se que a polícia encontre incidentalmente a uma busca um *smartphone*, poderá apreendê-lo e acessá-lo sem ordem judicial para tanto? Suponha-se, de outra parte, que se pretenda utilizar um sistema capaz de captar

emanações de calor de uma residência, para, assim, levantar indícios suficientes à obtenção de um mandado de busca e apreensão: se estará a restringir algum direito fundamental do interessado, a demandar a obtenção de um mandado expedido por magistrado imparcial de equidistante, sob pena de inutilizabilidade? O *e-mail*, incidentalmente alcançado por via da apreensão de um notebook, é uma "carta aberta ou não"? Enfim, o conceito de coisa, enquanto *res* tangível e sujeita a uma relação de pertencimento, persiste como referencial constitucionalmente ainda aplicável à tutela dos direitos fundamentais ou, caso concreto, deveria ser substituído por outro paradigma? Esse é um dos questionamentos básicos da aqui denominada de prova de terceira geração: "chega-se ao problema com o qual as Cortes interminavelmente se deparam, quando consideram os novos avanços tecnológicos: como aplicar a regra baseada em tecnologias passadas às presentes e aos futuros avanços tecnológicos". "Trata-se, pois, de um questionamento bem mais amplo, que convém, todavia, melhor examinar. [...]" (KNIJNIK, 2015)

Considerou então que o caso em tela, seria melhor analisado através da jurisprudência comparada, na então recentemente experiência da Suprema Corte norte-americana com o julgado *Riley v. Califórnia* a ser abordado no subcapítulo seguinte. Em outro voto-visto temos a seguinte ponderação, similar à posição dos EUA e do Canadá:

Não descarto, de forma absoluta, que, a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativo recém-abandonado: o acesso incontinenti aos dados ali mantidos pode ser decisivo para a libertação do sequestrado.

Durante a confecção deste trabalho, em 16 de junho de 2018, o STJ diante da visível dificuldade dos magistrados diante da intensa transformação tecnológica. Dentre os assuntos está a tese de prova ilícita para aquelas extraídas diretamente dos dados armazenados no celular do acusado caso não possuam uma prévia autorização judicial.

O STJ tem adotado a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado. A jurisprudência do tribunal entende que são inválidas mensagens de texto, SMS e conversas por meio de aplicativos como o WhatsApp obtidas diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial.

No caso analisado (AgRg no RHC 92.801), policiais civis acessaram as mensagens que apareciam no WhatsApp do celular do acusado no momento da prisão em flagrante, sem autorização judicial. Para a Quinta Turma, a prova obtida tornou-se ilícita, e teve de ser retirada dos autos, bem como os outros elementos probatórios derivados diretamente dela.

Segundo o ministro que relatou o caso, Felix Fischer, os dados armazenados nos celulares decorrentes de envio ou recebimento de dados via mensagens SMS, programas ou aplicativos de troca de mensagens, ou mesmo por correio eletrônico, dizem respeito à intimidade e à vida privada do indivíduo, sendo, portanto, invioláveis, nos termos do artigo 5º, X, da Constituição Federal.

Em outro caso (RHC 89.981), o STJ também anulou provas obtidas por policiais que acessaram as mensagens no celular de um suspeito que indicavam o repasse de informações sobre imóveis onde uma quadrilha pretendia cometer furtos.

“A análise dos dados armazenados nas conversas de WhatsApp revela manifesta violação da garantia constitucional à intimidade e à vida privada, razão pela qual se revela imprescindível autorização judicial devidamente motivada, o que nem sequer foi requerido”, concluiu o relator, ministro Reynaldo Soares da Fonseca, ao determinar o desentranhamento das provas. (BRASIL, 2018)

2.5 DOCTRINA INTERNACIONAL

Em 2013 em meio a escândalos envolvendo espionagem internacional pelos EUA, os governos brasileiro e alemão, vítimas, encaminharam à Organização das Nações Unidas um projeto de resolução intitulado "O direito à privacidade na era digital" (NAÇÕES UNIDAS, 2013):

[...] expressa a preocupação com o uso das novas tecnologias de informação e de comunicações por pessoas, empresas e governos na vigilância, interceptação e recopilação de dados, inclusive realizados extra territorialmente, já que essas práticas poderiam constituir violação de direitos humanos, em especial, quanto ao direito à privacidade, fundamental em uma sociedade democrática para materializar a liberdade de expressão, assim como se expressou preocupação com a liberdade de buscar, receber e difundir informações. **Dessa forma, reafirmou-se o direito à privacidade já protegido pelo art.12 da Declaração Universal dos Direitos Humanos e pelo art.17 do Pacto Internacional de Direitos Cívicos e Políticos;** reconheceu-se a natureza global e aberta da internet, razão pela qual o direito à privacidade também deve ser assegurado na rede. **Recomendou-se aos Estados que assegurassem o respeito e proteção do direito à privacidade no contexto das comunicações digitais, a abstenção da violação desses direitos pelos próprios Estados, a revisão dos procedimentos, práticas e legislações sobre vigilância e interceptação de comunicações e a recopilação de dados em grande escala,** assim como se mantenham mecanismos nacionais de supervisão independentes e capazes de assegurar a transparência dessas atividades, prestando contas delas. (TOMASEVICIUS FILHO, 2016, grifo nosso)

Percebe-se que o mundo enfrenta o avanço implacável da tecnologia sobre a privacidade e tenta formular políticas comuns que venham a subsumir as novas tecnologias de comunicação aos já existentes e defendidos conceitos de privacidade.

Já no tema específico deste trabalho o Supremo Tribunal dos Estados Unidos da América, em 2014, decidiu por unanimidade que a polícia não pode vasculhar os telefones celulares de suspeitos de crimes ao serem detidos sem um mandado judicial, uma vitória importante para o direito à privacidade.

Por uma votação de 9 a 0, os juízes disseram que *smartphones* e outros dispositivos eletrônicos não estavam na mesma categoria de carteiras, bolsas e veículos - todos então liberados para busca superficial pelas forças policiais. Geralmente, essas buscas são permitidas se houver "causa provável" de que um crime foi cometido, para garantir a segurança dos policiais e impedir a destruição de provas.

Dois suspeitos criminais em Massachusetts e na Califórnia foram condenados separadamente, depois que números de telefone, mensagens de texto, fotos e endereços obtidos de dispositivos eletrônicos pessoais os ligaram a atividade com drogas e gangues.

Esses casos foram apelados para o tribunal superior, criando a oportunidade de debate público sobre os limites dos direitos de privacidade, com foco no celular, onipresente e com seu vasto armazenamento de informações, imagens e vídeos.

Os recursos não foram relacionados à recente vigilância em massa dos metadados do telefone pela Agência de Segurança Nacional (NSA), que levantou preocupações constitucionais semelhantes.

[...] O fato de que a tecnologia agora permite que um indivíduo leve tais informações em suas mãos não torna a informação menos digna da proteção pela qual os Fundadores lutaram", disse a decisão. "Nossa resposta para a pergunta sobre o que a polícia deve fazer antes de vasculhar um telefone celular apreendido durante uma detenção é simples - peça um mandado. (MEARS, 2014, grifo nosso)

O Departamento de Justiça, disse que a agência trabalharia com as forças da lei para garantir o "cumprimento total" da decisão:

Utilizaremos qualquer tecnologia disponível para preservar evidências em telefones celulares enquanto procuramos um mandado, e ajudaremos nossos agentes a determinar quando circunstâncias especiais ou outra exceção aplicável ao requisito de autorização, permitirão que eles vasculhem o telefone imediatamente sem mandado. (MEARS, 2014)

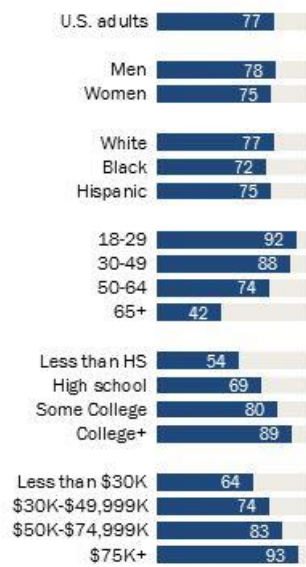
Uma pesquisa de 2014, afirma que na época, mais de 90% dos americanos possuíam ou usavam regularmente um celular, e 58% possuíam um *smartphone* mais sofisticado. Atualmente

temos que 77% dos americanos possuem um smartphone, chegando a 92% das pessoas entre 18-29 anos de idade (Gráfico 1).

Eles se tornaram a tecnologia mais rapidamente adotada de todos os tempos. Estima-se que a maioria dos 7 bilhões de pessoas tenha acesso a dispositivos móveis, de acordo com as Nações Unidas, algo em torno de 59% da população mundial (Gráfico 3), outros comparativos serão vistos adiante.

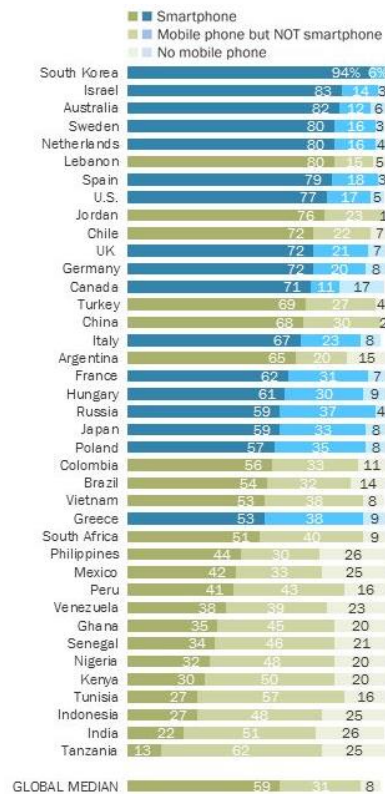
Gráfico 1 - Percentual nos EUA

% of U.S. adults who say they own a smartphone



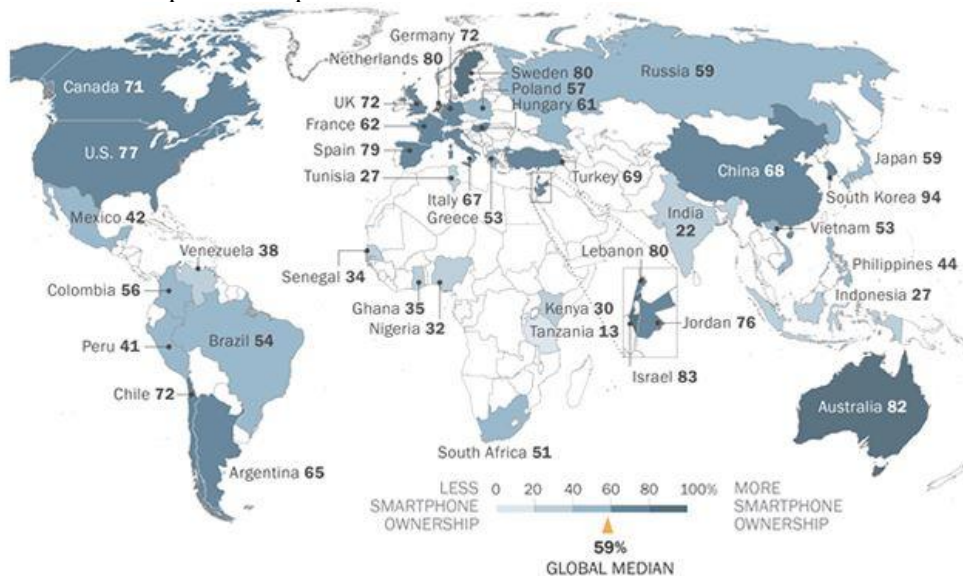
Note: Whites and blacks include only non-Hispanics.

Gráfico 2 - Percentual no mundo



Fonte: (POUSHTER, BISHOP e CHWE, 2018)

Gráfico 3 - Mapa com os percentuais



Fonte: (RAINIE e PERRIN, 2017)

Então o que ficou em evidência em qualquer assunto sobre privacidade *versus smartphones* foi a quantidade de pessoas, potencializada pela quantidade de dados possíveis de serem acessados, o que torna esse tipo de dispositivo um verdadeiro repositório online de informações sobre a população de um país.

Esse sentimento fez com que os tribunais de primeira instância nos EUA, ficassem divididos sobre como aplicar um precedente da alta corte, já com de 40 anos, permitindo buscas em pertences de um suspeito após a prisão. Nos EUA, buscas em casas geralmente exigem mandados e recebem maior proteção constitucional do que em veículos ou uma pessoa em público.

Um caso amplamente discutido foi o abordado pelo Supremo Tribunal, sobre David Riley. Ele foi detido em 2009 por ter um registro de veículo vencido e dirigir com uma licença suspensa. Quando as autoridades apreenderam seu veículo, armas carregadas foram encontradas escondidas sob o capô.

Após a prisão subsequente do estudante universitário, a polícia de San Diego deu uma vasculhada em seu *smartphone*. Mensagens de texto, contatos e vídeos no dispositivo levaram os policiais a acreditar que ele possuía conexões com o crime organizado. Isso a partir de uma fotografia de outro veículo de propriedade do suspeito, que estava ligado a um tiroteio anterior. Ele foi condenado em um tribunal estadual e recebeu uma sentença de 15 anos de prisão.

Em outro caso, Brima Wurie foi preso em 2007 por vender dois pacotes de crack. Ele tinha um celular antigo no bolso, e a polícia em Boston usava registros de chamadas no dispositivo para rastrear seu endereço real, depois que o suspeito forneceu um falso.

Nesta casa, oficiais com um mandado de busca encontraram mais drogas, uma arma e munição. Wurie foi condenado em tribunal federal e estava cumprindo 22 anos.

Em nenhum dos casos a polícia solicitou um mandado antes que os telefones fossem revistados. Em um tribunal de apelações, foi confirmada a condenação de Riley e em outro descartada a de Wurie.

Não está claro na decisão do tribunal superior se outros réus condenados por tais evidências eletrônicas também terão seus casos rejeitados. Mas o tribunal não mediu palavras para separar tais dispositivos de outras coisas que uma pessoa pode estar portando quando é detida pela polícia.

O presidente da Suprema Corte, John Roberts se manifestou:

Os telefones celulares modernos, como uma categoria, implicam preocupações com a privacidade muito além daqueles implicados pela busca de um maço de cigarros, uma carteira ou uma bolsa.

[...]

Os telefones celulares diferem em termos quantitativos e qualitativos de outros objetos que podem ser encontrados com uma pessoa presa. (MEARS, 2014)

A Quarta Emenda da Constituição dos EUA protege seus cidadãos contra "buscas e apreensões irracionais". Mas a Suprema Corte tem repetidamente afirmado a discricionariedade do governo em conduzir revistas e buscas superficiais em pessoas e veículos sem mandados, para garantir a segurança dos policiais e evitar a destruição de provas.

Isso após uma decisão de 1973 que confirmou a busca policial em uma caixa de cigarro amassada de um suspeito, onde foram descobertas cápsulas de heroína. O motorista primeiro foi parado por suspeita de dirigir com a licença suspensa.

Revistas policiais podem incluir outros objetos fechados, como carteiras e agenda de endereços, mesmo que inicialmente os itens não pareçam contrabandeados ou perigosos. Mas os defensores da privacidade e os advogados de defesa argumentam que os dispositivos portáteis tornam essas apelações diferentes. O tribunal, de forma unânime, concordou.

Interessante foi o voto-vista da Exma. Ministra do STJ, Maria Thereza de Assis Moura, proferido no RHC Nº 51.531 - RO (2014/0232367-7) e que traz brilhantemente um aparte sobre o entendimento do assunto em outros países, *in verbis*:

O tema, porém, é ainda bastante controverso. Pouco após a prolação da referida decisão nos EUA, a Suprema Corte do Canadá, ao decidir R. v. Fearon (2014 SCC 77, [2014] S.C.R. 621), entendeu, por maioria de 4 votos a 3, pela legitimidade do acesso pela polícia aos dados armazenados em aparelho celular, sem a necessidade de prévia ordem judicial, quando realizado tal acesso na sequência de uma prisão em flagrante.

No caso concreto, dois homens – um deles armado com uma espingarda – roubaram uma comerciante enquanto ela transferia joias para o seu carro, fugindo em seguida. No mesmo dia, mais tarde, policiais encontraram o veículo da fuga, prenderam os suspeitos e, ao revistar um deles, encontraram um aparelho celular em seu bolso.

Acessando imediatamente os dados constantes no aparelho, encontraram mensagens em que os suspeitos comunicavam que haviam realizado o roubo, bem como algumas fotos, inclusive da espingarda utilizada para a prática do crime. Um dia depois, com base em um mandado judicial de busca e apreensão para o exame do veículo, a espingarda, utilizada no roubo e retratada na foto, foi encontrada. Meses depois, as autoridades policiais requereram e obtiveram judicialmente a quebra do sigilo dos dados telefônicos, mas não foram encontradas novas evidências.

A Suprema Corte canadense admitiu a legitimidade do acesso aos dados incidentalmente à prisão, ainda que sem ordem judicial, e reconheceu a validade das provas obtidas por este meio.

De acordo com o entendimento adotado, a prerrogativa de acesso aos dados do aparelho celular incidente a uma prisão é admitida excepcionalmente, servindo a importantes objetivos da persecução penal, pois auxilia as autoridades policiais na identificação e mitigação de riscos à segurança pública, na localização de armas de fogo e produtos roubados, na identificação e localização de cúmplices dos delitos, na localização e preservação de provas, na prevenção da fuga de suspeitos, na identificação de possíveis riscos às autoridades policiais e na continuidade imediata da investigação. Reconheceu-se a existência de um “elemento de urgência” no acesso aos aparelhos celulares, que sustentam a extensão do poder ínsito à prisão em flagrante.

