XXV CONGRESSO DO CONPEDI - CURITIBA

INTERVENÇÃO ESTATAL, GOVERNANÇA CORPORATIVA E COMPLIANCE NO COMBATE À CORRUPÇÃO

EDIMUR FERREIRA DE FARIA

MIGUEL KFOURI NETO

Copyright © 2016 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos.
Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Raymundo Juliano Feitosa – UNICAP
Vice-presidente Sul - Prof. Dr. Ingo Wolfgang Sarlet – PUC - RS
Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim – UCAM
Vice-presidente Nordeste - Profa. Dra. Maria dos Remédios Fontes Silva – UFRN
Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes – IDP
Secretário Executivo - Prof. Dr. Orides Mezzaroba – UFSC
Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Representante Discente – Doutoranda Vivian de Almeida Gregori Torres – USP

Conselho Fiscal:
Prof. Msc. Caio Augusto Souza Lara – ESDH
Prof. Dr. José Querino Tavares Neto – UFG/PUC PR
Profa. Dra. Samyra Haydêe Dal Farra Naspolini Sanches – UNINOVE
Prof. Dr. Lucas Gonçalves da Silva – UFS (suplente)
Prof. Dr. Fernando Antonio de Carvalho Dantas – UFG (suplente)

Secretarias:
Relações Institucionais – Ministro José Barroso Filho – IDP
Prof. Dr. Liton Lanes Pilau Sobrinho – UPF
Educação Jurídica – Prof. Dr. Horácio Wanderlei Rodrigues – IMED/ABEDi
Eventos – Prof. Dr. Antônio Carlos Diniz Murta – FUMEC
Prof. Dr. Jose Luiz Quadros de Magalhaes – UFMG
Profa. Dra. Monica Herman Salem Caggiano – USP
Prof. Dr. Valter Moura do Carmo – UNIMAR
Profa. Dra. Viviane Coêlho de Séllos Knoerr – UNICURITIBA
Comunicação – Prof. Dr. Matheus Felipe de Castro – UNOESC

I61

Intervenção estatal, governança corporativa e compliance no combate à corrupção [Recurso eletrônico on-line] organização CONPEDI/UNICURITIBA;

Coordenadores: Edimur Ferreira De Faria, Miguel Kfouri Neto – Florianópolis: CONPEDI, 2016.

Inclui bibliografia
ISBN: 978-85-5505-349-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: CIDADANIA E DESENVOLVIMENTO SUSTENTÁVEL: o papel dos atores sociais no Estado Democrático de Direito.

1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Congressos. 2. Intervenção Estatal. 3. Governança Corporativa. 4. Compliance. 5. Corrupção I. Congresso Nacional do CONPEDI (25. : 2016 : Curitiba, PR).

CDU: 34

CONPEDI
Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXV CONGRESSO DO CONPEDI - CURITIBA

INTERVENÇÃO ESTATAL, GOVERNANÇA CORPORATIVA E COMPLIANCE NO COMBATE À CORRUPÇÃO

Apresentação

O Grupo de Trabalho "Intervenção Estatal, Governança Corporativa e Compliance no Combate à Corrupção: direitos especiais e tutela das minorias na atividade empresarial" reuniu no XXV Congresso do CONPEDI, realizado em Curitiba-PR, quinze artigos, sendo que um deles não foi apresentado pelos respectivos autores, por isso, não consta desta coletânea.

Os artigos defendidos foram escritos por doutores, doutorandos, mestres e mestrandos, individual ou em coautoria com respectivos orientadores ou professores. Os trabalhos são de alto nível, profundidade e discussão adequados e compatíveis com as exigências próprias dos trabalhos científicos. São textos originais contendo novidades nos campos investigados, abordando questões polêmicas e atuais, ainda pouco enfrentadas pela doutrina e jurisprudência pátrias.

Os debates e discussões que se seguiram após a cada cinco apresentações foram profícuos e relevantes para melhor compreensão das particularidades do temário do GT. Selecionaram-se, aleatoriamente, alguns dos assuntos objetos dos artigos: desafios do programa compliance social de caráter trabalhista da empresa JBS S.A; o compliance sob a ótica do combate à corrupção e a busca pela cidadania; a não intervenção estatal nas entidades sindicais patronais e a pretensão de fiscalização pelo Tribunal de Contas da União; autorregulação regulada e a lei anticorrupção no Brasil; compliance como aliado no combate à corrupção na Administração Pública; bloqueio do "WHATSAPP": a política de segurança de transferência de dados e as medidas de compliance; e responsabilidade civil e a aplicabilidade da teoria do desestímulo no ordenamento jurídico no Brasil.

Essa amostragem revela a diversidade e interdisciplinariedade dos temas debatidos sob a coordenação, apresentação e participação dos Professores Doutores que este subscrevem.

Mais uma vez o CONPEDI e a sua competente equipe estão de parabéns pela seleção das linhas de pesquisa e organização do evento. Neste particular "organização do evento" merecem reconhecimento a Diretoria, professores e funcionários da UNICURITIBA, que não mediram esforços para proporcionar aos participantes do evento a operante organização adequada e funcional da Universidade.

Espera-se que os leitores encontrem nos textos publicados, subsídios para as suas pesquisas.

Prof. Dr. Edimur Ferreira de Faria, Professor Doutor - PUC Minas

Prof. Dr. Miguel Kfouri Neto, Professor Doutor - UNICURITIBA

BLOQUEIO DO “WHATSAPP”: A POLÍTICA DE SEGURANÇA DE TRANSFERÊNCIA DE DADOS E AS MEDIDAS DE COMPLIANCE

“WHATSAPP” SHUTDOWN: DATA TRANSFER SECURITY POLICY AND COMPLIANCE MEASURES

Fernando Andrade Fernandes
Leonardo Simões Agapito

Resumo

Tem-se por objetivo compreender a adequação à legislação brasileira das recentes decisões judiciais que atribuíram aos gestores do aplicativo de celular “Whatsapp” o dever de oferecer informações sigilosas de seus usuários. Primeiramente, analisam-se, pelo método indutivo, os recentes casos de bloqueio e os mecanismos de “compliance” existentes nas leis n.12.850 /2013 e n.12.965/2014. Em seguida, analisa-se, sistematicamente, os “termos e condições de uso” do aplicativo “WhatsApp”, tendo por referência a regulação setorial, a competência da agência reguladora, suas normativas e entraves jurídicos, compreendendo particularidades do sistema de comunicação via internet. Ao final, buscam- se medidas possíveis de “enforcement” à lei brasileira.

