UNIVERSIDADE PRESBITERIANA MACKENZIE

CAMILA GIACOMETTI COLASUONNO

A IMPLANTAÇÃO DA CRIPTOGRAFIA DO WHATSAPP E A OBRIGAÇÃO DE FORNECIMENTO DE DADOS PELO FACEBOOK

São Paulo

2022

CAMILA GIACOMETTI COLASUONNO

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADOR: PROF. DR. JOÃO RICARDO BRANDÃO AGUIRRE

São Paulo

2022

CAMILA GIACOMETTI COLASUONNO

A IMPLANTAÇÃO DA CRIPTOGRAFIA DO WHATSAPP E A OBRIGAÇÃO DE FORNECIMENTO DE DADOS PELO FACEBOOK

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovada em:

BANCA EXAMINADORA

_____

Examinador(a):

_____

Examinador(a):

_____

Examinador(a):

AGRADECIMENTOS

Gostaria de agradecer, em primeiro lugar, à minha querida família, a quem serei eternamente grata por me proporcionar tudo para que eu pudesse chegar até aqui e, acima de tudo, por ser meu maior exemplo de Responsabilidade e Amor. É difícil expressar a gratidão que sinto por ter vocês na minha vida.

À esta Instituição e aos meus nobres Professores, que me forneceram o conhecimento e ensino de excelência necessário para o meu crescimento e amadurecimento acadêmico. Os Senhores foram minha grande fonte de inspiração nessa jornada. Um especial agradecimento ao meu querido Orientador, João Ricardo Brandão Aguirre, por me ajudar a desenvolver este trabalho.

Aos meus amigos, que tive o privilégio de conhecer durante a Graduação e compartilhar muitos momentos inesquecíveis, Bruno Grando, Cezar Liu, Gabriela Sanches, Igor Fonzar, Isabela Piva, Lucas Soriano, Luís Henrique Junqueira, Marília Emília Hutter, Matheus Nori, Raphael Faria, Thiago Sampaio, Vitor Fugita e Wagner Diniz. O meu carinho por vocês é fruto do nosso companheirismo e cumplicidade durante esses cinco anos e, por isso, muito obrigada. E, por fim, ao meu grande Amigo, Dr. Celso Charuri, por me ensinar o verdadeiro significado da Amizade e mostrar o caminho para a construção de um Mundo Bem Melhor.

O homem pretende ser imortal, e para isso defende princípios efêmeros. Um dia, inexoravelmente, descobrirá que para ser imortal deverá defender princípios absolutos. Nesse dia, morrerá para a carne, efêmera, e viverá para o espírito, eterno. Será imortal.

Dr. Celso Charuri

A IMPLANTAÇÃO DA CRIPTOGRAFIA DO WHATSAPP E A OBRIGAÇÃO DE FORNECIMENTO DE DADOS PELO FACEBOOK

Camila Giacometti Colasuonno[1]

Resumo: O presente trabalho tem como principal objetivo analisar juridicamente e tecnicamente a impossibilidade de fornecimento de dados pelo Facebook, em razão da imersiva utilização da criptografia de ponta a ponta pelo aplicativo WhatsApp e sua implicação no deslinde das quebras de sigilo, que tem como objeto a obtenção de informações sobre determinado usuário, a ser consequentemente identificado e responsabilizado por seus atos ilícitos na internet. Ao longo do estudo, serão abordados temas em discussão nos Tribunais Superiores, bem como aspectos técnicos sancionados pelo Marco Civil da Internet, bem como na Constituição Federal, a fim de expor os desafios enfrentados hoje nas ações de quebra de sigilo, ora à mercê do cumprimento da obrigação imposta pelo Juiz de fornecimento de dados criptografados pelo WhatsApp, que por sua vez insiste na impossibilidade da satisfação da ordem judicial. Para isso, será necessário esclarecer o caminho percorrido pela ação de quebra de sigilo, quais as principais espécies de dados pessoais, quem são os provedores de aplicação e de conexão, bem como a relação jurídica entre o Facebook e o WhatsApp e o funcionamento da guarda de dados pela plataforma.

Palavras chaves: Provedor de aplicação, criptografia de ponta a ponta, quebra de sigilo, Marco Civil da Internet, WhatsApp.

Abstract: The main purpose of this paper is to legally and technically analyze the impossibility of providing data by Facebook, due to the immersive use of end-to-end encryption by the WhatsApp application and its implication on the unraveling of breaches of secrecy, which aims to obtain information about a particular user, to be consequently identified and held responsible for their illegal acts on the Internet. Throughout the study, issues under discussion in Higher Courts will be addressed, as well as technical aspects sanctioned by the Marco Civil da Internet, and the Federal Constitution, in order to expose the challenges faced today in the actions of breach of confidentiality, now at the mercy of

[1] Graduanda da Faculdade de Direito da Universidade Presbiteriana Mackenzie

compliance with the obligation imposed by the judge to provide encrypted data by WhatsApp, which in turn insists on the impossibility of satisfaction of the court order. To do this, it will be necessary to clarify the path taken by the action of breach of secrecy, what are the main species of personal data, who are the application and connection providers, as well as the legal relationship between Facebook and WhatsApp and the operation of data storage by the platform.

Key words: Application provider, end-to-end encryption, breach of secrecy, Internet civil Mark, WhatsApp.

Sumário: I. Introdução II. Dados pessoais: Principais características e espécies III. Os Principais Registro Eletrônicos para o estudo do caso III.a. Endereço de IP III. Registros de acesso à internet III.c. Registros de conexão à internet IV. Provedores de Conexão e de Aplicação à luz do Marco Civil da Internet V. Classificação do WhatsApp como provedor de aplicação VI. A Criptografia do WhatsApp: funcionamento e características que obstam na identificação final de usuários VII. O descumprimento da ordem de fornecimento de dados e o entendimento jurisprudencial atual VIII. Conclusão.

I. INTRODUÇÃO

Este trabalho tem como objetivo analisar a quebra de sigilo de dados para a obtenção de informações capazes de identificar o usuário responsável quando da postagem de ilícitos ocorridos no ambiente do WhatsApp, em atenção ao dever suportado pelo provedor de aplicação de armazenamento dos dados dentro do prazo legal de 6 meses, definido pelo art. 15 do Marco Civil da Internet.

O estudo que se segue pretende desenvolver uma reflexão acerca de um tema complexo e com dimensões sutis que serão abordadas com base no Marco Civil da Internet (MCI), além de relevante apoio no entendimento jurisprudencial pátrio atual e no desenvolvimento de teses doutrinárias do ordenamento jurídico brasileiro, bem como de fontes do direito comparado, observando as dificuldades encontradas em ações de quebra de sigilo envolvendo o provedor de aplicação WhatsApp e abordando aspectos técnicos de registros eletrônicos capazes de identificar o usuário perseguido, a fim de expor as dificuldades do fornecimento de dados pela plataforma.

Para isso, será percorrido o histórico de relacionamento entre o Facebook e o WhatsApp, demonstrando qual a relação jurídica existente entre eles – em especial, a formação de grupo econômico - para então passar a analisar de maneira objetiva a responsabilidade e legitimidade das empresas quando figuram no polo passivo de demandas envolvendo a quebra de sigilo.