Por outro lado, consignou-se a necessidade de observância de quatro condições para a legitimidade da medida, com o objetivo de balancear os interesses inerentes à persecução penal e ao direito fundamental à privacidade:

- a) a prisão tem de ser lícita;
- b) o acesso aos dados do aparelho celular tem de ser verdadeiramente incidental à prisão, realizado imediatamente após o ato para servir efetivamente aos propósitos da persecução penal, que, nesse contexto, são os de proteger as autoridades policiais, o suspeito ou o público, preservar elementos de prova e, se a investigação puder ser impedida ou prejudicada significativamente, descobrir novas provas;
- c) a natureza e a extensão da medida tem de ser desenhadas para esses propósitos, o que indica que, em regra, apenas correspondências eletrônicas, textos, fotos e chamadas recentes podem ser escrutinadas;
- d) finalmente, as autoridades policiais devem tomar notas detalhadas dos dados examinados e de como se deu esse exame, com a indicação dos aplicativos verificados, do propósito, da extensão e do tempo do acesso.

Este último requerimento de manutenção de registros da medida auxilia na posterior revisão judicial e permite aos policiais agir em estrito cumprimento às demais condições expostas. (BRASIL, 2016)

Percebe-se que no Canadá, buscou-se algo como nos EUA, mas já definindo um maior poder nas situações de flagrante, contudo, com mais responsabilidades, visto o grau de documentação sobre os dados acessados, bem como em que circunstâncias ocorreram.

3 TIPOS DE COMUNICAÇÕES E SEUS AFASTAMENTOS DE SIGILO

Neste capítulo, abordaremos questões mais técnicas sobre os tipos de comunicação comparando-as às questões legais das quebras de sigilo existentes no ordenamento jurídico.

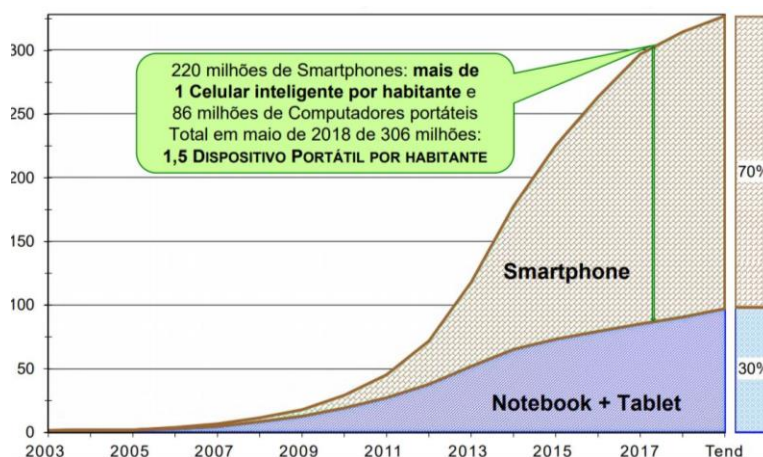
De um lado, temos uma crescente necessidade de conexão em sociedade e de informação em tempo real, seja por questões de trabalho, seja por questões pessoais. Do outro temos a necessidade de combater o uso da tecnologia como infraestrutura do crime.

Talvez o epicentro desse movimento, o ponto de fricção entre essas forças colossais, esteja em um pequeno aparelho eletrônico, motivo de piadas sobre suas capacidades ditas secundárias e que há muito suplantaram as de sua concepção, o telefone celular.

Engana-se quem confunde suas atuais capacidades como diferentes das que o idealizaram. Tais dispositivos ainda tem na comunicação móvel a sua força, mas aquela assim chamada de comunicação telefônica sim, essa aparentemente está em segundo plano.

Anteriormente, demonstramos a importância do assunto quando da decisão dos Estados Unidos da América em limitar buscas em aparelhos celulares e que dentre os motivos estava a abrangência destes frente à população norte-americana (Gráfico 1). No Gráfico 4, alguns números do Brasil, que em dezembro de 2017 tinha aproximadamente 210 milhões de habitantes, em que pese não serem comparáveis os percentuais, visto o primeiro efetivamente abordar quantos possuem o aparelho e a segunda apenas comparar o número de dispositivos com o número de habitantes (YUGE, 2018), ambos mostram o quão expressivo é a posse destes.

Gráfico 4 - Dispositivos Portáteis – móveis conectáveis à Internet



Fonte: (MEIRELLES, 2018)

Percebe-se então a profundidade do tema aqui abordado, estamos na penumbra da legislação frente ao rápido avanço da tecnologia. Onde podemos estar, na proporção de dois dispositivos móveis por habitante, sendo monitorados, ou gerando registros passíveis de uso pela persecução penal.

3.1 TIPOS DE COMUNICAÇÃO

Como veremos no subcapítulo reservado aos tipos de quebra, devido a um descolamento entre a nomenclatura adotada pelo legislador que se apegou a nomes utilizados em tecnologias e não aos reais tipos de comunicação, temos que fazer um aparte sobre os conceitos de

comunicação, de fato, podemos enxergar os tipos de comunicação como sendo de dois tipos: comunicação síncrona e assíncrona.

Como este trabalho baseia-se em estudos de casos, a seguir um exemplo de como essa prisão normativa conduz ao erro.

Certa vez, durante uma operação que tinha autorizados três tipos de quebra de sigilo, telefônico, telemático e de correspondência se deparou com uma situação inusitada. Os alvos falavam por telefone que passariam informações por e-mail.

Em contato com a empresa que detinha a conta de e-mail que era acessada, identificada na interceptação telefônica, a equipe recebeu uma conta espelho, onde todas as mensagens recebidas e enviadas seriam repassadas. Passados dias, percebeu-se que a comunicação transcorria normalmente, mas nenhum e-mail chegava. Questionando a provedora, a equipe foi informada que nenhuma comunicação tinha se dado pela conta alvo.

Ou seja, nenhum e-mail foi enviado ou recebido pela conta alvo, mas a provedora detectou que existia alteração na pasta de rascunhos de mensagens. A coisa funcionava da seguinte forma, quem quisesse deixar um recado escrevia um rascunho e apagava o anterior e assim a polícia nunca ia receber as mensagens enviadas ou recebidas, pois esses rascunhos nunca foram enviados.

Houve inclusive um momento no qual passou-se a discutir se existia, dentro do mandado, autorização para a cópia do rascunho, sendo que a provedora alegou inclusive que não havia comunicação acontecendo. Entre outras escusas.

Na situação narrada, claramente havia comunicação, entretanto, por fugir da nomenclatura padrão prevista no ordenamento, ocorreu o “ruído” com a provedora.

Classicamente, os tipos de comunicação aceitos são:

- Síncrona: quando o emissor está em contato “direto” com o receptor e vice-versa. Não há, em princípio, nenhum *delay* ou tempo a mais na comunicação. O exemplo clássico é a comunicação telefônica. Também modernamente temos as salas de conversações online entre duas ou mais pessoas e a áudio e videoconferências.
- Assíncrona: quando o emissor envia uma mensagem ao receptor e esse não necessariamente a recebe no mesmo momento, ou, se a recebe, não necessariamente a acessa naquele mesmo momento, daí o termo assíncrono. O exemplo clássico é a carta, que se transformou atualmente no e-mail, ou *eletronic mail*.

Aqui cabe um parêntese, alguns autores classificam as atuais ferramentas sociais como síncronas, mas na verdade algumas possuem recursos síncronos e assíncronos, possuem um chat assíncrono por texto e áudio, com possibilidade de verificação de recebimento e leitura, associado a comunicação síncrona por áudio e vídeo.

Tais ferramentas são chamadas de mensageiros instantâneos e por essa capacidade de comunicação em tempo real, permitem conversas online entre duas ou mais partes, podendo assim, serem usada quase que sincronamente.

A maioria desses sistemas, permitem o envio de mensagens para pessoas de modo *offline*, ou seja, as demais partes não estão conectadas, algo muito parecido com a infraestrutura de comunicação do e-mail, onde a mensagem passa por um intermediário, a figura de um carteiro, que encaminha a mensagem no momento que recebe se o destinatário está ausente, ou tenta em outro momento quando o destinatário ficar *online*.

Aqui uma característica de tais ferramentas e que mais a frente será o ponto de discussão. Essas ferramentas mantem históricos das conversas assíncronas, como textos, áudios e vídeos, ou seja, as comunicações síncronas de áudio e vídeo não são guardadas (a princípio) e, portanto, só poderiam ser capturadas no exato momento em que trafegaram pela rede.

Outro recurso muito utilizado nos mensageiros é a troca de arquivos, inicialmente fotos, depois vídeos e atualmente documentos em geral. Assemelhando ainda mais com o correio eletrônico. Tem-se então uma perspectiva diferente na apresentação do conteúdo. Um voltado aos seus contatos sociais, como sua agenda telefônica e outro voltado a contatos de correio eletrônico.

3.2 TIPOS DE AFASTAMENTO DE SIGILO

Depois de conceituarmos os tipos de comunicação passaremos a abordar os tipos de afastamento ou quebra de sigilo existentes no nosso ordenamento, bem como verificar se existe uma incompatibilidade entre os tipos de comunicação e os sigilos previstos.

A Constituição no artigo 5º, inciso XII diz ser “ 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” (BRASIL, 1988).

Mesmo nos dias de hoje encontramos quem defenda a tese de que a inviolabilidade dos dados do referido artigo abrigaria o direito ao sigilo bancário, também acolhido, para estes, sob a rubrica “direito à intimidade e à vida privada”. Tal defesa se baseia no entendimento de que a Carta Magna teria confiado à regulamentação infraconstitucional, apenas a interceptação das

ligações telefônicas, vedando-se, o afastamento do sigilo de correspondências, das comunicações telegráficas e dos dados.

Trata-se de mais uma famosa atecnia do nosso ordenamento, que obriga juízes a elucubrarem sobre o alcance de direitos frente ao abuso destes.

3.2.1 Comunicações privadas armazenadas

Alguns exemplos mais comuns de comunicações privadas armazenadas alvos de afastamento de sigilo são: correspondência, telegrafia, dados e registros de telefonia. De certa forma pacífico é o entendimento sobre o sigilo de correspondência e de telegrafia, se pensarmos em cartas e telegramas. Mas com o avanço da tecnologia e com o uso beirando a extinção de cartas e telegramas, substituídos por e-mails e mensagens instantâneas, as certezas sobre a aplicação do artigo 5º, inciso XII se torna obscura. Mais à frente voltaremos a este assunto.

E aqui temos um ponto de ruptura na doutrina, o que o legislador quis dizer com dados? O sigilo telefônico é sobre a conversa ou sobre os registros das conversas? O “no último caso” é somente sobre o sigilo telefônico?

Vamos à primeira pergunta: O que significava “dados” em 1988? Muitos sustentam que seja uma alusão a uma “modalidade tecnológica de comunicação” o que parece aceitável. Mas muitos doutrinadores assumem a palavra “dados” no sentido de registros, conforme Ives Gandra da Silva Martins assevera que a inviolabilidade do sigilo está consagrada no artigo que é inteiramente dedicado aos direitos individuais (Art. 5º da CRFB/88), assim:

A LC 105/2001, com muito mais razão, mostra-se ilegítima, pois, se nem emenda constitucional pode alterar o resguardo do sigilo de dados, à nitidez, muito menos a lei complementar poderia fazê-lo, razão pela qual tenho para mim que os dois exteriorizam manifesta inconstitucionalidade.

Parece-me, pois, que o direito do contribuinte de ter seu sigilo bancário preservado não poderá ser retirado - enquanto não houver uma ruptura institucional, o que ninguém deseja - podendo ser quebrado, apenas, por autorização judicial. (MARTINS, 2001)

Tal confusão é replicada quando entramos na seara do sigilo telefônico, pois para alguns trata-se de “grampear” o áudio de uma comunicação telefônica, para outros, trata-se da obtenção dos registros de determinado “terminal telefônico” junto a uma operadora de telefonia no *stricto sensu* (empresa homologada pela ANATEL).

Por fim e não menos importante, seria o limitador “no último caso” apenas uma figura de linguagem infeliz, ou queria o legislador que apenas o sigilo telefônico fosse passível de ser afastado por decisão judicial?

Os autores mais sensatos, acordam que nenhuma liberdade individual é absoluta e que mesmo o direito à vida tem previsão de pena capital em caso de guerra.

Para concluir este subcapítulo, mesmo que não elencados, encontramos decisões que permitem o afastamento do sigilo de correspondência, telegrafia, de “dados” no sentido de informações e os dados telefônicos.

Destes, os dois primeiros são comunicações privadas, como visto anteriormente são assíncronas; “dados” são informações sobre um usuário de um sistema, seja um banco, a receita ou uma empresa de comunicação; e os metadados (como os “dados telefônicos”), não possuem o conteúdo, mas fornecem as informações da informação, por exemplo, a data e hora de uma ligação. Não sabemos o conteúdo, mas sabemos “quem”, “com quem”, “onde”, “quando”, etc. Em comum são registros, passíveis de guarda e manuseio.

O Marco Civil da Internet, que versa sobre dados eletrônicos, conseguiu distinguir os tipos de sigilo e previu o afastamento destes:

Art. 7º [...]

III - inviolabilidade e sigilo de suas **comunicações privadas armazenadas**, salvo por ordem judicial;

VII - não fornecimento a terceiros de seus **dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet**, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

[...] (BRASIL, 2014, grifo nosso)

Podemos então reduzir as correspondências e mensagens instantâneas armazenadas ao III e os dados de cadastro e metadados no VII, sendo que este, não cita por ordem judicial, mas cita as hipóteses previstas em lei, o que me parece uma nova atecnia, deveria já prever a ordem judicial, deixando para outras leis o afastamento do sigilo dos dados de registro e metadados.

Art. 10. A guarda e a disponibilização dos **registros de conexão** e de **acesso a aplicações de internet** de que trata esta Lei, bem como de **dados pessoais e do conteúdo de comunicações privadas**, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar **os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das **comunicações privadas** somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

[...]

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os **registros de acesso** a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos **registros** de que trata este artigo **deverá ser precedida de autorização judicial**, conforme disposto na Seção IV deste Capítulo.

[...]

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de **registros de conexão ou de registros de acesso** a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

- I - fundados indícios da ocorrência do ilícito;
- II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
- III - período ao qual se referem os registros. (BRASIL, 2014, grifo nosso)

Aqui o legislador corrigiu, pois passou a prever o afastamento do sigilo dos metadados e dos dados de cadastro associados.

3.2.2 Interceptações de comunicações

Acabamos de classificar os sigilos sobre registros, que são ou comunicações assíncronas ou informações, ou metadados, não poderíamos deixar de falar sobre o “fluxo de comunicações em sistemas de informática e telemática”, previsto na lei das interceptações telefônicas e que a princípio não ficam armazenadas em seu destino ou origem.

Como já abordado no capítulo 2.4, a falta de uma tipificação baseada no fato genérico, naquilo que seria uma cópia, uma análise, um acesso ao fluxo de comunicação, causado por um excesso de especificidade da lei 9.296/96, mas, na esfera dos dados eletrônicos, devidamente corrigido no Marco Civil da Internet:

Art. 7º [...]

II - inviolabilidade e sigilo do **fluxo de suas comunicações** pela internet, salvo por ordem judicial, na forma da lei;

[...] Art. 10º [...]

§ 2º O conteúdo das **comunicações privadas** somente poderá ser disponibilizado **mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. (BRASIL, 2014, grifo nosso)

Aqui temos o sigilo sobre o fluxo de comunicação afastado por ordem judicial, mas na forma da lei, mas diferentemente dos dados (ordem judicial), metadados e registros (art. 22 do próprio MCI) as interceptações não gozaram de uma previsão expressa, talvez por se considerarem abarcadas na lei 9.296/96.

3.2.3 Busca e apreensão

É comum a alegação de que algumas formas de interceptação não são permitidas por existir a possibilidade de o magistrado emitir um mandado de busca e apreensão, por exemplo, permitir a interceptação de uma carta dentro dos correios, ou aguardar a chegada da mesma na residência do investigado e solicitar a busca na casa do suspeito, no intuito de apreender tal correspondência. Vejamos o que nos traz o Código de Processo Penal de 1941:

Art. 240. A busca será domiciliar ou pessoal.

§ 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:

- a) prender criminosos;
- b) apreender coisas achadas ou obtidas por meios criminosos;
- c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
- d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
- e) descobrir objetos necessários à prova de infração ou à defesa do réu;
- f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
- g) apreender pessoas vítimas de crimes;
- h) colher qualquer elemento de convicção.

Art. 244. A busca pessoal independe de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar. (BRASIL, 1941)

O mesmo pensamento pode ser atualizado para as mensagens eletrônicas, sejam e-mails ou mensagens instantâneas. Parece ser mais gravoso, entretanto mais transparente, a busca. Isto pela alínea “h”, que amplia a profundidade da busca em termos difíceis de saber até onde a privacidade pode ser flexionada.

Acrescente-se o fato de que durante uma investigação pode ser necessária a coleta de informações que levem aos demais integrantes de uma organização criminosa, fazendo sentido em se autorizar uma interceptação ao invés de realizar uma busca e alertar os demais integrantes.

3.3 TIPOS DE VESTÍGIOS ENCONTRADOS

Ao serem submetidos à exames, o normal é que o celular possua como sistema operacional ou Android do Google, ou IOS da Apple. Que esteja bloqueado, bloqueado com a senha fornecida, ou mesmo desbloqueado.

O tipo de extração varia com cada situação específica e envolve graus diferentes de alterações no software do aparelho, podendo inclusive ocasionar a perda de todo o conteúdo do mesmo. Entre as ferramentas mais comuns, temos a israelense Cellebrite, com sua família UFED, cuja propaganda alega:

Bloqueios complicados, barreiras de criptografia, conteúdo apagado e desconhecido e outros obstáculos para recuperar dados de dispositivos podem impedir a descoberta de provas importantes. Para que as investigações avancem, as equipes precisam de ferramentas robustas, eficientes para examinar os dados dos dispositivos e produzir pistas significativas sem atraso.

O UFED Ultimate proporciona acesso líder de mercado a dispositivos digitais e recursos inigualáveis para extrair e decodificar cada milésimo de dados. Mergulhe profundamente para analisar de forma completa os sistemas de arquivos lógicos e dados extraídos fisicamente, descobrir indícios críticos e compartilhe suas descobertas com a equipe de investigação inteira. Com as atualizações progressivas de software e suporte numa variedade de plataformas de hardware, garanta que as equipes tenham os recursos de ponta para realizar perícias forenses digitais quando e onde eles forem mais necessários. (CELLEBRITE, 2018)

No dia-a-dia o processo não é tão automatizado, em função da miríade de dispositivos, com hardwares, softwares e configurações diferentes. Muitas vezes a extração se dá por falhas de segurança encontradas e que em algum momento recebem atualizações de segurança. Por vezes inviabilizando os exames. Mas, quando do sucesso na extração, uma infinidade de informações pode ser alcançada. Telefonemas, mensagens instantâneas, imagens, vídeos, áudios, registros de localização, agendas, etc.

