

(IN)APLICABILIDADE DA DOCTRINA “FOREGONE CONCLUSION” E O ACESSO A DISPOSITIVOS CIFRADOS NO PROCESSO PENAL BRASILEIRO

(IN)APPLICABILITY OF THE “FOREGONE CONCLUSION” DOCTRINE AND ACCESS TO
ENCRYPTED DEVICES IN BRAZILIAN CRIMINAL PROCEDURAL LAW

**Carlos Hélder Carvalho
Furtado Mendes**

Doutor e Mestre em Ciências Criminais pela PUC-RS. Advogado.

Link Lattes: <http://lattes.cnpq.br/3034060693231004>

ORCID: <https://orcid.org/0000-0001-5256-1297>

helder@madeiraadvogados.com.br

Yuri Felix

Doutor e Mestre em Ciências Criminais pela PUC-RS.

Professor, palestrante e parecerista com artigos publicados
em revistas especializadas. Advogado.

Link Lattes: <http://lattes.cnpq.br/0866064520436785>

ORCID: <https://orcid.org/0000-0003-1494-9535>

advyuri@gmail.com

Resumo: O presente artigo tem como objetivo analisar a aplicabilidade da doutrina “foregone conclusion” estadunidense no Direito Processual Penal Brasileiro, em situações de investigação criminal que busca alcançar dados informáticos armazenados em dispositivos codificados, cujo acesso se dá a partir de senhas pessoais ou sensores biométricos. Parte-se do estudo de casos americanos em que se funda a referida doutrina, especificando seus critérios e possibilidades de aplicação, para posteriormente as tensionar com as regras do Direito Processual Penal brasileiro, notadamente o Direito à não autoincriminação e a presunção de inocência como regra de tratamento, regra de julgamento e regra probatória. Utiliza-se precedentes dos Tribunais Superiores brasileiros para confirmar os argumentos adotados e para o estabelecimento de conclusões.

Palavras-chave: Dispositivos cifrados; Direito à não autoincriminação; *Foregone Conclusion*; Direito Processual Penal Brasileiro.

Abstract: This article aims to analyze the applicability of the US “foregone conclusion” doctrine in Brazilian Criminal Procedural Law, in criminal investigation situations that seek to access computer data stored in encrypted devices, whose access is based on personal passwords or biometric sensors. It starts with the study of American cases on which this doctrine is based, specifying its criteria and application possibilities, in order to later confront them with the rules of Brazilian Criminal Procedural Law, notably the Right to non-self-incrimination and the presumption of innocence as a treatment rule, a judgment rule, and an evidence rule. Precedents from the Brazilian Superior Courts are used to confirm the arguments adopted and to establish conclusions.

Keywords: Encrypted Devices; Right not to self-incrimination; Foregone Conclusion; Brazilian Criminal Procedural Law.

A característica de um dispositivo informático cifrado decorre de um procedimento tecnológico desenvolvido por complexas fórmulas matemáticas, em que as informações e os dados nele armazenados se tornam ilegíveis, sendo somente possível o seu acesso e decodificação por meio do uso de senhas pessoais. Tal ferramenta é disponibilizada por diversas empresas para garantir, em alguma medida, que a privacidade, a intimidade e a segurança possam se manter em comunicações realizadas e no armazenamento de arquivos em memória (PORTILLO; MATTEO, 2021, p. 179).

Essas informações despertam interesse das autoridades de persecução penal para a obtenção de conhecimento sobre fatos e pessoas suspeitas de práticas ilícitas. Neste sentido, o tema importa sensivelmente às suas repercussões quanto aos limites da investigação diante da identificação e obtenção de fontes de prova digital. Quando o fornecimento do acesso, por senha, transmitida oralmente ou por escrito, de maneira voluntária e consciente

(BRASIL, 2001) pelo suspeito à autoridade policial não aparentando qualquer vício na voluntariedade do fornecimento, não haveria que se falar em violações ao direito contra a autoincriminação (OLIVEIRA E SILVA, 2019, p. 357-358).