Dando continuidade à análise dos provedores de aplicação, serão abordados elementos técnicos sobre o mecanismo singular utilizado pela plataforma WhatsApp para o tratamento dos dados, que serão fundamentais para compreender os motivos da alegada impossibilidade de fornecimento dos mesmos e, consequentemente, as dificuldades enfrentadas no deslinde das quebras de sigilo.

Ante a negativa de fornecimento de dados evidenciada em estudo jurisprudencial e de ações de obrigação de fazer e não fazer perante o Tribunal de Justiça de São Paulo, a aplicação de medidas coercitivas é ímpar para a tentativa do cumprimento das medidas liminares e sentenças deferidas pelo Juízo. Em ações de quebra de sigilo em que há a participação de provedores de internet, por exemplo, a eficácia das astreintes são evidentes, uma vez que a forma de tratamento de dados difere-se da criptografia. Não serão abordados temas envolvendo a inviolabilidade de conversas e mensagens trocadas no ambiente do WhatsApp, mas sim aspectos técnicos que dizem respeito a maneira de gestão de dados e seu impacto no deslinde dos processos e na responsabilidade do usuário final, ou seja, do agente causador de atos ilícitos. Dito isso, será analisada a efetividade da aplicação de astreintes pela autoridade judiciária ao provedor WhatsApp, na posição do polo passivo das demandas cíveis, com enfoque na garantia do cumprimento da obrigação de fornecimento de dados.

Por fim, esta análise pretende evidenciar a cultura de negativa de fornecimento de dados do WhatsApp, baseada no argumento de impossibilidade de disponibilização dos mesmos, em razão da implantação da criptografia utilizada e o prejuízo decorrente dessa forma de tratamento de dados, afastando por completo a possibilidade de identificação cabal do responsável pelo ato ilícito praticado no ambiente do App de conversa e, por conseguinte, sua responsabilização nas esferas cível, criminal e trabalhista.

II. DADOS PESSOAIS: PRINCIPAIS CARACTERÍSTICAS E ESPÉCIES

A fim de compreender as implicações de uma quebra de sigilo, bem como aprofundar em questões técnicas envolvendo os registros eletrônicos, é de suma importância entender o

objeto da ação em questão, percorrendo inicialmente sobre as diferentes espécies de dados pessoais e suas características frente a um universo de informações sensíveis.

O dado pessoal é todo e qualquer informação capaz de identificar um indivíduo, seja por seu sexo, religião, características comportamentais, posicionamento político e assim por diante, isto é, à letra do art. 5º da LGPD, *dado pessoal é informação relacionada a pessoa natural identificada ou identificável*. E, dentro do grupo de dados pessoais, existem os dados diretos indiretos, sendo o primeiro dado de cadastro, como RG, CPF, endereços de e-mail, nome e telefone e, o segundo, informações sobre o sexo, profissão, idade, hábitos de consumo, comportamentos etc.

Além destes, têm-se os chamados dados pessoais sensíveis, capazes de identificar a pessoa por meio de informações ligados à sua saúde, cor da pele, origens étnicas e raciais, e por diante.

Existem, também, os dados chamados anonimizados, que não são capazes de identificar uma pessoa por si só, somente por outros meios técnicos específicos a eles aplicados.

Os dados pseudonimizados, por sua vez, são o enfoque da presente pesquisa, dotados de proteção técnica, de impossível associação com o usuário, apenas quando ligados com informações adicionais armazenadas por seu controlador. Estas são características de dados criptografados e de *hash* como autenticação, por exemplo.

De toda sorte, independente da espécie do dado em tratamento, os princípios legais estabelecidos pelo Art. 6º da Lei Geral de Proteção de Dados e artigos 2º, 3º e 4º do MCI, permeiam integralmente por todos eles, de modo que assegura os direitos e garantias dos princípios da liberdade de expressão, do princípio da transparência e da publicidade quando do tratamento de informações pessoais no ambiente digital.

III. OS PRINCIPAIS REGISTROS ELETRÔNICOS PARA O PRESENTE ESTUDO

Para o presente estudo, é de extrema importância reconhecer o conceito de registros eletrônicos chamados estáticos, que representam em sua categoria os dados de *Internet Protocol* (IP), bem como entender a definição de números de registros de acesso e conexão à internet.

III. a. ENDEREÇO DE IP

O IP, conhecido como *internet protocol*, por Vinton Cerf and Robert Kahn[2], é a numeração atribuída pelo provedor de conexão - sujeito que será explicado em tópico futuro - ao usuário quando este se conecta à internet, por meio de um provedor de internet.

Nas palavras do Professor Marcel Leonardi:

> A priori, o endereço IP, tal como telefone, é uma atribuição lógica dada ao usuário para se conectar à internet. Tal atribuição lógica determina uma geolocalização e pode ser acessada por todos que o reconhecem. Contudo, com relação à internet, o endereço IP é muito mais que uma atribuição lógica, é um caminho aberto de possibilidades de se poder acessar muito mais dados do seu usuário. Se o usuário estiver num dispositivo móvel, o endereço IP informa onde ele está em todos os momentos. É com base no endereço IP que o usuário troca dados com servidores no mundo todo.[3]

Este número de IP, portanto, é necessário para acessar as plataformas dos provedores de aplicação de internet, que contempla outros dados referentes ao usuário, como a geolocalização formada pelo conjunto de data, hora e fuso horário, armazenados pelos provedores de conexão, chamados conjuntamente de dados cadastrais.

III. b. REGISTROS DE ACESSO À INTERNET

São dados armazenados pelos provedores de aplicação, definidos pelo conjunto de informações atreladas à data e hora de uso de uma determinada aplicação de internet, a partir de um endereço de IP, conforme caracterização atribuída pelo art. 5º, III, do MCI.

III. c. REGISTROS DE CONEXÃO À INTERNET

Os registros de conexão à internet, por sua vez, são dados armazenados pelos provedores de conexão, contendo informações relativas ao momento em que determinado usuário se conectou à rede mundial de computadores por meio da internet.

IV - PROVEDORES DE CONEXÃO E DE APLICAÇÃO À LUZ DO MARCO CIVIL DA INTERNET

O provedor de conexão à internet é a pessoa física ou jurídica responsável por atribuir um número de IP ao usuário que pretende acessar à internet. É o provedor que concede o

---

[2] LEINER, Barry M.; CERF, Vinton G.; CLARK, David. D; [et al]. Ob. cit. p. 107
[3] LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo:Juarez de Oliveira, 2005. Pag. 100

acesso à internet, papel desempenhado por exemplo pelas empresas de telefonia móvel como TIM, CLARO e VIVO.

Leciona Victor Hugo:

> o provedor de acesso à internet fornece uma série de IP (protocolos de internet) válidos (fixos ou dinâmicos), para que o usuário possa se conectar à internet. Assim, o usuário de internet, com o endereço IP atribuído pelo provedor de conexão, conecta-se com os provedores de aplicações de internet. O dispositivo de informação e comunicação, com o seu endereço IP já atribuído, conecta-se com os provedores de aplicações de internet dessa forma. (...) Provedor de conexão à internet é a pessoa física ou jurídica, que atribui endereços lógicos de acesso necessários aos usuários para se utilizarem das redes de informação e comunicação[4].

