

PROCESSO PENAL DIGITAL

Guilherme Banterli

Priscilla Guimarães Cornélio

Sávio Belineli

Resumo

O processo penal digital é um tema de grande relevância para os alunos, especialmente aqueles que estão estudando direito. Neste artigo, iremos explorar os aspectos essenciais desse assunto, discutindo desde sua definição e características até os impactos que ele pode ter no sistema judiciário. Com uma abordagem intelectual, buscamos fornecer um panorama abrangente sobre o assunto, permitindo que os alunos aprofundem seus conhecimentos nessa área em constante evolução.

Palavras-chave: Direito Processual Penal; Direito Penal

Abstract

The digital criminal procedure is a topic of great relevance for students, especially those who are studying law. In this article, we will explore the essential aspects of this subject, discussing everything from its definition and characteristics to the impacts it can have on the judicial system. With an intellectual approach, we seek to provide a comprehensive overview of the subject, allowing students to deepen their knowledge in this constantly evolving area.

Keywords: Criminal Procedural Law; criminal law

Introdução

A utilização das tecnologias possibilitou o aprimoramento do *modus operandi* de crimes que já encontram previsão no Código Penal tempos antes do advento desses recursos. Somado a isso, outros crimes que antes sequer eram

considerados como condutas possivelmente realizáveis, passaram a ser frequentes no universo da internet.

Nesse contexto, a persecução penal precisa se ajustar a nova dinâmica delitiva. Ou seja, a persecução penal deve estar adaptada para compreender e adaptar-se as novas tecnologias, bem como para permitir a localização e identificação desses crimes.

A título de exemplo tem-se a Lei 9.296/96 que regulamenta a interceptação telefônica enquanto meio de obtenção de prova. Na atualidade, contudo, tal meio torna-se cada vez mais obsoleto, pois, com a ascensão das redes sociais e outros meios de comunicação como o Whatsapp, a prática delitiva pela via telefônica - ligação telefônica - é cada vez mais rara.

1. Dificuldades na persecução

Há uma clara dificuldade na própria elucidação dos crimes cometidos com a utilização de instrumentos tecnológicos, notadamente no contexto em que existem uma série de sistemas de segurança que impedem o acesso aos dados, como a criptografia ponta a ponta.

Além disso a própria preservação da cadeia de custódia é uma tarefa árdua, diante da fluidez dos dados e facilidade com a qual estes e, conseqüentemente, os rastros do delito, podem ser apagados.

Por diversas vezes, os crimes possuem vítimas difusas, implicando em dificuldades na produção probatória, além da maior gravidade das condutas, posto que são capazes de atingir um número indeterminado de indivíduos.

A definição do tempo do crime e também da competência para o processo e julgamento é outro ponto de destaque e que gera discussão na doutrina e jurisprudência.

A solução para a maior parte dessas questões perpassa pelo uso das novas tecnologias também na persecução penal, ou seja, na apuração dos crimes. Contudo, nesse momento, temos outro ponto de embate que é o direito constitucional a privacidade, garantia à intimidade e à vida privada.

Não obstante, nota-se que a própria legislação processual penal tem tentado se adequar a essa nova realidade. Nesse sentido, destaca-se o art. 13-B, incluído ao CPP pela Lei 13.344/16:

Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os **meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.**

Além disso, a legislação especial tem inovado com a regulamentação de meios de obtenção de prova que se valem das novas tecnologias. Nesse contexto destaca-se a infiltração virtual de agentes.

1.1. Comunicação dos atos processuais

Em 2021, nos autos do RHC 159.560/RS o STJ reconheceu a possibilidade de que a **citação do acusado** seja realizada por **WhatsApp**. A legalidade do ato, contudo, depende da adoção de medidas para atestar a autenticidade do número telefônico e a identidade do destinatário do ato processual.

Sobre o tema, ainda:

(...) 5. O Tribunal de origem deixou bem registrado que, no caso concreto, foram observadas todas as diretrizes previstas para a prática do ato, sendo a lisura da citação do paciente pelo aplicativo WhatsApp demonstrada ao menos pelos seguintes elementos: número telefônico fornecido pelo concunhado; confirmação da sua identidade por telefone pelo oficial de justiça quando da citação e certificação realizada por ele; utilização do mesmo número de telefone para confirmação de sua identidade, com posterior comparecimento para interrogatório, pela autoridade policial; anuência quanto à realização do ato; informação de que o réu não possuía condições para contratação de profissional para patrocinar sua defesa, de modo que foi nomeada a Defensoria Pública. 6. Ora, fica cristalino que foi indicado com precisão todo o procedimento adotado para identificar o citando e atestar a sua identidade, o que garante a higidez das diretrizes previstas no artigo 357 do Código de Processo Penal. Destaque-se que, no mencionado dispositivo, não há exigência do encontro físico do citando com o oficial de justiça. **Verificada a identidade e cumpridas as diretrizes previstas na norma procedimental, ainda que de forma remota, a citação é válida.** (AgRg no HC 685.286/PR, Rel. Ministro ANTONIO SALDANHA PALHEIRO, SEXTA TURMA, julgado em 22/02/2022, DJe 25/02/2022)

Já no tocante a vítima, desde a edição da Lei 11.690/08, que alterou a redação do art. 201, §3º do CPP, admite-se a **intimação por meio eletrônico**.

