06

DA VALIDADE DOS ELEMENTOS DE INFORMAÇÃO POLICIAL COLHIDOS COM PERFIL FICTÍCIO EM REDES SOCIAIS

THE VALIDITY OF THE POLICY INFORMATION ELEMENTS GATHERED WITH FAKE PROFILE IN SOCIAL MEDIA

Daniel Sclifo Zucon[1]
Rodrigo Bueno Gusso[2]
Anselmo Firmo Cruz[3]

Resumo: O presente estudo versa sobre os limites de utilização de um perfil de usuário falso pela polícia judiciária, com fins investigativos, em redes de relacionamento. Parte do princípio da atipicidade da conduta de sua criação, cujos meandros desse tema não serão objeto de análise. Serão abordados, em seguida, a imprescindibilidade e a importância de sua utilização como técnica investigativa, principalmente devido à necessidade de proteção da identidade do policial, o sigilo das investigações e a maciça utilização dessas plataformas virtuais no Brasil. No tocante à prova processual penal, a análise recairá sobre o regime de validade das provas, o princípio da ampla liberdade probatória e a licitude dos elementos obtidos em redes sociais. Posteriormente, passar-se-á à análise dos limites de sua utilização em um Estado Democrático de Direito, abordando os temas relativos à privacidade na internet e julgados das Cortes norte-americanas.

Palavras-chave: Rede social; perfil falso; prova; privacidade.

Abstract: The article studies the limits of a false user profile by the police, with investigative purposes, in social media. The importance of its use as an investigative technique will be discussed, mainly due to the need of protecting the identity of the police officer, the secrecy of the investigations and the massive use of these virtual platforms in Brazil. Regarding criminal procedural evidence, the analysis will be based on the validity of the evidence system, the principle of ample probative freedom and the legitimacy of elements obtained in social media. Subsequently, the limits of its use in a Democratic State ruled by Law will be analyzed addressing issues related to privacy on the internet and the US doctrine.

Keywords: Social media; fake profile; evidence; privacy.

1. Delegado de Polícia Civil. Pós-graduado em Direito Processual pela Universidade do Sul de Santa Catarina, em Direito Administrativo pela Faculdades Integradas de Jacarepaguá. Especialista em Segurança Pública e Investigação Criminal Aplicada (ACADEPOL-PCSC). E-mail: zucon@pc.sc.gov.br.
2. Delegado de Polícia Civil. Especialista em Segurança Pública, Mestre em Direito, Doutor em Sociologia. Pesquisador do Centro de Estudos em Segurança Pública e Direitos Humanos (CESPDH) da Universidade Federal do Paraná (UFPR). Pós-Doutor em Democracia e Direitos Humanos pela Universidade de Coimbra, Portugal. E-mail: gusso@gusso.com.br.
3. Delegado de Polícia Civil. Bacharel em Direito. Especialista em Ciências Penais. E-mail: anselmo@pc.sc.gov.br.

1 INTRODUÇÃO

A interconexão descentralizada entre computadores foi inicialmente concebida pelos Estados Unidos, durante a Guerra Fria, para fins militares, de modo a evitar que eventual ataque e destruição de um dos servidores comprometesse as informações e a comunicação entre os demais. Concomitantemente, serviu para interligar Universidades e Centros de Pesquisa, expandindo-se e tornando-se pública, até chegar no que hoje denominamos de internet.

Prevendo a evolução que os computadores teriam na vida das pessoas, no final dos anos 1980 o cientista norte-americano da área de informática Mark Weiser cunhou o termo "computação ubíqua" na publicação do artigo "A computação do século 21". Esta seria a terceira era da computação, logo após a era dos mainframes (computadores de grande porte) e dos personal computers - PC (computadores pessoais) (WEISER, 1991).

Para Weiser, computação ubíqua seria a evolução da computação, na medida em que o desenvolvimento tecnológico faria os computadores tão integrados na vida das pessoas que se tornariam imperceptíveis no cotidiano. Na prática eles continuariam existindo, porém a atenção do usuário estaria voltada para a tarefa e não para a ferramenta (MONQUEIRO, 2008). Seria como se comunicar com uma pessoa sem se dar conta de que está usando um dispositivo informático.

Essa é a realidade em que vivemos e que está em constante desenvolvimento. Trocamos mensagens, publicamos fotos e fazemos chamadas de vídeo, de maneira tão automática e natural que mal nos damos conta do meio utilizado. Tal característica guarda reflexos com a privacidade virtual, que muitas vezes deixamos em segundo plano.

Com essa revolução, o ambiente virtual não só passou a ser utilizado para a prática criminosa como também se mostrou um campo vasto para coleta de vestígios.

Nas apurações criminais, a prova testemunhal - mais amplamente utilizada - tem se revelado extremamente frágil e insuficiente. Além disso, essa nova realidade descortina dificuldades técnicas e legais não antes previstas, gerando falta de mecanismos e embaraços para apurar determinadas condutas cuja prova se encontra de forma virtual, meio utilizado pela maioria da população.

Para se ter uma dimensão da amplitude do uso de sites de relacionamento, um estudo de 2017 revelou que cerca de 57% da população brasileira acessa redes sociais,[4] com média diária de uso de 3 horas e 39 minutos, ocupando o Brasil a segunda colocação no mundo entre os países que usam por mais tempo essas plataformas (COELHO, 2018).

Numa época em que os relacionamentos virtuais ocupam boa parte da vida das pessoas, as publicações em sites dessa natureza se tornam fontes valiosas de prova. Novas formas de atuação da criminalidade requerem novos meios de coibição pela polícia judiciária, principalmente em razão de a evidência digital ter como características: ser volátil, anônima (em princípio), alterável e/ou modificável, podendo ser eliminada a qualquer instante (BARRETO; BRASIL, 2016, p. 29).