Todavia, a questão problemática direciona-se à possibilidade de as Autoridades Investigativas ou Judiciais forçarem o sujeito investigado ao fornecimento da senha para acesso, ou ainda de utilizarem meios enganosos para a obtenção deste. Neste sentido, aponta-se a estreita relação desta investida e as repercussões com o direito à não autoincriminação. A análise da temática sob o prisma do *privilege against self-incrimination* norte-americano, traz reflexões interessantes quanto às investidas coercitivas. Conforme salienta **Casey** (2011, p. 116), o privilégio é composto por três aspectos: i) compulsão que é marcada pela intenção de “extorquir” informações de comunicação; ii) “testemunhal”, orais ou escritas; com iii) conteúdo incriminatório.

Sendo a criptografia ferramenta utilizada para proteger o conteúdo de informações em um computador ou em outra mídia de armazenamento, o fornecimento de "senha" para acesso mediante compulsão – seja em momento de prisão em flagrante delito, seja após determinação judicial –, violaria o direito à não incriminação. É claro que a "senha" por si só não tem conteúdo autoincriminatório, todavia, torna-se responsável pelo desencadeamento de atos capazes de alcançarem provas necessárias (com conteúdo incriminatório) para que se possa subsidiar uma acusação formalizada. O fornecimento da "senha" seria, portanto, aquilo considerado uma declaração de pensamento. As autoridades de persecução penal, neste cenário, por compulsão, alcançariam uma informação de caráter "testemunhal" útil para a aquisição de conteúdo incriminatório (KERR, 2019, p. 3).

Entretanto, as conclusões não são semelhantes quando o acesso aos dispositivos informáticos, para além do uso de senhas pessoais, também é possível por meio de dispositivo *Touch ID* (sensor biométrico), reconhecimentos faciais ou leituras da íris do usuário. Diante destes instrumentos de acesso e, portanto, decodificação dos arquivos e informações constantes no dispositivo visado, tais critérios de materialização do *privilege against self-incrimination* não são suficientes para garantir um nível de proteção razoável ao imputado (SACHAROFF, 2018).

Nestas situações, a jurisprudência norte-americana tem fixado entendimento diverso. Quanto ao acesso a partir de sensor biométrico, no caso *Commonwealth of Virginia v. Baust* (ESTADOS UNIDOS, 2014), David Charles Baust foi compelido a desbloquear o seu dispositivo informático, colocando sua impressão digital para leitura biométrica, justificando-se que tal decisão não implicaria em qualquer violação ao *privilege against self-incrimination*, pois a ação determinada a Baust não teria caráter testemunhal. O caráter testemunhal de um ato, para fins de proteção do privilégio, caracteriza-se quando o imputado: "deve revelar o conteúdo de seu pensamento" (KERR, 2019, p. 771). Neste sentido, o embasamento para sustentação decisória se guiou também por outros precedentes americanos de que, por vezes, ainda que o acusado não produza qualquer declaração oral, seu corpo pode ser utilizado como fonte de prova (ESTADOS UNIDOS, 1966).

Polansky (2020, p. 82-86), em comparação entre a jurisprudência norte-americana e a jurisprudência argentina, aponta que, em um segundo caso, o Governo dos Estados Unidos investigava um domicílio no qual considerava possível a existência de acesso a materiais de pornografia infantil. Desta forma, requereu mandado judicial para que ao ingressar no lugar, pudesse apreender dispositivos de armazenamento digital e posterior análise de seu conteúdo. Ademais, requereu que, caso encontrados celulares ou tablets, pudesse obrigar os sujeitos presentes a desbloquearem os dispositivos mediante sensor biométrico de impressão digital.

A ordem judicial deferiu parcialmente o requerimento, afirmando que seria possível a apreensão, porém os desbloqueios compulsivos não se justificavam no caso em concreto, uma vez que o pedido era "genérico", sem elementos probatórios suficientes para autorização, pois não se faziam presentes informações sobre quais pessoas e dispositivos se encontrariam no domicílio investigado. Segundo narra o autor, o argumento que justificou o indeferimento parcial, era o desconhecimento acerca da propriedade dos celulares, portanto: "o desbloqueio compulsivo destes possuiria conteúdo 'testemunhal implícito'". Porém, tal decisão foi reformada posteriormente, sob a argumentação de que a medida de desbloqueio não carecia de conteúdo testemunhal, logo estaria autorizada constitucionalmente: "desde que a Autoridade Policial indicasse quais dos dedos deviam ser colocados nos dispositivos, assim a medida não dependeria de atividade comunicativa por parte dos usuários-alvos".