Isto é, o provedor de conexão possui o dever legal intransferível de armazenar os registros de conexão à internet, definidos pelo conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados, pelo prazo de 1 (um) ano, consoante o artigo 13, do Marco Civil da Internet.

O provedor de aplicação, por sua vez, corresponde pelo responsável do ambiente no qual o usuário pretende navegar, podendo ser um site buscador ou um aplicativo, isto é, algum sítio existente na rede mundial de computadores. Conforme leciona o Professor Victor Hugo, "o provedor de Aplicações de internet é a pessoa jurídica que presta serviços ou comercializa produtos nas redes de informação e comunicação que não envolvam acesso e conexão lógica de usuários"[5]

O provedor de aplicação possui como principal obrigação, a guarda dos registros de acesso a aplicações de internet, definidos pelo prazo de 6 (seis) meses, determinado pelo art. 15, do Marco Civil da Internet.

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de

[4] GONÇALVES, Victor Hugo P. Marco Civil da Internet Comentado. São Paulo. Grupo GEN, 2016. Pág. 83. E-book. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 02 nov. 2022.

[5] GONÇALVES, Victor Hugo P. Marco Civil da Internet Comentado. São Paulo. Grupo GEN, 2016. Pág. 85. E-book. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 02 nov. 2022

> internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> § 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.
>
> § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Para tanto, é necessário que "no exercício da sua atividade empresarial, além da busca do lucro e da prestação dos melhores serviços e produtos, deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança."[6]

Os provedores de aplicação, segundo a lei, deverão acolher os usuários de internet em seus serviços, seja uma rede social ou um site, devendo armazenar as informações a ele atreladas e ao seu acesso. No entanto, o art. 15 do MCI não deixa claro quais os dados e informações que deverão ser guardadas pelo provedor. Isto porque, ao acessar o domínio de um provedor de aplicação, o usuário de internet, como já mencionado, traz consigo diversas informações, como endereço de IP, a geolocalização (data, hora e fuso horário do acesso), sistema operacional e demais dados atrelados aos cookies. Esta é mais uma questão enfrentada pelos provedores de aplicação e de acesso que, em razão das especificidades técnicas de determinados dados, não conseguem atingir o cumprimento exigido pelas autoridades, ou seja, as empresas de aplicação muitas vezes não sabem 1) quais informações a autoridade pede e 2) como conseguir essas informações.

Em resumo, é o viés da doutrina majoritária brasileira, conforme trecho colacionado:

> Estabelecer direitos e deveres sem os meios e garantias para o exercício deles é torná-los inócuos, inexequíveis. O Marco Civil, como "constituição" da internet, em

[6] GONÇALVES, Victor Hugo P. Marco Civil da Internet Comentado. São Paulo. Grupo GEN, 2016. Pág. 85. E-book. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 02 nov. 2022

> muitos momentos, falha fragorosamente no estabelecimento de garantias para a fruição e apropriação dos direitos. Há sempre algo que não se resolve, que não se implementa por falta de regulamentação ou clareza normativa. E o *caput* do art. 15 caminha para essa direção de direitos e deveres que não têm direcionamento nem forma.[7]

Em resposta à essas perguntas, o judiciário entende (em vários casos) pelo enquadramento da hipótese de obstrução à justiça e resistência do cumprimento da ordem, aplicando então as sanções previstas no art. 12 do MCI, sendo a fixação de multa a mais frequente.

V. O WHATSAPP COMO PROVEDOR DE APLICAÇÃO

Dentre as categorias de provedores propostas pelo Marco Civil da Internet, o WhatsApp se caracteriza como provedor de aplicação, mediante a definição do art. 11, e cujas atribuições legais encontram respaldo nos artigos 14, 15 e 19 do mesmo diploma legal. Isto porque, a empresa não fornece o serviço de conexão à internet propriamente dito, mas sim acolhe o usuário, conectado à internet, para acessar sua plataforma, aplicativo, site ou rede social e está sujeito, portanto, à legislação pátria em casos de armazenamento de dados tratados no território nacional, consoante o art. 11 do MCI.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

Logo, quando tratamos de decisões judiciais que determinam o armazenamento e/ou o fornecimento de dados do WhatsApp provenientes do território nacional nas ações de quebra de sigilo, deverá o provedor atentar-se ao art. 19, no sentido de cumprir com sua obrigação legal, mediante ordem específica, contendo, por exemplo a URL do conteúdo danoso a ser indisponibilizado da plataforma.

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu

[7] GONÇALVES, Victor Hugo P. Marco Civil da Internet Comentado. São Paulo. Grupo GEN, 2016. Pág. 126. E-book. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 02 nov. 2022

> serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Posto isso, é importante mencionar que, para a guarda de dados, é exigido dos provedores de conexão e de aplicação a utilização de meios técnicos e equipamentos informáticos que possibilitem a identificação dos dados dos usuários, a fim de que as informações exigidas sejam devidamente apresentadas pela empresa responsável pelo dado. Caso contrário, consoante previsão do Professor Marcel Leonardi, da Fundação Getúlio Vargas, a ausência de armazenamento de dados poderá inviabilizar, inclusive por outros meios, a identificação ou localização dos responsáveis pelos atos ilícitos, sujeitando-se a responder solidariamente pelo ato cometido por terceiro que não foi identificado, em razão de sua própria omissão[8].

O artigo 19 do MCI, propõe a proteção da liberdade de expressão e o impedimento à censura quando tratar da responsabilidade do provedor de aplicação por danos decorrentes de conteúdos publicados por terceiros, de modo que resta nítida a causa para a responsabilização.

É cediço que os provedores de aplicação não podem prever e nem devem adiantar o conhecimento do conteúdo a ser gerado pelo usuário, isto é, conhecer previamente aquilo que será postado ou publicado pelo sujeito, com o intuito de censurá-lo, por isso, a expressa vedação no diploma legal da internet sobre a importância da liberdade de expressão e sobretudo da proteção a ela concedida, em concordância com o art. 5º, IX e a proibição da censura prevista no art. 220, § 2º, da Carta Magna.

Aos provedores de aplicação é também previsto no art. 15, sobre o qual colaciona-se a ementa a seguir, que remete ao entendimento do Tribunal de Justiça de São Paulo.

> "Apelação. Marco Civil da Internet. Ação de tutela antecipada requerida em caráter antecedente. Pedido de exclusão de perfil falso do Instagram e para fornecimento de dados técnicos e pessoais de usuário. Sentença de procedência. Insurgência da requerida. Acolhimento. Na qualidade de provedora de aplicações de internet, a requerida está sujeita ao dever de guarda apenas de informações relativas aos registros de acesso à aplicação. Inteligência dos artigos 15 e 5º, VIII, da Lei 12.965/2014. Distinção dos deveres de guarda

[8] LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo:Juarez de Oliveira, 2005, p. 228

> entre provedores de aplicação e provedores de acesso à internet. Estes é que tem a obrigação legal de fornecer os dados pessoais/cadastrais do usuário. Jurisprudência do E. Superior Tribunal de Justiça. Constatação do cumprimento da obrigação legal da recorrente de fornecer as informações compreendias no seu dever de guarda. Ônus de sucumbência. Inexistência. Necessidade de provimento jurisdicional para apresentação das informações requeridas. Ausência de resistência à pretensão. Precedentes desta E. Corte. Recurso provido. Sentença reformada." (TJSP; Apelação Cível 1091461-32.2020.8.26.0100; Relator (a): Christiano Jorge; Órgão Julgador: 6ª Câmara de Direito Privado; Foro Central Cível - 41ª Vara Cível; Data do Julgamento: 25/10/2022; Data de Registro: 25/10/2022).