A utilização de redes sociais para investigação é amplamente utilizada pelas forças policiais dos Estados Unidos. A pesquisa realizada em 2015 pela Associação Internacional dos Chefes de Polícia (International Association of Chiefs of Police - IACP) (IACP, 2015) revelou que 88,7% delas fazem uso de mídias sociais para investigações criminais, sendo que, para 85,5%, é útil para a solução de crimes. Além disso, 92,3% as utilizam para analisar perfis e atividades de suspeitos e 67,2% afirmaram utilizá-las com identidade dissimulada para monitoramento e angariamento de informações. As plataformas mais utilizadas são Facebook (94,2%), Twitter (71,2%) e YouTube (40,0%).

4. "Redes sociais, no mundo virtual, são sites e aplicativos que operam em níveis diversos — como profissional, de relacionamento, dentre outros — mas sempre permitindo o compartilhamento de informações entre pessoas e/ou empresas". Como exemplo de redes sociais podem ser citadas: Linkedin, Facebook, Instagram, Twitter, etc. (RESULTADOS DIGITAIS, 2017).

Os acessos dessas redes de relacionamento para fins investigativos são muitas vezes efetuados pela polícia por perfis falsos (*fake*[5]), criados exclusivamente para esse fim, por questão de necessidade técnica.

Nesse atual cenário, algumas indagações começam a surgir: as publicações do investigado nas redes de relacionamento poderiam ser utilizadas como prova? Qual seria o limite da utilização do perfil *fake* como forma de investigação? Poderia ser utilizado como elemento de informação aquilo que se encontra acessível a todos? E as publicações mais restritas, aquelas compartilhadas ao seu grupo restrito de amigos? Haveria violação ao direito de intimidade ingressar com esse perfil *fake* na rede de amigos para coleta de vestígios relacionados ao fato investigado e coleta de outras informações? Poderia esse mesmo perfil interagir com o investigado e a conversa ser utilizada para fins investigativos?

A atuação estatal na persecução penal, em especial no exercício da atividade investigativa aqui tratada, deve ser compatibilizada com os preceitos constitucionais existentes. Acreditamos que, apesar de as pessoas consentirem em abrir mão de parcela de sua privacidade com o uso de redes sociais, há limite para a invasão da intimidade e angariamento de elementos de informação para fins criminais sem a necessidade de ordem judicial. O limite seria justamente passar da observação e acompanhamento para a interação com o suspeito, que não violaria somente a intimidade e a vida privada, mas também o *nemo tenetur se detegere* (ninguém é obrigado a se acusar).

O presente trabalho abordará os limites de utilização de um perfil de usuário falso pela polícia judiciária, com fins investigativos, em redes de relacionamento. Tratará da imprescindibilidade e da importância de sua utilização como técnica investigativa, da análise sobre o regime de validade das provas, do princípio da ampla liberdade probatória e da licitude dos elementos obtidos em redes sociais. Posteriormente, passará à análise dos limites de sua utilização em um estado democrático de direito, abordando os temas relativos à privacidade na internet, julgados das Cortes norte-americanas, arrematando com as considerações finais.

2 DA AMPLA LIBERDADE PROBATÓRIA E LICITUDE DAS PROVAS OBTIDAS EM REDES SOCIAIS

Como as redes sociais fazem parte da vida da maioria da população brasileira, suas publicações podem conter informações de interesse criminal. Dessa forma, inicialmente é necessário analisar se elas podem ser utilizadas como prova no processo penal.

Provar é demonstrar a veracidade do que se afirma, do que se alega. É o instrumento de verificação do *thema probandum* (TOURINHO FILHO, 2017, p. 513), destinando-se ao convencimento do juiz sobre determinada alegação.

Nesse atual panorama, as publicações das pessoas na internet nada mais são que fontes de prova, na medida em que, praticado um fato criminoso, a partir delas é possível obter elementos probatórios.

Lima (2015, p. 577-578) diferencia de forma criteriosa fonte de prova, meio de prova e meios de investigação da prova (ou obtenção da prova). Para o autor, fonte de prova é a expressão "[...] utilizada para designar as pessoas ou coisas das quais se consegue a prova, daí resultando a classificação em fontes pessoais (ofendido, peritos, acusado, testemunhas) e fontes reais (documentos, em sentido amplo)". Meios de prova, que podem ser lícitos ou ilícitos, "[...] são os instrumentos através dos quais as fontes de prova são introduzidas no processo", referindo-se, portanto, a uma atividade endoprocessual. Um documento seria uma

5. Anglicismo que significa "falso" ou "falsificado".

fonte de prova, e sua incorporação no processo um meio de prova. Já os meios de investigação da prova (ou obtenção da prova) seriam os procedimentos (em regra, extraprocessuais) regulados por lei, com o objetivo de conseguir provas materiais. Podem ser realizados por outros funcionários que não o juiz (v.g., policiais). E prossegue o doutrinador: "Importante ressaltar que, em regra, esses meios de investigação devem ser produzidos sem prévia comunicação à parte contrária, funcionando a surpresa como importante traço peculiar, sem a qual seria inviável a obtenção das fontes de prova".

Essa distinção entre meio de prova e meios de obtenção de prova não é meramente conceitual, vez que as consequências de eventuais irregularidades na sua produção possuem desfechos diversos. Os vícios que atingirem os meios de prova terão como consequência a nulidade da prova produzida, pois se trata de atividade endoprocessual. Já as irregularidades que inquinarem os meios de obtenção de prova, trarão como consequência o reconhecimento de sua inadmissibilidade no processo, diante da violação de regras relacionadas à sua obtenção (art. 5º, LVI, CF), com o consequente desentranhamento dos autos do processo (art. 157, caput, CPP) (LIMA, 2015, p. 577-578).

Dessa forma, no tocante à limitação ao direito de prova, a Constituição Federal dispõe no art. 5º, LVI que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos". Sem adentrar em discussões terminológicas acerca de prova "ilícita", "ilegal" e "ilegítima", consideramos como "ilícitas" as peculiaridades das provas que não podem ser admitidas pelo ordenamento jurídico, assim também disciplinado no caput do artigo 157[6] do Código de Processo Penal.