Figura 1 - Tela inicial, com os dados de propriedade e do dispositivo em si

The screenshot displays the 'Reader' application interface. The main window is titled 'Extraction Summary (2)'. The left sidebar shows a file tree with categories like 'Logical (1)', 'Logical (2)', 'File Systems', 'Analyzed Data', 'Autofill (347)', 'Bluetooth Devices (227) (11)', 'Calendar (208) (33)', 'Call Log (708) (180)', 'Chats (358) (34)', 'Contacts (3105) (37)', 'Cookies (5230) (12)', 'Device Locations (4523)', 'Locations (4523)', 'Installed Applications (418)', 'Log Entries (1071)', 'Notes (51) (3)', 'Passwords (397)', 'Searched Items (1021) (2)', 'SIM Data (7)', 'SMS Messages (32) (1)', 'User Accounts (57)', 'Web Bookmarks (12)', 'Web History (2880) (302)', 'Wireless Networks (130)', 'Data Files', 'Audio (1941)', 'Configurations (77499) (2)', 'Databases (169)', 'Documents (86)', 'Images (42588)', 'Text (40)', 'Videos (1996)', 'Carving', 'Images', 'Timeline (5607)', and 'Tags (8)'. The main content area shows 'Extraction Summary' with two logical extractions: 'Logical (1) SIM Card SIM Lógico' and 'Logical (2) Lógico [Method 1]'. Below this is 'Case Information' (SETEC/SC) and 'Device Info' for an iPhone 7 (A1778) with details like serial number, model, IMEI, and activation date. The 'Device Content' panel on the right lists various data categories and their counts, such as 'Autofill: 347', 'Bluetooth Devices: 227 (11)', 'Calendar: 208 (33)', 'Call Log: 708 (180)', 'Chats: 358 (34)', 'Contacts: 3105 (37)', 'Cookies: 5230 (12)', 'Device Locations: 4523', 'Installed Applications: 418', 'Log Entries: 1071', 'Notes: 51 (3)', 'Passwords: 397', 'Searched Items: 1021 (2)', 'SIM Data: 7', 'SMS Messages: 32 (1)', 'User Accounts: 57', 'Web Bookmarks: 12', 'Web History: 2880 (302)', and 'Wireless Networks: 130'. A notification at the bottom right says 'Convert BSSID (wireless networks) an... This extraction includes BSSID/cell tower values that can be converted to physical locations. Use Don't show again'.

Figura 2 - Chamadas pelo WhatsApp e seus metadados

The screenshot displays the 'Reader' application interface showing a 'WhatsApp (199)' extraction. The main window shows a list of call log entries with columns: ID, status, parties, timestamp, duration, type, and country code. The list contains 19 items. The 'Call Log' panel on the right shows details for a specific call: Timestamp: 25/03/2018 00:17:57(UTC-3), Duration: 00:01:05, Type: Outgoing, Country code: Outgoing, Network code: , Network Name: , Source: WhatsApp, Video call: False, Extraction: Logical (2), and Source file: . The 'Parties' section shows 'From: [redacted]@whatsapp.net (owner)' and 'To: 55-[redacted]@whatsapp.net'. The bottom status bar indicates 'Total: 199 Deduplications: 0 Items: 199/199 Selected: 199'.

Figura 3 - Chat do WhatsApp com mensagens e arquivos anexos

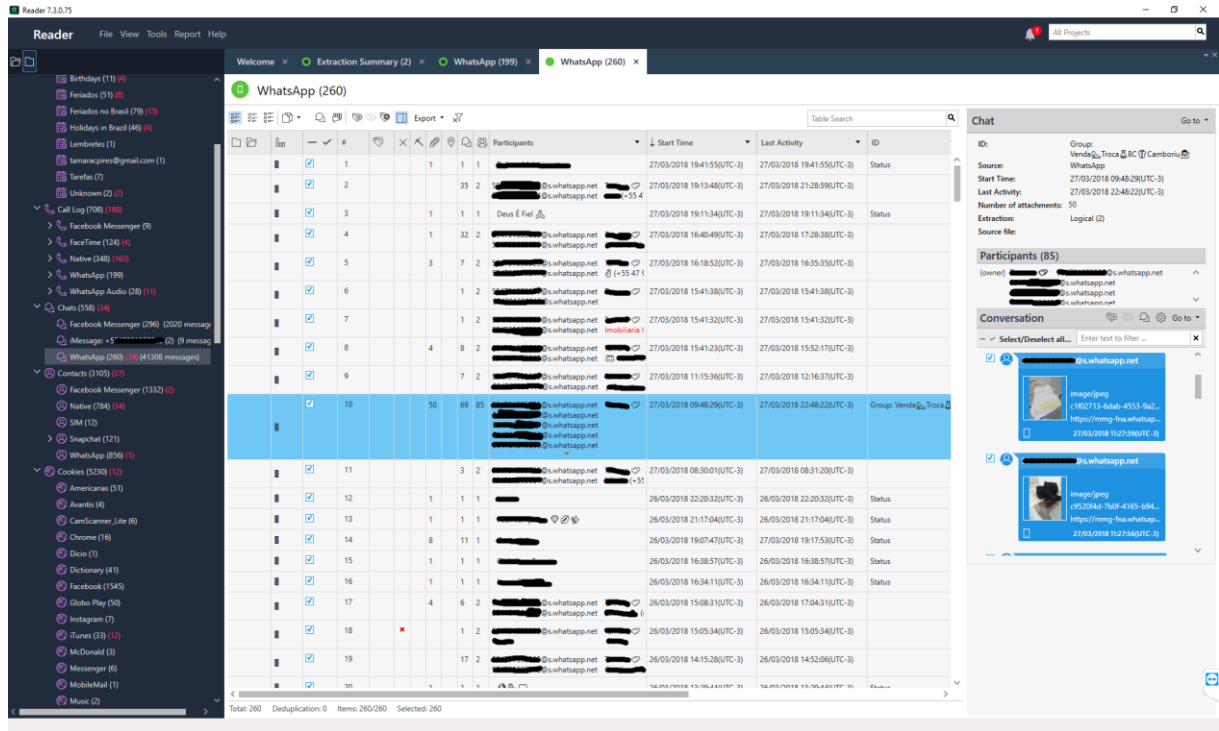


Figura 4 - Localizações e sua origem, na seleção uma imagem e suas coordenadas

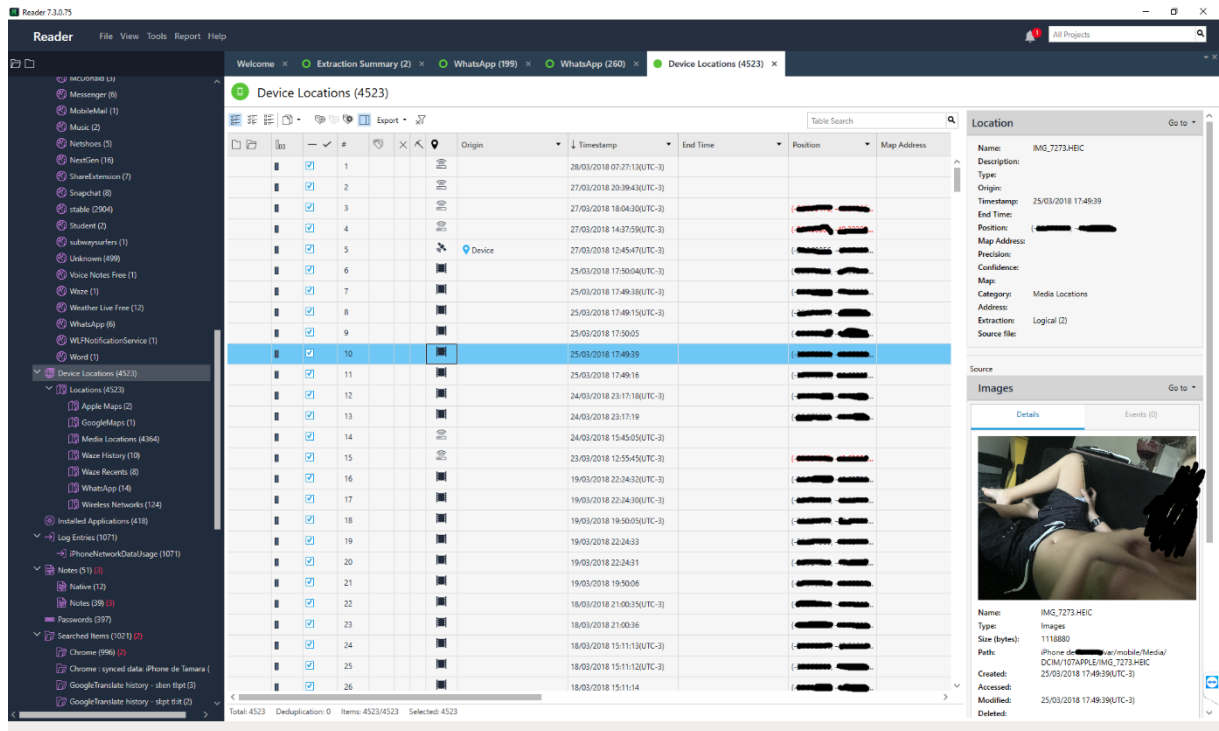


Figura 5 - Imagens encontradas e visualização estendida da seleção

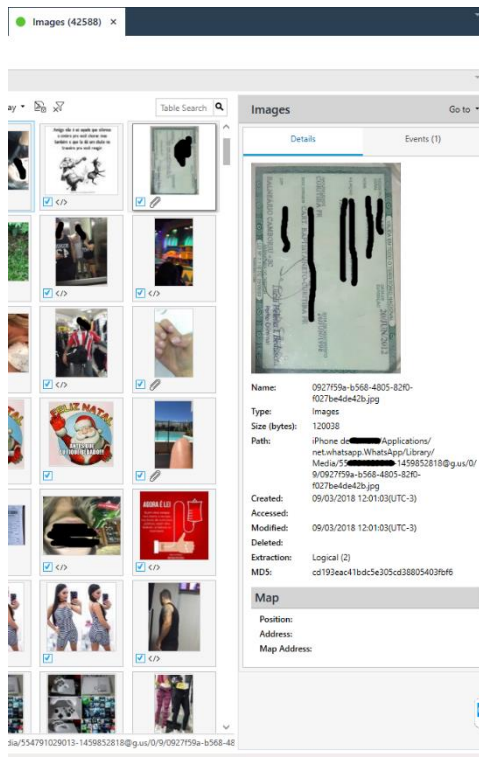
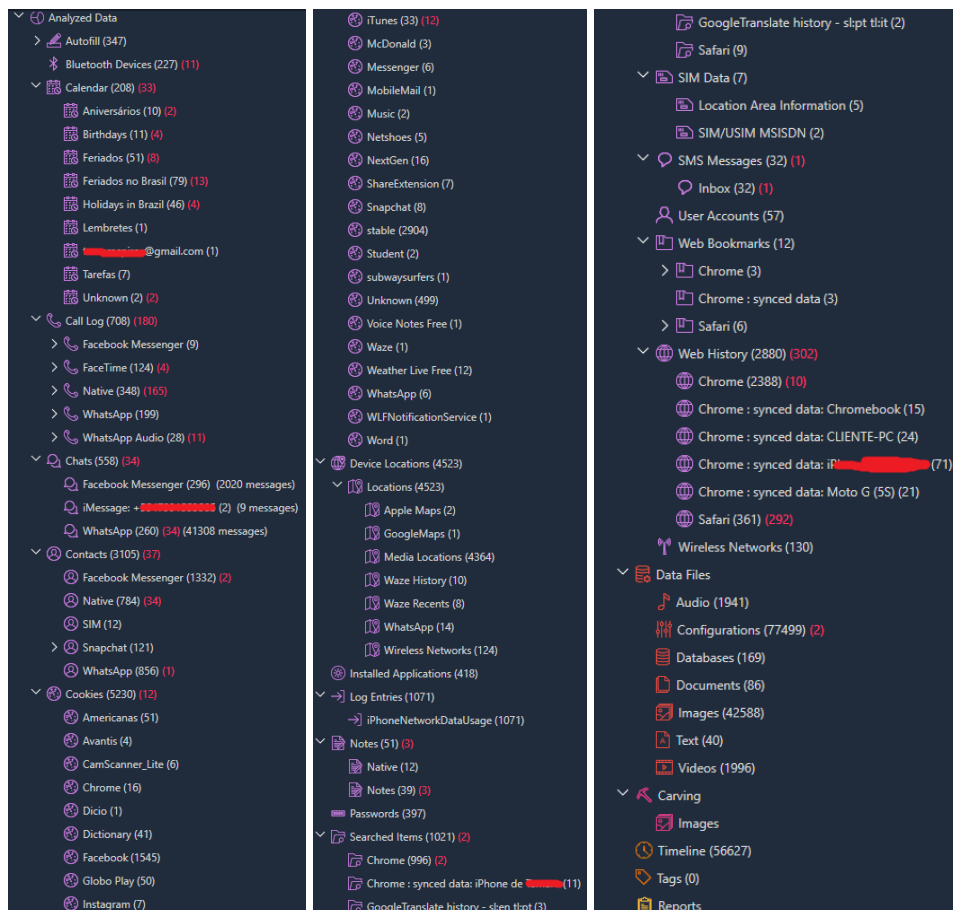


Figura 6 - Lista de informações encontradas



Fonte: Figuras de 1 a 6 elaboradas pelo autor

Se olharmos o montante de informações compiladas em um relatório, de um único dispositivo (Figura 1 a 6), não classificarei como impossível, mas impraticável reproduzir de punho em acesso manual tal compêndio de dados.

Trata-se daquele fluxo onde dados crus são organizados de forma a trazer uma informação de forma rápida e coerente, se possível já com certo conhecimento embutido.

Figura 7 - Classes de informação



Fonte: lilianasoes.wordpress.com (2012).

Se olharmos a Figura 6, veremos que a ferramenta faz um demorado processamento dos dados encontrados, de forma a separar, inclusive visualmente, os tipos de informações geradas. Fornece relatórios baseado em análises cruzadas das informações obtidas, como podemos observar nas Figuras 3, 4 e 5 e vai além, gera uma análise temporal de como todas estas aconteceram, uma *timeline* de informações. E tudo isso pode ser acrescido de marcadores e relatórios pelos peritos e pela equipe de análise.

4 REMOÇÃO DE DADOS - ESTUDO DE CASOS: ACUSAÇÃO, DEFESA E DECISÕES

Neste capítulo, traremos casos concretos onde decisões judiciais, cujos motivos serão devidamente analisados, determinaram a remoção ou manutenção, parcial ou total, de conteúdo extraído de dispositivos eletrônicos portáteis, como telefones celulares e *tablets*.

Cotejaremos os argumentos pela manutenção, em geral advindos das forças policiais e do Ministério Público, frente às ilações dos advogados e da Defensoria Pública. Analisando por fim se a decisão do(s) magistrado(s) foram coerentes com a situação fática apresentadas nos autos.

Como parte mais importante desta pesquisa, analisaremos se os fundamentos e afirmações de todos os atores envolvidos estão alinhados aos conceitos e normas esmiuçados nos capítulos anteriores. Visando validar a hipótese de que o direito à privacidade dos investigados está sendo violado no âmbito das investigações.

4.1 CASO SC: (DES)NECESSIDADE DE AUTORIZAÇÃO

Este é um caso onde a origem se deu, conforme decisão contida no Texto 2, a partir da realização de exame pericial e consequente emissão de laudo em 16 de janeiro de 2015, sem que a autoridade policial houvesse solicitado autorização judicial.

Em 04 de fevereiro de 2015, o delegado despacha nos autos, cujo teor é citado pelo magistrado no Texto 2 e encontra-se na íntegra no Anexo A, e em 1º de abril de 2015 encaminha ao MP cópia da mídia do laudo para análise e manifestação, conforme o Texto 1.

Texto 1 – Caso 1: Delegado encaminha mídia ao MP

Ofício n.º [REDACTED] 2015 - RE [REDACTED] /2015-4 DPF/DCQ/SC

Dionísio Cerqueira/SC, 01 de abril de 2015.

A SUA EXCELÊNCIA O SENHOR
PROCURADOR DA REPÚBLICA
SÃO MIGUEL DO OESTE - SC

Assunto: Encaminha documento (mídia - CD)
E-PROC: [REDACTED]

Senhor Procurador da República,

Visando instruir os autos da Representação pela Quebra de Sigilo Telefônico (Processo [REDACTED]), em cumprimento à Decisão Judicial, encaminho a Vossa Excelência cópia da mídia (CD) acostada às fls. 105 do processo [REDACTED] para fins de análise e manifestação.

Em 24 de abril de 2015 o Ministério Público se manifesta sobre pedido de quebra de sigilo de vários números e IMEIs de telefones móveis (Anexo B), dando como motivação os desdobramentos do flagrante:

A medida é desdobramento do acesso à agenda do telefone celular encontrado com os indiciados XXXXXXXX e XXXXXXXX, na oportunidade de suas prisões em flagrante por contrabando, quando transportavam, aproximadamente, 75 mil pacotes de cigarros em um caminhão. O resultado da análise pericial dos celulares levou à identificação dos números e IMEIs acima apontados, conforme Laudo n. 046/2015 - SETEC/SR/DPF/SC (fl. 103), complementado pela mídia encaminhada diretamente ao MPF por meio do Ofício n. 0XXX/2015/DPF/DCQ/SC.

Pelo desenrolar dos autos, aparentemente, o juiz ao receber o relatório do inquérito e com a manifestação favorável do *Parquet*, percebeu a falta da quebra de sigilo telefônico e de dados, argumenta que o delegado afirmou serem os exames realizados “com a devida autorização judicial”, repassando a seguir quais informações que considerou pertinentes como prova.