Palavras-chave: Compliance, Meios de comunicação, Regulação, Decisões judiciais

Abstract/Resumen/Résumé

The current paper pursuit to understand the adequacy to Brazilian legislation of recent court decisions that attributed to "Whatsapp"’s managers a duty to provide sensitive information of its users. First, it’s analyzed, by the inductive method, the recent cases of shutdown and the mechanisms of "compliance" in existing brazilian acts 12.850/2013 and 12.965/2014. Then it’ s analyzed systematically the "terms and conditions" of the "WhatsApp" application, with reference to sector’s regulation, the competence of the regulatory agency, its regulatory and legal obstacles, including the communication system characteristics by internet. Finally, there is some possible measures of brazilian law “enforcement".

Keywords/Palabras-claves/Mots-clés: Compliance, Media, Regulation, Judicial decision

1. Introdução

O aplicativo de celular “WhatsApp” foi adquirido pelo grupo econômico “Facebook” em 2014, já com milhões de usuários em diferentes países. Seu sistema permite a comunicação por mensagens escritas, imagens, áudios e vídeos entre usuários, mais recentemente passou a oferecer a possibilidade de ligações. Em agosto de 2016, os termos e condições de uso foram adaptados para permitir que sua plataforma conecte empresas e consumidores, bem como direcionar publicidade apresentada na rede social “facebook”, além de sugerir novos contatos na rede “instagram”. Para sua utilização, o “WhatsApp” tem acesso irrestrito à agenda de contatos, fotos e dados pessoais que se encontrem no aparelho celular do usuário.

Em função de suas facilidades e baixíssimo custo ao usuário, comparado aos serviços das empresas de telefonia, sua popularidade o tornou protagonista nas comunicações pessoais. A partir disso, algumas decisões judiciais passaram a exigir que a empresa oferecesse dados de seus usuários para auxiliar investigações criminais. Tais pedidos foram negados pelo grupo econômico, o que gerou ordens de bloqueio ao serviço utilizado e até mesmo a prisão de um executivo da companhia no Brasil.

Diante das diversas posições técnicas, quanto à possibilidade de tais informações serem oferecidas, e de política criminal, quanto à necessidade dessas exigências, o presente artigo, a partir de um estudo indutivo dos casos e da legislação pertinente, propõe-se a analisar as exigências feitas, viabilidade e, ao final, propor medidas de *enforcement* à política criminal brasileira. Tal análise necessariamente leva ainda em consideração a legislação americana sobre regulação de meios de comunicação e medidas de *compliance*.

2. Os recentes casos de bloqueio do aplicativo: pontos principais

Inicialmente, devem-se apresentar os quatro casos de bloqueio do aplicativo que ocorreram no Brasil até o fechamento do presente artigo. Não se pretende fazer uma análise aprofundada e exaustiva de cada decisão judicial, mas destacar a razão e a forma como cada uma destas se deu. Em função do sigilo das investigações e dificuldade de acesso aos processos na íntegra, utilizar-se-ão as notícias veiculadas na mídia, tendo em vista os esclarecimentos que foram apresentados por assessorias de imprensa, como base para os elementos mínimos da análise.

A primeira decisão determinando o bloqueio do aplicativo foi expedido em 11 de fevereiro de 2015, pelo Juiz de Direito da Central de Inquéritos da Comarca de Teresina, Piauí, tendo como partes obrigadas todas as empresas que oferecem serviço de internet, fixa ou móvel, sob pena de crime de desobediência. A medida de bloqueio deveria se dar pela

restrição aos domínios “whatsapp.com” e “whatsapp.net”. A ordem teve por justificativa o descumprimento de diversas solicitações das comunicações entre investigados em processo de proteção a crianças e adolescentes.

A segunda decisão adveio da 1ª Vara Criminal de São Bernardo do Campo, São Paulo, em 16 de dezembro de 2015. Semelhantemente ao primeiro caso, o processo investigava uma organização, neste caso envolvendo tráfico de entorpecentes, solicitando aos administradores as conversas entre uma linha brasileira e duas paraguaias, configurando uma organização criminosa pela trans-nacionalidade (art.1º, §1º, Lei n.12.850/2013). Após o reiterada negativa de cumprimento, expediram-se mandados a todas as empresas de serviços de internet determinando o bloqueio por 48 horas. No entanto, o Tribunal de Justiça de São Paulo considerou a medida desproporcional e concedeu liminar após 12 horas de bloqueio.

Os dois últimos bloqueios ocorreram em 2 de maio de 2016, por determinação da Vara criminal da Comarca de Lagarto, em Sergipe, e em 19 de julho de 2016, por determinação da Vara de Execuções de Duque de Caxias, Rio de Janeiro. Ambos os casos investigavam tráfico de entorpecentes e, alegando descumprimento de reiterados pedidos de cooperação, expediram mandados às empresas que oferecem serviços de internet fixa e móvel para bloqueio dos domínios.

Por esta razão, destacam-se das decisões que todas tinham em comum os reiterados pedidos, com base no Marco Civil da Internet (lei n.12.965/2014), e analisavam casos envolvendo organizações criminosas (lei n.12.850/2013).

3. A regulação das comunicações pela internet

A legislação brasileira acerca desta temática é bastante recente e, jurisprudencialmente, o que existe ainda é inconclusivo. Por esta razão, tendo em vista os casos apresentados anteriormente, focar-se-ão para o presente debate apenas as duas leis supracitadas, com objetivo de compreender os deveres atribuídos por elas às empresas que oferecem serviço de internet, bem como os deveres de colaboração em casos que tenham por objeto o delito de organização criminosa.

3.1 O marco civil da internet

Em vigência desde 23 de junho de 2014, o marco civil da internet, em seu art.7º, define alguns dos direitos dos usuários da rede, dentre eles, cabe destacar: a) inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; b) inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; c) informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de

proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; d) 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; e) informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; f) consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; g) exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; h) publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet.

Em suma, tem por fim a referida lei proteger a transação de dados, sem inviabilizar os serviços utilizados pela população ou impedir investigações judiciais, tendo como estágio necessário o consentimento prévio do usuário, de modo que até mesmo o oferecimento dessas informações para o governo deve ser esclarecido no momento da adesão, já que registros precisam ser armazenados por período de tempo não irrelevante.