Art. 201. § 3º As comunicações ao ofendido deverão ser feitas no endereço por ele indicado, admitindo-se, por opção do ofendido, o uso de meio eletrônico.

2. Provas Digitais

As provas digitais estão intimamente conectadas aos crimes digitais. Mas quais são os crimes digitais? É preciso analisar os delitos sob duas perspectivas para responder a esse questionamento: os bens jurídicos protegidos e o *modus operandi*.

A doutrina classifica os crimes digitais em **próprios ou puros** quando o bem jurídico protegido é o sistema informático e os dados informáticos. Assim, a conduta criminosa recai sobre o computador e seus componentes ou sobre o sistema operacional e seus programas. Ex.: art. 154-A, CP.

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

Lado outro, os crimes digitais **impróprios ou impuros** utilizam a tecnologia de forma acidental, como instrumento para a execução do crime, incidindo sobre o *modus operandi*. Ex.: crimes contra a honra praticados por meio das redes sociais.

Feita a devida conceituação, podemos adentrar no tema das provas propriamente ditas.

As atitudes realizadas com suporte eletrônico deixam rastros, logo, é necessário saber encontrá-los, pois servirão de provas no processo penal.

2.1. Perícia forense digital ou computacional

A perícia computacional é um braço da ciência forense especializada em buscar vestígios de usuários que se utilizam da informática para as atividades ilícitas. As atividades realizadas no ambiente virtual fazem com que os sistemas operacionais gravem arquivos que revelem conteúdo, datas, horas e os números de IP envolvidos – número que identifica o usuário na internet –, esses dados digitais descobertos, quando materializados, irão integrar o processo judicial. Mesmo que os infratores deletem arquivos para despistar a suspeita contra eles, os dados

continuam gravados até que sejam sobrepostos e definitivamente descartados. É neste momento, na tentativa de recuperar os dados e usá-los para auxiliar a Justiça, que entra o trabalho da perícia forense computacional.

A perícia forense digital trabalha com evidências digitais que serão filtradas, quer sejam em componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais. Nesse contexto, o profissional precisa ser altamente capacitado e atualizado, possuindo uma habilidade para a recuperação de dados, análise de dados na internet e em tráfego de redes, análise de vírus, análise de ataques e dados entre os quais já foram apagados, cifrados ou danificados há um tempo.

Trata-se de um campo novo no Brasil, ainda em desenvolvimento e que carece de uma padronização dos procedimentos periciais. Nesse contexto, a doutrina de Carlos Henrique Calazans e Sandra Maria Calazans aponta que, para garantir o seu valor judicial, procedimentos serão ordenados estritamente às normas gerais que abrangem todo o tipo de perícia.

2.2. Requerimento de guarda de registros de acesso

Autoridade policial, administrativa e o Ministério Público, independentemente de autorização judicial, podem requerer a guarda dos registros de acesso a aplicações de internet ou registros de conexão. Ou seja, as autoridades podem solicitar a preservação das informações diretamente às empresas que as têm sob custódia.

Assim dispõe a Lei 12.965/14 (Marco Civil da Internet):

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público **poderá requerer cautelarmente que os registros de conexão sejam guardados** por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

§ 5º 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.

Conforme entendimento do STJ, inclusive, o requerimento pode extrapolar os prazos previstos em lei, independentemente de prévia autorização judicial. Vejamos:

O requerimento de simples guarda dos registros de acesso a aplicações de internet ou registros de conexão por prazo superior ao legal, feito por autoridade policial, administrativa ou Ministério Público, prescinde de prévia autorização judicial.

Caso concreto: o MP instaurou procedimento de investigação criminal. O Promotor enviou ofícios à Apple e a Google requerendo que tais empresas preservassem os dados telemáticos dos investigados enquanto o Poder Judiciário não aprecia os pedidos de quebra do sigilo. Não há ilegalidade nesse pedido, não sendo necessária prévia autorização judicial.