São diversas as inviolabilidades pessoais protegidas em normas constitucionais e infraconstitucionais. No entanto, no que se refere à produção probatória, algumas geralmente são mais atingidas, como a intimidade, a vida privada, a honra e a imagem (art. 5º, X, CF), a inviolabilidade do domicílio (art. 5º, XI, CF), bem como a inviolabilidade do sigilo das comunicações (art. 5º, XII, CF), etc.

A solução encontrada pela Constituição Federal para provas produzidas com violações desta natureza é a sua inadmissibilidade, isto é, não poderão compor o conjunto probatório processual penal. Como dito anteriormente, caso a ilegalidade seja oriunda de meio de obtenção de prova - procedimento de investigação - no curso de inquérito policial, ou até mesmo antes deste, a solução será o desentranhamento dos autos do processo, bem como demais provas dele derivadas (art. 157, §1º, do CPP).

Em termos principiológicos, temos como elementos norteadores do processo penal a busca da verdade e da liberdade probatória, que culminam na mais ampla liberdade probatória. O Código de Processo Penal não adotou o sistema taxativo dos meios de prova admitidos, podendo ser aceitos os inominados, desde que moralmente legítimos e produzidos por meios lícitos.

Corroborando essa afirmação, o parágrafo único, do art. 155, do CPP, ao tratar do sistema de valoração da prova do livre convencimento motivado ou persuasão racional, assevera não haver limitações na produção probatória, exceto quanto ao estado das pessoas.[7]

No mesmo sentido, o art. 369 do Código de Processo Civil, aplicado de maneira subsidiária ao processo penal (art. 3º do CPP), disciplina que "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz".

6. Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.
7. Art.155, parágrafo único, do CPP "somente quanto ao estado das pessoas serão observadas as restrições estabelecidas na lei civil".

Pela aceitabilidade, de maneira excepcional, de provas atípicas ou inominadas, leciona Lopes Junior (2015, p. 391):

> Em suma, como regra, somente podem ser admitidas as provas tipificadas no CPP. Excepcionalmente, podem ser admitidas provas atípicas ou inominadas, desde que não constituam subversão da forma estabelecida para uma prova nominada, e, ainda, guardem estrita conformidade com as regras constitucionais e processuais atinentes à prova penal.

Em linhas gerais, desde que respeitados os ditames legais, não há óbice na utilização de informações postadas na internet, cuja conversão em elemento documental se revela necessária para a preservação da evidência cibernética. Na prática, para que se confira confiabilidade aos *prints* e *screenshots* obtidos das publicações nas mídias sociais, é necessário que sua coleta, conferência e formalização sejam feitos por quem detenha fé pública, o escrivão de polícia ou outro servidor que, por meio de lei própria tenha esse atributo, ou, ainda, por meio de ata notarial, em cartório de registro de notas (BARRETO; BRASIL, 2016, p. 41).

Por óbvio, cautelas devem ser adotadas em seu emprego, que podem ser corroboradas por outros elementos, pois os verdadeiros autores das publicações podem se valer de perfis falsos.

3 DA NECESSIDADE DE UTILIZAÇÃO DE PERFIL DE USUÁRIO FALSO (FAKE) PARA INVESTIGAÇÃO

Perfis *fakes* são feitos com utilização de imagens de pessoas reais ou com a criação de personagem fictício. No primeiro caso, paira dúvida acerca da tipicidade da conduta, se ela poderia configurar o delito de falsidade ideológica (art. 299, do CP)[8] ou de falsa identidade (art. 307, do CP).[9] A controvérsia sucede principalmente em relação à abrangência, ou não, para documentos virtuais e também no tocante ao preenchimento dos elementos subjetivos dos tipos (propósito de "prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante", no caso do crime de falsidade ideológica, ou com o fim de "obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem", para falsa identidade). No entanto, essa análise não será objeto do presente estudo.

Ultrapassada essa questão, a criação de perfil de usuário fictício pela polícia judiciária para fins investigativos não se trata tão somente da necessidade de se aproximar e interagir com o investigado, mas da importância da proteção do próprio policial e atendimento a questões técnicas para o não comprometimento da investigação.

A primeira das consequências ocorreria por descuido do próprio investigador. Imagine que um policial, utilizando seu próprio perfil, ao investigar determinado fato, de maneira equivocada, faça solicitação de amizade, "curta" alguma foto ou publique algo na *timeline*[10] do perfil investigado. Quem utiliza o ambiente virtual sabe que todos estão sujeitos a tais erros. Mas, como se trata de uma atuação policial, esse descuido pode custar a sua exposição e a própria investigação, na medida em que o suspeito, ao notar essa ação, verifica que está sendo observado por um policial e exclui todas as suas publicações, extinguindo assim os vestígios de sua atividade criminosa.

8. Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante: Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.
9. Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.
10. Linha do tempo. Sequência de publicações de um determinado usuário.

Outra dificuldade enfrentada com a utilização do próprio perfil para a investigação é a forma com que a rede social lida com as ações dos usuários. Para disponibilização de conteúdo, sugestão de amizades etc., são utilizados algoritmos[11] que acompanham o comportamento da pessoa na rede. A forma com que a rede social lida com as ações e informações das pessoas está em constante mudança e nem sempre é clara.

No caso do Facebook, a maior rede social do mundo,[12] o algoritmo contém mais de 100 mil variáveis que "hackeiam" o comportamento dos usuários e a interação com o conteúdo disponível na rede social (VIEIRA, 2017).

Algumas análises por empresas particulares já foram efetuadas para saber o alcance dos algoritmos das ações na rede, inclusive a sua interação com aplicativos de propriedade da empresa, como Instagram e WhatsApp (CANALTECH, 2017). A verdade é que esse provedor de serviços sabe mais sobre seus usuários do que estes imaginam.