"SENDO A CRIPTOGRAFIA FERRAMENTA UTILIZADA PARA PROTEGER O CONTEÚDO DE INFORMAÇÕES EM UM COMPUTADOR OU EM OUTRA MÍDIA DE ARMAZENAMENTO, O FORNECIMENTO DE "SENHA" PARA ACESSO MEDIANTE COMPULSÃO – SEJA EM MOMENTO DE PRISÃO EM FLAGRANTE DELITO, SEJA APOS DETERMINAÇÃO JUDICIAL –, VIOLARIA O DIREITO A NÃO INCRIMINAÇÃO."

Semelhante situação, segundo o autor (POLANSKY, 2020, p. 82-86), pode ser observada no caso *State of Minnesota v. Matthew Vaughn Diamond* (ESTADOS UNIDOS, 2018, p. 6). Neste caso, a Corte considerou que o desbloqueio de um celular mediante acesso biométrico do acusado não violaria a garantia contra a autoincriminação, pois existem certos atos físicos que o imputado pode ser obrigado a praticar sem que isso implique em violação ao privilégio contra a autoincriminação (ESTADOS UNIDOS, 2018, p. 7).

Polansky (2020, p. 82-86), reforça que no Direito norte-americano, entende-se que alguns atos físicos até podem representar "testemunhos" explícitos ou implícitos, como a entrega de documentação em que se deduz o controle e a posse por parte do acusado, mas não se aplicaria ao caso em questão. Contudo, esta mesma orientação jurisprudencial não se aplica quando o acesso aos dispositivos digitais se efetiva mediante o

reconhecimento facial ou leitor de íris. Salienta o autor que a jurisprudência argentina tem se aproximado desses entendimentos.

Todavia, argumenta **Polansky** em sentido diverso. Sustenta o autor que as medidas de desbloqueio de dispositivos visados dispõem de conteúdo "testemunhal" implícito, pois a partir da atividade de desbloqueio, o indivíduo informa: "às autoridades estatais que é o usuário deste dispositivo, que tem controle sobre ele e, portanto (salvo prova em contrário), que seu conteúdo lhe pertence" (2020, p. 90). A exceção a tal entendimento, segundo o autor, somente se justificaria em casos que as autoridades estatais já tivessem, antes de sua produção, conhecimento de quem utiliza e controla o conteúdo do telefone. Assim, as informações implícitas que se derivariam do desbloqueio compulsivo do telefone não aportariam nenhuma informação nova. Ratificar-se-ia um conhecimento que os órgãos de persecução penal já teriam anteriormente. É dizer: "a evidência independente do governo, de que o suspeito conhece

a senha, significa que o conhecimento do suspeito não está em questão" (KERR, 2019, p. 783). Tal entendimento se firmaria na doutrina estadunidense denominada "*foregone conclusion*" (POLANSKY, 2020, p. 95).

Segundo o autor, justificar-se-ia, assim, a medida compulsória de desbloqueio, sem resultar na violação à garantia contra a autoincriminação – tolerável, portanto, – nos casos em que o Estado demonstrasse ter conhecimento *a priori*, da informação implícita que se derivaria do desbloqueio (KERR, 2019, p. 773). Ou seja, que tem conhecimento de quem é o usuário do dispositivo informático e de quem tem o controle sobre o conteúdo do dispositivo.

Porém, como explica Kerr (2019, p. 774-775), o entendimento da doutrina *foregone conclusion*, firma-se na proibição de uma vantagem processual. É dizer, se as autoridades estatais já conhecem o fato e têm outra forma de prová-lo, então não obtêm vantagem testemunhal ao alcançar as informações implícitas do réu mediante compulsão. Segundo palavras do autor, a doutrina é obscura, pois, de um lado, coloca o ônus de provar às autoridades estatais quanto ao conhecimento prévio das informações a se obter, por outro lado, não torna claro sobre o grau de certeza que o Estado deve dispor. Por isso, tendencialmente os tribunais americanos expressam que as autoridades estatais de investigação dispõem de um ônus quanto à "especificidade da descrição dos documentos solicitados".

O questionamento proposto pelo autor é se, após a superação da proteção pelo *privilege*, as autoridades estatais poderiam utilizar dos "testemunhos implícitos" do acusado para provar sua culpa no julgamento. A conclusão que alcança é negativa, informando ser este um limite sensato, pois se a possibilidade de obrigar a execução de um ato compulsório ao acusado implica numa inexistência de vantagem, o conhecimento posterior à realização do ato compulsório mostrar-se-ia desnecessário para a comprovação da culpa (KERR, 2019, p. 776).