Posto isso, insta pontuar um breve histórico de relacionamento do Facebook com o WhatsApp, a fim de compreender a relação existente entre as empresas.

É cediço que a empresa WhatsApp Inc. é a desenvolvedora do aplicativo WhatsApp, a qual foi adquirida pelo Facebook em uma operação finalizada em outubro de 2014 pelo valor de, aproximadamente, US$ 22 bilhões, conforme amplamente divulgado pela mídia à época da aquisição[9].

A partir disso, portanto, o Facebook passou a administrar o funcionamento do aplicativo WhatsApp, ficando responsável por administrar seu conteúdo, bem como responder por suas obrigações legais e jurídicas adquiridas pelo WhatsApp.

A título de exemplo, vide as empresas cujo Facebook é responsável, a seguir listadas[10].

- Facebook Payments Inc.;
- Meta Platforms Technologies, LLC e Meta Platforms Technologies Ireland Limited;
- WhatsApp LLC e WhatsApp Ireland Limited;
- Novi Financial, Inc. e as entidades afiliadas globais da Novi (individual e coletivamente, "Novi");

---

[9] Disponível em https://g1.globo.com/economia/negocios/noticia/2014/10/preco-de-compra-do-whatsapp-pelo-facebook-sobe-us-22-bilhoes.html#:~:text=Fundador%20do%20WhatsApp%20receber%C3%A1%20incentivo%20para%20permanecer%20na%20empresa.&text=O%20Facebook%20finalizou%20a%20aquisi%C3%A7%C3%A3o,do%20Facebook%20nos%20%C3%BAltimos%20meses Acessado em 23.10.2022, às 12:46.

[10] Disponível em https://www.facebook.com/help/111814505650678 Acessado em 24.10.2022, às 8:52.

- CrowdTangle da Meta;
- Facebook Pagamentos do Brasil Ltda.

Diante disso, em razão da matriz Facebook Inc. dispor da representante localizada no Brasil Facebook Serviços Online do Brasil LTDA, inscrita no CNPJ 13.347.016/0001-17, possui uma extensão da gestão e administração da matriz com relação às demais empresas por ela adquiridas. Para Patrícia Peck, o caráter da territorialidade das empresas, diante de determinada obrigação legal é de suma importância, uma vez que "se o provedor de aplicação não tivesse filial no Brasil, não era aplicada a lei brasileira; no entanto, com a mudança (da lei), mesmo que a atividade seja exercida por pessoa jurídica no exterior será aplicada a lei brasileira."[11].

A plataforma WhatsApp além de ser dependente do Facebook Brasil, possui, por óbvio, mesma gestão administrativa e é daí que se justifica a caracterização de grupo econômico entre o Facebook e o WhatsApp, no cenário da responsabilização e, consequentemente, da legitimidade passiva do Facebook Brasil nas demandas cíveis de quebra de sigilo.

Sobre o tema, vide entendimento uníssono da jurisprudência pátria.

> "AGRAVO DE INSTRUMENTO – Ação de obrigação de fazer – Decisão que concede em parte antecipação dos efeitos da tutela para que o agravante suspenda a conta do aplicativo WhatsApp de linha telefônica – Alegação de ilegitimidade passiva – Inocorrência – Empresas que pertencem ao mesmo grupo econômico – Legitimidade passiva da agravante para responder pelo aplicativo, tendo em vista que é o único representante do grupo econômico no Brasil – Decisão confirmada – Recurso desprovido" (TJSP, 17ª Câmara de Direito Privado, AI nº 2246331-61.2019.8.26.0000, Rel. Des. Irineu Fava, Julgado em 15.04.2020)
>
> "APELAÇÃO CÍVEL. Ação de Obrigação de Fazer. Sentença de Procedência. Inconformismo. Não acolhimento. Ilegitimidade passiva "ad causam" não configurada. Pretensão de obtenção dos registros

[11] PINHEIRO, Patrícia P. Direito Digital. [São Paulo]: Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 03 nov. 2022.

relativos à Empresa Whatsapp. Possibilidade. Empresa Ré que integra o mesmo grupo econômico, sendo a única sediada neste Território. Via eleita adequada para obtenção da pretensão. Sentença mantida. Ratificação, nos termos do artigo 252, do Regimento Interno. RECURSO NÃO PROVIDO, majorando-se a verba honorária em sede recursal para o valor de R$2.000,00 (dois mil reais).” (TJSP, 2ª Câmara de Direito Privado, Apl. nº 1071227-97.2018.8.26.0100, Rel. Des. Penna Machado, Julgado em 25.03.2020)

“AGRAVO DE INSTRUMENTO – AÇÃO DE OBRIGAÇÃO DE FAZER – FACEBOOK – WHATSAPP – TUTELA DE URGÊNCIA – DETERMINAÇÃO PARA FORNECER DADOS CADASTRADOS E NÚMEROS DE IPS – LEGITIMIDADE – POSSIBILIDADE – APLICATIVOS PERTENCENTES AO MESMO GRUPO ECONÔMICO – (...) É fato público e notório que a empresa Whatsapp foi adquirida pela empresa norte-americana Facebook Inc., sendo o Whatsapp pertencente ao mesmo grupo econômico do Facebook Serviços Online do Brasil Ltda., restando nítida a relação jurídica entre elas – Restando evidenciado nos autos a probabilidade do direito invocado, diante da violação de direito de personalidade, bem como o perigo da demora, é de se manter a decisão agravada que deferiu parcialmente a antecipação dos efeitos da tutela, determinando aos agravantes que informassem os dados cadastrados dos titulares, e números dos IP’s (Internet Protocol), das contas do aplicativo Whatsapp, sob pena de multa diária.” (TJMG, 13ª Câmara Cível, AI nº 1.0000.19.037362-1/001, Rel. Des. Rogério Medeiros, Julgado em 08.08.2019)

“AGRAVO DE INSTRUMENTO – LIMINAR – RETIRADA DE IMAGEM DO BANCO DE DADOS DO SERVIÇO WHATSAPP – REQUISITOS – PRESENÇA– POSSIBILIDADE – RECURSO DESPROVIDO. Para o deferimento do pedido de liminar devem estar presentes os requisitos fumus boni iuris e periculum in mora, de modo que se caracterize a plausibilidade aparente da pretensão aviada e o