Há dados que remetem à existência de um "perfil sombra", um perfil construído pelo próprio Facebook (e que a pessoa não pode controlar) a partir das informações de caixas de entrada e smartphones de outros usuários (como agenda de contatos e informações a estes associadas, endereço de e-mail e endereços de locais onde já morou). Informações nunca fornecidas ficam associadas à sua conta, mapeando de forma mais completa as conexões sociais do usuário (HILL, 2017).

Essas considerações se aplicam às mais diversas redes sociais, cada qual com sua rotina de análise de dados e termos de uso.

Mas, qual a relação com a investigação criminal? Ora, se o mesmo policial utilizar seu perfil pessoal para vasculhar a vida de determinado investigado e sua rede de contatos, isso pode ser entendido pelo site de relacionamento como interesse por aquela pessoa. O site passará a fazer o encadeamento de contatos, sugerindo amizades e publicações recíprocas, o que pode alertar o investigado, que perceberá que está sendo vigiado.

Além disso, poderá haver a exposição desnecessária do próprio policial, colocando em risco sua segurança. Esses fatores tornam não só prudente, mas necessária a criação de um perfil *fake* para investigação.

4 INTERNET, PRIVACIDADE E VEDAÇÃO À AUTOINCRIMINAÇÃO

A inviolabilidade à intimidade e a privacidade integra as chamadas liberdades públicas (núcleo dos direitos fundamentais [FERREIRA FILHO, 2008, p. 28]), que nada mais são que normas constitucionais positivadas para limitar intervenções por parte do Estado e por terceiros. Um dos objetivos é a limitação do exercício do poder punitivo do Estado.

A inviolabilidade está prevista no art. 5º, inciso X, da Constituição Federal, que assim dispõe: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Dessa forma, a ordem constitucional brasileira erigiu à categoria dos direitos fundamentais pessoais a intimidade e a vida privada, que mantêm relação direta com a garantia da dignidade da pessoa humana, na medida em que compõe o próprio desenvolvimento da personalidade do indivíduo.

Como o texto da Carta Magna previu os dois termos "intimidade" e "vida privada", há quem procure diferenciá-los, afirmando que o primeiro se refere à vida secreta do indivíduo, que pode querer evitar que os demais tenham conhecimento, ou, ainda, o modo de ser da pessoa. O segundo termo, como o conjunto de informações acerca do indivíduo que ele pode decidir manter sob o seu exclusivo controle ou comunicar, decidindo a quem, quando, onde e em que condições, sem poder ser legalmente sujeito (CHIMENTI et al., 2008, p. 77).

11 Sequência de instruções para se executar uma tarefa.
12 Com mais de 2,2 bilhões de usuários ativos mensalmente (BELING, 2018).

Para Bulos (2015, p. 572), a diferença entre privacidade e intimidade seria quase imperceptível, na medida em que ambas diriam respeito às particularidades do ser humano. A vida privada, que envolve todos os relacionamentos do indivíduo (comerciais, trabalho, convívio) seria mais ampla do que a intimidade (relações íntimas e pessoais do indivíduo, amigos e familiares que participam da vida pessoal).

Há dificuldades para enquadrar as terminologias de forma rígida, diante dos mais diversos acontecimentos cotidianos. Tavares (2012, p. 290, apud SARLET; MARINONI; MITIDIERO, 2014, p. 408) desenvolve o raciocínio de diferenciar a abrangência da privacidade conforme a proteção se circunscreva a aspectos mais íntimos ou menos íntimos das pessoas, na chamada Teoria das Esferas, que também não é isenta de críticas:

> A noção, desenvolvida por setores da doutrina e pela jurisprudência constitucional alemã, de que se podem, no âmbito do direito à privacidade, distinguir três esferas (a assim chamada teoria das esferas), uma esfera íntima (que constitui o núcleo essencial e intangível do direito à intimidade e privacidade), uma esfera privada (que diz com aspectos não sigilosos ou restritos da vida familiar, profissional e comercial do indivíduo, sendo passível de uma ponderação em relação a outros bens jurídicos) e uma esfera social (onde se situam os direitos à imagem e à palavra, mas não mais a intimidade e a privacidade), tem sido criticada como insuficiente para dar conta da diversidade de casos que envolvem a proteção da vida privada.

Parece mais razoável o entendimento de que a distinção é difícil de ser sustentada, principalmente em razão da fluidez entre as diversas esferas da vida privada (que inclui a intimidade) (TAVARES, 2012, p. 676, apud SARLET; MARINONI; MITIDIERO, 2014, p. 407). Aqui será adotada essa visão, em que a intimidade está incluída na proteção da privacidade. No entanto, ainda como direito subjetivo fundamental, não recai sobre ela a indisponibilidade absoluta.

Sobre esse tema, diferenciam-se dois aspectos inerentes ao direito à privacidade. O primeiro comportaria a dimensão objetiva (dever de proteção estatal contra intervenções de terceiros e garantia das condições constitutivas da fruição da vida privada). O segundo, a dimensão subjetiva (direito de defesa - de não intervenção por parte do Estado e terceiros - e expressão de sua liberdade pessoal), relacionando-se esta com a possibilidade de a pessoa dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal e que não interferem em direitos de terceiros, sendo também a privacidade o direito de autodeterminação do indivíduo (KLOEPFER, 2010, p. 152, apud SARLET; MARINONI; MITIDIERO, 2014, p. 410).

Diante da previsão constitucional, o direito à privacidade se refere a um direito fundamental autônomo, que deve ser protegido e respeitado, necessário ao desenvolvimento da personalidade, mas não absolutamente indisponível. Considerando as duas dimensões acima, em seu aspecto subjetivo, a privacidade relacionada com as informações relativas a sua vida pessoal, o indivíduo pode livremente dispor.

Assim, desde que essa disponibilização não atinja a dignidade da pessoa humana, é possível que haja sua autolimitação, renúncia parcial ou que ocorra uma espécie de indisponibilidade relativa pelo seu próprio detentor (SARLET; MARINONI; MITIDIERO, 2014, p. 401-405).