STJ. 6ª Turma. HC 626.983-PR, Rel. Min. Olindo Menezes (Desembargador Convocado do TRF da 1ª Região), julgado em 08/02/2022 (Info 724).

Nesse ponto, contudo, cabe analisar a questão relativa a **criptografia ponta a ponta**.

O sistema de segurança mediante criptografia ponta a ponta impede o acesso da própria empresa fornecedora do serviço do acesso às informações veiculadas por seus usuários, como ocorre nas mensagens enviadas via Whatsapp.

Logo, a Corte reconhece a impossibilidade técnica de fornecimento das informações, razão pela qual descabe impor a multa (astreintes) decorrente do descumprimento de uma obrigação judicial. Sobre o tema, inclusive, há ações de controle de constitucionalidade em trâmite no STF, cujo acompanhamento é importante, pois assim que julgadas certamente será cobrada em provas. Trata-se da ADI 5527 e da ADPF 403.

3. Delegacias Especializadas

O Estado de São Paulo, atento ao desenvolvimento dos crimes praticados com o uso da internet, desde 2001, criou uma Delegacia especializada em crimes de informática (Decreto n. 46.149, de 2 de outubro de 2001).

A Unidade investiga crimes de informática próprios e impróprios, atuando somente nos praticados na cidade de São Paulo, sendo que tal competência se estabelece pelo domicílio da vítima. Nos demais municípios do Estado, que não possuem delegacia especializada, os crimes de informática são investigados pelas Delegacias de Polícia locais.

Além disso, quando há necessidade da realização de perícias, estas são feitas pelo Instituto de Criminalística, que possui um núcleo de informática.

Nessa área de investigação a Polícia Civil do Estado de São Paulo é referência nacional, visto que começou a trabalhar especificamente na área quando ainda não se falava tanto no assunto pelo país, antes do desenvolvimento das modalidades delitivas mais complexas, que hoje são perpetradas no meio virtual.

Em 2012 foi promulgada no Brasil a Lei 12.735/12, cujo art. 4º dispõe que os órgãos da polícia judiciária estruturarão, conforme regulamentação, setores e equipes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Nesse contexto, outros Estados passaram a seguir o exemplo paulista e instituir delegacias especializadas, como é o caso do Rio de Janeiro, Curitiba e Belo Horizonte.

Considerações Finais

Diante do estudo realizado, ficou evidente que o Delegado de Polícia, enquanto detentor de cargo de natureza jurídica, tem capacidade técnica para aplicar o princípio da insignificância. Não se trata, pois, de uma faculdade da autoridade, mas um dever diante da função que lhe fora constitucionalmente atribuída, enquanto primeiro garantidor dos direitos fundamentais do indivíduo no contexto do Estado Democrático de Direito.

Referências

- AVENA, Norberto. **Processo Penal**. 10.ed.rev., atual. e ampl. Rio de Janeiro: Forense, São Paulo: Método, 2018.
- CAPEZ, Fernando. **Curso de Processo Penal**. 23ª ed. São Paulo: Saraiva, 2016.
- CUNHA, Rogério Sanches. **Manual de Direito Penal: parte geral**. 2.ed. Bahia: JusPodivm, 2014.
- GOMES, Luiz Flávio Gomes; SCLIAR, Fábio. **Investigação preliminar, polícia judiciária e autonomia**. 21/10/2008. Disponível em: <<http://www.lfg.com.br>>. Acesso em 01/05/2021.
- LIMA, Renato Brasileiro de. **Legislação criminal especial comentada**. 4 ed. Salvador: Juspodivm, 2014.
- MENDES DE ALMEIDA, Joaquim Canuto. **Princípios fundamentais do processo penal**. São Paulo: Revista dos Tribunais, 1973.

MIRABETE, Julio Fabbrini; FABBRINI, Renato. **Manual de direito penal – parte geral, v. I.** 23ª ed. São Paulo: Atlas, 2006.

NICOLITT, André. **Manuel de processo penal.** 2 ed. Rio de Janeiro: Elsevier, 2010.

NUCCI, Guilherme de Souza. **Manual de processo penal e execução penal.** 11 ed. Rio de Janeiro: Forense, 2014.

PEREIRA, Eliomar da Silva. In: DEZAN, Sandro Lúcio; PEREIRA, Eliomar da Silva (Org.). **Investigação criminal.** 1 ed. Curitiba: Juruá, 2013.

RANGEL, Paulo. **Direito Processual Penal.** 23 ed. Rio de Janeiro: Atlas S.A., 2015.

SANTOS, Juarez Cirino dos. **Direito Penal: Parte Geral.** Curitiba: Lumen Juris, 2008.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal.** 11 ed. Salvador: JusPodivm, 2016.