Particularmente quanto às demandas judiciais por provas, o art.22 da referida lei dispõe que qualquer parte interessada (o que inclui a intervenção de terceiros no processo civil e o auxiliar de acusação no processo penal) poderá requerer o fornecimento de “registros de conexão” e “registros de acesso a aplicações de internet”, sendo requisitos para admissibilidade pelo magistrado: a) fundados indícios da ocorrência do ilícito; b) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; c) período ao qual se referem os registros. Em nenhuma hipótese está prevista a solicitação de ofício pelo magistrado, sendo este apenas responsável por verificar a admissibilidade do pedido e zelar pelo sigilo dos dados dentro do processo, que não se tornam públicos em hipótese legal alguma.

No entanto, o Instituto brasileiro de defesa do Consumidor (IDEC) elaborou um parecer discutindo a aplicação do art.12, que permitiria o bloqueio de aplicativos, mas que deveria ser interpretado a partir do interesse dos consumidores (ZANATTA, 2016, p.1). O parecer ainda explicava que o art. 9º impedia as operadoras de internet a restringirem determinadas aplicações, atuando como filtros, sendo incorreta a forma como se deram todos

os bloqueios no Brasil. O referido artigo somente permitiria a restrição quando não houvesse a possibilidade de prestação adequada dos serviços ou quando houvesse a necessidade de priorização de outro serviço de emergência.

Quanto a tais considerações, para ambas cabe a mesma ressalva: um ambiente que não pode ser regulado e em que as comunicações são completamente livres da aplicação da lei não aproveitam ao interesse público, bem como se mostra uma prestação inadequada. Pelo contrário, tal ambiente oferece demasiado risco aos consumidores, tendo em vista a viabilização de todo tipo de compartilhamento de material ilegal ou ofensivo à margem da proteção do Estado.

3.2 A lei de organizações criminosas (lei n.12.850/2013)

Ao analisar a legislação espanhola, Miguel Polaino-Orts demonstra que o tipo penal que trata das organizações criminosas é um claro exemplo de legislação que observa a periculosidade ao próprio delito pela necessidade de estabilização da norma antes mesmo da lesão para se mostrar eficaz, razão pela qual os meios de prova na lei n.12.850/2013, no ordenamento brasileiro, são particularmente invasivos, reduzindo a esfera de liberdade do indivíduo significativamente para lhe oferecer a segurança mínima que se espera (2014, p.104 e ss).

Neste sentido, a referida lei, em seu art.2º, estabelece pena de 3 a 8 anos, além de multa, para todo aquele que participa da organização criminosa, mas assemelha este àquele que "de qualquer forma, embaraça a investigação de infração penal que envolva organização criminosa" (§1º, art.2º). Aqui, no entanto, cabe destacar, não inclui aquele que deixa de oferecer as informações solicitadas. Por embaraçar, caberia interpretar aquele que oferece informações incorretas ou altera os dados antes de os fornecer. Para evitar malabarismos hermenêuticos incorretos, o art.21 estabelece expressamente a responsabilidade daquele que se omite no cumprimento de solicitações oficiais, com pena de seis meses a dois anos, além de multa.

As referidas solicitações podem advir do delegado de polícia ou do Ministério Público, mesmo sem autorização do juiz competente, caso solicitem "qualificação pessoal, a filiação e o endereço mantidos" (art.15). No caso das empresas de transporte (e aqui se entende as empresas que fazem transporte de bens, valores e pessoas), estas ainda devem manter um arquivo de todos os registros de viagens e dados de reservas dos últimos cinco anos, com acesso livre para o delegado de polícia e o Ministério Público (art.16).

De acordo com a lei de organizações criminosas, são partes obrigadas a fornecer as informações do art. 15, ainda que sem autorização judicial (bem como outras informações

relevantes, desde que com autorização expressa do juiz competente), a Justiça Eleitoral, as empresas telefônicas, as instituições financeiras, os provedores de internet e as administradoras de cartão de crédito. Quanto às concessionárias de telefonia fixa e móvel, faz-se uma especial exigência, a saber, a manutenção de um arquivo de todos os registros de identificação e ligações, desde internacionais a locais, dos últimos cinco anos de atividade.

Deve-se recordar que o art.5º, XII, da Constituição Federal, dispõe acerca do sigilo das comunicações como inviolável exceto em caso de investigação criminal nos termos da lei especial. Esta veio a ser definida pela lei n.9.296/96, que trata da interceptação telefônica, mas que não se confunde com o mencionado pela lei de organizações criminosas. Não se trata de uma interceptação feita pelos órgãos de investigação independente do consentimento da concessionária, mas da responsabilidade da própria empresa fornecer tais informações. Razão pela qual não se aprofunda aqui quanto à capacidade dos órgãos de investigação interpretarem a criptografia criada pelo aplicativo para proteção das comunicações, mas de um dever de colaborar.

Tal dever já se encontrava na lei n.8.625/93, em seu art.26, II, ao dispor das prerrogativas do Ministério Público, incluindo "requisitar informações e documentos a entidades privadas, para instruir procedimentos ou processo em que oficie". Por entidades privadas estão abrangidas as organizações que operam com comunicação, enquanto o art.15 da lei de organizações criminosas institui uma profundidade específica de tais informações, no qual se pode aqui compreender abrangidos, sem violar qualquer preceito hermenêutico penal, as empresas que, pela rede mundial de computadores, prestem o mesmo serviço das concessionárias de telefonia, tendo em vista ser finalidade buscada pelo usuário a mesma, com o diferencial do baixo custo.

3.3 Os mecanismos de compliance

Feita a análise dos artigos do marco civil da internet, que permitem a solicitação de dados produzidos na rede, bem como da lei de organizações criminosas de 2013, que disciplina o acesso no caso específico de organizações investigadas, facilitando o acesso antes previsto pela lei n.9.034/95, resta analisar se há a necessidade de maior regulamentação destes deveres para sua aplicabilidade.

Neste sentido, Vicente Greco Filho considera que os art. 15, 16 e 17 da lei n.12.850/2013 carecem de regulação pelas agências estatais setoriais (2014, p.66), que devem impor padrões para a coleta, armazenamento e proteção destes dados.

