Penal, processo penal e tecnologia

13/03/2025

A tecnologia destina-se a atender às necessidades do ser humano, facilitando a vida e proporcionando conforto, dividindo-se em diversas áreas, tais como tecnologia da informação, tecnologia industrial, tecnologia médica, tecnologia da comunicação, dentre outras. No campo do Direito, concentram-se os interesses na informação e na comunicação.

Desfrutando das vantagens e buscando contornar as desvantagens, a tecnologia está presente no Direito Penal e no Processo Penal. Há vantagens evidentes no campo da produção de provas, como, por exemplo: formação da materialidade por meio de avançadas técnicas (exame de DNA, reconstituição virtual do crime, hematologia forense etc.), informatização do processo (rapidez no trâmite, facilidade de acesso das partes, publicidade mais abrangente, otimização de arquivos para processos físicos), existência do reconhecimento fácil (favorecimento da identificação de criminosos foragidos), monitoramento cada vez mais extenso de lugares públicos por sofisticadas câmeras (registro de práticas de crimes, com posterior uso em juízo), programas de cálculo de penas com softwares específicos (facilitador de cálculos, evitando-se erros materiais), admissibilidade de recursos por inteligência artificial (aceleração do processamento de recursos especial e extraordinário), medidas assecuratórias efetivadas online, assim como mandados de prisão inseridos em banco de dados nacional, propiciando a detenção de procurados em qualquer lugar do território, registro de depoimentos em mídia audiovisual (favorecimento de análise do conteúdo e da firmeza ou insegurança das testemunhas, das vítimas e réus pelos julgadores nos tribunais), viabilização de teleaudiências e julgamentos telepresenciais nos tribunais (facilitar a participação das partes à distância).

As desvantagens podem gerar alguns problemas, como a *pericialização* das provas em prejuízo das demais e da avaliação judicial (predomínio cada vez maior do parecer pericial, podendo superar outras relevantes provas e até mesmo o critério judicial de análise do conjunto probatório), os recursos atinentes a reconhecimento facial e monitoração por câmeras constituem instrumentos de invasão de privacidade e de intimidade (pessoas inocentes podem ser acompanhadas em seus afazeres cotidianos), os programas para o cálculo de penas podem levar os julgadores a desacostumar do procedimento (conforme a amplitude, é possível desencadear a padronização da aplicação da pena, desvinculada da análise individualizada dos casos), a inteligência artificial comete erros e fornece dados falsos, pois está em constante *aprendizado* (há registros de erros judiciários ou das partes ao formatar peças nos processos, com confiança excessiva na IA), a rejeição de recursos pode basear-se em equívoco da inteligência artificial (exige da parte interessada pronta atuação para reclamar, por meio de recurso apropriado), a geração de culpa prematura e indevida, além do denominado *cancelamento digital* (o prejulgamento de pessoas suspeitas da prática de crimes têm levado a imediata *condenação* pela opinião pública das redes sociais, com consequências imediatas e concretas para os presumidos autores).

Já no âmbito do Tribunal do Júri, a disseminação de informações do crime e do suspeito pode atingir os potenciais jurados (não há nem mesmo fundamento para o desaforamento, pois inexiste prova do alcance das notícias do delito). Além disso, a desigualdade digital, gerando o engajamento cada vez maior de alguns e o distanciamento de muitos outros, visto que camadas menos favorecidas economicamente têm precário acesso à internet e à inteligência artificial (reflexos no desequilíbrio das partes no processo, com deficiência na defesa de réus hipossuficientes), a complexidade tecnológica (o domínio dos operadores do direito não é fácil, desacostumados ao ambiente digital e ainda habituados às ferramentas tradicionais), a falsificação de provas (programas avançados e inteligência artificial são capazes de montar fotos, vídeos e áudios inverídicos, com efeitos no processo), a paralisação de sistemas informatizados por invasão de *hackers* (influência no trâmite processual, com lentidão ou suspensão de trabalhos forenses) e a captação de dados sigilosos armazenados nos sistemas dos tribunais (invasões podem violar segredos das partes).

O avanço da legislação penal é uma realidade no cenário digital. No âmbito dos crimes contra a vida, em 2019, o artigo 122 do Código Penal foi alterado para incluir, junto ao induzimento, instigação e auxílio ao suicídio, as mesmas condutas para a automutilação. Um dos principais motivos para gerar a modificação do tipo penal originou-se do jogo denominado “baleia azul”, com origem na Rússia, espalhando-se pelo mundo. Consistia em promover, pela internet, desafios com cerca de 50 níveis de dificuldade, atingindo o fecho, que é o suicídio.