> perigo fundado de dano, antes do provimento final. Restando evidenciado nos autos a plausibilidade do direito invocado, notadamente diante da violação de direito de personalidade, bem como o perigo da demora, é de se manter o deferimento do pedido liminar para retirada de imagens íntimas do banco de dados do serviço Whatsapp. Recurso desprovido.(...) No tocante as alegações da agravante quanto à ilegitimidade passiva e impossibilidade de cumprimento da obrigação imposta, diante da aquisição do aplicativo Whatsapp pelo Facebook não ter sido concluída, como bem explicitado pelo Des. Salles Rossi, do Tribunal de Justiça de São Paulo, quando do Julgamento do agravo de instrumento nº 2114774-24.2014.8.26.0000:"A alegação da agravante de que não possui gerência sobre o Whatsapp (que, por seu turno, tem sede apenas nos EUA) não se sustenta, conquanto notória a aquisição pelo FACEBOOK do referido aplicativo(que somente no Brasil, conta com mais de 30 milhões de usuários).Bem por isso, o fato de Whatsapp não possuir representação em território nacional não impede o ajuizamento da medida em face do FACEBOOK (pessoa jurídica que possui representação no país, com registro na JUCESP e, como já dito, adquiriu o aplicativo referido).Some-se a isso que serviço do Whatsapp é amplamente difundido no Brasil e, uma vez adquirido pelo FACEBOOK e somente este possuindo representação no país, deve guardar e manter os registros respectivos, propiciando meios para identificação dos usuários e teor de conversas ali inseridas." (Agravo de instrumento n° 1.0148.14.003020-3/001, Rel. Des. Amorim Siqueira,9ª Câmara Cível do TJ/MG. Julgado em 07.04.2015)

Logo, é fato notório que a empresa Facebook Serviços Online do Brasil LTDA possui legitimidade para figurar no polo passivo da demanda judicial que envolva a ocorrência de ilícitos dentro da plataforma de troca de mensagens.

VI - A CRIPTOGRAFIA DO WHATSAPP: FUNCIONAMENTO E CARACTERÍSTICAS QUE OBSTAM NA IDENTIFICAÇÃO FINAL DE USUÁRIOS

Como ponto de partida, é importante entender a definição de criptografia de ponta a ponta, a fim de compreender o mecanismo técnico utilizado nas mensagens trocadas dentro do aplicativo de conversas do WhatsApp e seus consequentes impactos para o presente estudo.

A criptografia é um mecanismo técnico que permite esconder o conteúdo da informação transmitida, por meio da aplicação de algoritmos capazes de confundir o dado, embaralhando, assim, a mensagem e impedindo o acesso e desvendamento do mesmo por um terceiro. O algoritmo aplicado nada mais é do que uma chave específica concedida à mensagem, que só poderá ser "descriptografada" pelo próprio detentor da informação transmitida.

Já a criptografia de ponta a ponta, especificamente, corresponde à codificação dos dados desde o momento do envio da informação até o recebimento da mensagem pelo destinatário, ou seja, o conteúdo é protegido por toda a sua existência (por todo o seu caminho). Nesses casos, cada sujeito dessa troca (emissor e receptor) recebe uma chave diferente, cuja numeração atribuída a uma é complementar à outra. Sobre o funcionamento da chave, explica Marinna Coutinho:

> [...] dois tipos de chaves são usados para cada ponta da comunicação, uma chave pública e uma chave privada. As chaves públicas estão disponíveis para as ambas as partes e para qualquer outra pessoa, na verdade, porque todos compartilham suas chaves públicas antes da comunicação. Cada pessoa possui um par de chaves, que são complementares. [...] O conteúdo só poderá ser descriptografado usando essa chave pública [...] junto à chave privada [...]. Essa chave privada é o único elemento que torna impossível para qualquer outro agente descriptografar a mensagem, já que ela não precisa ser compartilhada.

Nesse sentido, o próprio WhatsApp traz publicidade para o fato de que nem ele próprio ou o Facebook são capazes de acessar os dados criptografados, em razão da alta complexidade de um sistema tão incorruptível que até seu criador tem sua acessibilidade limitada. Vide o entendimento da empresa WhatsApp INC. sobre sua criptografia.

> O WhatsApp define criptografia de ponta a ponta como comunicações que permanecem criptografadas em um aparelho controlado pelo remetente para um aparelho controlado pelo destinatário do qual terceiros não podem acessar esse conteúdo, nem mesmo o WhatsApp ou a empresa controladora Facebook. Um terceiro nesse contexto significa qualquer organização que não seja o remetente ou destinatário que participa diretamente da conversa. (...) Todas as mensagens do WhatsApp são enviadas com o mesmo protocolo de sinal destacado acima. O WhatsApp considera todas as mensagens, chamadas de voz e chamadas de vídeo enviadas entre todos os aparelhos controlados por um usuário remetente e todos os

> aparelhos controlados por um usuário destinatário como protegidos com a criptografia de ponta a ponta.[12]

Para elucidar, vide o fluxograma simplificado contendo o funcionamento do sistema de criptografia do WhatsApp:

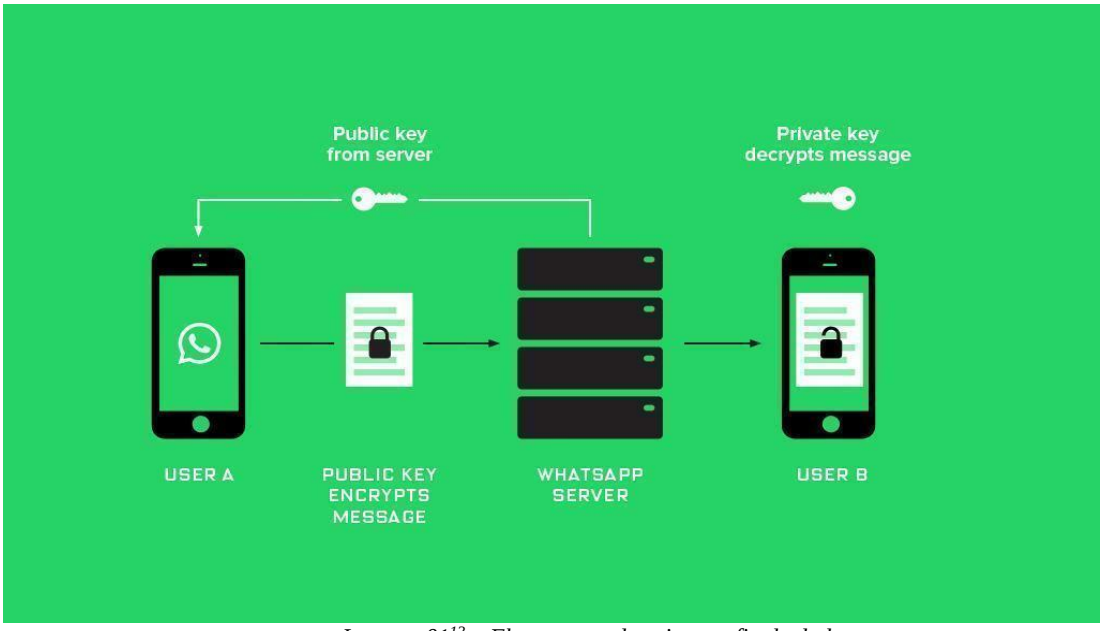


Imagem 01[13] – Fluxograma da criptografia de dados

O maior grau de monitoramento que o WhatsApp tecnicamente possui, é por meio da implementação da nova política de uso nas conversas, permitindo que os próprios usuários controlem a disseminação de conteúdo em massa, ou seja, vídeos, fotos e links encaminhados diversas vezes para grupos e contatos, que podem ou não conter informações inverídicas.