Sendo a Agência Nacional de Telecomunicações (ANATEL) o órgão regulador responsável, deve-se observar suas prerrogativas instituídas pela lei n.9.472/97. Sua

competência para regulação do aplicativo “WhatsApp” reside no art.69, parágrafo único, da referida lei, ao definir como telecomunicação “modo específico de transmitir informação, decorrente de características particulares de transdução, de transmissão, de apresentação da informação ou de combinação destas, considerando-se formas de telecomunicação, entre outras, a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens”. O caput deste artigo ainda atribui à ANATEL o papel de diferenciador das distintas formas de telecomunicação a partir de “sua finalidade, âmbito de prestação, forma, meio de transmissão, tecnologia empregada ou de outros atributos”.

Particularmente o art.19, V, define tal competência para editar normas administrativas. Em seu art.2º, dentre os deveres atribuídos à ANATEL, se encontram: a) adotar medidas que promovam a competição e a diversidade dos serviços, incrementem sua oferta e propiciem padrões de qualidade compatíveis com a exigência dos usuários (reforçado pelo art.5º); b) fortalecer o papel regulador do Estado; c) criar condições para que o desenvolvimento do setor seja harmônico com as metas de desenvolvimento social do País. Equivale aqui dizer que nenhum tipo de serviço pode ser tratado com diferenciação em sua regulação, mantendo o Estado deveres de controle e fiscalização efetiva, bem como garantir que os serviços oferecidos atendam aos fins apropriados para o desenvolvimento social. Mais do que qualquer proselitismo político do presente diploma legal, busca-se aqui garantir imparcialidade, segurança e concorrência. Em um modelo de regulação, não cabe ao setor privado determinar modelos ou condições, mas se adequar os moldes propostos por aqueles que representam o interesse comum.

Quanto a esta ponderação, há críticas consideráveis pela teoria da captura das agências reguladoras. Iniciada com Willian Jordan, em 1972, a teoria da captura surge com o objetivo de explicar a dinâmica existente entre as agências reguladores e os interesses do setor regulado. A conclusão de Jordan seria de que a regulação não era capaz de impedir a formação de cartéis, muitas vezes, pelo contrário, é mecanismo que auxilia o seu surgimento (PELTZMAN, 2004, p.85).

Analisando a obra de Bernstein, Fernanda de Abreu Pirotta apresenta o que seria um ciclo de existência das agências reguladoras, que resulta na final captura, a saber: a) fase inicial, em que há grande disposição e energia para o cumprimento dos fins determinados e os “interesses coletivos”; b) fase de maturidade, em que já não há mais o controle sobre os segmentos sob sua fiscalização e toda ação passa a depender das informações prestadas pelos agentes regulados, que por sua vez ganham cada vez maior relevância na determinação das políticas desenvolvidas; c) fase de velhice, em que há um acordo colusivo entre reguladores e

regulados, passando as agências a depender totalmente de seus controlados (PIROTTA, 2013, p.4).

Em grande medida, a tendência se explica pela superioridade organizacional das empresas em relação às agências. A sobreposição não apenas frustram os fins da agência, como ainda a transformam em filtro de mercado, sendo empecilho apenas às empresas menores, incapazes de se sobreporem a estas.

Outro fenômeno que justifica o ciclo de vida das agências consiste no *revolving door* ("Porta giratória"). Criado também na doutrina americana, consiste em um termo bastante comum no âmbito político para explicar certas decisões legislativas. Nestes casos, pensasse em uma relação entre o setor público e o setor privado intercambiando privilégios (capital, influência, informações). O trabalho de *lobby* e o uso de influências políticas para acordos entre países estrangeiros e empresas privadas nacionais poderiam ser exemplos clássicos. No âmbito das agências reguladoras, o que se vê é uma exigência de determinados conhecimentos técnicos para a outorga de um cargo público (em especial, um diretor ou presidente), extremamente justificada, mas que acaba por limitar aos indivíduos que possuem tais conhecimentos exatamente por atuarem enquanto administradores dos entes regulados. Assim, ainda que não inicialmente, a tendência é que, cedo ou tarde, estes administradores assumirão tais cargos com perspectivas opostas àquelas que motivaram a criação da agência (PIROTTA, 2013, p.5 e ss). Da mesma forma, embora haja o período mínimo exigido de afastamento, muitos ex-diretores das agências retornam às atividades, porém no âmbito dos entes regulados, o que lhe permite o uso de conhecimentos privilegiados e influência.

A conclusão mais simples a que se chega, embora extremamente desanimadora, é de que a captura seria um fenômeno natural, inerente ao modelo regulatório atual. Contudo, ainda que se deva considerar tais elementos, estes não podem servir de pretexto para furtar o regulador ou o regulado de buscar tais objetivos ou cumprir normas administrativas. Pelo contrário, são tais entraves desafios a serem dirimidos.

Neste sentido, a referida lei, em seu art.3º dispõe dos direitos do consumidor (aquele que faz uso dos serviços oferecidos), dentre os quais, destaca-se (inciso V) a "inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas". No art.4º listam-se como deveres deste consumidor ainda: a) utilizar adequadamente os serviços, equipamentos e redes de telecomunicações; b) respeitar os bens públicos e aqueles voltados à utilização do público em geral; c) comunicar às autoridades irregularidades ocorridas e atos ilícitos cometidos por prestadora de serviço de telecomunicações.

Portanto, ao definir a atuação do consumidor, compreendeu o legislador: a) que existem situações que ao poder público é permitido violar o sigilo de informações, estando tais situações devidamente previstas por leis (não por normas administrativas); b) que o uso gera responsabilidades, ainda que não haja uma supervisão ostensiva; c) que há o dever do consumidor fiscalizar ilícitos cometidos pela prestadora, não necessariamente cometidos por outros usuários.

O já mencionado art.19 define em seu inciso XII garante à ANATEL a competência para "expedir normas e padrões a serem cumpridos pelas prestadoras de serviços de telecomunicações quanto aos equipamentos que utilizarem". A isto equivale dizer que, caso haja uma técnica específica ou equipamento utilizado que impossibilite o cumprimento de deveres ou a segurança da rede (seja pela vulnerabilidade dos dados, seja por impedir a fiscalização), cabe a ANATEL determinar formas adequadas de uso e operação. O art.62, parágrafo único, apenas faz a ressalva de que para os serviços de interesse comum (aqueles que são oferecidos a todo interessado, não apenas um grupo específico) deve-se considerar, quando aplicadas restrições, o não prejuízo da exploração. No art.128, dispõe o legislador que, particularmente aos serviços no regime privado, deve a ANATEL observar: a) a liberdade como regra, constituindo exceção as proibições, restrições e interferências do Poder Público; b) os condicionamentos deverão ter vínculos, tanto de necessidade como de adequação, com finalidades públicas específicas e relevantes; c) o proveito coletivo gerado pelo condicionamento deverá ser proporcional à privação que ele impuser; d) haverá relação de equilíbrio entre os deveres impostos às prestadoras e os direitos a elas reconhecidos.