Isso é o que sucede com a utilização das redes sociais na internet. Muitas vezes, sem que o próprio usuário se dê conta, está abrindo mão de sua privacidade. A exposição em publicações de caráter público, acessíveis a todos, é uma autolimitação do direito à privacidade, podendo ser usadas por qualquer pessoa, inclusive para fins de instrução processual penal, não havendo que falar em ilicitude por violação de direito fundamental.

Nesse sentido, Barreto (2016b, p. 137) esclarece:

> Não há, portanto, nenhum óbice na utilização de informações postadas na internet quando a Polícia Judiciária acosta ao procedimento administrativo fotos, vídeos ou textos postados por determinado indivíduo em perfis abertos. Permissa Vênia, não há proteção constitucional da privacidade quando esse conteúdo é postado em uma rede social. Quem posta o conteúdo de forma livre na web precisa entender que não está colocando informações em um diário privado e sim para todo mundo.

Assim, seja coletando os vestígios cibernéticos com um perfil pessoal do próprio investigador, ou com um perfil *fake* (retomando, a nosso ver, a necessidade de sua utilização), não haverá questionamento sobre a sua validade, posto que presumidas públicas e de domínio coletivo. No entanto, solução diversa pode ocorrer na utilização de publicações realizadas no âmbito de "perfis fechados", ou seja, limitado a um número restrito de pessoas, as quais o seu titular aceita como "amigos".

Para Barreto (2016b, p. 137), as publicações enviadas a uma quantidade de usuários restritos gera uma expectativa de privacidade de acesso ao seu conteúdo, cuja opção de autogerenciamento da privacidade é feita pelo próprio usuário na utilização da plataforma. Em sendo o perfil fechado, há necessidade de ordem judicial para o acesso.

No mesmo sentido, Silva (2016) afirma que a invasão ou obtenção furtiva de informação pelos órgãos de investigação em sites de relacionamento com restrição a determinado grupo de amigos, viola o direito à intimidade, devido à existência de expectativa subjetiva de privacidade.

Prosseguindo o raciocínio, o autor assevera que em relação às informações postadas na internet, a intimidade está sempre relacionada com a confiança depositada no interlocutor. Considerando que ninguém confia segredos a estranhos, pode-se invocar direito à intimidade quando existe uma "confiança quebrada".

Após discorrer um pouco mais sobre o tema, Silva conclui:

> Realçamos, pois, dois pontos fundamentais na apreciação da existência de privacidade das informações obtidas em um diálogo limitado a grupo restrito de usuário em um site de relacionamento: o número de interlocutores e a confiabilidade deles, elementos que devem ser apreciados de forma conjugada no caso concreto (SILVA, 2016, p. 57).

No entanto, acerca da utilização de perfil falso pelos órgãos policiais, o mesmo autor vai além:

> Quando a polícia recorre a meios ardilosos e ilegais para obter uma prova perdemos, então, os freios e contrapesos que valorizamos em nosso sistema de justiça criminal. A ação policial disfarçada (fake), sem autorização judicial, configura patente violação à intimidade do usuário de site de relacionamento e assemelha-se a uma "ação encoberta" sem autorização judicial, viciando a prova e envenenando as informações obtidas por derivação (SILVA, 2016, p. 14).

Apesar do embasamento esposado pelos autores acima, acreditamos, em sentido oposto, que não se pode considerar *ab initio* nula a prova obtida com utilização de perfil falso pelos órgãos policiais em perfis restritos, desde que diferenciadas as formas de relacionamento com o suspeito.

Já foi explanada a necessidade de criação de um perfil falso para uso policial, seja para manutenção do sigilo das investigações, seja para proteção do próprio policial. Ora, se um perfil desses é criado, a pessoa inexiste. Em sendo feita solicitação de amizade (ou outra forma semelhante dependendo da plataforma) ao investigado para que seja incluído no rol de pessoas que terão acesso às suas publicações restritas, acreditamos que o próprio investigado dispõe de sua intimidade ao aceitar pessoa que de fato não conhece.

Além disso, não raro o indivíduo detém centenas ou milhares de pessoas no seu círculo de amizades "restrito", dentre as quais haverá inúmeras outras desconhecidas. Isso faz com que não haja confiabilidade nos interlocutores, equiparando o seu perfil "privado" a um de domínio público.

Nesta esteira, em nosso entendimento, não há que o investigado alegar violação da intimidade por "quebra de confiança", pois não há como confiar em alguém que o usuário sequer conhece/existe.

Não estamos aqui falando de criação de perfil falso de pessoa existente e próxima do investigado, pois, aí sim poderia haver violação da confiança dos interlocutores e transgressão do direito fundamental à privacidade.

Complementando essa análise, cabe tecer algumas considerações acerca das ações policiais no tocante ao grau de relacionamento com o suspeito. O autor português Manuel Augusto Alves Meireis (apud PORTO, 2016, p. 9) adota uma divisão tripartida dos chamados "homens de confiança". Ela abrangeria as figuras do agente encoberto, agente infiltrado e do agente provocador, cuja diferenciação tomaria por critério o grau de ingerência na esfera dos direitos e liberdades fundamentais dos particulares.

"Agente infiltrado" designa o policial que, ocultando sua identidade ou qualidade, mediante interação com o investigado, conquista sua confiança. Acompanha as suas ações e pratica, se necessário, atos criminosos, com a finalidade de obter provas incriminatórias ou prevenir futuros crimes (MEIREIS, 1999, p. 163-164; 2006, p. 94-95, apud PORTO, 2016, p. 10).

O "agente encoberto" seria aquele que, igualmente sem revelar sua identidade ou qualidade, vai aos locais ligados ao crime, com o fito de desvelar eventuais infratores, sem interferir nas condutas criminosas ou estabelecer qualquer proximidade. A conduta é "de absoluta passividade relativamente à decisão criminosa", pois "naquele lugar e naquele momento poderia estar qualquer outra pessoa e as coisas aconteceriam da mesma forma" (MEIREIS, 1999, p. 192; 2006, p. 93 e 94, apud PORTO, 2016, p. 10).