O juiz então citou a inexistência de autorização para acesso ao conteúdo da memória do aparelho celular, intimando o delegado para que esclarecesse o fato.

Os esclarecimentos foram prestados no Anexo C, onde foi assumido o equívoco na afirmação da preexistência de autorização, mas que, alegadamente, um primeiro delegado, provavelmente no momento do flagrante, encaminhou os aparelhos de telefonia celular para exames, entendendo desnecessária a existência de prévia autorização judicial (Texto 2).

Ainda no Texto 2, o delegado consigna pela existência de divergência jurisprudencial e doutrinária sobre o assunto e pede a retificação da representação pela não existência da autorização prévia, mas representa para que, mesmo que a *posteriori*, seja autorizado o acesso ao conteúdo dos aparelhos de telefone celular apreendidos nos autos e consequente autorização para o uso do laudo já encaminhado.

O Ministério Público em sua manifestação (Anexo D), reforçou pela não necessidade de prévia autorização, deferindo integralmente os pedidos da autoridade policial, colocando a grandeza da apreensão e do esquema envolvido, bem como suas cifras. Asseverou da necessidade em encontrar os demais envolvidos e que para tanto, se faziam necessárias as referidas quebras de sigilo.

Depois o Ministério Público afirmou que a perícia realizada não estaria violando o direito constitucional do sigilo (art. 5º, inciso XII da CF), em razão de que a indisponível reserva de jurisdição se refere à comunicação de dados, e não propriamente dos dados obtidos diretamente do aparelho. E encerra afirmando desnecessário “pleitear-se autorização judicial para acesso daquilo que já foi acessado”.

Fazendo uma comparação entre o que foi alegado no corpo do processo com o discutido nos capítulos anteriores, o primeiro delegado solicitou exames em um aparelho de celular, no intuito de correlacionar os suspeitos presos em flagrante através das ligações e mensagens. Sem entanto solicitar o afastamento do sigilo telefônico, visto a jurisprudência entender que o acesso aos registros de ligações encontrados em um telefone não enseja a quebra do sigilo do conteúdo das ligações.

O procurador no anexo D, considera que os dados encontrados no celular, não estão protegidos pelo artigo 5º, inciso XII, por de fato não ser uma interceptação de dados. Em

seguida também desclassifica o ato como uma interceptação telefônica, visto as conversas em si não terem tido seus conteúdos analisados. Finaliza com o entendimento de que a análise dos registros telefônicos contidos no celular não configura quebra do sigilo telefônico, diante da possibilidade de nele serem encontradas provas relacionadas ao fato.

A quebra em si não nasce da correlação ou possibilidade de se encontrar prova de crime, acredito que melhor seria a tese de que em dada circunstância, devidamente motivada por uma situação extrema, como uma chance única, ou pelo princípio da oportunidade, mas nunca pelo simples fato de se achar a prova no celular.

O magistrado deu razão ao MP, no que este trabalho entende como acesso a registros e metadados armazenados, ou seja, a agenda do celular, seu número, registros de chamadas e mensagens, sem que o conteúdo destas duas últimas seja violado.

Em seguida apontou que o acesso ao conteúdo das mensagens instantâneas de alguns aplicativos, violou o sigilo de correspondência e de comunicações e que deveriam ser precedidos de autorização judicial, portanto, provas ilícitas e que deveriam ser desentranhadas do processo.

Interessante perceber a dificuldade de se dar nome aos objetos assegurados pelo sigilo. Para o magistrado seriam correspondências e comunicações, mas a correspondência é uma forma de comunicação. Seria então uma correspondência que trafegou por comunicação eletrônica? A resposta está no Marco Civil da Internet em seu art. 7º, que elenca como sendo direito do usuário: “III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial”.

Percebe-se que tanto a acusação quanto o magistrado usaram de julgados anteriores ao Marco Civil da Internet, o que demonstra a dificuldade enfrentada em se adotar uma lei como jurisprudência pacífica no Brasil o que foi identificado pelo STJ, que em 17 de junho de 2018, publicou um levantamento, já citado na seção 2.4.

Texto 2 - Caso 1: Remoção parcial, necessidade de autorização

DESPACHO/DECISÃO

O Delegado de Polícia Federal em Dionísio Cerqueira/SC representou pela a quebra de sigilo de registros/dados relativamente aos terminais de telefônicos e IMEIs por ele indicados no evento 1, obtidos a partir da análise da perícia realizada nos aparelhos de telefone celular apreendidos por ocasião da prisão em flagrante de [REDACTED], ocorrida em 29/01/2014 (inquérito policial nº [REDACTED] - IPL: [REDACTED]).

Segundo a autoridade policial, o exame pericial realizado com "a devida autorização judicial" forneceu as informações a seguir transcritas, consideradas relevantes:

[...]

a) em relação aos aparelhos de telefone celular apreendidos com [REDACTED]

- BlackBerry 9220 Curve - utilizava o número [REDACTED], operadora VIVO. Percebeu-se que a última ligação telefônica teria, em tese, ocorrido no dia 23/01/2014. Quanto ao conteúdo restante, não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado.

- BlackBerry 9220 Curve Branco - utilizava o IMEI [REDACTED]. Não foi identificado o número de telefone que era utilizado, somente sabendo-se que era da operadora VIVO. Sem outros dados.

- Nokia, modelo 1616, IMEI [REDACTED], operadora TIM, não foi identificado o número de telefone utilizado. Cite-se a existência de diversas ligações, em dias próximos à prisão em flagrante, para os números de telefone [REDACTED]. Quanto ao conteúdo restante, não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado.

b) em relação ao aparelho de telefone celular apreendido com [REDACTED] trata-se do SAMSUNG GT S7560, contendo cartão SIM da operadora TIM. Pelo teor das conversas do investigado, percebe-se que o número por ele utilizado seria o [REDACTED] (operadora TIM), mas, conforme por ele mesmo referido em diversas conversas via mensagens, também poderia ser encontrado nos números [REDACTED] (operadora TIM) e [REDACTED] (operadora VIVO). Percebe-se a existência de centenas de conversas em aplicativos (Facebook e WhatsApp), entretanto não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado. Destaca-se que, em dias próximos à prisão em flagrante, constam diversas ligações para o número de telefone [REDACTED].

[...]

Constatada a inexistência de decisão judicial autorizando o acesso ao conteúdo da memória dos telefones celulares apreendidos (evento 18), determinou-se a intimação da autoridade policial para adequar o pedido formulado na representação (evento 19).

Intimada, a autoridade policial se manifestou no evento 24, esclarecendo que houve equívoco na representação juntada no evento 1, ao fazer menção a uma decisão judicial anterior autorizando o acesso ao conteúdo dos aparelhos de telefone celular apreendidos, e que a ausência de tal decisão decorreu de entendimento da autoridade policial que a antecedeu, no sentido da desnecessidade de autorização judicial para tanto. Retificou, dessa forma, os termos da representação juntada no evento 1, *"pois a perícia nos aparelhos de telefone celular ocorreu sem prévia decisão judicial"*, bem como requereu autorização, *"mesmo que a posteriori"*, para acesso ao conteúdo dos aparelhos de telefone celular apreendidos, autorizando-se a utilização do Laudo nº 046/2015-SETEC/SR/DPF/SC.

O Ministério Público Federal se manifestou favoravelmente ao pleito da autoridade policial, ao argumento de que *"a perícia realizada pela Polícia Federal nos celulares em razão da apreensão destes não se mostra violadora do direito constitucional ao sigilo (art. 5º, inciso XII das CF), em razão de que a indisponível reserva de jurisdição se irradia à comunicação de dados (v.g., interceptação telefônica), e não propriamente dos dados obtidos na base física apreendida pelos meios legais (v.g., apreensão de objetos – corpus delicti)"*. Ressaltou, ademais, que, apesar da praxe de requerer autorização judicial para o acesso aos dados contidos na memória de celulares apreendidos, no caso concreto, em que já foi juntado aos autos laudo pericial contendo os registros de ligações e mensagens de texto enviadas e recebidas, mostra-se desnecessário *"pleitear-se autorização judicial para acesso daquilo que já foi acessado"*.

Vieram os autos conclusos para decisão.

Com razão a manifestação do Ministério Público Federal no tocante à desnecessidade de prévia autorização judicial para acesso à memória de telefones legalmente apreendidos em poder dos flagrados, visando a obtenção dos registros das ligações e mensagens de texto efetuadas e recebidas, bem como números de telefones de contatos existentes nas agendas dos aparelhos.

De fato, tal procedimento não caracteriza ofensa ao sigilo de comunicação telefônica protegido pela Constituição Federal e regulamentado pela Lei 9.296/96, porquanto não há acesso ao conteúdo das conversas telefônicas realizadas, mas apenas verificação de registro gravado no próprio aparelho.

Conforme destacado em um dos julgados colacionados pelo Ministério Público Federal em seu parecer, *"[o] fato de ter sido verificado o registro das últimas chamadas efetuadas e recebidas pelos dois celulares apreendidos em poder do co-réu, cujos registros se encontravam gravados nos próprios aparelhos, não configura quebra do sigilo telefônico, pois não houve requerimento à empresa responsável pelas linhas telefônicas, no tocante à lista geral das chamadas originadas e recebidas, tampouco conhecimento do conteúdo das conversas efetuadas por meio destas linhas. [...]"*. (STJ, HC Nº 66.368 - PA / 2006/0201607-4, Relator: Ministro GILSON DIPP, Data de Julgamento: 05/06/2007, T5 - QUINTA TURMA).

No mesmo sentido:

EMENTA: PENAL. TENTATIVA DE ESTELIONATO. ART. 171 C/C ART. 14, II DO CP. ALEGAÇÃO DE TORTURA NA ESFERA POLICIAL. VIOLAÇÃO DE SIGILO TELEFÔNICO. INOCORRÊNCIA. MATERIALIDADE E AUTORIA. DOLO. VANTAGEM ILÍCITA NÃO OBTIDA POR CIRCUNSTÂNCIAS ALHEIAS À VONTADE DOS AGENTES. QUADRILHA OU BANDO. ART. 288 DO CP. CARACTERIZAÇÃO. [...] 2. A simples verificação dos números das últimas chamadas feitas e recebidas constantes na memória do telefone celular não significa, por si só, violação ao sigilo telefônico desde que a apreensão do aparelho seja legítima. A garantia constitucional da inviolabilidade das comunicações telefônicas se refere à vedação de escutas clandestinas, a qual não se configura com a simples checagem dos últimos números registrados na memória do aparelho, ainda que esta seja realizada por outra pessoa que não o proprietário. [...]. (TRF4, ACR 2002.04.01.029123-1, Sétima Turma, Relator Fábio Bittencourt da Rosa, DJ 21/05/2003)

Tendo isso em vista, não há dúvida quanto à higidez das provas obtidas a partir do acesso aos registros gravados nos telefones celulares BlackBerry 9220 Curve, BlackBerry Curve Branco e Nokia 1616, apreendidos em poder de [REDACTED], bem como no SIM Card do telefone celular Samsung GT-ST560M, apreendido em poder de [REDACTED].

Entretanto, no tocante às provas obtidas a partir do acesso à memória do próprio celular Samsung GT-ST560M, a situação é mais complexa, porquanto, segundo se verifica do conteúdo da pasta nomeada como "Samsung GSM_GT-S7560M", gravada na mídia que acompanha o Laudo Pericial nº 46/2015 - SETEC/SR/DPF/SC (evento 84 - INQ1, p. 7-10 do IP), houve acesso ao conteúdo de mensagens instantâneas entre o investigado [REDACTED] e terceiros, por meio dos aplicativos 'Facebook', 'Facebook Messenger' e 'Whatsapp'.

Como consectário lógico do princípio constitucional da não violação de correspondências e das comunicações, cujo objetivo é a proteção da privacidade e da intimidade das pessoas, evidente que, em se tratando de mensagens privadas trocadas pelos usuários dos referidos aplicativos, os respectivos conteúdos somente podem servir como prova se obtidos mediante prévia autorização judicial.

Conclui-se, dessa forma, que os números de telefone [REDACTED] e [REDACTED] foram obtidos com violação de correspondência e comunicações, já que extraídos de uma conversa do investigado [REDACTED] no 'Facebook Messenger', tratando-se, portanto, de prova ilícita, nos termos do art. 5º, LVI, da CF, e do art. 157 do CPP.

Ressalta-se que o vício que atinge a prova em questão possui caráter absoluto, não podendo ser sanado nem mesmo mediante autorização "a posteriori", como requerido pela autoridade policial, até porque, em assim agindo, estar-se-ia burlando o ordenamento jurídico.

Como o ordenamento pátrio não admite o emprego de provas ilícitas para instruir a persecução penal (CF, art. 5º, inc. LVI), em havendo a produção destas, devem ser desentranhadas do processo (CPP, art. 157). No caso concreto, devem ser excluídos do inquérito policial todos os arquivos relativos às conversas travadas por meio dos aplicativos 'Facebook', 'Facebook Messenger' e 'Whatsapp', extraídos do aparelho de telefone celular Samsung GT-S7560M, apreendido em poder de [REDACTED].

Registre-se, ademais, que, de acordo com o §1º, do art. 157 do CPP, que positivou a jurisprudência solidificada (STF, HC 82.788/RJ; HC 87.907/RJ; RHC 90.376/RJ; HC 93.050/RJ, e.g.), o mesmo destino merecem as provas derivadas das ilícitas, em aplicação da teoria cunhada pela Suprema Corte Norte-Americana dos frutos da árvore envenenada (*fruits of the poisonous tree*). Isso significa que devem ser descartados também os meios probatórios que, embora produzidos validamente em momento posterior, acham-se contaminados pelo grave vício da ilicitude originária. Tal conclusão torna patente a inviabilidade da medida pleiteada na representação do evento 1, relativamente aos telefone números [REDACTED] e [REDACTED] porquanto o resultado estaria eivado de nulidade.

A única forma de viabilizar a utilização dos referidos números de telefone seria a demonstração de possibilidade de obtenção da informação por outro meio, sem nenhuma relação com as mensagens privadas mantidas pelo investigado, conforme autoriza o §1º, segunda parte, c.c. o §2º, ambos do art. 157 do CPP. Situação que, ao menos por ora, não se vislumbra nos autos.

Diverso é o caso do telefone número ([REDACTED]) que, segundo afirmado pela autoridade policial na representação do evento 1, "[p]elo teor das conversas do investigado" seria o número do aparelho de telefone celular apreendido com [REDACTED]. Tendo em vista que o número em questão foi informado pelo próprio flagrado por ocasião do seu interrogatório policial (evento evento 1 - INQ1, p. 5, do inquérito policial nº [REDACTED] - IPL: [REDACTED] DPF/DCQ/SC), é perfeitamente admissível a utilização dessa informação como prova válida.

Ultrapassada a questão da licitude das provas obtidas com o acesso à memória dos celulares apreendidos no inquérito policial nº [REDACTED] [REDACTED] - IPL: [REDACTED]/SC, passa-se à análise do pedido de quebra do sigilo telefônico dos titulares dos terminais telefônicos cujos dados foram obtidos por meio lícito.

Nesse sentido, considerando as informações prestadas pela autoridade policial e os elementos existentes nos autos do inquérito policial até o momento, conclui-se que as diligências pretendidas pela autoridade policial são necessárias e têm potencial utilidade para instruir esta etapa da persecução criminal.

As medidas pleiteadas não se afiguram despropositadas, pelo contrário, mostram-se adequadas, até mesmo imprescindíveis ao fim que se busca, que é a possível descoberta da identidade de todos aqueles relacionados com a prática do delito em apuração, mesmo porque não se tem, ao menos nesse momento da investigação, outros caminhos para se apurar a existência e se chegar à identificação de possíveis coautores do crime de contrabando investigado no IPL nº [REDACTED]/SC.

Na espécie, a privacidade, direito fundamental do indivíduo - mas não absoluto - deve ceder, frente ao interesse público que se impõe na apuração do fato criminoso.

Anote-se, ademais, que a obtenção dos dados cadastrais e históricos de chamadas relativos aos telefones indicados pela autoridade policial também tem utilidade como meio de evidenciar que os seus respectivos titulares não têm participação na possível conduta criminosa.

Ante o exposto, e considerando o parecer favorável do Ministério Público Federal, defiro em parte os requerimentos formulados pela autoridade policial para o fim de:

1) decretar a quebra do sigilo telefônico dos titulares dos terminais telefônicos de números [REDACTED] (operadora TIM), [REDACTED] (operadora [...])

Ressalta-se, por fim, que deverão ser observadas as cautelas pertinentes para preservação do sigilo das informações, as quais deverão ficar adstritas ao inquérito policial em que solicitado tal acesso.

Preclusa a decisão de desentranhamento da prova considerada ilícita, determino, desde já, a exclusão dos arquivos correspondentes. A medida deve ser cumprida pela autoridade policial no inquérito policial nº [REDACTED]

[REDACTED] - IPL: [REDACTED]/SC, intimando-se as partes, para fins do art. 157, § 3º do CPP. A mídia enviada a esta Vara Federal deverá ser destruída, assim como eventuais cópias acauteladas em secretaria e no âmbito do Ministério Público Federal, mediante certidão/informação nos autos do IP. Efetivada a medida, deverá a autoridade policial encaminhar ao juízo nova mídia contendo os arquivos relativos ao Laudo Pericial nº 46/2015 - SETEC/SR/DPF/SC.

Intimem-se. Após, o feito deverá aguardar suspenso a conclusão das investigações. Concluídas estas, dê-se baixa definitiva.

4.2 CASO AC: ANULAÇÃO E NOVO LAUDO

A análise do próximo caso é de suma importância para este estudo, pois conforme decisão do Juiz Federal de 1ª Instância (Texto 3), as provas extraídas dos aparelhos celulares sem autorização foram consideradas ilícitas e conseqüentemente desentranhadas dos autos, mas aludiu que a apreensão dos celulares fora lícita e, portanto, agora com autorização, requereu novo exame nos mesmos.

Mas vamos aos fatos. O presente caso envolveu uma estrangeira, originária do Camboja, que adquiriu mais de 1kg de cocaína no Peru e adentrou território brasileiro com a substância. Sendo então presa em flagrante. Teve seus pertences devidamente apreendidos e encaminhados para exames, entretanto, sem pedido de afastamento do sigilo de dados dos dispositivos com ela apreendidos.