Apesar de todo o exposto, cabe aqui dizer que a ANATEL não se manifestou sobre possível regulação do aplicativo, bem como não emitiu qualquer parecer acerca dos casos de bloqueio do aplicativo. Tal posição poderia ser justificada pelo entendimento de que o aplicativo opera pelo sistema OTT (*over the top*), para o qual não se aplica a lei n.9.742/97, porém, tal diferenciação também não foi expressada em nenhuma normativa da ANATEL, à qual caberia, nos termos do art.69. De forma redundante, o Ministério das Comunicações prepara um projeto de lei a partir de uma consulta pública[1], inserindo ao art.5º do marco civil da internet o dever da ANATEL fiscalizar e normatizar o uso de aplicações de internet.

Diante de todo o exposto, cabe sintetizar os seguintes pontos: a) a comunicação por "WhatsApp", embora se diferencie das comunicações por telefonia móvel, consiste em uma forma de comunicação submetida à lei n.12.850/2013, bem como ao marco civil da internet;

[1] A minuta da consulta se encontra disponível no site do Ministério da Justiça, no link: http://pensando.mj.gov.br/marcocivil/texto-em-debate/minuta/, acessado em: 03/09/2016.

b) padrões de atividade e normas de conformidade (*compliance*) devem ser estabelecidos por agência reguladora e normas administrativas; c) como meio de comunicação cabe à ANATEL sua definição, diferenciação e regulação; d) juridicamente a ANATEL tem prerrogativas e meios para exercer a regulação ou, até mesmo, a isentar de maior regulação em benefício do interesse público; e) atualmente a ANATEL não tem se posicionado, enquanto o poder Executivo prepara um projeto de lei para pressionar a regulação do aplicativo.

3.4 Os termos e condições do "WhatsApp"

Diante do exposto, há de se analisar, portanto, os mecanismos do aplicativo "WhatsApp" que tem servido de justificativa pela empresa para se negar a cumprir as decisões judiciais. Para tanto, faz-se aqui uma análise detida dos principais pontos dos Termos e condições instituídos pelos desenvolvedores do aplicativo e que requerem adesão para a utilização dos serviços[2].

Primeiramente, quanto às informações coletadas pelo aplicativo, o contrato estabelece que, para o recebimento de mensagens e ligações, deve o usuário fornecer seu número, lista de contatos e álbum de fotos, podendo tanto a empresa, quanto terceiros, utilizar desse contato para se comunicar com o usuário. Ao coletar tais informações, o aplicativo ainda informa em seus termos e condições que o usuário pode incluir um "nome", uma foto de perfil e um "*status* para mensagens". Estes elementos compõem as informações básicas para a conta.

Outro nível de informações coletadas consiste na identificação dos horários de uso. O aplicativo registra quando o usuário está utilizando o aplicativo e quando foi a última vez que verificou suas mensagens recebidas. De acordo com os termos e condições do aplicativo, embora seja possível não permitir que os demais usuários tenham essa informação, não há ressalva que impeça a companhia de ter registrar tais informações. Pode parecer pouco, mas tais informações permitem compreender toda a rotina do usuário, horários de sono e trabalho, momentos de lazer e identificar momentos em que se deram certas atividades específicas.

O aplicativo ainda informa em seus termos e condições que as informações de seus usuários são coletadas não apenas a partir do próprio aparelho do usuário, mas dos aparelhos de outros usuários, o que lhes permite realizar as comunicações entre estes, bem como oferecer seus serviços àqueles que ainda não utilizam do aplicativo. Destaca-se, não há limitação quanto aos usuários. Estes podem ser pessoas físicas ou companhias, que utilizem o

[2] Os termos e condições a seguir mencionados se encontram na página do aplicativo, em inglês, e sem numeração de páginas. Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016. Até o momento, a última modificação dos mencionados termos ocorreu em 25 de agosto de 2016.

aplicativo para oferecer seus serviços e fazer cobranças, como restaurantes que façam entregas ou bancos que ofereçam crédito. É, portanto, o aplicativo "WhatsApp", um meio para captação de clientes. O aplicativo ainda pode ser usado por empregadores, que não precisam mais oferecer um "aparelho celular corporativo". Em suma, na mesma rede social se concentram os papéis de amigo, cliente e empregado, em que se faz uso de um mesmo número, nome e imagem de perfil.

Também há provedores de outros aplicativos que cooperam com o aplicativo "WhatsApp", seja para adquirir o aplicativo (por exemplo, loja Windows, Apple Store, Google Play, AppBrain), seja plataforma parceira que permita outros serviços, como o armazenamento de arquivos e seu compartilhamento (por exemplo, ICloud e Google drive, sites de jornais que permitam compartilhamento facilitado de notícias e artigos). Estas companhias garantem umas as outras o fornecimento de informações que permitam "operar, melhorar, compreender os usuários, adaptar os serviços, oferecer suporte e vender" seus serviços[3]. Apenas como exemplo, os termos e condições informa que tais aplicativos podem trocar entre si pesquisas que identifiquem perfis de usuários.

Dentre estes, destacam os termos e condições à cooperação entre os demais aplicativos da companhia "Facebook" (por exemplo, *Facebook* e *Instagram*). A recente mudança nos termos e condições ofereceu aos usuários do aplicativo "WhatsApp" a possibilidade da rede *Facebook* fazer uso dos contatos da lista telefônica do aparelho celular do usuário para sugerir novos contatos e direcionar propagandas (responsável pelo valor milionário da companhia no índice NASDAQ, sendo sua principal fonte de arrecadação). A cooperação entre estas ainda se estenderia, de acordo com os termos e condições do "WhatsApp", à prevenção de fraudes e combate ao compartilhamento de "spams" e softwares indesejados.

Outro tipo de informações coletadas pelo aplicativo são os chamados "cookies". Estes são relatórios, que podem ser complexos ou bastante simples, quanto às preferências do usuário e suas rotinas. Diversos sites da internet utilizam este recurso para saber a língua em que o usuário se sente mais confortável, por exemplo[4].