O "agente provocador" diz respeito àquele que instiga ou provoca o investigado à prática delitiva com a intenção de incriminá-lo, cujas consequências se enquadrariam nos ditames da Súmula 145 do Supremo Tribunal Federal.[13]

Conquanto essa divisão comporte controvérsias dogmáticas, que não serão abordadas no presente trabalho, é importante para diferenciar a forma de ação do investigador em relação ao investigado.

Isso posto, na elucidação de um delito, o investigador pode se relacionar de diversas formas com o suspeito. Pode agir de maneira passiva, acompanhando e observando o investigado, sem com ele travar um diálogo ou estabelecer um vínculo íntimo de confiança. Pode, por outro lado, não só espreitá-lo anonimamente, mas com ele firmar vínculo de confiança, comunicando-se e interagindo com ele. Mas pode ir além, instigando ou provocando o investigado à prática criminosa.

A ação de gerar um perfil falso para investigar determinado suspeito em sua rede social, ainda que na sua esfera privada de "amigos", se equipara às ações de um agente encoberto (tomando como base a definição do autor antes citado), uma vez que o agente público age em total passividade na coleta de informações que o próprio investigado posta.

13 Súmula 145. Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação.

Portanto, o mero acompanhamento das publicações privadas do investigado mediante a utilização de perfil *fake* pela polícia judiciária não violaria o direito fundamental à privacidade.

Apesar de não terem sido localizadas decisões judiciais que enfrentassem tais questões, a tendência das Cortes norte-americanas parece ser no sentido de que a utilização de perfis falsos pelos órgãos policiais não violaria a intimidade do indivíduo (Quarta Emenda[14] da Constituição dos Estados Unidos). Ele consentiu que aquele a quem adicionou como amigo viesse a acompanhar suas publicações, não podendo alegar desrespeito à expectativa de privacidade.

No caso United States v. Meregildo,[15] a defesa pediu a supressão processual de evidência coletada por um colaborador, integrante da rede de "amigos" do Facebook do investigado, e fornecida à polícia, alegando violação à Quarta Emenda. Na decisão, a corte afirmou que, ao confiar na pessoa adicionada como amigo, o titular do perfil assumiu o risco que aquele revelasse suas informações para a polícia e, portanto, não poderia ter uma "expectativa razoável de privacidade".

Já no caso United States v. Gatson (CASEMINE, 2014)[16] a polícia norte- americana, mediante a utilização de um perfil falso, se tornou "amigo" de Gatson na rede social Instagram, o que permitiu aos policiais terem acesso às fotos do investigado e a outras informações. Na decisão, a corte afirmou que "nenhum mandado é necessário para a troca consensual desse tipo de informação".

Em decisão mais recente (29 de maio de 2018), no caso Everett v. State (FINDLAW, 2018), a Suprema Corte do Estado de Delaware enfrentou a questão da validade da prova obtida mediante utilização de perfil fictício pela polícia para angariar informações do suspeito. Nesse caso, durante cerca de dois anos, um detetive do Departamento de Polícia da cidade de New Castle monitorou reiteradamente um criminoso local conhecido, chamado Terrance Everett. O monitoramento foi realizado mediante a utilização de um perfil falso no Facebook (incluindo nome e imagens falsas). Durante o monitoramento, o detetive fez uma "solicitação de amizade" a Everett, que o aceitou. Em novembro de 2015, o detetive visualizou uma foto postada por Everett com uma arma. No mesmo dia solicitou um mandado de busca. Expedido e cumprido no mesmo mês, Everett foi preso por possuir ilegalmente arma de fogo e munições. A defesa de Everett recorreu da condenação alegando, dentre outros itens, que o monitoramento realizado pela polícia era ilegal e teria contaminado a prova colhida pela teoria dos frutos da árvore envenenada, pois a colheita da prova teria violado a Quarta Emenda da Constituição Norte-americana, bem como a Constituição do Estado de Delaware, uma vez que Everett detinha expectativa de privacidade nas suas publicações. Na decisão, ficou consignado:

14. Não será infringido o direito do povo à inviolabilidade de sua pessoa, casas, papéis e haveres, contra buscas e apreensões irrazoáveis e não se expedirá mandado a não ser mediante indícios de culpabilidade, confirmados por juramento ou declaração, e nele se descreverão particularmente o lugar da busca e as pessoas ou coisas que tiverem de ser apreendidas. Disponível em:
<https://www1.folha.uol.com.br/fsp/mais/fs20129807.htm>. Acesso em: 17 nov. 2018.
15. 883 F.Supp.2d 523 (S.D.N.Y 2012). Disponível em: <https://casetext.com/case/united-states-v-meregildo>. Acesso em: 17 nov. 2018.
16. Disponível em: https://www.casemine.com/judgement/us/5914f9d6add7b049349a4961

> Here, we need not explore the edges and boundary lines defining a person's legitimate expectation of privacy in information shared with third parties such as Internet providers or social media platforms such as Facebook, Twitter, and Snapchat. Rather, we resolve the case on narrow grounds—namely, that the Fourth Amendment does not guard against the risk that the person from whom one accepts a "friend request" and to whom one voluntary disclosed such information might turn out to be an undercover officer or a "false friend." One cannot reasonably believe that such "false friends" will not disclose incriminating statements or information to law enforcement—and acts under the risk that one such person might actually be an undercover government agent. And thus, one does not have a reasonable expectation of privacy in incriminating information shared with them because that is not an expectation that the United States Supreme Court has said that society is prepared to recognize as reasonable.[17]

Dessa forma, afirmando a ausência de expectativa razoável de que os *posts* compartilhados voluntariamente com o perfil falso e outros "amigos" não seriam divulgados, e assumindo o risco de que essas informações fossem acessadas por órgão policial, ainda que disfarçados, a corte concluiu que a visualização da página restrita do Facebook pelo detetive não violou a Quarta Emenda ou a Constituição de Delaware.