Tal ausência ensejou por entendimento de que os acessos às informações contidas nos dispositivos não possuem a proteção constitucional da privacidade, pois tais aparelhos de telefonia celular seriam tão somente ferramentas utilizadas para o crime em questão.

Ao se verificar o Auto de Apresentação e Apreensão, temos que com a investigada foram encontrados dois aparelhos celulares e quinze cartões SIM, de diversas operadoras, uma situação comum aos que compram cartões SIM (chip de celular) para usar e descartar, evitando ser rastreado.

Apesar da situação na qual foram encontrados, o Laudo que examinou os dispositivos e cartões SIM, foi considerado pelo juiz *a quo* como sendo prova ilícita e foi desentranhado dos autos do processo.

Em seqüência à decisão do magistrado, o Ministério Público, alegando que a apreensão dos itens elencados nos Autos se deu de forma lícita, restando questionado somente o acesso sem prévia autorização, solicitou que fossem realizados novos exames.

A defesa, insurgindo contra o pedido do *parquet*, trouxe que não poderiam ser convalidadas as provas já declaradas como ilícitas.

O juiz *a quo*, ordenou então a renovação dos exames, e acrescentou que de fato, a materialidade delitiva restava comprovada por Laudos que atestam que a substância de fato seria ilícita, e trazida do Peru para o Brasil, onde a suspeita foi presa em flagrante. Justificando como necessária a quebra do sigilo dos dados do celular para aprofundamento das investigações “a fim de que reste elucidada a possível participação de outros indivíduos na empreitada delitiva, a destinação da droga, dentre outras circunstâncias”.

DECISÃO

Postula o Ministério Público Federal, às fls. 175/175v, a realização de prova outrora já produzida nos autos – consistente na colheita de dados constantes do aparelho celular apreendido em poder da acusada SREYLEAP TAN –, cuja nulidade foi oportunamente reconhecida em decisão proferida por este Juízo às fls. 166/168, ocasião em que se determinou o desentranhamento do respectivo laudo pericial.

2. Instada a se manifestar, a defesa da ré se insurgiu contra o pleito, sustentando, em suma, que a ilicitude da prova não pode ser convalidada.

3. Decido.

4. No caso, reputo que o intento da acusação de extração dos dados do aparelho telefônico apreendido nos autos não encontra óbice frente ao reconhecimento de ilicitude do laudo pericial anteriormente produzido. Isto porque, como restou claro na decisão suprarreferenciada, o vício inquinado circunscreve-se tão somente ao laudo pericial outrora produzido pela Polícia Federal e já desentranhado dos autos, na medida em que **o procedimento adotado** nas investigações demandava a obtenção de prévia autorização judicial para viabilizar a devassa dos dados do aparelho celular apreendido com a flagranteada ora acusada. Tratava-se, portanto, de prova ilegítima, tendo em vista a ocorrência de violação de normas de caráter processual, sendo que o seu expurgo não prejudica, se possível, a realização de prova idêntica – observadas as normas processuais pertinentes.

5. Com efeito, verifico que a apreensão do aparelho celular se deu de forma idônea, na esteira do que preceitua o artigo 6º, incisos II e III do Código de Processo Penal, sendo que a permanência de seu acautelamento remanesce imaculada, alheia ao vício outrora reconhecido por este Juízo. Assim, a pretensão ministerial de acesso aos dados constantes do telefone se revela possível, notadamente por se tratar de prova repetível. Neste sentido, já entendeu o Superior Tribunal de Justiça no bojo da Reclamação n. 32.311/RO que a decisão judicial proferida ao longo de instrução criminal que determina a realização de nova perícia em aparelho celular apreendido está desvinculada de decisão judicial anterior, exarada pela Corte Superior, que tenha determinado o desentranhamento de laudo pericial reconhecidamente ilícito – por vícios análogos ao caso ora em apreço. Tal caso restou ementado nos seguintes moldes:

PENAL E PROCESSO PENAL. AGRAVO REGIMENTAL NA RECLAMAÇÃO. ATO ATACADO QUE NÃO CONSTITUÍ

DESCUMPRIMENTO. MERO REFAZER DO ATO QUESTIONADO. AGRAVO REGIMENTAL IMPROVIDO.

1. É assente nesta Corte Superior de Justiça que o agravo regimental deve trazer novos argumentos capazes de alterar o entendimento anteriormente firmado, sob pena de ser mantida a r. decisão vergastada pelos próprios fundamentos.

2. **Ao analisar o requerimento do Ministério Público, foi proferida nova decisão que examinou as teses e alegações ministeriais em que se pleiteava novo e diverso exame pericial no aparelho celular.**

3. **Nessa conduta do juiz de primeiro grau não se tem descumprimento, mas simples refazer do ato questionado.**

4. O novo ato decisório é independente, a merecer o específico exame e eventual enfrentamento recursal, sendo, por sua vez, vedado a essa Corte também a concessão de habeas corpus de ofício, sob pena de indevida supressão de instância.

5. Agravo Regimental improvido.

(STJ – Terceira Seção, AgRg na Rcl 32.311/RO, Rel. Min. Nefi Cordeiro, j. 14/9/2016, destaquei)

6. Não há que se alegar, portanto, que o reconhecimento da ilicitude do laudo pericial anterior findaria por inviabilizar novo exame dos dados constantes no aparelho celular ainda apreendido nos autos, já que o vício procedimental apurado terá sido expurgado dos autos após a observância do rito legalmente estabelecido.

7. Fixada tais premissas, entendo que a materialidade delitiva está devidamente comprovada – conforme já assinalado na decisão prolatada por ocasião da audiência de custódia (fls. 85/87) –, pois o Auto de Apresentação e Apreensão, o Laudo de Exame Preliminar de Constatação de Substância e o Laudo de Perícia em Química Forense (fls. 41/45) demonstram a apreensão de 1,103kg (um quilograma e cento e três gramas) de cocaína em posse de SREYLEAP TAN. De igual modo, os indícios de autoria decorrem tanto da apreensão do produto em posse da acusada como em razão dos depoimentos e interrogatório em sede policial (fls. 2/4).

8. Além disso, as circunstâncias envoltas à situação de flagrância – estrangeira natural do Camboja, adquirindo droga apreendida no país vizinho Peru, com subsequente ingresso em território brasileiro – constituem elementos indiciários suficientes a justificar o aprofundamento das investigações, a fim de que reste elucidada a possível participação de outros indivíduos na empreitada delitiva, a destinação da droga, dentre outras circunstâncias. Nesse sentido, a quebra do sigilo dos dados requerida é medida indispensável, inexistindo no momento outro meio de prova apto a elucidar o papel desenvolvido por outro(s) indivíduo(s) no transporte da droga apreendida.

9. Diante desses fatos e por não constituírem a intimidade e a privacidade das pessoas um direito absoluto, isento de sofrer restrições, quando presentes os requisitos do art. 5º, inciso XII, da Constituição Federal, o sigilo dos dados (tais como mensagens, arquivos, registros de ligações, etc) contidos no celular apreendido em posse da flagranteada deve ser afastado para melhor elucidar em que consistiu a participação deste envolvido nos fatos em apuração.

10. Com estas razões, AUTORIZO a quebra de sigilo de dados do

aparelho celular apreendido em posse de SREYLEAP TAN, propiciando o acesso ao conteúdo das mensagens, arquivos, ligações e demais registros ali contidos, conforme requerido pelo Ministério Público Federal.

11. Intimem-se. Ainda, notifique-se a autoridade policial responsável pelo inquérito policial, para que providencie a realização da prova supradeferida, inclusive com remessa do aparelho celular apreendido – acaso se encontre acautelado nesta Seccional.

12. Após, remanesça os autos em Secretaria, aguardando a devolução da Carta Precatória expedida à Comarca de Epitaciolândia/AC (item 15, fl. 168) para subsequente cumprimento do item 16 da decisão de fls. 166/168.

Rio Branco/AC, 29 de novembro de 2016.

Conforme podemos verificar no Texto 3, o juiz usou como jurisprudência a reclamação que versa sobre o caso que abordaremos na seção 4.3, onde em uma reviravolta jurídica, o juiz *a quo* ordenou o desentranhamento das provas declaradas ilícitas pelo STJ, mas analisou como lícita a apreensão dos celulares apreendidos e determinou nova extração dos dados armazenados nos dispositivos.

[...] No que se refere à convalidação da prova ilícita contrariando acórdão proferido por este Tribunal, anoto que, por ocasião do julgamento do habeas corpus n. 0003819-97.2016.822.0000, acompanhando o recente entendimento esposado pelo Superior Tribunal de Justiça (RHC 51531 RO 2014/022367-7), declarou-se a nulidade das provas obtidas, sem autorização judicial, obtidas no aplicativo de whatsapp dos celulares apreendidos, determinando-se, em consequência, o seu desentranhamento destas da ação penal.

Infere-se das decisões colacionadas (fls. 24/25 v.) que entendendo por repetíveis as provas desentranhadas, o juízo a quo determinou nova extração dos dados constantes nos aparelhos celulares apreendidos.

Anoto que não desconheço o posicionamento recente adotado pela 2ª Câmara Criminal deste Tribunal, o qual, em caso semelhante, à unanimidade, no dia 17/08/2016, denegou a ordem de habeas corpus, sob o n. 0003924-74.2016.822.0000, com fundamento de que tendo em vista a regular apreensão do aparelho celular, os seus dados e conversas, enquanto interessarem ao processo, serão mantidos nesta qualidade, podendo, desta forma, serem reexaminados, mediante autorização judicial, sem que isso configure ato ilícito.

Não obstante o alegado, conquanto lícita a apreensão dos celulares por ocasião da prisão em flagrante, entendo que a extração dos dados nele registrados, trata-se de violação de dados e comunicações, assemelhando-se a uma interceptação telefônica sem autorização judicial, o que viola direito protegido nos dispositivos das Leis 9.294/96, 9.472/97 e 12.965/14, conforme decidido por maioria na 1ª Câmara Criminal no aludido habeas corpus julgado em 4/8/2016.

Na hipótese apresentada, embora a apreensão dos aparelhos celulares seja lícita do ponto de vista formal, é certo que a autoridade policial não obteve a prévia e indispensável autorização judicial, o que configura a ilegalidade material das provas obtidas por este meio. Sobre o tema:

2. É direito constitucional do réu ter as provas obtidas por meios ilícitos expurgadas do processo a que responde, sendo igualmente inadmissíveis, nos termos do art. 157, § 1º, do Código de Processo Penal, as provas que derivam da prova ilícita, razão pela qual devem ter o mesmo destino. As provas derivadas apenas podem ser mantidas nos autos nos casos em que não ficar evidenciado o nexo de causalidade, ou seja, quando não se verificar a derivação, ou quando demonstrado que poderiam ser obtidas por uma fonte independente, cabendo ao Magistrado justificar (STJ - HC 301488/MT djE 06/09/2016).

A extração, gravação, impressão ou transcrição dos dados dos celulares apreendidos, mediante autorização posterior à declaração de nulidade, não têm o condão de legitimar as provas obtidas ilicitamente. Consigno por oportuno que em caso semelhante (RHC 51.531/RO), a Reclamação n. 32.311-RO (2016/0212282-6), interposta perante o STJ, com decisão publicada no DJe: 05/08/2016, julgou incabível o pedido de Reclamação por ausência de ato em descumprimento de decisão do Superior Tribunal de Justiça, **no entanto, não analisou o mérito ora discutido**. Naquele caso, o Rel. Min. Nefi Cordeiro consignou que o Juízo reclamado, ao tomar conhecimento do acórdão no RHC n. 51531, deu cumprimento a determinação da Corte e determinou o desentranhamento dos documentos declarados ilícitos; portanto, a nova decisão proferida em primeiro grau que autorizou a repetição das provas declaradas ilícitas, não se trata de descumprimento da decisão do STJ, **mas de refazimento do ato questionado**, circunstância que não merece enfrentamento pela Corte Superior por inadequação da via eleita, sendo vedado *in casu*, a concessão de habeas corpus de ofício, sob pena de configurar indevida supressão de instância.

Por outro lado, **o Recurso Ordinário interposto perante o Superior Tribunal de Justiça (RHC n. 77.371-RO 2016/0275566-6) que se refere ao HC acima (RHC 51.531/RO), não analisou o mérito recursal, apenas indeferiu o pedido liminar, tendo em vista o caráter perfunctório do juízo em medida liminar e, por considerar a pretensão de cassação da decisão interlocutória que determinou a realização de nova perícia no aparelho celular como claramente satisfativa, circunstância que obsta a concessão liminar e impõe um exame de mérito pelo colegiado, a fim de garantir a segurança jurídica processual.**

Destarte, divergindo do entendimento adotado pelo 2ª Câmara Criminal deste Tribunal, entendo que, inexistindo prévia autorização judicial, imperiosa é a declaração de nulidade da prova para que não surta efeitos na ação penal deflagrada em desfavor dos pacientes e demais corréus. Em caso semelhante esta 1ª Câmara Criminal, à unanimidade, concedeu a ordem de habeas corpus para determinar o desentranhamento de eventuais extrações, gravações, impressões ou transcrições de dados obtidos em celulares apreendidos,

mediante autorização posterior à declaração de nulidade. (TJRO HC 0003954-12.2016.822.0000, Relator Des. Valter de Oliveira, Julgamento 01/09/2016).

Assim, esta prova deve ser desentranhada do processo, bem como deve ser obstada a reprodução das provas já declaradas ilícitas. (TRIBUNAL DE JUSTIÇA DE RONDÔNIA, 2016)

Novamente uma batalha jurídica está sendo travada, agora no âmbito do Direito Processual Penal, visto que em outra decisão proferida pelo TJ/RO o Desembargador Relator teve seu voto vencido quando analisou o mérito da questão e chamou atenção para o fato de que a jurisprudência utilizada no caso ainda encontrava-se pendente de análise de mérito, visto o Recurso Ordinário ter sido indeferido por ser “claramente satisfativa, circunstância que obsta a concessão liminar e impõe um exame de mérito pelo colegiado”.

O voto vencedor trouxe que:

HABEAS CORPUS. PROCESSO PENAL. ASSOCIAÇÃO E TRÁFICO DE DROGAS. VIA ADEQUADA. REEXAME DE PROVA PERICIAL. APARELHO CELULAR. DADOS DO CELULAR E CONVERSAS DE WHATSAPP. NULIDADE ABSOLUTA (STJ). RHC N. 51.531. RENOVAÇÃO DO ATO PERMITIDO. PRECLUSÃO. IMPOSSIBILIDADE. ORDEM DENEGADA.

1. A decisão judicial que determina a realização de nova perícia, imprescindível para o deslinde dos fatos, torna-se ato capaz de ensejar, ainda que indiretamente, a constrição da liberdade do paciente (provisória ou permanente) e, nesta qualidade, será passível de análise na via estreita do habeas corpus.

2. Encontrando-se no plano da validade, a declaração de nulidade absoluta, mesmo tendo sido proferida por instância superior (STJ - RHC N. 51.531), não produz, em regra, efeitos na órbita jurídica, tampouco sanção capaz de impossibilitar a renovação do ato. 3. O aparelho celular regularmente apreendido, bem como o seu conteúdo (dados de celular e conversas de WhatsApp) enquanto interessarem ao processo serão mantidos nesta qualidade, podendo, desta forma, serem reexaminados, mediante fundamentação judicial idônea e sob o crivo do contraditório e da ampla defesa. Sem que isto configure ato ilícito.

4. O instituto da preclusão temporal não encontra amparo em matéria de nulidade absoluta (ordem pública).

5. Ordem denegada.

(Habeas Corpus, Processo nº 0003924-74.2016.822.0000, Tribunal de Justiça do Estado de Rondônia, 2ª Câmara Criminal, Relator (a) do Acórdão: Des. Valdeci Castellar Citon, Data de julgamento: 17/08/2016) (TRIBUNAL DE JUSTIÇA DE RONDÔNIA, 2016)

O principal fundamento deste voto, reside em que os celulares foram legalmente apreendidos e que continuavam legalmente em posse e à disposição. Tendo o juiz *a quo* apenas

renovado a prova, não se tratando, portanto, de convalidação da prova nula e sim renovação de prova repetível, agora licitamente autorizada.

4.3 CASO STJ 2016: RHC 51.531 - RO (2014/0232367-7)

O caso em questão, foi o primeiro a chegar ao STJ em Recurso de Habeas Corpus, visando a nulidade das provas colhidas no flagrante do réu. A defesa sustentou o seguinte:

[...] após a apreensão do aparelho celular, sem qualquer autorização, a polícia obrigatoriamente teria que ter oficiado do Juízo, com o conhecimento do MP, antes de proceder à devassa unilateral no conteúdo do aparato, que, necessariamente, teria que ser acompanhada pelo MP e especial pela Defesa, diante dos riscos naturais do desvirtuamento, acréscimo e exclusões do conteúdo a ser extraído. (fl. 84)

[...]

[...] a prova obtida sem requerimento ao Juiz natural (PERÍCIA DE, APARELHO CELULAR) que teve trâmite após a detenção do Paciente, portanto, perícia realizada em objeto já apreendido e sob a responsabilidade da Polícia, sem que para isso houvesse sido requerida a autorização judicial, com os conseqüentes fiscalizadores e asseguradores daí advindos viola os ditames do art. 5º, XII, da CF, sendo inadmissível a prova obtida de forma ilícita (art. 5º, LVI/CF), do mesmo modo disciplinando o art. 157, do CPP, razões essas, mais que suficientes para o desentranhamento das provas aqui mencionadas. (fl. 93)

Ao analisarmos a narrativa, temos que a prisão em flagrante se deu em 18/03/2014, portanto, temos que a própria defesa não se utilizou da recém editada Lei Nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet, preferindo citar o já combatido art. 5º, inciso XII, confundindo sua tese. Tendo então o remédio constitucional negado pelo Tribunal de Rondônia em 6/8/2014, com o seguinte acórdão:

Em breve narrativa fática, consta dos autos que o paciente foi preso no dia 18/03/2014, sob a acusação de praticar o delito de tráfico de entorpecentes e ainda associação para o tráfico.