---

[3] No original: "We use all the information we have to help us operate, provide, improve, understand, customize, support, and market our Services". Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

[4] Para uma melhor compreensão do uso de "cookies", ver: http://www.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm, disponível em 05.09.2016.

Há ainda a coleta de informações quanto ao desempenho do aplicativo e diagnósticos de eventuais problemas, que são oferecidos pelo próprio aparelho, pelos usuários voluntariamente ou por aplicativos "parceiros" que utilizem seu sistema.

Por fim, em caso de desistência do usuário, o aplicativo informa que todas as informações e mensagens não entregues são automaticamente apagadas de seus servidores. Porém, a conta somente é apagada totalmente com o uso do próprio aplicativo, ou seja, não basta o desinstalar do aplicativo em seu aparelho. Ainda se faz a ressalva de que o encerramento da conta do usuário não retira as informações já compartilhadas com outros usuários (conversas, imagens, vídeos).

3.4.1 A criptografia do aplicativo

O aplicativo destaca que utiliza um sistema de criptografia chamado "end-to-end", em que somente os aparelhos conectados tem acesso ao que é compartilhado. Este sistema foi implantado em 2 de abril de 2016, após um dos diretores da companhia ser preso no Brasil por sonegar informações. Nem os servidores do aplicativo, nem autoridades, teriam acesso a tais conteúdos. A criptografia consiste em um código, em que uma determinada mensagem em código binário (conexão digital) é alterada para outro código, que somente pode ser interpretado por um software que conheça previamente o código que se está utilizando (chave). Dessa forma, os aparelhos conectados pelo aplicativo possuiriam, para cada comunicação, um código próprio, gerado por um algoritmo (aleatoriamente). A criptografia ainda pode ser produzida com repetidos códigos, ou seja, sua interpretação dependeria de mais "chaves", utilizadas na ordem correta.

Em função de tal sistema, o aplicativo ainda informa que não armazena em seus servidores as informações transmitidas. Assim que uma mensagem é recebida por um aparelho celular, ela é apagada dos servidores. Caso o aparelho perca seus registros, estes são irrecuperáveis. Se um aparelho não recebe um determinado conteúdo, o servidor o mantém em seu sistema pelo prazo de 30 dias ou até que o aparelho o receba[5]. Transcorridos os 30 dias, esta também será excluída do servidores.

Há, no entanto, algo que não fica claro. De acordo com os termos e condições:

> "Para melhorar a performance e entregar conteúdos de mensagem com maior eficiência, quando muitas pessoas compartilham uma foto ou vídeo popular,

[5] No original: "Our Privacy Policy helps explain our information (including message) practices. For example, we talk about what information we collect and how this affects you. We also explain the steps we take to protect your privacy – like building WhatsApp so delivered messages aren't stored and giving you control over who you communicate with on our Services". Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

> nós poderemos reter este conteúdo em nossos servidores por um período de tempo mais longo" (tradução livre)[6].

Dessa forma, duas considerações precisam ser feitas aqui: a) pelo volume de mensagens, não há a possibilidade de que todas sejam armazenadas por um longo período de tempo, mas os servidores podem manter registro de comunicações específicas; b) a criptografia não é essencial para o funcionamento do aplicativo, tendo sido implantado recentemente, o que permitiria a suspensão de seu uso ou a alteração de suas chaves sem que os usuários sejam informados. Em suma, tal qual as comunicações telefônicas, oferecidas pelas companhias, é possível oferecer interceptações às autoridades que investigam possíveis crimes, bem como iniciar um registro com o oferecimento de relatórios a partir de um determinado momento, ainda que o período anterior realmente seja inviável.

3.4.2 As regras de uso: jurisdição e compliance

Os termos e condições não deixam claro seus meios, mas destacam que aos gestores do aplicativo é atribuída a função de promotores da segurança ("safety and security") dos serviços oferecidos, podendo investigar atividades e violações dos termos e condições e garantir que seu uso esteja dentro da legalidade. Pode-se pensar aqui de uma violação por sabotagem ("hack") do aplicativo, ou ainda de seu uso em comunicações para divulgação de pornografia infantil, envio de vírus ("softwares" danosos ao aparelho celular) realização de fraudes ou ofensas graves e injúrias raciais.

De acordo com os termos e condições, são regras de uso: a) não violar a privacidade, publicidade, a propriedade intelectual e direitos da propriedade de usuários ou do próprio aplicativo; b) não compartilhar material ilegal, obseno, difamatório, ameaçador, intimidador, vexatório, que incite ódio, racista ou ofensivo à ética, que incite condutas ilegais, inapropriadas ou promova crimes violentos; c) que envolva notícias falsas, deturpadas ou declarações enganosas; d) que personifique de forma vexatória alguém; e) a prática de comunicações ilegais ou não permitidas, como mensagens em massa, "auto-mensagens", discagem automática e assemelhados; f) comunicações impessoais sem prévia autorização do WhatsApp[7].

---

[6] No original: "To improve performance and deliver media messages more efficiently, such as when many people are sharing a popular photo or video, we may retain that content on our servers for a longer period of time." Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

[7] No original: "You must access and use our Services only for legal, authorized, and acceptable purposes. You will not use (or assist others in using) our Services in ways that: (a) violate, misappropriate, or infringe the rights of WhatsApp, our users, or others, including privacy, publicity, intellectual property, or other proprietary rights; (b) are illegal, obscene, defamatory, threatening, intimidating, harassing, hateful, racially, or ethnically offensive, or instigate or encourage conduct that would be illegal, or otherwise inappropriate, including promoting violent crimes; (c) involve publishing falsehoods, misrepresentations, or misleading statements; (d)

Com relação aos aplicativos com os quais o "WhatsApp" é compatível, já mecionados acima, faz-se a ressalva de que estes possuem seus próprios termos e condições, que podem ser mais ou menos restritos, mas que delimitam a segurança e o sigilo das informações neles geridas.

A partir das restrições feitas, o aplicativo reserva para si a possibilidade de modificar, suspender ou encerrar definitivamente o acesso ou o uso de determinado usuário por qualquer razão que considerar necessária, ponderando como exemplares situações em que há violação "da letra ou do espírito" nos termos e condições, situações de lesão, risco ou possível exposição legal indesejada pelos gestores.