No entanto, sabemos que o tema levanta polêmicas e que não é possível o estabelecimento de respostas prontas e inequívocas às mais diversas casuísticas, mormente porque requer a análise acerca do malferimento de direitos e garantias fundamentais, cuja análise da violação do direito à privacidade deverá ser aferida à luz das circunstâncias do caso concreto (HORN, p. 197, apud SARLET; MARINONI; MITIDIERO, 2014, p. 408).

De outro norte, se além de ser aceito com perfil fictício na esfera de "amigos" do investigado o agente policial inicia um relacionamento mais estreito com este, mantendo diálogo e ganhando sua confiança, cremos que essas informações estarão revestidas de ilicitude.

Primeiro porque passa a se equiparar com o instituto de infiltração virtual de agentes,[18] técnica especial de investigação, com regramento específico, em que o agente policial, ocultando sua identidade, passa a se envolver com determinado grupo de pessoas. O objetivo é manter relação de confiança com seus integrantes para obtenção de elementos de autoria e materialidade, reservadas a algumas hipóteses legais e dependentes de circunstanciada autorização judicial.

Em segundo lugar porque violaria o princípio do *nemo tenetur se detegere*, que abrange o direito ao silêncio do suspeito. O art. 5o., inciso LXIII, da Constituição Federal assegura o direito ao silêncio, que deverá ser respeitado por ocasião do interrogatório. A não observância desse preceito invalida a prova colhida.

17. Aqui, não precisamos explorar as bordas e linhas de contorno que definem a expectativa legítima de privacidade de uma pessoa em informações compartilhadas com terceiros, como provedores de Internet ou plataformas de mídia social, como Facebook, Twitter e Snapchat. Em vez disso, resolvemos o caso com base em argumentos estreitos - a saber, que a Quarta Emenda não protege contra o risco de que a pessoa de quem se aceita um "pedido de amizade" e a quem uma informação divulgada voluntariamente possa ser um agente disfarçado ou um "falso amigo". Não se pode razoavelmente acreditar que tais "falsos amigos" não divulgarão as declarações incriminatórias ou informações aos órgãos policiais - e age sob o risco de que uma dessas pessoas possa, na verdade, ser um agente secreto do governo. E assim, não se tem uma expectativa razoável de privacidade na informação incriminatória compartilhada com eles, porque isso não é uma expectativa que a Suprema Corte dos Estados Unidos tenha dito que a sociedade está preparada para reconhecer como razoável (FINDLAW, 2018, tradução nossa).

18. Regulamentada pela Lei no. 13.441/17 que acrescentou dispositivos ao Estatuto da Criança e do Adolescente, oriunda do Projeto de Lei do Senado no. 100, de 2010 e constante da CPI da Pedofilia, criada por meio do Requerimento no. 2, de 2005-CN, "com o objetivo de investigar e apurar a utilização da Internet para a prática de crimes de 'pedofilia, bem como a relação desses crimes com o crime organizado".

Nas palavras de Queijo (2003):

> A advertência do acusado quanto ao direito ao silêncio, antes de iniciado o interrogatório, é essencial para assegurar que a opção por cooperar ou não neste seja decorrente de sua autodeterminação [...] Busca-se evitar, com a advertência, que nada mais deve ser do que instrução do acusado quanto ao seu direito, auto-incriminações involuntárias, por desconhecimento do direito. Dessa forma, a falta da advertência quanto ao direito ao silêncio e de que do exercício desse direito não podem advir consequências prejudiciais à defesa viola o nemo tenetur se detegere. É o que ocorre, v. g., nas denominadas "declarações informais" colhidas do suspeito, na fase de investigações, ou mesmo em entrevistas realizadas pela imprensa com o acusado.

Assim sendo, as declarações colhidas nessas circunstâncias serão revestidas de ilicitude por atentar contra o direito de não se autoincriminar, podendo invalidar as demais provas delas decorrentes.

5 CONSIDERAÇÕES FINAIS

A evolução da internet mudou o comportamento das pessoas. Em grande parte, os relacionamentos passaram para o ambiente virtual, que se mostrou um campo fértil e vasto para a coleta de vestígios de práticas criminosas.

Essa transformação precisou ser acompanhada pela polícia judiciária, que passou a angariar elementos probatórios dessas fontes. Mas, no Estado Democrático de Direito, a atuação estatal na *persecutio criminis* é limitada, devendo obediência aos princípios constitucionais estabelecidos e aos direitos e garantias fundamentais.

Na atividade investigativa, alguns direitos fundamentais são mais atingidos, como o direito à privacidade, previsto no art. 5º, inciso X, da Constituição Federal. Caso a sua mitigação não seja revestida dos contornos legais, poderá tornar o elemento colhido inválido, atingindo as demais provas dele decorrentes pela teoria dos frutos da árvore envenenada.

No entanto, apesar de representar um direito que garante o desenvolvimento da personalidade do indivíduo, não se trata de direito indisponível, podendo o seu titular dele abrir mão. Isso ocorre com frequência nas mídias sociais, em que o indivíduo aceita pessoas desconhecidas na rede privada de amigos e expõe deliberadamente sua vida particular nas publicações da *timeline*.

Nesse panorama, a ação policial investigativa é feita com a utilização de perfis falsos, criados por questões de necessidade técnica (proteção do policial e garantia do sigilo das investigações) para angariar elementos de informação dos suspeitos. Mas, ainda que com a utilização desses perfis, há um campo aberto de maneiras que os investigadores podem se relacionar com o investigado, nem todas legais.

Como exposto no presente trabalho, as informações colhidas em Publicações efetuadas em perfis "abertos", acessíveis a qualquer pessoa, não encontram óbice em sua utilização.