A denúncia descreve que uma denúncia anônima informou que no dia em que foi preso o paciente receberia, via correios, uma carga de entorpecente.

Foi realizado acompanhamento pela polícia militar e tão logo a encomenda fora entregue realizaram a abordagem, logrando êxito em apreender na posse do paciente um recipiente contendo 300 (trezentos) comprimidos de ecstasy.

Investigações complementares demonstraram que o paciente se associou com os corréus com a finalidade específica de perpetrar o delito de tráfico de entorpecentes, cada um exercendo uma tarefa específica.

Em informações apresentadas às fls. 40/42 a autoridade impetrada afirmou que o aparelho de telefone celular foi apreendido com o paciente por ocasião de sua prisão em flagrante, apontando que a perícia realizada no aparelho tem fundamento no art. 6º, incs. II, III e VII do CPP.

Informou ainda que o acesso aos dados constantes do aparelho, no caso dos autos, não encontra o mesmo impedimento da interceptação telefônica e que a autoridade policial agiu estritamente para cumprimento da Lei.

A discussão apresentada pelo impetrante circunda a possibilidade de realização unilateral da perícia no aparelho de telefone celular apreendido quando da prisão em flagrante sem a alegada imprescindível autorização judicial.

Entendo que a tese apresentada pelo impetrante é desprovida de fundamento porquanto a proteção do acesso aos dados constantes do aparelho não se assemelha à interceptação telefônica.

Inicialmente relato que o **telefone celular foi apreendido no momento da prisão em flagrante do paciente, ocasião em que os policiais recolheram todos os instrumentos que poderiam estar relacionados ao crime**, incluindo este aparelho, encaminhando-o à autoridade policial competente.

Após a apreensão a autoridade policial conduziu a investigação conforme disposto no art. 6º do CPP, determinando a realização de perícia do entorpecente apreendido e ainda extração das conversações do aparelho celular do paciente.

Assim dispõe o referido texto legal:

Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

[...]

II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)

III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;

[...]

VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;

Nota-se que o legislador não atribuiu discricionariedade ao ato impugnado, pelo contrário, determina que a autoridade policial realize as ações descritas nos incisos do referido artigo.

Entendo não ser imprescindível a decisão judicial para realização de perícia em aparelho celular apreendido pois a lei permite até mesmo a violação de domicílio para efetuar prisão em flagrante.

Relato ainda que o Direito Penal e Processual Penal possuem natureza pública, geridos pelo Estado, representante das vontades e interesses da coletividade.

Cito este fato em razão do questionamento da atividade pericial realizada, e saliento que a perícia foi realizada por agentes oficiais do Estado, legalmente incumbidos da realização dos estudos realizados, recaindo sobre eles a necessidade de observação explícita dos princípios constitucionais da legalidade, moralidade, impessoalidade, dentre outros.

Apresentar meras ilações acerca da possibilidade de algum dos policiais prejudicar o paciente é demasiadamente pueril, até mesmo porque não demonstrou objetivamente tal condição, não sendo relatado em momento algum dos autos a preexistência de qualquer animosidade pretérita ao fato. (BRASIL, 2016, grifo nosso)

Percebe-se rapidamente a confusão sobre o tipo de sigilo que estaria ou não sendo violado, partindo o magistrado estadual para uma prova lógica por inversão, do tipo: “Se algo não é morcego, então não é mamífero”, alegou que o acesso aos dados armazenados no celular não se trata de interceptação telefônica e, portanto, não precisa de autorização judicial para ser executado.

E, conforme jurisprudência amplamente utilizada até hoje, considerou o aparelho como uma ferramenta utilizada no crime, o que indiretamente não deixa de ser verdade, e aplicou o CPP de 1941 que pelos incisos II, III e VII do Art. 6º permitiria os exames.

Em seu voto o ministro relator, mesmo após citar e grifar o art. 7º, inciso III do Marco Civil da Internet “**III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;**” também confunde o tipo de violação do caso em tela:

Nas conversas mantidas pelo programa WhatsApp, que é forma de comunicação escrita, imediata, entre interlocutores, tem-se efetiva **interceptação inautorizada de comunicações**. É situação similar às conversas mantidas por e-mail, onde para o acesso tem-se igualmente exigido a prévia ordem judicial. (BRASIL, 2016, grifo nosso)

Acertando na comparação com o e-mail, quando extraído do dispositivo questionado, como “comunicação privadas armazenada”, se o mesmo fosse obtido via ordem judicial a uma operadora de internet/provedora de e-mail, estaríamos falando do inciso II do mesmo artigo, que diz: “II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;”. Mas em ambos os casos existe a expressa necessidade de prévia ordem judicial.

E encerrou seu voto:

Atualmente, o celular deixou de ser apenas um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo, no caso, a verificação da **correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a**

comunicação por meio de troca de dados de forma similar à telefonia convencional.

Deste modo, ilícita é tanto a devassa de dados, como das conversas de WhatsApp obtidos de celular apreendido, porquanto realizada sem ordem judicial.

Ante o exposto, voto por dar provimento ao recurso ordinário em habeas corpus, para **declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.** (BRASIL, 2016, grifo nosso)

Ao analisar a contextualização do crime, encontramos um fato interessante para a discussão sobre os tipos de ações que podem ensejar na obtenção de provas, no caso saindo do mundo virtual e retornando ao nosso cotidiano, qual seja:

[...]

Em breve narrativa fática, consta dos autos que o paciente foi preso no dia 18/03/2014, sob a acusação de praticar o delito de tráfico de entorpecentes e ainda associação para o tráfico.

A denúncia descreve que uma denúncia anônima informou que no dia em que foi preso o paciente receberia, via correios, uma carga de entorpecente.

Foi realizado acompanhamento pela polícia militar e tão logo a encomenda fora entregue realizaram a abordagem, logrando êxito em apreender na posse do paciente um recipiente contendo 300 (trezentos) comprimidos de ecstasy.

Investigações complementares demonstraram que o paciente se associou com os corréus com a finalidade específica de perpetrar o delito de tráfico de entorpecentes, cada um exercendo uma tarefa específica.

Em informações apresentadas às fls. 40/42 a autoridade impetrada afirmou que o aparelho de telefone celular foi apreendido com o paciente por ocasião de sua prisão em flagrante, apontando que a perícia realizada no aparelho tem fundamento no art. 6º, incs. II, III e VII do CPP. (BRASIL, 2016)

Percebe-se que a ação escolhida pela Polícia Militar foi a da busca, visto ter optado por não interceptar nos correios a encomenda de ecstasy. Não vou tecer comentários sobre como a PM estaria recebendo uma denúncia anônima e realizando uma busca, acredito que até entrando na residência do suspeito sem um mandado de busca.

Atualmente, na Polícia Federal, recebe-se uma quantidade significativa de encomendas interceptadas devido à detecção de drogas em seu interior.

Mas retornando ao caso, a busca deveria ter sido precedida de autorização judicial, mas tal ação não seria aceita, visto a PM não ser a Polícia Judiciária. Esta ao receber a denúncia (que provavelmente veio dos correios) deveria ter acionado os demais *players* da persecução penal. A fim de que a formalidade da ação não fosse questionada, como de fato o foi.

Como já citado na seção 2.4, em determinado momento um dos ministros em seu voto-vista, afirmou que não desconhece o precedente até então utilizado pelo STF, mas que o mesmo já se encontrava superado, em virtude dos fatos narrados serem de uma época em que os celulares, basicamente, apenas serviam para realiza ligações, conforme podemos ver no Gráfico 4, que se encontra na página 28 deste trabalho.

Como também já citado na seção 2.4, o ministro passa a analisar o direito ora pleiteado sob a perspectiva de um direito probatório de terceira geração, no qual estão as "provas invasivas, altamente tecnológicas, que permitem alcançar conhecimentos e resultados inatingíveis pelos sentidos e pelas técnicas tradicionais". O que, conforme análise na seção 3.3, na página 39, é um arcabouço de dados, informações e conhecimento gerado sobre o réu que torna a prova praticamente intransponível para a defesa.

4.4 CASO STJ 2017: RHC 89.981 - MG (2017/0250966-3)

Esse RHC consta na jurisprudência apresentada pelo STJ recentemente, mas já na ementa erros conceituais saltam aos olhos. Afirma o acórdão que “[...] a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 **nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação telefônica [...]**” (BRASIL, 2017, grifo nosso).

Partindo da análise da peça em sua origem, vemos que a Corte local denegou o pleiteado remédio com a seguinte ementa:

EMENTA: *HABEAS CORPUS* - CRIME DE FURTO QUALIFICADO - ASSOCIAÇÃO CRIMINOSA - NULIDADE POR ILEGALIDADE E ILICITUDE DAS PROVAS PRODUZIDAS - AUSÊNCIA DE CONSTRANGIMENTO ILEGAL EVIDENTE - ORDEM DENEGADA.

- O habeas corpus não se presta ao exame aprofundado de questões meritórias, a não ser que se verifique patente constrangimento ilegal, o que não ocorre *in casu*.
- Diante da ausência de manifesto constrangimento ilegal, sanável de ofício, denega-se a ordem.
- Ordem denegada (BRASIL, 2017)

Foi a questão assim decidida no Tribunal de origem:

Analisando os argumentos despendidos no presente writ, verifica-se que a impetração alega suposto constrangimento ilegal tendo em vista que **"os Policiais Militares realizaram devassa no aparelho de telefonia celular de um corréu sem autorização judicial para tanto"**.

Pretendem a concessão da presente ordem para declarar a nulidade das provas colhidas nos autos.

Contudo, o presente writ, tecnicamente, não é o instrumento adequado para valoração do mérito da própria ação penal, por exigir exame aprofundado da prova, a não ser diante da possibilidade de lesão ou ameaça de lesão à liberdade ambulatorial do paciente, nos termos do art. 50, LXVIII da Constituição Federal, o que não se vislumbra no presente caso.

Além disso, conforme se observa da decisão de fls.09/11- TJ, a tese de nulidade foi arguida na resposta à acusação e rechaçada pelo magistrado *a quo*, senão vejamos:

"(...) Outrossim, infundada a tese de nulidade da prova obtida através do acesso imediato ao aplicativo mensageiro WhatsApp do aparelho celular dos denunciados sem autorização judicial.

Isto porque, não obstante a privacidade, intimidade e o sigilo das comunicações telefônicas encontrem-se constitucionalmente assegurados (art. 5º, X e XII, da CF/88), **o acesso aos dados constantes em aparelho celular regularmente apreendido pelos policiais na sequência de uma prisão em flagrante caracteriza-se hipótese de exame em instrumento utilizado na prática de crime**, constituindo corpo de delito, sendo legítima sua apreensão e análise, a fim de constatar os vestígios da infração. Aliás, o Código de Processo Penal, em seu art. 6º, determina a apreensão imediata de todos os objetos que tenham relação com o fato, bem como de todas as provas que servirem ao seu esclarecimento. E dever do agente proceder de tal modo, o que, no caso dos celulares, significa extrair os dados neles constantes, independentemente de autorização judicial, a fim de saber se possuem alguma relação com a ocorrência investigada.

Além disso, há evidente elemento de urgência no acesso aos aparelhos, já que a demora decorrente da obtenção de um mandado judicial pode trazer prejuízos concretos à investigação, notadamente pela possibilidade de que, em poucos segundos, todos os dados constantes do dispositivo sejam apagados remotamente por qualquer pessoa com acesso à conta do titular. Assim, exigir que o aparelho celular seja primeiramente apreendido, e apenas posteriormente requerida e obtida judicialmente a quebra do sigilo do conteúdo nele armazenado, resultaria na inutilidade da diligência, **porque certamente os dados não mais existirão.**

Registra-se, ademais, que **não se tratou propriamente de devassa aos dados constantes dos aparelhos apreendidos, já que somente o aplicativo mensageiro WhatsApp foi examinado.** Situação diversa seria o exame aprofundado de outras funções do aparelho, como a tentativa de recuperação de mensagens já apagadas, o acesso à localização para descobrir os últimos locais frequentados etc, que poderiam justificar eventual necessidade de autorização judicial.

Destarte, tratando-se de prisão em flagrante que seguiu o delineado pelo Art. 304 e seguintes do CPP, inexistindo qualquer irregularidade, **bem como constatado que o acesso aos dados do aparelho celular foi realizado imediatamente após o flagrante, para servir efetivamente aos propósitos da persecução penal**, visando especialmente **preservar os elementos probatórios**, inexistência a ser declarada, afigurando-se lícitas as provas colhidas, (...)"

[...]

Assim, ausente manifesto constrangimento ilegal sanável de ofício,

DENEGO A ORDEM. (BRASIL, 2017, grifo nosso)

Vamos analisar a decisão primeira, do juiz a quo, que inicia afirmando o celular ser ferramenta utilizada para a prática de crime por um corréu, e que a partir dessa prova o paciente foi inserido como partícipe da ação delituosa.

Passou então a defender a urgência de uma análise dos vestígios pelos policiais pela seguinte razão: “já que a demora decorrente da obtenção de um mandado judicial pode trazer prejuízos concretos à investigação, notadamente pela possibilidade de que, em poucos segundos, todos os dados constantes do dispositivo sejam apagados remotamente por qualquer pessoa com acesso à conta do titular”, não querendo advogar sobre tal ilação, mas esta foge verticalmente da realidade, visto bastar apenas que os telefones fossem desligados, ou já que tinham acesso ao seu conteúdo, colocados em modo *off-line*/avião e então estariam seguros contra um possível acesso remoto. Portanto se esta era o único motivo de urgência, não merecia acolhimento.

Na sequência argumentou que “não se tratou propriamente de devassa aos dados constantes dos aparelhos apreendidos, já que somente o aplicativo mensageiro WhatsApp foi examinado”, tal argumento se mostra difícil de defender, dado ao atual uso do aplicativo citado, que ensejou até ações pelas operadoras de telefonia, que alegam que esta ferramenta implicou em reduções expressivas de seus serviços de voz e mensagens SMS.

Acredito que o único bom argumento e que não foi devidamente fundamentado, foi “bem como constatado que o acesso aos dados do aparelho celular foi realizado imediatamente após o flagrante, para servir efetivamente aos propósitos da persecução penal”, tal afirmação poderia trazer elementos reais, como o momento do acesso e o que foi extraído e por quais motivos reais, não poderiam aguardar pela autorização judicial, mas findou justificado apenas na necessidade de preservação dos vestígios, o que conforme já demonstramos não se sustenta.

Voltando ao voto do juiz da Corte estadual, o mesmo incluiu outras duas decisões recentes daquele Tribunal:

(...) - A garantia constitucional de inviolabilidade das comunicações telefônicas diz respeito à vedação de escutas clandestinas, a qual não se confunde com a mera checagem de textos, mensagens ou imagens do celular apreendido. (...) (Habeas Corpus Criminal 1.0000.17.023709-3/000, Relator(a): Des.(a) Jaubert Carneiro Jaques, **Data de Julgamento 18/04/2017**, Data da Publicação 04/05/2017)

[...]

A salvaguarda Constitucional do sigilo das comunicações não acoberta direito à prática de ilícito criminal, nem diz respeito à dados armazenados em aparelhos que foram utilizados na execução de crimes. Se forem atendidas as exigências previstas na Lei nº 9.296/96 não há nulidade da prova produzida em decorrência de interceptação telefônica." (...) (Habeas Corpus Criminal 1.0000.16.086709-9/000, Relator(a): Des.(a) Fernando Caldeira Brant, **Data de Julgamento 08/03/2017**, Data da Publicação 15/03/2017)

Assim, ausente manifesto constrangimento ilegal sanável de ofício, DENEGO A ORDEM. (BRASIL, 2017, grifo nosso)

Impressiona que em pleno 2017 duas decisões foram tomadas sem o uso de jurisprudência já em curso pelo STJ, bem como de legislação, senão perfeita, mas claramente mais afeita ao assunto em questão, qual seja o Marco Civil da Internet. Acrescente-se o desprezo pelo tipo de conteúdo devassado, afinal foi “mera checagem de textos, mensagens ou imagens do celular apreendido”.

Na segunda ementa, inclusive, o tema como em muitos casos confuso, pois parece tratar de interceptação, mas afirma que “[...] nem diz respeito à dados armazenados em aparelhos que foram utilizados na execução de crimes. Se forem atendidas as exigências previstas na Lei nº 9.296/96 não há nulidade da prova produzida em decorrência de interceptação telefônica”, ou seja, não faz o mínimo sentido.

Passando para o não menos confuso voto do ministro relator, temos:

Com efeito, a situação retratada nos autos não se encontra albergada pelo comando do art. 5º, inciso XII, da Constituição Federal, o qual assegura a inviolabilidade das comunicações, ressalvando a possibilidade de quebra de sigilo telefônico, por ordem judicial, nas hipóteses e na forma estabelecida pela Lei n. 9.296/1996, para fins de investigação criminal ou instrução processual penal.

Note-se que não foram interceptadas as comunicações telefônicas, nem mesmo as mensagens armazenadas no aparelho celular dos acusados, razão pela qual não há se falar igualmente em inobservância do art. 7º, incisos II e III, da Lei n. 12.965/2014, a qual estabelece os princípios, garantias e deveres para uso da internet no Brasil.

A propósito, transcrevo a norma acima referida:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I – (...).

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

(...).

Contudo, embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 **nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação ou de acesso a mensagens de texto armazenadas**, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da Constituição Federal, **houve sim violação dos dados armazenados no celular de um dos acusados**.

[...]

Ante o exposto, dou provimento ao recurso ordinário em habeas corpus, para reconhecer a ilicitude da colheita de dados dos aparelhos telefônicos (conversas de WhatsApp), sem autorização judicial, devendo mencionadas provas, bem como as derivadas, serem desentranhadas dos autos. (BRASIL, 2017, grifo nosso)

Acredito que o tema mereça um amplo debate, uma jurisprudência clara, figuras e diagramas, para um melhor entendimento do que se está a tratar. Fica latente que o Exmo. Relator não subsumiu os fatos ao art. 7º, inciso III, que ele mesmo transcreveu em sua decisão, pois afirmou que o Marco Civil não protegeu a situação retratada, mas em um movimento inesperado após tal negativa, afirmou “houve sim violação dos dados armazenados no celular de um dos acusados”.