Tal vigilância recebe reforço nos termos e condições quando este exige o consentimento do usuário para coleta e encaminhamento de informações para "os Estados Unidos e outros países" em que são utilizados provedores ou firmados acordos de parceria "independentemente de onde se utilizem os serviços", tendo em vista que as leis, a regulação e os padrões de onde a "informação é armazenada e processada pode ser distinta" dos países em que se encontram os usuários[8].

Por utilizar os servidores da companhia "Facebook", o aplicativo tem seus dados armazenados nos Estados Unidos (Prineville, Ashburn, Forest City, Santa Clara, San Jose e San Francisco) e na Suécia (Lulea). Os termos e condições compreendem que por esta razão somente são aplicadas as leis destes países para regulação do armazenamento de informações. Quanto aos demais países, seria aplicável somente as leis que regulassem a importação e exportação de informações. Por esta razão, explica-se que o aplicativo não presta seus serviços: a) a pessoas, instituições e países aos quais se proíba o tráfego de informações; b) a qualquer pessoa que, por algum governo, esteja impedida de se comunicar desta forma; c) para o tráfego de informações sigilosas, como armas nucleares, químicas ou biológicas. De acordo com os termos, a aquisição do aplicativo no aparelho celular em um país em que tais serviços não possam ser prestados é vedada, tal qual a alteração da localização do IP

---

impersonate someone; (e) involve sending illegal or impermissible communications such as bulk messaging, auto-messaging, auto-dialing, and the like; or (f) involve any non-personal use of our Services unless otherwise authorized by us". Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

[8] No original: "WhatsApp cares about your privacy. WhatsApp's Privacy Policy describes our information (including message) practices, including the types of information we receive and collect from you and how we use and share this information. You agree to our data practices, including the collection, use, processing, and sharing of your information as described in our Privacy Policy, as well as the transfer and processing of your information to the United States and other countries globally where we have or use facilities, service providers, or partners, regardless of where you use our Services. You acknowledge that the laws, regulations, and standards of the country in which your information is stored or processed may be different from those of your own country". Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

("internet protocol", código numérico de identificação do aparelho para rastreamento na rede) por métodos irregulares.

Ao final dos termos e condições, fazem-se duas considerações: a) diz-se expressamente "nada em nossos termos nos isentará de cumprir com a lei"[9]; b) qualquer um dos termos, caso seja ilegal ou impraticável, não será válido, sem que os demais sejam invalidados. Dessa forma, resta compreender quais leis se aplicam na regulação de tais termos e quais os desafios de se considerar a informação armazenada em servidores no estrangeiro.

3.5 O problema da lei penal no espaço

De acordo com a já mencionada lei n.9.742/93, em seu art.18, cabe ao poder executivo, regular a participação estrangeira no capital de prestadora de serviços de telecomunicações, tendo em vista o interesse nacional. Neste caso, o Ministério das Comunicações imporia um limite para investidores estrangeiros na "Facebook Serviços Online do Brasil LTDA", algo que não existe atualmente. Além deste fator, pelos art.170 a 172, a companhia, que faz uso de comunicação via satélite, está submetida ao uso preferencial de satélites brasileiros, sendo permitido o uso de estrangeiro na falta de similar.

Uma vez estabelecida no Brasil, a companhia pode operar com comunicações em território nacional, mas não há qualquer limitação quanto aos servidores ou uma regulação particular da importação ou exportação de informações. O art.170, particularmente, atribui à ANATEL competência "independentemente de o acesso a ele [satélite] ocorrer a partir do território nacional ou do exterior". Pela vagueza, a legislação brasileira acaba por considerar tal comunicação, bem como todas as demais comunicações via satélite, independentemente da origem do sinal ou seu local de armazenamento, como uma comunicação em território nacional e totalmente regulada por seu ordenamento. Vale dizer, ocupa-se a legislação com o tráfego, pois, de fato, é esta que importa ao consumidor final.

Desta forma, a "Facebook Serviços Online do Brasil LTDA" estaria obrigada, nos mesmos casos em que a lei permite a interceptação telefônica, a colaborar em função da comunicação que é viabilizada no Brasil, ainda que tal regulação gere efeitos extraterritoriais em função do armazenamento no estrangeiro.

3.6 Decisões contrárias nos tribunais brasileiros

Diante de todo o analisado, pode-se ressaltar que normas administrativas seriam responsáveis por delimitar obrigações e modelos para cooperação entre o referido aplicativo e

[9] No original: "Nothing in our Terms will prevent us from complying with the law". Disponível em: https://www.whatsapp.com/legal/, acessado em 05/09/2016.

as autoridades responsáveis pelas investigações e juízo de crimes em que couber a interceptação das comunicações.

Porém, na falta de tal regulamentação, a jurisprudência brasileira segue incerta. Apesar dos mencionados casos de bloqueio, a decisão da comarca de Lagarto, em Sergipe, em 2 de maio de 2016, trouxe outras decisões curiosas.

No dia 3 de maio de 2016, o juiz federal titular da 7ª Vara criminal federal da subseção de São Paulo expediu uma liminar, com base no art.251, código de processo penal, para suspender a decisão do juiz estadual, tendo em vista que esta afetava o uso do aplicativo para citações e envio de provas, bem como comunicação entre advogados, que fora regulada pela portaria n.10/2010, com o nome de "Processo-cidadão". Pela impossibilidade da liberação unicamente da linha utilizada pela 7ª Vara, todos as linhas deveriam ser liberadas por incorrer em conflito de competência (decisão estadual contraria a portaria federal). Dessa forma, crê-se que o magistrado se compreendeu ainda capaz de impedir qualquer processo futuro de falência ou extinção da prestadora de serviços, pois igualmente violaria a referida portaria, chancelada, em suas palavras, pelos órgãos superiores.

A segunda decisão ocorreu em 19 de junho, do mesmo ano, em um juízo de admissibilidade que concedeu cautelar solicitada na Arguição de descumprimento de preceito fundamental (ADPF) n.403 de Sergipe, encaminhada pelo Partido Popular Socialista (PPS), considerando que, a despeito da falta de regulação, a interpretação dada pelo magistrado de Lagarto era incorreta e violava o interesse da coletividade. Pelo principio da proporcionalidade e por compreender o aplicativo como meio de democratização da comunicação, o Min. Ricardo Lewandowski suspendeu o bloqueio determinado pela magistrada de Duque de Caxias.