Apesar do obscurantismo apontado por **Kerr**, cabe pensar se tal doutrina poderia ser aplicada no Direito brasileiro. A resposta parece ser negativa. Pela doutrina americana seria possível que pessoas presas em posse de dispositivos informáticos fossem compelidas a desbloquear os aparelhos se fosse plausível o seu controle e domínio pelo sujeito preso. Obviamente, os indivíduos normalmente sabem a senha dos dispositivos que usam regularmente. Logo, a "evidência" de que a pessoa usa regularmente um determinado dispositivo geralmente deve ser suficiente para mostrar o conhecimento da senha. Nesse caso, indicar-se-ia que o imputado conhece a senha, portanto, estaria apto ao desbloqueio compulsivo.

Em tais contextos, a jurisprudência dos tribunais superiores brasileiros aponta para a afirmação e sustentação do direito à não autoincriminação que se materializa na recusa do imputado em apresentar senha de aparelho celular, ainda que legalmente apreendido. A título ilustrativo, o Superior Tribunal de Justiça asseverou em julgado (BRASIL, 2020a) que:

Em atenção ao direito à não autoincriminação, o acusado não pode ser compelido a colaborar com a persecução criminal. Assim, o fornecimento de senhas para o acesso a aparelhos telefônicos, ainda que determinado em decisão judicial, constitui faculdade do acusado, que tem o direito de não fornecê-las, sendo vedada a imposição de sanções penais e/ou processuais pela não adesão do Réu à produção probatória.

Mesmo constituindo faculdade do acusado, há uma preocupação

recente do Supremo Tribunal Federal em grau de exigência comprobatória da voluntariedade. Os argumentos trazidos pelo Min. **Gilmar Mendes**, do Supremo Tribunal Federal, em voto proferido nos autos do processo de *Habeas Corpus* 168.052-SP (BRASIL, 2020b), servem também, de modo ilustrativo, que aos órgãos de persecução penal deve se impor uma comprovação do grau de voluntariedade relacionado ao direito à não autoincriminação.

Assim, afirmou o Ministro que:

O STF poderia caminhar para a criação de uma fórmula de garantia dos direitos das pessoas investigadas cuja inobservância leve à nulidade dos atos de investigação e coleta de provas, mesmo que durante o inquérito policial – tal como ocorreu no relevante precedente estabelecido pela Suprema Corte dos Estados Unidos em 1966, no julgamento do caso *Miranda v. Arizona* (384 U.S. 436) (BRASIL, 2020b).

Cita o Ministro que:

A Suprema Corte dos Estados Unidos decidiu que a acusação não poderia se utilizar de declarações obtidas por agentes policiais após a apreensão ou detenção de acusados, sem a demonstração da utilização de procedimentos que evidenciassem a proteção contra a autoincriminação (BRASIL, 2020b).

O entendimento do Supremo Tribunal Federal também demonstra que o direito à não autoincriminação veda a obrigatoriedade de fornecimento de senha de acesso por parte do imputado às autoridades investigativas. No Agravo em Recurso Extraordinário 1350870/MS, de Relatoria do Min. **Alexandre de Moraes**, julgado no ano de 2021, afirmou o Ministro que:

Apesar de ter sido demonstrado que a intenção do Acusado seria de burlar a investigação para que não fosse encontrado o conteúdo existente no seu celular, não há falar na caracterização do crime de obstrução à justiça, visto que a conduta praticada pelo Apelante ficou acobertada pelos princípios da ampla defesa e da não autoincriminação (*nemo tenetur se detegere*), previsto no Art. 5º, LXIII, da Lei Maior e art. 8º, seção 2, "g", do Pacto de São José da Costa Rica, que permite ao Acusado se abster de produzir provas que o incriminem (BRASIL, 2021).