Baseou sua decisão na Carta Magna, em seu artigo 5º, inciso X, talvez por perceber o alcance do conteúdo a ser encontrado em um aparelho celular e de que tal devassa, sem a devida autorização judicial, manifestamente violaria a garantia à intimidade e à vida privada. Terminou então por dar provimento ao recurso, reconhecendo a ilicitude da colheita de provas e que as mesmas deveriam ser desentranhadas dos autos.

5 CONCLUSÃO

Este trabalho iniciou muito antes da disciplina de Projeto de Pesquisa em Direito. Iniciou no dia-a-dia, quando os primeiros *smartphones* passaram a surgir e por assistir a aurora da migração das comunicações para as então chamadas redes sociais, que nada mais são do que outra forma e comunicação.

Existe um movimento capitaneado pelo Instituto Nacional de Criminalística da Polícia Federal, com sede em Brasília, de promover minicursos nas diversas Justiças Federais dos estados, muitas vezes em parceria com as Escolas da Magistratura Federais.

O problema examinado neste trabalho, surgiu como discussão em uma visita de magistrados federais às instalações do Setor Técnico Científico da Polícia Federal em Santa Catarina em junho de 2015. Onde perguntado sobre como eram realizados os exames em aparelhos celulares e outros dispositivos móveis, começaram as perguntas sobre se encontrávamos muito conteúdo “pessoal” e quando informamos que era corriqueiro, nos perguntaram em como fazíamos para separar tais conteúdos, no que afirmamos não ser viável tal separação.

Demos exemplos da quantidade de informações encontradas, mesmo para os casos mais simples, vide figuras 1 a 6, e questionamos sobre os tipos de quebras/afastamentos de sigilo que eram solicitadas, no que tivemos a informação de que em muitos casos nem pedidos haviam e que em outros apenas existia o pedido de autorização para acessar os dados junto às operadoras de telefonia.

No segundo semestre de 2016, como resultado da disciplina de projeto, surgiu o primeiro desenho da estrutura deste trabalho. Que no primeiro semestre de 2018 passou a levantar casos em que decisões judiciais ensejaram na remoção de conteúdo extraído de dispositivos móveis e quais foram as alegações de defesa, acusação e quais os fundamentos adotados pelos magistrados em suas decisões.

Claro que antes foi preciso um extenso trabalho de classificação dos objetos do tema:

O que é a privacidade? Como ela se desenvolveu conceitualmente? Como a legislação brasileira a prevê? Como ela é prevista em alguns países? Qual o nível de abrangência do tema?

O que é a comunicação? Como ela se dá? De que forma a legislação permite que o seu sigilo seja afastado? O que encontraremos?

Não são tantas perguntas, mas talvez pela intersecção de conceitos jurídicos com conceitos tecnológicos, as mesmas tomem uma proporção maior, talvez por isso o próprio STJ tenha divulgado, há poucos dias da entrega desta monografia, quais os novos desafios para a

jurisprudência, em assuntos que envolvem crimes ou serviços no ciberespaço, como as mensagens instantâneas e o direito à privacidade sobre estas quando obtidas diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial.

Dos casos analisados, dois foram de investigações da Polícia Federal, em que não foram solicitados os afastamentos de sigilo por se entender que, conforme o CPP/41, os dispositivos são ferramentas utilizadas no crime, bem como o acesso aos dados contidos nestes não são interceptações telefônicas e que, portanto, não necessitam de autorização para terem seus conteúdos acessados.

Cabe acrescentar, que conforme normativos internos emitidos pela Corregedoria da Polícia Federal, não cabe aos Peritos questionar sobre a existência e apresentação da autorização judicial para que procedam aos exames em quaisquer dispositivos encaminhados pela Autoridade Policial.

Os outros dois casos, tiveram seus Recursos em *Habeas Corpus* julgados pelo STJ e em ambos se tratou de acesso a mensagens instantâneas obtidas por policiais militares em situações de flagrante.

Restou latente a incapacidade dos membros da persecução penal e das instâncias inferiores em subsumir os fatos à legislação existente, pois todos os casos são posteriores ao advento do Marco Civil da Internet, que em seu bojo, não trata apenas do fluxo de comunicação da grande rede, mas também dos registros, metadados e dados armazenados, seja entre as partes que se comunicaram, seja com terceiros que viabilizaram tais comunicações.

Quando da análise pelo Superior Tribunal de Justiça no RHC 51.531 em 2016, o voto do relator e os votos-vista desenharam um excelente panorama, de nível internacional, sobre o tema. Já não se pode dizer o mesmo sobre o RHC 89.981 de 2017 do mesmo Tribunal.

A conclusão que chega esse trabalho, agora sobre o tema em si, é de que existe uma necessidade legal de prévia autorização para acesso ao conteúdo de dispositivos móveis conectados à internet, mas devem ser previstas situações de urgência, nas quais a persecução penal, sob fundamentado motivo, realizará o acesso ao conteúdo de tais aparelhos. Primando com isso o Estado Democrático de Direito.

Claro que isso gerará uma dificuldade, já vislumbrada pela persecução penal americana, que residirá em dar meios para que o policial prossiga com a investigação em casos que demandem a expedição de mandado de busca, através da agilidade na concessão do mandado, para aproveitar-se da oportunidade, talvez única, de desarticular uma organização criminosa.

Algumas perguntas nascem deste trabalho e ficam como trabalho futuros:

Quais os casos em que não caberiam mandado? Acredito que sejam em menor número, por isso, devem estar em um rol taxativo e não exemplificativo, sendo as situações residuais todas abrangidas pela proteção à privacidade. Como os EUA estão lidando com a situação desde 2014?

Dentro do próprio mandado, existem limites? Variáveis? Poderíamos vislumbrar um sistema online no qual o magistrado recebe um pedido eletrônico, assinado pelo agente e devolve um mandado eletrônico com os parâmetros permitidos na busca, como tipos de mídias, tipos de comunicação, dados de localização, registros, tudo isso com possíveis filtros de data.

E além, quem sabe seria possível a integração com os fabricantes de dispositivos eletrônicos portáteis, para que, com as devidas permissões de acesso, fosse possível os exames sem a necessidade de recorrer a ferramentas de terceiros, um acesso controlado e auditado e cujo resultado ficasse restrito ao filtro imposto pelo magistrado.

Uma extração total, mas que permaneceria criptografada, onde a ferramenta de análise use como entrada o mandado de busca, com os parâmetros das quebras de sigilo autorizadas, sem retrabalho, se o magistrado ampliar o escopo de busca a mesma extração poderá ser usada.

REFERÊNCIAS

AMERICANOS, ORGANIZAÇÃO DOS ESTADOS. **Pacto de San José de Costa Rica**. Convenção Americana sobre Direitos Humanos. San José: OEA. 1969.

BRASIL. Código de Processo Penal (1941). **Decreto Lei nº 3.689 de 03 de Outubro de 1941**, Rio de Janeiro, RJ, 03 out. 1941.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**, Brasília, DF: Senado Federal, 1988.

BRASIL. Lei da Interceptação Telefônica. **Lei Nº 9.296, de 24 de julho de 1996**, Brasília, DF, 24 julho 1996.

BRASIL. Código Civil (2002). **Lei 10.406, de 10 de janeiro de 2002**, Brasília, DF: Senado Federal, 2002.

BRASIL. Marco Civil da Internet. **Lei Nº 12.965, de 23 de Abril de 2014**, Brasília, DF, 23 Abril 2014.

BRASIL. Código de Processo Civil (2015). **Lei 13.105, de 16 de março de 2015**, Brasília, DF: Senado Federal, 2015.

BRASIL. Recurso em Habeas Corpus Nº 51.531 - RO (2014/0232367-7). **Superior Tribunal de Justiça**, 2016. Disponível em:

<<http://stj.jusbrasil.com.br/jurisprudencia/340165638/recurso-ordinario-em-habeas-corpus-rhc-51531-ro-2014-0232367-7/relatorio-e-voto-340165682>>. Acesso em: 30 jun. 2018.

BRASIL. Recurso em Habeas Corpus Nº 89.981 - MG (2017/0250966-3). **Superior Tribunal de Justiça**, 2017. Disponível em:

<https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1663002&num_registro=201702509663&data=20171213&formato=PDF>. Acesso em: 30 jun. 2018.

BRASIL. Crimes pela internet, novos desafios para a jurisprudência. **Superior Tribunal de Justiça**, 2018. Disponível em:

<http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Crimes-pela-internet,-novos-desafios-para-a-jurisprud%C3%Aancia>. Acesso em: 30 junho 2018.

BRIGATTO, G. Mercado de smartphones volta a crescer no Brasil após 2 anos de queda. **Valor Econômico**, 2018. Disponível em:

<<https://www.valor.com.br/empresas/5409615/mercado-de-smartphones-volta-crescer-no-brasil-apos-2-anos-de-queda>>. Acesso em: 03 jul. 2018.

CELLEBRITE. UFED Ultimate. **Cellebrite**, 2018. Disponível em: <<https://www.cellebrite.com/pt/products/ufed-ultimate-pt/>>. Acesso em: 25 Junho 2018.

KNIJNIK, D. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do Século XXI. **Temas de direito penal, criminologia e processo penal**, Porto Alegre, p. 173-190, 2015.

KONVITZ, M. R. Privacy and the Law: a Philosophical Prelude. **Law and Contemporary Problems**, v. 31, p. 272-280, 1966.

MARTINS, I. G. D. S. Inconstitucionalidades da Lei Complementar 105/2001. **Revista de Direito Bancário, do Mercado de Capitais e da Arbitragem**, São Paulo, v. 4, n. 11, p. 37-38, jan./mar. 2001.

MEARS, B. Supreme Court: Police need warrant to search cell phones. **CNN International**, 2014. Disponível em: <<https://edition.cnn.com/2014/06/25/justice/supreme-court-cell-phones/index.html>>. Acesso em: 25 Junho 2018.

MEIRELLES, F. S. 29ª Pesquisa Anual do Uso de TI, 2018. **Fundação Getúlio Vargas**, 2018. Disponível em: <<https://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2018gvciappt.pdf>>. Acesso em: 25 Junho 2018.

MILLER, A. R. **The assault on privacy: computers, data banks, and dossiers**. [S.l.]: University of Michigan Press, 1971.

MILLER, A. R. apud TEIXEIRA, M.; MENDES, V. **Casos e temas de direito das comunicações**. Porto: Legis, 1996. 161 p.

MORAES, A. D. **Direitos Humanos Fundamentais: teoria geral, comentários aos arts. 1º e 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. 3. ed. São Paulo: Atlas, 2000.

MORAES, A. D. **Direito Constitucional**. 24. ed. São Paulo: Atlas, 2009.

NAÇÕES UNIDAS. **The Right to privacy in digital age**. Assembleia Geral. Genebra. 2013.

PAOLA, J. Direito civil, direito de estar só. **Passei Direto**, 2017. Disponível em: <<https://www.passeidireto.com/arquivo/37512159/direito-civil-direito-de-estar-so>>. Acesso em: 30 jun. 2018.

PONTES DE MIRANDA, F. C. **Tratados de Direito Privado**. 4. ed. Rio de Janeiro: Revista dos Tribunais, v. VII, 1983.

POUSHTER, ; BISHOP, C.; CHWE, H. Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones. **Pew Research Center**, 2018. Disponível em: <<http://www.pewglobal.org/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/>>. Acesso em: 25 Junho 2018.

RAINIE, ; PERRIN, A. 10 facts about smartphones. **Pew Research Center**, 2017. Disponível em: <<http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones>>. Acesso em: 25 Junho 2018.

SOLOVE, D. J. Conceptualizing Privacy. **CALIFORNIA LAW REVIEW**, v. 90, p. 1087-1155, Julho 2002.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, abr 2016. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=pt&nrm=iso>. Acesso em: 25 junho 2018.

TRIBUNAL DE JUSTIÇA DE RONDÔNIA. Habeas Corpus : HC 00060197720168220000 RO 0006019-77.2016.822.0000. **Jusbrasil**, 2016. Disponível em: <<https://tj-ro.jusbrasil.com.br/jurisprudencia/411909099/habeas-corpus-hc-60197720168220000-ro-0006019-7720168220000>>. Acesso em: 03 jul. 2018.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. **Harvard Law Review**, v. 4, p. 193-220, Dezembro 1890. ISSN 5.

YUGE, C. Brasil supera marca de mais de um smartphone por habitante, diz FGV. **TecMundo**, 2018. Disponível em: <<https://www.tecmundo.com.br/mercado/129497-brasil-supera-marca-smartphone-habitante-diz-fgv.htm>>. Acesso em: 25 Junho 2018.

ZAVALA DE GONZÁLEZ, M. M. **Derecho a la intimidad**. Buenos Aires, Republica Argentina: Abeledo-Perrot, 1982.

ANEXO A – DESPACHO SOBRE LAUDO DE CELULARES**DESPACHO**

1. Junte-se aos autos o memorando 73/2015 SETEC/SR/SC.

2. O memorando acima referido trata da perícia realizada nos aparelhos de telefone celular apreendidos, sendo que o SETEC extraiu o conteúdo dos mesmos e o gravou em mídia, em relação a qual faço breve análise.

a) em relação aos aparelhos de telefone celular apreendidos com [REDACTED]:

- *BlackBerry 9220 Curve* - utilizava o número [REDACTED], operadora VIVO. Percebe-se que a última ligação telefônica teria, em tese, ocorrido no dia 23/01/2014. Quanto ao conteúdo restante, não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado.

- *BlackBerry 9220 Curve Branco* - utilizava o IMEI [REDACTED]. Não foi identificado o número de telefone que era utilizado, somente sabendo-se que era da operadora VIVO. Sem outros dados.

- *Nokia*, modelo 1616, IMEI [REDACTED], operadora TIM. Cite-se a existência de diversas ligações, em dias próximos à prisão em flagrante, para os números de telefone (45) [REDACTED]. Quanto ao conteúdo restante, não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado.

b) em relação ao aparelho de telefone celular apreendido com [REDACTED]: trata-se do *SAMSUNG GT S7560*, contendo cartão SIM da operadora TIM. Pelo teor das conversas do investigado, percebe-se que o número por ele utilizado seria o [REDACTED] (operadora TIM), mas, conforme por ele mesmo referido em diversas conversas via mensagens, também poderia ser encontrado nos números [REDACTED] (operadora TIM) e

IPL Nº [REDACTED] 3/2014

fls. 1 / 2

[REDACTED] (operadora VIVO). Percebe-se a existência de centenas de conversas em aplicativos (*Facebook* e *WhatsApp*), entretanto não se evidencia nada que, com os dados disponíveis, possa ser relacionado ao crime investigado. Destaca-se que, em dias próximos à prisão em flagrante, constam diversas ligações para o número de telefone [REDACTED].

3. Considerando a data em que ocorreram os fatos, não há qualquer óbice na realização de diligências complementares, visando ao pleno esclarecimento do ocorrido.

ANEXO B – MANIFESTAÇÃO DO MP SOBRE QUEBRA DE SIGILO



MPF Procuradoria
da República em
São Miguel do Oeste
Ministério Público Federal

1

EXCELENTÍSSIMO(A) SENHOR(A) JUIZ(A) FEDERAL DA 1ª VARA FEDERAL DE SÃO MIGUEL DO OESTE

Pedido de quebra de sigilo de dados e/ou telefônicos

e-Proc n. [REDAZIDA]

CONTRABANDO. ARTIGO 334 DO CÓDIGO PENAL. REPRESENTAÇÃO POLICIAL PELA AUTORIZAÇÃO JUDICIAL DE ACESSO A REGISTROS DE LIGAÇÕES EFETUADAS. DIREITO À INTIMIDADE, À VIDA PRIVADA E AO SIGILO DE INFORMAÇÕES E DADOS DO INDIVÍDUO (ART. 5º, INCISOS X).

A representação do Delegado de Polícia Federal em Dionísio Cerqueira/SC visa, em razão da necessidade de dar prosseguimento às investigações desenvolvidas no âmbito do Inquérito Policial n. [REDAZIDA]-DPF/DCQ/SC, que apura a prática do crime de contrabando previsto no art. 334 do Código Penal, sob a redação anterior à Lei 13.008/2014, à obtenção de autorização judicial para acessar registros telefônicos dos seguintes terminais: [REDAZIDA]

[REDAZIDA], dos IMEIs [REDAZIDA] no período de 02/01/2014 a 30/01/2014.

A medida é desdobramento do acesso à agenda do telefone celular encontrado com os indiciados [REDAZIDA], na oportunidade de suas prisões em flagrante por contrabando, quando transportavam, aproximadamente, 75 mil pacotes de cigarros em um caminhão. O resultado da análise pericial dos celulares levou à identificação dos números e IMEIs acima apontados, conforme Laudo n. 046/2015 - SETEC/SR/DPF/SC (fl. 103), complementado pela mídia

encaminhada diretamente ao MPF por meio do Ofício n. [REDACTED]/DPF/DCQ/SC.

O caso concreto justifica a medida de afastamento de sigilo telefônico. Trata-se, possivelmente, de grande esquema de contrabando. Para se ter uma ideia, os tributos que a importação lícita de uma carga de cigarros similar à que foi apreendida gerariam alcançam a cifra de R\$ 860.021,28 (fl. 78), o que pressupõe um valor de compra de alguns milhões de reais.

Ainda, há fortes indícios de falsificação da documentação fiscal encontrada com os indiciados, adulteração do chassi do caminhão que fez o transporte dos cigarros, além da presença de batedor, rádio comunicadores e R\$ 11.000,00 reais em espécie, tudo fazendo crer tratar-se de associação criminosa bastante estruturada.

Necessário, dessa maneira, saber-se quem são os titulares dos números de celular com os quais os indiciados mantiveram contato, para se chegar aos demais autores do delito, quais sejam, os fornecedores e os adquirentes da carga de cigarros.

Do ponto de vista fático, portanto, a medida de quebra de sigilo dos números de telefone está plenamente justificada. Não há outras diligências policiais que se mostrem, por ora, úteis à identificação dos demais coautores, senão a alvitrada pela autoridade policial, tendo a investigação que adotar este caminho sob pena de frustração do aprofundamento da própria persecução criminal.