3.7 A operação "Hashtag"

Por fim, quanto ao atual cenário brasileiro, destaca-se um último caso envolvendo o aplicativo. Em 21 de julho de 2016, às vésperas do início das Olimpíadas de verão no Rio de Janeiro, a Polícia Federal realizou a prisão de dez pessoas sob a alegação de envolvimento com o grupo Estado Islãmico. O Ministério da Justiça informou que as investigações lograram sucesso em função do acompanhamento de conversas entre os integrantes do grupo pelo aplicativo WhatsApp. Não houve esclarecimento quanto à forma como se deu essa interceptação pela polícia federal.

O portal eletrônico de notícias da rede "O Globo" veiculou um artigo levantando possíveis formas de interceptação das comunicações, a saber: a) a participação de agente infiltrado, nos termos da seção III da lei n.12.850/2013, que estaria também incluído nas

comunicações pelo aplicativo; b) a obtenção do backup da conversa, feito automaticamente por um dos aplicativos parceiros do "WhatsApp" (*e.g.* Google drive ou ICloud) e oferecido às autoridades brasileiras; c) a instalação de um *malware* (um *software* espião capaz de coletar dados após sua tradução pela chave criptográfica); d) a clonagem do número dos investigados com auxílio de uma das operadoras[10].

Com exceção da cooperação por um aplicativo parceiro, que demandaria uma abertura também nas políticas de oferecimento de informações, bem como a participação de agente infiltrado, permitida em casos bastante restritos pela legislação, tanto a clonagem quanto a instalação de um *malware* são operações tecnicamente simples, que estariam a disposição não apenas do Estado, o que careceria de uma regulação para limitar seu uso indiscriminado, mas também de terceiros mal-intencionados, demonstrando fragilidades sérias do sistema.

4. Conclusões: possibilidades de "enforcement"

Ao final da presente análise, cabe pontuar: 1) diante dos recentes casos de bloqueio do aplicativo "WhatsApp", as decisões encontraram fundamento nas leis n.12.850/2013 e 12.965/2014; b) embora tais leis tenham abertura para tanto, faz-se necessária uma regulação específica que define a forma que como tais informações devem ser prestadas e modelos de controle; c) a responsabilidade para tal regulação, ainda que o aplicativo possua arquivos armazenados no exterior, o que é indiferente para a legislação atual, é da ANATEL, mas até o momento esta não o fez, enquanto o Ministério das Comunicações prepara uma reforma do marco civil da internet; d) embora os termos e condições do aplicativo "WhatsApp" permita a colaboração com as autoridades brasileiras, esta apenas carece de regulação para que o aplicativo não permaneça à margem da lei brasileira, pois em termos práticos, há meios técnicos muito mais simples para se obter tais informações; e) a suspensão das atividades é sanção administrativa aplicável pela ANATEL, processualmente (em âmbito penal) cabe a pena de multa e prisão; f) a obtenção de tais informações por meio outros, que dispensam totalmente a pena de bloqueio das atividades como instrumento processual, deve igualmente ser regulada pela ANATEL.

Diante de tal panorama, pode-se pensar apenas uma *enforcement* (mecanismos que garantam a efetividade de suas normas) para garantir a adequação do aplicativo "WhatsApp" ao ordenamento jurídico. Existem sanções que podem ser aplicadas pela ANATEL, com base

[10] A notícia foi produzida por um técnico em informática na seção de tecnologia do sítio eletrônico. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-o-governo-teria-grampeado-terroristas-no-whatsapp.html, acessado em: 05.09.2016.

no art.173, da lei n.9.742/97, em função do descumprimento das normas de regulação. Ou seja, a partir do momento em que existem condutas determinadas esperadas, se a prestadora do serviço permanece à margem, pode-se pensar em uma das seguintes medidas: a) advertência; b) multa; c) suspensão temporária; d) declaração de inidoneidade[11].

Por esta razão, a regulação do *compliance* para este determinado modelo de comunicação é urgente, sob pena de favorecimento de uma companhia em razão de seu tamanho. Existem disponíveis diversos outros aplicativos que poderiam ser utilizados pelos usuários comuns ou adotados em portarias de fóruns. Na defesa da livre concorrência, a partir da regulação, será privilegiado o aplicativo que melhor se adaptar ao modelo brasileiro de regulação, ao invés da regulação se adaptar aos interesses da maior companhia.

Para tanto, deve-se pensar cuidadosamente as exigências destas normas administrativas, delimitando com precisão: a) padrões de segurança das comunicações (atualmente vulneráveis); b) possíveis flexibilizações em função de requisições feitas sob os termos da legislação brasileira; c) tempo determinado de armazenamento seguro e necessário dos conteúdos produzidos nos servidores do aplicativo; d) canais controlados de denúncia pelos próprios clientes diante de possíveis abusos por outros usuários; e) clareza das políticas de uso adequado e das informações coletadas pelo aplicativo; f) mecanismos de conscientização da importância de instrumentos de segurança e da cooperação por meio de denúncias.

5. Bibliografia

GRECO FILHO, Vicente. **Comentários à Lei de Organização criminosa: Lei n.12.850/13.** São Paulo, Saraiva, 2014.

MENDRONI, Marcelo Batlouni. **Crime organizado: aspectos gerais e mecanismos legais.** São Paulo, Juarez de Oliveira, 2002.

PELTZMAN, **A Teoria Econômica da Regulação depois de uma década de desregulação.** In: PAULO TODESCAN LESSA MATTOS (coord.) Regulação econômica e democracia: o debate norte-americano, Editora 34, São Paulo, 2004, pág. 81-127.

PIROTTA, **O fenômeno da captura nas agências reguladoras.** Jus Navegandi, Teresina, ano 10, n.1142, 10 de outubro de 2013.

POLAINO-ORTS, Miguel. **Lições de direito penal do inimigo.** São Paulo, Liber Ars, 2014.

[11] Não se fez menção aqui à caducidade em função de não haver necessidade para concessão de tais serviços.

SILVEIRA, Renato de Mello Jorge; SAAD-DINIZ, Eduardo. **Compliance, direito penal e lei anticorrupção.** São Paulo, Saraiva: 2015.

ZANATTA, Rafael A.F. **Nota técnica sobre a decisão de bloqueio do WhatsApp.** Disponível em: http://www.idec.org.br/pdf/nota-tecnica-bloqueio-whatsapp.pdf. Acessado em 05.09.2016.