As divergências começam a surgir com indagação acerca da legalidade da coleta de informações em perfis "fechados", restrito a rede de amigos do investigado. Acreditamos que, ainda que a Polícia se utilize de perfil fictício, a aceitação voluntária deste novo indivíduo, pelo investigado, na sua rede privada de amigos, afastaria a alegação de expectativa de privacidade de suas publicações, as quais poderiam ser utilizadas na persecução penal, mormente por se tratar de atividade passiva de observância dos conteúdos.

No entanto, a utilização desses perfis para comunicação com o investigado com o fim de estabelecer um vínculo de confiança, inclusive para obter eventual confissão, violaria o direito à privacidade e o princípio do *nemo tenetur se detegere*.

Reconhecemos, contudo, que o tema é controverso, suscita interessantes e, talvez, infindos debates, os quais deverão avançar e serem enfrentados pelos tribunais superiores.

REFERÊNCIAS

BARRETO, Alesandro Golçalvez; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. 1. ed. Rio de Janeiro: Brasport, 2016a.

BARRETO, Alesandro Gonçalves. **Utilização de fontes abertas na investigação policial**. In: Orgs. BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso.
Combate ao Crime Cibernético - doutrina e prática. A visão do Delegado de Polícia.
1. ed. Rio de Janeiro: Mallet Editora, 2016b.

BELING, Fernanda. **As 10 maiores redes sociais**: Atualizado. 2018. Disponível em: https://www.oficinadanet.com.br/post/16064-quais-sao-as-dez-maiores-redes-sociais. Acesso em 25 set. 2021.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 03 set. 2021.

BRASIL. Decreto-Lei Nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponivel em: <http://www.planalto.gov.br/ccivil_03/Decreto- Lei/Del3689.htm>. Acesso em: 03 set. 2021.

BRASIL. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponivel em: ttp://www.planalto.gov.br/ccivil_03/decreto- lei/Del2848compilado.html
. Acesso em: 03 set. 2021.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2015.

CANALTECH. **Especialistas em dados analisam o poder dos algoritmos do Facebook**. 2017. Disponível em:
https://canaltech.com.br/redes-sociais/especialistas-em-dados-analisam-o-poder-dos-algoritmos-do-facebook- 94580/. Acesso em: 06 set. 2021.

CASEMINE. **United States v. Gatson**. 2014 WL 7182275. Disponível em: https://www.casemine.com/judgement/us/5914f9d6add7b049349a4961. Acesso em: 17 set. 2021.

CHIMENTI, Ricardo Cunha et al. **Curso de Direito Constitucional**. 5. ed. São Paulo: Saraiva, 2008.

COELHO, Taysa. **10 fatos sobre o uso de redes sociais no Brasil que você precisa saber**. 2018.Disponível em: <https://www.techtudo.com.br/noticias/2018/02/10-fatos-sobre-o-uso-de-redes-sociais-no-brasil-que-voce-precisa-saber.ghtml>. Acesso em: 20 set. 2021.

FERREIRA FILHO, Manoel Gonçalves. **Direitos humanos fundamentais**. 10. ed. São Paulo: Saraiva, 2008.

FINDLAW. **Everett v. State**. 2018. WL. 2409511. Disponível em: https://caselaw.findlaw.com/de-supreme-court/1896796.html. Acesso em: 17 set. 2021.

HILL, Kashmir. **Mas afinal por que o Facebook acha que eu conheço esses caras?**. 2017. Disponível em: <https://gizmodo.uol.com.br/facebook-perfil-sombra/>. Acesso em: 06 out. 2018.

IACP. **Social Media Survey Results**. 2015. Disponível em: <http://www.iacpsocialmedia.org/wp-content/uploads/2017/01/FULL-2015-Social-Media-Survey-Results.compressed.pdf>. Acesso em: 24 set. 2021.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**: Volume Único. 3. ed. Salvador: JusPODIVM, 2015.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 12. ed. São Paulo: Saraiva, 2015.

MONQUEIRO, Julio Cesar Bessa. **Computação ubíqua**. 2008. Disponível em: <https://www.hardware.com.br/artigos/computacao-ubiqua/>. Acesso em: 07 set. 2021.

QUEIJO, Maria Elizabeth. **O direito de não produzir prova contra si mesmo** (o princípio nemo tenetur se detegere e suas decorrências no processo penal). 1 ed. São Paulo: Saraiva, 2003.

REGO, Sara Daniela Quintas Couto. **Do Agente Encoberto ao Agente Provocador** - A Fronteira entre a Irresponsabilidade e a Responsabilidade Penal. Porto, 2016. 52 f. Dissertação (Mestrado em Direito Criminal) Universidade Católica Portuguesa. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/21538/1/Disserta%C3%A7%C3%A3o_Sara Rego.pdf. Acesso em: 10 set. 2021.

RESULTADOS DIGITAIS. **Computação ubíqua**. 2017. Disponível em: https://resultadosdigitais.com.br/redes-sociais/ Acesso em: 20 set. 2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 3. ed. São Paulo: Revista dos Tribunais, 2014.

SILVA, Danni Sales. **Da validade processual penal das provas obtidas em sites de relacionamento e a infiltração de agentes policiais no meio virtual**. 2016. Disponível em: http://www.mpgo.mp.br/portal/arquivos/2016/08/01/12_08_28_0_Artigo_Dr._Danni_publica%C3%A7%C3%A3o_revista_do_IBCCrim.pdf. Acesso em: 06 out. 2018.

TOURINHO FILHO, Fernando da Costa. **Manual de Processo Penal**. 9. ed. São Paulo: Saraiva, 2017.

VIEIRA, Isabelle. **Como funcionam os algoritmos do Facebook, Instagram e Twitter**. 2017. Disponível em: https://resultadosdigitais.com.br/blog/algoritmo-facebook-instagram-twitter/#. Acesso em: 06 set. 2021.

WEISER, Mark. **The Computer for the 21st Century**. 1991. Disponível em: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Acesso em: 07 out. 2018.