No mesmo sentido, consegue-se extrair o entendimento do *Habeas Corpus* 131.946-MG (BRASIL, 2016), de Relatoria do Min. **Edson Fachin**. Este afirmou que: "embora a decisão não esclareça de que modo o paciente estaria ocultando provas, os relatórios policiais afirmam que o acusado não desbloqueou o seu aparelho celular e, dessa forma, não franqueou acesso de tais informações às forças policiais". De acordo com o entendimento afirmado: "tal argumento é neutro à obstrução da persecução", pois:

O direito ao silêncio, compreendido em sentido amplo, abarca resultados probatórios que pressuponham condutas ativas do acusado, sob pena de que se admita a exigência de contribuição involuntária por parte do acusado com o intuito de suprir o encargo probatório que incumbe à acusação (BRASIL, 2016).

Ressalta ainda o Ministro que:

Se assim não fosse, admitindo-se consequência gravosa como resultado de uma prerrogativa, negar-se-ia a essência do princípio do *nemo tenetur se detegere* e, na prática, haveria verdadeira inversão do ônus da prova, providência que, à obvidade, não se conforma com o sistema processual penal (BRASIL, 2016).

Ou seja, observa-se que a essência do direito à não autoincriminação que uma vez negado refletiria em inversão do ônus probatório no processo penal, é – verdadeiramente – a presunção de inocência. A presunção de inocência, vale ressaltar, em seu aspecto de regra de tratamento e probatória. Como assevera **Illuminati** (1979, p. 28), a

leitura alternativa da presunção de inocência como regra de tratamento do imputado, ou como regra probatória e de julgamento, deve ser resolvida no sentido de que os significados apresentam grau de coexistência.

Neste contexto, quanto às mencionadas vedações da imposição de condutas ativas do acusado, esboçada pelo Ministro do Supremo Tribunal Federal, cabe ressaltar o que **Kerr** (2019, p. 781) aponta, a decodificação pelo sujeito imputado acarreta na revelação do conteúdo armazenado. O conteúdo legível, portanto, pode incorrer em uma confissão assinada de maneira forçada. Com a decodificação, seja por qualquer forma de acesso biométrico, a informação de valor probatório passa a existir de forma tal, diferente do que ocorre com a proteção pela codificação/criptografia. Com a codificação, a informação de valor probatório inexistente. Portanto, o ato de acesso, compelido ou voluntário, traduz no ato de revelação.

O *Habeas Corpus* 131.946-MG, de Relatoria do Min. **Edson Fachin**, também esboça outro argumento capaz de sustentar a inaplicabilidade da doutrina norte-americana denominada *foregone conclusion*. Ressalta o Ministro que:

Em outros sistemas, é garantido que o acusado opte entre prestar declarações ou não. Mas, o fazendo, submete-se ao dever de dizer a verdade, sob pena de perjúrio. A hipótese brasileira não consagra essa obrigatoriedade, subtraindo do acusado, ainda que faltante com a verdade, a responsabilização penal (BRASIL, 2016).

Esta roupagem jurisprudencial esclarece aquilo apontado por **Illuminati** (1979, p. 28), os dois modos de entender a presunção de inocência têm matrizes histórico-culturais distintas, que fixam suas raízes, respectivamente no legalismo dos iluministas continentais e no pragmatismo da gnoseologia jurídica anglo-saxônica.

Para a doutrina esboçada pelos precedentes americanos, isso não impacta na violação do *privilege against self-incrimination*. Todavia, para o Direito brasileiro, tal argumento é de extrema relevância, pois implica dizer que somente passa a existir uma informação de valor probatório relevante, mediante a atuação do sujeito imputado, que contribui para a revelação do seu conteúdo. Não por outra razão, mas pelo fato de ser o Direito brasileiro, de matriz continental,

atrelado à presunção de inocência como fundamento essencial. Uma regra, que como dito, tem três facetas bem demarcadas, com duas compatíveis implicações: i) uma necessária rigidez sob pena de violação do núcleo essencial da presunção de inocência; e ii) o afastamento do sujeito imputado de uma posição colaborativa com a persecução penal, notadamente quanto ao campo probatório processual.

Como aponta **Oliveira e Silva**, um sistema que se propõe a incluir o direito à não autoincriminação em suas coordenadas fundamentais deve reconhecer a faculdade da escolha livre ao imputado tanto em relação à declaração sobre a matéria da imputação, quanto ao exercício do direito ao silêncio. Refere-se, portanto, à liberdade de declaração, afastando todas as formas de compulsão para fornecer declarações utilizáveis como prova acusatória. Como aponta a autora: "cumprindo uma função de tutela antecipada do arguido" (2019, p. 392).