Em entrevista com a Revista InternetLab, o Head do WhatsApp, Will Cathcart, esclarece como se opera a nova ferramenta do aplicativo:

> Ao clicar no botão, o aplicativo sugere uma pesquisa sobre o assunto na internet. A ideia é que, com uma consulta rápida a fontes confiáveis, você possa descobrir se aquilo é falso ou não. Caso o usuário concorde, ele será direcionado automaticamente à busca pelo navegador padrão do celular ou computador. Como o WhatsApp possui criptografia de ponta-a-ponta, o servidor do app não armazena e nem consegue ver o conteúdo das mensagens — o julgamento do que é suspeito é baseado somente no espalhamento do link. Também na tentativa de reduzir a

[12] Visão Geraç da Criptografia do WhatsApp – Documento Técnico. Versão 6 atualizada em 15 de novembro de 2021. Disponível em: https://scontent-gru2-2.xx.fbcdn.net/v/t39.8562-6/278602514_356472073207936_2447507657138466122_n.pdf?_nc_cat=102&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=Gp3xe0eLLBYAX_H8ptU&_nc_ht=scontent-gru2-2.xx&oh=00_AT_SiHVnaEc6Px_Dv1XuoxDkfrMU9mlVo5edyDCw15jusg&oe=6355487A. Acessado em 19.10.2022, às 10:12

[13] Disponível em https://brasil.elpais.com/brasil/2016/04/06/tecnologia/1459942001_217614.html Acessado em 03.10.2022, às 20:46

> disseminação de conteúdos enganosos, o WhatsApp já limitou mais de uma vez a quantidade de encaminhamentos de mensagens.[14]

Essa ferramenta de controle prévio de disseminação de informações inverídicas ou parcialmente verdadeiras, foi desenvolvida para assumir importante papel durante as eleições presidenciais no país em 2018, a fim de combater a manipulação da opinião pública constituída pela disseminação de notícias falsas, já que as campanhas eleitorais tiveram crescente destaque com sua veiculação via grupos de WhatsApp.

A utilização do aplicativo no Brasil, principalmente, permitiu que os candidatos mais visados para o cargo da Presidência no ano de 2018 semeassem a chamada "computational propaganda", de Woolley & Howard (2018), definida pela aplicação de artifícios técnicos, como algoritmos, automação e ciência de dados na comunicação de informações ou desinformações nas mídias sociais. Ou seja, por meio da implementação desta ferramenta de controle de informações veiculadas propositalmente, foi possível atingir a opinião das massas, direcionando determinado conteúdo à grupos específicos de eleitores. Com isso, as campanhas políticas tiveram efeitos muito positivos no número de votos à Jair Messias Bolsonaro que, ao final, auxiliaram em sua efetiva eleição.

Em resumo, apesar da inserção dessa técnica de controle indireto do conteúdo pelo próprio usuário, o WhatsApp ainda não possui um mecanismo, pelo menos até então conhecido, que permita acessar diretamente o conteúdo ou obter os dados atrelados ao usuário e à mensagem encaminhada.

Ainda sobre a inviolabilidade das mensagens trocadas, vide a eficácia da criptografia analisada em trecho de artigo técnico publicado pela MacMaster University, em Hamilton, US.

> The latter two functionalities are what make WhatsApp uniquely vulnerable to misinformation campaigns. End-to-end encryption makes it difficult for researchers and fact checkers to see what messanges are being shared and find out the extent of the dissemination of the misinformation on the app. This effectively makes WhatsApp a "black-box of viral information" (Wang, 2018).[15]

Dessa forma, resta evidente a impossibilidade de acesso pela plataforma ao conteúdo da mensagem trocada, bem como dos registros de acesso dos usuários, fato que certamente

---

[14] Disponível em https://www.tecmundo.com.br/software/155822-novo-recurso-whatsapp-ajuda-verificar-algo-fake-news.htm Acessado em 02.11.2022, às 10:58

[15] Bots and Fake News: **The Role of WhatsApp in the 2018 Brazilian Presidential Election**. Latifa Adbin , Masters of Globalization, MacMaster University. Hamilton, ON - Canada. 2019

impossibilita o cumprimento de ordens judiciais que determinam o fornecimento de tais dados seja no âmbito civil ou penal.

VII. O DESCUMPRIMENTO DA ORDEM DE FORNECIMENTO DE DADOS E SUA CONSEQUÊNCIA

Hoje, existe forte entendimento no Tribunal de Justiça de São Paulo no sentido de que a criptografia implicaria sim no fornecimento de dados e demais tratamento de dados, bem como na identificação do agente, pelo provedor de aplicação, em razão da alta complexidade técnica do funcionamento da criptografia, conforme verifica-se a seguir.

> "Agravo de Instrumento – Ação indenizatória - Danos morais – Tutela antecipada deferida para retirar conteúdo ofensivo e impor a corré Facebook o dever de identificar e fornecer dados dos usuários, inclusive referentes ao WhatsApp e Twitter – Alegada impossibilidade técnica de identificação dos usuários do aplicativo WhatsApp, sem a apresentação do número das linhas telefônicas – Alegação relevante, mercê da existência de sistema de criptografia ponto-a-ponto e da dinâmica de uso do aplicativo, a envolver o salvamento de imagens nos próprios aparelhos dos usuários – Matéria que demanda dilação probatória – Excluída, por hora, a obrigação de identificar os usuários do aplicativo WhatsApp – Impossibilidade de impor ao FACEBOOK obrigações atinentes a identificação de usuários do TWITTER – Pessoas jurídicas diversas que não integram o mesmo grupo econômico – Recurso parcialmente provido. (...) De fato, na presente fase de cognição sumária, subsiste relevância da alegação da agravante sobre a impossibilidade técnica da exclusão de imagens e mensagens compartilhadas a partir de número telefônico cadastrado no aplicativo Whatsapp. **agravante Facebook Brasil tem condições técnicas de identificar os usuários do aplicativo WhatsApp, que propagaram a suposta mensagem ofensiva, sem que haja qualquer indicação do número de telefone, pois trata-se de questão eminentemente técnica**, que depende de elucidação mediante instrução probatória, inexistente, até o momento, notícia de algum

> caso equivalente definitivamente julgado em que já tivesse sido solucionada essa problemática.” (TJSP; Agravo de Instrumento 2287086-30.2019.8.26.0000; Relator (a): Moreira Viegas; Órgão Julgador: 5ª Câmara de Direito Privado; Foro Central Cível - 11ª Vara Cível; Data do Julgamento: 11/03/2020; Data de Registro: 11/03/2020) .

Em mesmo sentido, o reconhecimento pelo Tribunal da impossibilidade de identificação, remoção ou bloqueio de dados, ou seja, de qualquer forma de tratamento pela plataforma, é latente, fundamentação que ora trouxe a inadmissão do recurso, conforme abaixo.