Com efeito, verifica-se, a partir dos autos, que as informações buscadas pela autoridade policial são imprescindíveis à elucidação da existência e conhecimento dos coautores da conduta apurada no citado inquérito policial.

Os dados solicitados pela Autoridade Policial estão protegidos pelo Direito Brasileiro que garante, constitucionalmente, a proteção ao direito à intimidade, à vida privada e ao sigilo de informações e dados do indivíduo (art. 5º, incisos X). Entretanto, tais garantias – assim como os demais direitos protegidos por nossas normas – não se revestem de caráter absoluto. Ao contrário, podem elas, em algumas hipóteses, ser excepcionadas, desde que demonstrada, com segurança e baseada no Princípio da Razoabilidade, a existência de indícios de autoria e prova de materialidade da conduta delituosa, além da utilidade, pertinência e necessidade da medida a ser tomada.

Tal posicionamento encontra ampla guarida na Jurisprudência pátria, da qual é exemplo a seguinte decisão do Egrégio Tribunal Regional Federal da 4ª Região:

CORREIÇÃO PARCIAL Processo: 200504010310410 UF:RS Órgão Julgador: OITAVA TURMA Data da decisão: 10/08/2005 - Documento: TRF400110241 - Relator(a): PAULO AFONSO BRUM VAZ. Decisão: A TURMA, POR UNANIMIDADE, DEFERIU O PEDIDO DE CORREIÇÃO PARCIAL, NOS TERMOS DO VOTO DO RELATOR.

Ementa: PROCESSO PENAL. **INQUÉRITO POLICIAL. SIGILO TELEFÔNICO. CF, ART. 5º, X E XII. PROTEÇÃO RELATIVA. CONTRAPOSIÇÃO AO INTERESSE DA SOCIEDADE.**

- **Não obstante os sigilos bancário, fiscal e telefônico encontrem-se assegurados pelo art. 5º, X e XII, da Carta Magna, o entendimento dos Tribunais pátrios é uníssono no sentido de que a proteção constitucionalmente deferida a tais dados não tem caráter absoluto, cedendo, mediante decisão judicial fundamentada, ao interesse público refletido na necessidade de se apurar fato que, em tese, perfectibilize infração penal** (sem grifos no texto original).

Desta forma, o direito constitucional à inviolabilidade da intimidade e da vida privada – o que inclui informações particulares – não pode ser utilizado para se acobertar a prática de atividades ilícitas e criminosas, devendo ceder espaço quando o interesse público reclamar prevalência sobre o interesse particular. Inexiste direito fundamental, seja ele individual ou coletivo, sob o manto da proteção absoluta. Ao contrário, as garantias individuais encontram limitação em postulados jurídicos de maior envergadura. Exatamente como ocorre no presente caso, em que os elementos trazidos pela autoridade policial demonstram que o direito ao sigilo não pode prevalecer sobre a necessidade de ampla apuração dos fatos aqui tratados.

Registre-se, por oportuno, que o termo “quebra” não corresponde, semanticamente, à medida pleiteada. Afirma-se isto porque os dados obtidos não passam a ser públicos – palavra que, no presente contexto, se oporia ao sigilo. O que há é, tão-somente, a permissão judicial para acesso aos dados cadastrais dos usuários e das ligações por eles efetuadas ou recebidas, que continuarão sob proteção de violação. Daí a razão de parte da doutrina referir-se à expressão “ampliação a terceiros do dever de sigilo”, ou em “ampliação da esfera de sigilo” ou, ainda, em “transferência da obrigação de sigilo”. Enfim, qualquer que seja a expressão, a ideia é que o acesso franqueado a outros órgãos públicos deve restringir-se ao exercício de suas funções respectivas sob pena de, inclusive, responsabilização penal.

Com fundamento no exposto, o **MINISTÉRIO PÚBLICO FEDERAL**, por seu Procurador da República signatário, encampa a representação policial e requer sejam integralmente deferidas as diligências propostas pela autoridade policial no documento presente no evento 1. Outrossim, informa a esse nobre Juízo que, nesta data, está encaminhando fisicamente a mídia digital remetida pela Polícia Federal através do Ofício n. [REDACTED] 2015 – RE [REDACTED] 2015-4 DPF/DCQ/SC.

São Miguel do Oeste/SC, 24 de abril de 2015.

ANEXO C – RETIFICAÇÃO DA REPRESENTAÇÃO INICIAL

Assunto: **RETIFICAÇÃO REPRESENTAÇÃO INICIAL**

e-Proc: [REDACTED]

Excelentíssimo Senhor Juiz.

Em atenção aos eventos 18 e seguintes destes autos, faço as considerações que seguem.

Na representação que ensejou a instauração deste procedimento constou, por equívoco do signatário, que o conteúdo dos aparelhos de telefone celular havia sido examinado "após a devida autorização judicial".

Nesse contexto, cumpre referir que o signatário adota como praxe o envio dos aparelhos de telefone celular para exame pericial somente após existir decisão judicial autorizando tal perícia. Assim, ao receber o laudo pericial referente aos aparelhos de telefone celular apreendidos nos autos do inquérito policial relacionado a este feito, imaginava-se que teria existido decisão judicial autorizando a realização do mesmo.

Entretanto, melhor analisando o inquérito policial, verifica-se que a Autoridade Policial que antecedeu ao signatário possuía outro entendimento, entendendo desnecessária autorização judicial para tanto, sendo que o exame pericial nos aparelhos de telefone celular foi realizado sem a mesma. Consigne-se, nesse sentido, que existem divergências jurisprudenciais e doutrinárias sobre a necessidade de autorização judicial para realização de tal perícia.

Assim, **retificam-se os termos da representação presente no evento 01, pois a perícia nos aparelhos de telefone celular ocorreu sem prévia decisão judicial.**

Por outro lado, **representa-se para que seja, mesmo que a posteriori, autorizado o acesso ao conteúdo dos aparelhos de telefone celular apreendidos nos autos do IPL [REDACTED]/2014 (item 06 do auto de apreensão de fls. 08/09 do IPL e item 04 do auto de apreensão de fl. 18 do IPL), autorizando-se a utilização do laudo presente nas fls. 102 a 106 do mesmo.**

Caso deferida tal utilização, reiteram-se os pedidos presentes na representação do evento 01 deste processo.

Respeitosamente,

ANEXO D – MP: PEDIDO DE ACESSO AOS DADOS TELEFÔNICOS



MPF Procuradoria
da República em
São Miguel do Oeste
Ministério Público Federal

1

EXCELENTÍSSIMO(A) SENHOR(A) JUIZ(A) FEDERAL DA 1ª VARA FEDERAL DE SÃO MIGUEL DO OESTE – SEÇÃO JUDICIÁRIA DE SANTA CATARINA

Pedido de acesso a dados telefônicos

e-Proc n. 5000575-47.2015.4.04.7210

PERMISSÃO DE ACESSO A DADOS DE CADASTROS E DE REGISTRO DE LIGAÇÕES. CRIME DE CONTRABANDO. DIREITO À INTIMIDADE E À VIDA PRIVADA DO INDIVÍDUO (ART. 5º, INCISOS X E XII). CELULARES APREENDIDOS. LAUDO PERICIAL JÁ PRODUZIDO. INEXISTÊNCIA DE VIOLAÇÃO A DIREITO CONSTITUCIONAL. MANIFESTAÇÃO PELA DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL.

O **Ministério Público Federal**, por seu Procurador da República signatário, em atenção à representação presente no evento 24, vem perante Vossa Excelência manifestar-se nos seguintes termos:

Visa o Delegado de Polícia Federal em Dionísio Cerqueira/SC retificar a Representação pela quebra de sigilo telefônico presente no evento 1 destes autos, para excluir a afirmação “*Após a devida autorização judicial [...]*” presente naquela representação, justificando que o acesso ao conteúdo da memória dos celulares apreendidos no inquérito policial, conforme Laudo de Perícia Criminal Federal n.º 046/2015 (evento 84 – INQ1, do inquérito policial n.º 5000581-88.2014.4.04.7210), deu-se sem autorização do Juízo, tendo em vista o entendimento diverso manifestado pelo Delegado que presidia o referido inquérito à época. Pede, portanto, autorização judicial para utilizar-se do laudo confeccionado, ainda que o pedido seja feito *a posteriori* (Evento 24 – REPRESENTAÇÃO_BUSCA1).

De fato, a perícia realizada pela Polícia Federal nos celulares em razão da apreensão destes não se mostra violadora do direito constitucional ao sigilo (art. 5º, inciso XII das CF), em razão de que a indisponível reserva de jurisdição se irradia à comunicação de dados (*v.g.*, interceptação telefônica), e não propriamente dos dados obtidos na base física apreendida pelos meios legais (*v.g.*, apreensão de objetos – *corpus delicti*), parafraseando o Ministro Sepúlveda Pertence nos autos do HC 91867, citando voto do então Ministro Néri da Silveira nos autos do MS n.º 21.729, *verbis*:



*EMENTA: I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem "interessantes à investigação" que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a "Fiscalização do INSS" também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, "observado o sigilo imposto ao feito". IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. **A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).** V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal). (RE 418416, Relator(a): Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233) - grifo nosso.*

A Suprema Corte Brasileira já se pronunciou sobre fato análogo, registrando que o objeto de proteção jurídica da comunicação de dados não se confunde com a proteção dada aos dados obtidos com a apreensão de elemento de corpo de delito, nos termos do relator Ministro Gilmar Mendes nos autos do HC n.º 91.867:

HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA. 1. Inépcia da denúncia. Improcedência. Preenchimento dos requisitos do art. 41 do CPP. A denúncia narra, de forma pormenorizada, os fatos e as circunstâncias.



Pretensas omissões – nomes completos de outras vítimas, relacionadas a fatos que não constituem objeto da imputação – não importam em prejuízo à defesa. 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corrêu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corrêu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º. 3. Ilicitude da prova das interceptações telefônicas de conversas dos acusados com advogados, ao argumento de que essas gravações ofenderiam o disposto no art. 7º, II, da Lei n. 8.906/96, que garante o sigilo dessas conversas. 3.1 Nos termos do art. 7º, II, da Lei 8.906/94, o Estatuto da Advocacia garante ao advogado a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia. 3.2 Na hipótese, o magistrado de primeiro grau, por reputar necessária a realização da prova, determinou, de forma fundamentada, a interceptação telefônica direcionada às pessoas investigadas, não tendo, em momento algum, ordenado a devassa das linhas telefônicas dos advogados dos pacientes. Mitigação que pode, eventualmente, burlar a proteção jurídica. 3.3 Sucede que, no curso da execução da medida, os diálogos travados entre o paciente e o advogado do corrêu acabaram, de maneira automática, interceptados, aliás, como qualquer outra conversa direcionada ao ramal do paciente. Inexistência, no caso, de relação jurídica cliente-advogado. 3.4 Não cabe aos policiais executores da medida proceder a uma espécie de filtragem das escutas interceptadas. A impossibilidade desse filtro atua, inclusive, como verdadeira garantia ao cidadão, porquanto retira da esfera de arbítrio da polícia escolher o que é ou não conveniente ser interceptado e gravado. Valoração, e eventual exclusão, que cabe ao magistrado a quem a prova é dirigida. 4. Ordem denegada. (HC 91867, Relator(a): Min. GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012) – grifo nosso.

Há precedentes, inclusive do Superior Tribunal de Justiça, manifestando-se nos mesmos termos:

CRIMINAL. HC. HOMICÍDIO QUALIFICADO. TRANCAMENTO DA AÇÃO PENAL. INÉPCIA DA DENÚNCIA. INEXISTÊNCIA DE DESCRIÇÃO MÍNIMA DAS ELEMENTARES DOS CRIMES. OFENSA AO ART. 41 DO CPP. NÃO OCORRÊNCIA. NOME COMPLETO DAS VÍTIMAS NÃO EXPLICITADO. IRRELEVÂNCIA. CERCEAMENTO DE DEFESA NÃO DEMONSTRADO. ILEGALIDADE DE PROVA COLHIDA NO INQUÉRITO POLICIAL. INEXISTÊNCIA DE QUEBRA DE SIGILO



TELEFÔNICO. INTERCEPTAÇÃO TELEFÔNICA. CONVERSAS ENTRE OS RÉUS E SEUS DEFENSORES. INTERCEPTAÇÃO NOS TELEFONES DOS INVESTIGADOS. FILTRAGEM QUE NÃO DEVE SER FEITA PELA AUTORIDADE POLICIAL. AFRONTA AO ESTATUTO DO ADVOGADO NÃO CONFIGURADA. DOCUMENTOS QUE PODEM SER DESCARTADOS PELO JUÍZO.

SENTENÇA NÃO PROFERIDA. ORDEM DENEGADA.

Eventual inépcia da denúncia só pode ser acolhida quando demonstrada inequívoca deficiência a impedir a compreensão da acusação, em flagrante prejuízo à defesa dos acusados, ou na ocorrência de qualquer das falhas apontadas no art. 43 do CPP – o que não se vislumbra no presente caso.

Se o órgão de acusação descreveu minuciosamente os fatos praticados pelo co-réu, esclarecendo que os pacientes, juntamente com os outros dois denunciados, seriam os mandantes da prática delitiva, demonstrando por meio de provas testemunhais os motivos do delito, bem como a ligação destes com o contratado para efetuar os disparos fatais, resta evidenciada a existência de elementos suficientes a embasar a acusação, não havendo que se falar em ofensa ao art. 41 do CPP.

O fato de os nomes das vítimas de outros homicídios citados na exordial não terem sido apresentados de forma completa não prejudica a defesa dos acusados, pois, além de se tratarem de delitos praticados em pequeno município, onde a comunidade tem conhecimento generalizado dos fatos que ali acontecem, a supressão destes dados não impede a associação da narrativa com a realidade fática.

Existindo vinculação mínima entre os fatos da denúncia e a conduta dos pacientes, mesmo que a autoria não se mostre claramente comprovada, a fumaça do bom direito deve ser abrandada, dentro do contexto fático de que dispõe o Ministério Público no limiar da ação penal, não sendo indispensável a descrição pormenorizada da conduta de cada agente.

O fato de ter sido verificado o registro das últimas chamadas efetuadas e recebidas pelos dois celulares apreendidos em poder do co-réu, cujos registros se encontravam gravados nos próprios aparelhos, não configura quebra do sigilo telefônico, pois não houve requerimento à empresa responsável pelas linhas telefônicas, no tocante à lista geral das chamadas originadas e recebidas, tampouco conhecimento do conteúdo das conversas efetuadas por meio destas linhas.

É dever da Autoridade policial apreender os objetos que tiverem relação com o fato, o que, no presente caso, significava saber se os dados constantes da agenda dos aparelhos celulares teriam alguma relação com a ocorrência investigada.

Se o Magistrado singular, ao determinar a escuta telefônica, o fez em relação às pessoas investigadas, explicitando os números dos telefones, não cabe à Autoridade policial fazer qualquer tipo de "filtragem".

Mesmo que em algumas interceptações os investigados tenham recebido e feito ligações para os seus defensores, estas foram gravadas e transcritas de maneira automática, do mesmo modo como ocorreu com as demais conversas efetivadas através dos celulares dos pacientes.

Cabe ao Juiz, quando da sentença, avaliar os diálogos que serão usados como prova, podendo determinar a destruição de parte do documento, se assim achar conveniente, no momento da prolação da sentença.

Ordem denegada.

(HC 66.368/PA, Rel. Ministro GILSON DIPP, QUINTA TURMA, julgado em 05/06/2007, DJ 29/06/2007, p. 673) – grifo nosso.

O Egrégio Tribunal Regional Federal da 4ª Região já se manifestou no mesmo sentido:

EMENTA: HABEAS CORPUS. PRISÃO PREVENTIVA. PRESENÇA DOS REQUISITOS. GARANTIA DA ORDEM PÚBLICA. LIBERDADE PROVISÓRIA INDEFERIDA. VIOLAÇÃO DE SIGILO TELEFÔNICO. INOCORRÊNCIA. 1. A prisão preventiva é medida rigorosa que, no entanto, se justifica nas hipóteses em que se mostre necessária para assegurar a imediata proteção de bens jurídicos relevantes. 2. São pressupostos para a decretação da prisão preventiva a prova da materialidade e indícios de autoria. Os elementos da investigação realizada pela autoridade policial são suficientes, nessa fase, como prova de materialidade e autoria. 3. A prisão

preventiva deve ser justificada por pelo menos um dos fundamentos alternativos previstos no art. 312 do Código de Processo Penal. 4. Não configura quebra do sigilo telefônico o fato de ter sido verificado os registros contidos no aparelho celular do réu apreendido, diante da possibilidade de nele serem encontradas provas relacionadas ao fato criminoso. Precedentes do STJ. 5. Ordem de habeas corpus denegada. (TRF4, HC 5015269-54.2014.404.0000, Oitava Turma, Relator p/ Acórdão João Pedro Gebran Neto, juntado aos autos em 18/07/2014) – grifo nosso.

É de conhecimento a praxe (o que não desnatura o direito/dever previstos no art. 6º, incisos II, III e VII do Código de Processo Penal) de obter-se autorização judicial para o acesso aos dados contidos na memória de celulares apreendidos como possíveis instrumentos do crime, inclusive com parecer favorável deste *PARQUET FEDERAL*, não se mostrando desarrazoado tal procedimento, dado que amplia, de certa forma, as garantias processuais do indiciado sem qualquer prejuízo tanto à acusação quanto à defesa.

No entanto, dadas as peculiaridades do caso, em que já há Laudo Pericial produzido pela Polícia Federal sobre os registros de ligações e mensagens de texto enviadas e recebidas, entendo desnecessário, no caso concreto, pleitear-se autorização judicial para acesso daquilo que já foi acessado, pelos fundamentos expostos.

Assim, o **Ministério Público Federal**, por seu Procurador da República signatário, manifesta-se pela desnecessidade de obtenção de autorização judicial para obter-se o acesso aos dados contidos nos celulares apreendidos no inquérito policial n.º 5000581-88.2014.4.04.7210, pois já devida e legalmente periciados, e reitera a manifestação ministerial presente no evento 13.