Sendo assim, o direito à não autoincriminação, vinculado à regra da presunção de inocência aparenta ser proteção suficiente para evitar devassas investigativas a partir da sujeição do imputado a um comportamento colaborativo. Porém, a máxima proteção imposta pela regra, mostra-se mais elevada quando em comparação ao Direito norte-americano com reflexos da 5ª Emenda (KERR, 2019, p. 799).

O Direito norte-americano, como afirma **Kerr** (2019, p. 799), em que pese a demonstrada fragilidade do *privilege against self-incrimination*, aponta para uma doutrina de equilíbrio vinculada à 4ª Emenda, que regulamenta buscas e apreensões, evitando assim devassas nas informações pessoais dos imputados. O Direito brasileiro, em contrapartida, apesar da proteção fundamental imposta pela presunção de inocência como regra de tratamento, regra de julgamento e regra probatória, apresenta fragilidades quanto aos limites de proteção contra a amplitude de buscas investigativas. A solução, portanto, similar ao apontado pelo autor, não é uma adoção da doutrina do "equilíbrio" ao direito à não autoincriminação, mas, uma regulamentação adequada às buscas em dispositivos eletrônicos (BRASIL, 2012).

Referências

- BRASIL. Supremo Tribunal Federal. HC 80.949/SP. Rel. Min. Sepúlveda Pertence, Primeira Turma, Dje 14/12/2001.
- BRASIL. Supremo Tribunal Federal. HC 91.867/PA. Rel. Min. Gilmar Mendes, Segunda Turma, Dje 20/09/2012.
- BRASIL. Supremo Tribunal Federal. HC 131.946/MG. Rel. Min. Edson Fachin. Julgamento: 16/12/2015; Dje 01/02/2016.
- BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1875514-MS (2020/0120173-6). Rel. Min. Laurita Vaz. HC 580.664/RJ, Rel. Ministro Nefi Cordeiro, Sexta Turma, julgado em 20/10/2020, Dje 12/11/2020a.
- BRASIL. Supremo Tribunal Federal. HC 168.052/SP. Rel. Min. Gilmar Mendes, Dje 20/10/2020b.
- BRASIL. Supremo Tribunal Federal. ARE 1350870/MS. Recurso Extraordinário com Agravo. Rel. Min. Alexandre de Moraes. Julgamento: 11/10/2021.
- CASEY, Eoghan. Digital evidence and computer crime. 3. ed. San Diego: Elsevier, 2011.
- ESTADOS UNIDOS. U.S. Supreme Court. Schmerber v. California. 384 U.S. 757, n. 658, p. 384, U. S. 760-765, 1966.
- ESTADOS UNIDOS. Commonwealth of Virginia v. Baust. CR14-1439, 2nd Cir. Oct. 28, 2014.
- ESTADOS UNIDOS. State of Minnesota in Supreme Court. State of Minnesota v. Matthew Vaughn Diamond. A15-2075, 2018. Disponível em: <https://mn.gov/law-library-stat/archive/supct/2018/OPA152075-011718.pdf>. Acesso em: set. 2022.
- ILLUMINATI, Giulio. La presunzione d'innocenza dell'imputato. Serie di Diritto. Bologna: Zanichelli, 1979.
- KERR, Orin. Compelled decryption and the privilege against self-incrimination. Texas Law Review, v. 97, n. 767, p. 3, 2019.
- OLIVEIRA E SILVA, Sandra. O arguido como meio de prova contra si mesmo: considerações em torno do princípio nemo tenetur se ipsum accusare. Coimbra: Almedina, 2019.
- POLANSKY, Jonathan. Garantias constitucionales del procedimiento penal en el entorno digital. Buenos Aires: Hammurabi, 2020.
- PORTILLO, Víctor Hugo; MATTEO, Juan Manuel. Autoincriminación y nuevas tecnologías. In: RIQUERT, Marcelo; SUEIRO, Carlos Christian. Sistema penal e informática: cibercrimes, evidencia digital, tics. v. 2. Buenos Aires: Hammurabi, 2021.
- SACHAROFF, Laurent. Unlocking the fifth amendment: passwords and encrypted devices. 87 Fordham Law, v. 87, n. 1, Rev. 203, 2018. Disponível em: <https://irlawnet.fordham.edu/flr/vol87/iss1/9>