> “AÇÃO COMINATÓRIA C.C. INDENIZAÇÃO POR DANOS MORAIS. INTERNET. Pretensão da autora de remover e bloquear a sua fotografia contendo informação de que estaria oferecendo serviços sexuais veiculada no "Facebook" e "Whatsapp", além de indenização por danos morais. Sentença de parcial procedência. Irresignação das partes. **Prova pericial que é clara no sentido de que não é possível à ré identificar, remover ou bloquear a fotografia da autora, tampouco impedir que seja novamente postada ou enviada por meio do "Whatsapp".** Aplicativo que utiliza criptografia de ponta a ponta. Valor do código "hash" que não se mostra eficiente à identificação clara e específica do conteúdo ofensivo que se pretende excluir do "Facebook". Retirada de um conteúdo da Internet que deve ser determinada pelo Poder Judiciário e, como requisito de validade, deve ser identificado claramente. Necessidade de indicação da URL da postagem denunciada. Inteligência do § 1º do art. 19 da Lei nº 12.973/2014. Autora que não indicou corretamente as URLs das postagens. Impossibilidade de cumprimento da decisão que concedeu a tutela de urgência e da r. sentença que a confirmou. Inviável a responsabilização civil da ré, nos termos do "caput" do art. 19 da Lei nº 12.973-2014. Ação improcedente. Sentença reformada. RECURSO DA AUTORA DESPROVIDO, PROVIDO O DA RÉ.” (TJSP; Apelação Cível 1047696-50.2016.8.26.0100; Relator (a): Alexandre

> Marcondes; Órgão Julgador: 6ª Câmara de Direito Privado; Foro Central Cível - 32ª Vara Cível; Data do Julgamento: 10/12/2020; Data de Registro: 10/12/2020)

A legitimidade passiva, já analisada, e o ônus do Facebook nas ações civis de quebra de sigilo são indiscutíveis, portanto, quando tratamos da obrigação legal imposta à empresa, uma vez caracterizada como provedora de aplicação, deve armazenar os dados atrelados aos registros de aplicação e demais dados a eles atrelados nos moldes do art. 15 do MCI, pelo período de 6 (seis) meses, sob pena de aplicação das sanções previstas no art. 12 do MCI.

Em virtude da incapacidade técnica, portanto, resta ao Juiz condenar o Facebook, na maioria dos casos envolvendo a quebra da criptografia do WhatsApp, em perdas e danos, ante a perda do objeto da demanda, quando imprescindível para a identificação do usuário e, posteriormente, para sua responsabilização nas esferas aplicáveis ao ato ilícito cometido. Responsabilização esta que descende não da ausência de identificação do agente suspeito, mas pelo não cumprimento da obrigação legal de mera guarda ou fornecimento de dados, conforme pode-se destacar na ementa a seguir.

> “RESPONSABILIDADE CIVIL - Ação de obrigação de fazer, cumulada com preceito cominatório, objetivando compelir a provedora ré Facebook a fornecer dados de acesso e conexões à aplicação de internet "WhatsApp Web", no período de 29/07/2019 a 02/07/2019, na conta da autora (55 11 996902120), com todas as informações disponíveis, incluindo IP de origem, navegador usado, data de conexão, duração da conexão e ações realizadas, bem como a preservação dos registros - Sentença de procedência para cumprimento da decisão liminar de fl. 34, com todas as informações disponíveis, sob pena de multa por descumprimento em R$ 1.000,00 diários, limitada a R$ 50.000,00, nos termos da decisão complementar de fl. 101 - Inconformismo exclusivo da empresa demandada - Descabimento - Legitimidade passiva do Facebook caracterizada - Representante do aplicativo no Brasil, que integra o mesmo grupo econômico - Interesse processual presente - Medida que visa identificar usuário infrator por prática de atos ilícitos, ante fundado receio de violação ao sigilo de informações pessoais da autora -

> Obrigação de identificação reconhecida pela Lei do Marco Civil da Internet - Exegese dos artigos 7º, 10º, 15º, §1º e 22, § único da mencionada lei - Multa cominatória - Cabimento - Finalidade coercitiva - Apelo desprovido." (TJSP; Apelação Cível 1125383-98.2019.8.26.0100; Relator (a): Galdino Toledo Júnior; Órgão Julgador: 9ª Câmara de Direito Privado; Foro Central Cível - 5ª Vara Cível; Data do Julgamento: 02/12/2020; Data de Registro: 02/12/2020)

Isto porque, na maioria das quebras de sigilo, é necessário não só o dado fornecido pelo provedor de aplicação, mas também do fornecimento de dados pelo provedor de conexão. Explica-se. Conforme já suscitado anteriormente, a navegação do usuário na internet gera dois eventos, sendo eles: (i) a atribuição de um endereço IP pelo provedor de conexão que permite ao usuário conectar-se à internet e (ii) o rastro de seu acesso à plataformas, sites e redes sociais traduzido pelos registros de acesso à aplicações de internet, de responsabilidade dos provedores de aplicação.

Dessa forma, quando é determinada a identificação de um usuário da internet pela autoridade judiciária, é necessário percorrer o "caminho inverso" do acesso daquele agente, por meio da quebra do sigilo de ambos os elementos informacionais do provedor de aplicação e do provedor de conexão, pois a obtenção de informações de somente um dos provedores não é suficiente para a cabal identificação do agente, conforme demonstrado em infográfico abaixo.

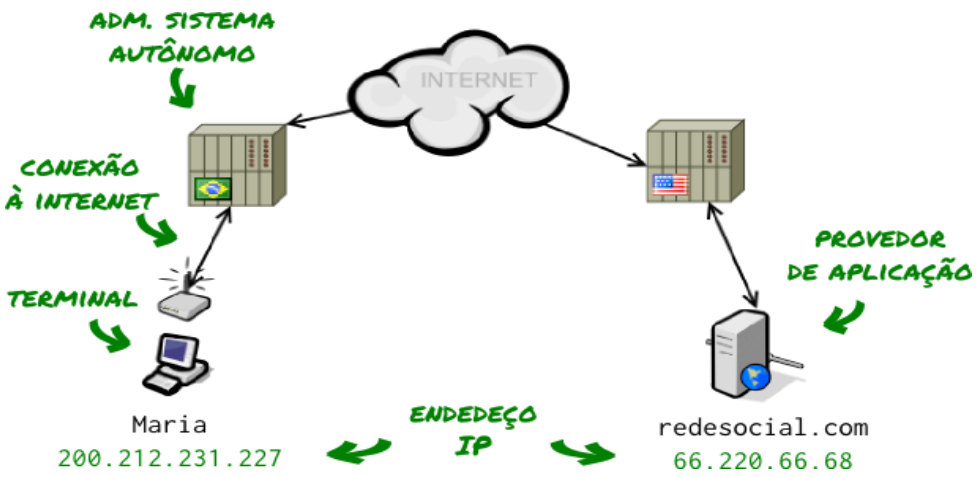


Imagem 02[16] *– Infográfico de acesso à internet*

[16] Disponível em: https://cpiciber.codingrights.org/marco-civil/ Acessado em 03.10.2022, às 20:13.

Logo, com o fornecimento de ambos os dados, bastaria “cruzá-los” a fim de chegar a um único terminal, isto é, ao ator do ilícito praticado. O que significa que, resgatando o cenário do presente estudo, na hipótese de o WhatsApp apresentar as informações atreladas ao acesso à aplicação, estaria contribuindo para a junção e comparação de dados atrelados ao autor do crime e não necessariamente identificando cabalmente o usuário perseguido.

De todo modo, ainda que a jurisprudência dos Tribunais analise juridicamente todos os aspectos da aplicação do art. 15 do MCI, acompanhado da fixação de multa por descumprimento, quando cabível, a fim de ver a obrigação legal respeitada pelo Facebook, não é suficiente para superar o desafio técnico de quebra da criptografia do WhatsApp. Os esforços desmedidos do judiciário para a resolução da questão são mais que necessários, até para manter a segurança jurídica e dar efetividade à lei, mais especificamente ao Marco Civil da Internet.

Contudo, é indispensável um estudo técnico-científico de todas as nuances do sistema de segurança adotado pelo WhatsApp em detrimento à proteção da privacidade do usuário, que enfrenta o outro lado da balança de combate ao anonimato vedado expressamente pelo art. 5º, IV da CF, de modo que inúmeras demandas de perseguição do responsável pelo cometimento de atos ilícitos na internet caem por terra, considerando a complexa arquitetura de dados do aplicativo.

Sendo assim, nas ações cíveis, “o sigilo dos dados cadastrais e de conexão é protegido pelo direito à privacidade, que não prevalece em face do ato ilícito cometido, pois, do contrário, permitir-se-ia que o infrator permanecesse no anonimato”[17].

VIII. CONCLUSÃO

Ante o exposto, resta evidente a área cinzenta formada pela perseguição de dados de usuários quando os atos ilícitos são cometidos dentro do aplicativo do WhatsApp, administrado pelo Facebook. Conforme evidenciado pelas ementas abarcadas, a empresa é bombardeada por decisões desfavoráveis, com a fixação de multas por descumprimento, tendo em vista a ausência do fornecimento de informações fundamentais para a satisfação das quebras de sigilo.

[17] LEONARDI, Marcel. **Determinação da responsabilidade civil pelos ilícitos na rede**. In Responsabilidade civil na internet e nos demais meios de comunicação. SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos. (Coords.). 2.Ed. São Paulo: Saraiva, 2012, p. 107

Foi possível compreender por meio do presente estudo que, por um lado, as sanções aplicáveis ao Facebook em concordância com o Marco Civil da Internet visam compelir o provedor de aplicação a cumprir com sua obrigação legal de armazenamento de registros eletrônicos de acesso pelo período de 6 (seis) meses e, de outro, a incapacidade técnica para tanto, inibindo a efetividade das ações de quebras de sigilo.

Não obstante, conclui-se que o admirável esforço do judiciário em aplicar o Marco Civil da Internet às provedoras de conexão e aplicação se mostra hoje insuficiente para verificar inequívoca efetividade da lei, no que tange o grande objetivo das demandas de quebra de sigilo, seja na esfera cível, trabalhista ou criminal, de obtenção de dados e informações suficientemente concretas e fidedignas, para a cabal identificação do responsável dotado do manto do anonimato.

Apesar do válido argumento sobre a incapacidade técnica do WhatsApp de prover os dados determinados, não podemos nos esquecer que por trás de um delito digital, há uma vítima, de calúnia, difamação, de fotos íntimas vazadas, de suas obras intelectuais violadas e muitos outros direitos desrespeitados.

Em resumo, as quebras de sigilo contra o Facebook, por vezes são encerradas por uma mera execução em perdas e danos, já que o fornecimento de dados pelo WhatsApp é um fator totalmente utópico. Em outras palavras, é desafiador e simultaneamente angustiante testemunhar casos concretos em que empresas notórias perderem sua reputação e idoneidade por articulações falsas propagados pelo WhatsApp ou até pessoas físicas lesadas por golpes financeiros, sem que haja uma responsabilização do usuário. Independente da natureza da vítima, pessoa física ou jurídica, os atos cometidos podem causar danos materiais e morais que, dentro do cenário da inviolabilidade da criptografia, se tornam irreparáveis.

REFERÊNCIAS

ABDIN, Latifa. Bots and Fake News: **The Role of WhatsApp in the 2018 Brazilian Presidential Election**. Masters of Globalization, Publicado por MacMaster University. Hamilton, ON - Canada. 2019.

CPICIBER. Nota Técnica da Sociedade Civil para a CPI de Crimes Cibernéticos. Disponível em: https://cpiciber.codingrights.org/marco-civil/ Acessado em 03.10.2022, às 20:13.

DA REUTERS. Facebook finaliza aquisição do WhatsApp por US$ 22 bilhões. Via G1. Publicado em 06/10/2014 16h55 - Atualizado em 07/10/2014 20h40. Disponível em https://g1.globo.com/economia/negocios/noticia/2014/10/preco-de-compra-do-whatsapp-pelo-facebook-sobe-us-22-bilhoes.html#:~:text=Fundador%20do%20WhatsApp%20receber%C3%A1%20incentivo%20para%20permanecer%20na%20empresa.&text=O%20Facebook%20finalizou%20a%20aquisi%C3%A7%C3%A3o,do%20Facebook%20nos%20%C3%BAltimos%20meses Acessado em 23.10.2022, às 12:46.

FAQ.WHATSAPP. Visão Geração da Criptografia do WhatsApp – Documento Técnico. Versão 6 atualizada em 15 de novembro de 2021. Disponível em: https://scontent.fcgh13-1.fna.fbcdn.net/v/t39.8562-6/309931030_1190816831854425_566987148724978105_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=ae5e01&_nc_ohc=q-2GzlUQn1YAX8NvW_l&_nc_ht=scontent.fcgh13-1.fna&oh=00_AfDdjAQLHWmZe6n911jVrjkaKT9DRwL7LARurSOHhlqFPQ&oe=6372C336 em 19.10.2022, às 10:12.

GONÇALVES, Victor Hugo P. Marco Civil da Internet Comentado. São Paulo. Grupo GEN, 2016. E-book. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 02 nov. 2022.

KLEINA. Nilton. Novo recurso do WhatsApp ajuda a verificar se algo é Fake News. Publicado em TechMundo, em 04.08.2020, às 10:30. Disponível em https://www.tecmundo.com.br/software/155822-novo-recurso-whatsapp-ajuda-verificar-algo-fake-news.htm Acessado em 02.11.2022, às 10:58.

LEINER, Barry M.; CERF, Vinton G.; CLARK, David. D; [et al]. Ob. cit.

LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo:Juarez de Oliveira, 2005.

LEONARDI, Marcel. **Determinação da responsabilidade civil pelos ilícitos na rede**. In Responsabilidade civil na internet e nos demais meios de comunicação. SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos. (Coords.). 2.Ed. São Paulo: Saraiva, 2012.

META. As Empresas da Meta. Disponível em https://www.facebook.com/help/111814505650678 Acessado em 24.10.2022, às 8:52.

PINHEIRO, Patrícia P. Direito Digital. [São Paulo]: Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 03 nov. 2022.

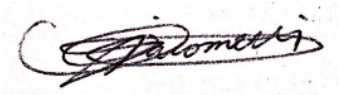
ZURIARRAIN, José Mendiola. O que é a criptografia no WhatsApp e porque é tão importante. Publicado em EL País, em 07.04.2016, 17:44 BRT. Disponível em https://brasil.elpais.com/brasil/2016/04/06/tecnologia/1459942001_217614.html Acessado em 03.10.2022, às 20:46

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Camila Giacometti Colasuonno discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº (inserir TIA), período (inserir período), turma (inserir turma), tendo realizado o TCC com o título: "A IMPLANTAÇÃO DA CRIPTOGRAFIA DO WHATSAPP E A OBRIGAÇÃO DE FORNECIMENTO DE DADOS PELO FACEBOOK" sob a orientação do(a) Professor(a) João Ricardo Brandão Aguirre declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 11 de novembro de 2022.



Assinatura do discente