Vários adolescentes integraram esse jogo, além de adultos. As tarefas baseavam-se em desafios mais simples, no início, como assistir filmes de terror, durante a madrugada, subir em telhados de edifícios, fazer desenhos na própria pele com instrumentos cortantes até chegar à automutilação e, por consequência, ao suicídio. Foram registradas mortes de adolescentes em cidades brasileiras e outros casos de lesões leves e graves. Por isso, a alteração do tipo penal do artigo 122 do Código Penal, levando em consideração os meios tecnológicos – digitais – pelos quais os agentes criminosos

atingem suas vítimas.

Estende-se amplamente, pela rede mundial de computadores e pelos aplicativos de mensagens, a prática de crimes contra a honra (calúnia, difamação e injúria), levando-se em consideração a facilidade de se postar qualquer comentário ofensivo à reputação de outrem e, com isso, alcançar um número inestimável de pessoas. O delito contra a honra ganha relevo peculiar, quando praticado pela internet, tanto que o legislador inseriu, em 2019, uma causa específica de aumento de pena (CP, artigo 141, § 2º. Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena).

A liberdade individual pode ser afetada por crimes cometidos pela internet, dentre os quais se encontram a intimidação sistemática (*cyberbullying*), a ameaça, a perseguição (*stalking*) e violência psicológica contra a mulher. As diversas formas de intimidar, perseguir e humilhar pessoas se tornam facilitadas, quando o veículo é a rede mundial de computadores e os aplicativos de mensagens, pois o agente alcança a vítima a qualquer hora.

O crime cibernético próprio, que lida com a inviolabilidade dos segredos, é a invasão de dispositivo informático (artigo 154-A, CP), conectado ou não à internet, com a finalidade de obter, adulterar ou destruir dados ou informações, sem autorização clara ou tácita do usuário, bem como instalar vulnerabilidades para alcançar vantagem ilícita, com pena de reclusão, de 1 a 4 anos, e multa. Ingressa nesse campo a introdução de vírus ou *malware* em dispositivo informático, tanto com o objetivo de causar danos como para conseguir uma vantagem indevida. Inclui-se no crime quem produz, oferece, distribui, vende ou difunde um dispositivo ou programa de computador visando à prática da invasão. A forma qualificada diz respeito, especificamente, ao bem jurídico tutelado e indicado no título da Seção IV (inviolabilidade dos segredos), de modo que, se a invasão provocar a efetiva obtenção de conteúdo de comunicações eletrônicas privadas e sigilosas, gera a pena de reclusão, de 2 a 5 anos, e multa.

No âmbito dos crimes contra o patrimônio, diversas ocorrências fáticas demonstraram a necessidade da criação de tipos incriminadores específicos para lidar com a tecnologia: furto e estelionato com emprego de dispositivos eletrônicos ou informáticos. O furto qualificado (artigo 155, § 4º-B) indica que a subtração de coisa móvel alheia se faz mediante fraude, valendo-se o agente de dispositivo eletrônico ou informático, com acesso ou não à internet, havendo ou não a violação de qualquer mecanismo de segurança ou o emprego de programa malicioso (*malware*), ampliando-se, por interpretação analógica, a qualquer outro mecanismo fraudulento.

A pena é severa: reclusão, de 4 a 8 anos, e multa. Se na invasão a dispositivo informático do artigo 154-A busca o agente alcançar dados sigilosos ou danificar o seu conteúdo, no caso do furto, por uso de dispositivo informático, a invasão proporciona a *subtração* de valores da vítima. Por isso, o primeiro se dirige à violação da vida privada e da inviolabilidade de segredos e o segundo se volta ao patrimônio.

Noutro campo, o estelionato foi titulado como *fraude eletrônica* (artigo 171, § 2º-A, CP), porque o meio para gerar o erro e o engano, que proporcione ao agente a vantagem indevida, se dá com o uso de informações fornecidas pela própria vítima ou terceira pessoa, induzida por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico falso – abrindo-se a porta, ainda, para qualquer outro meio fraudulento análogo. Aliás, mais grave a pena – corretamente previsto em lei –, tanto para o furto, quanto para o estelionato, quando o servidor da internet se encontra fora do território nacional, o que prejudica a investigação e a apuração do delito, bem como na situação de ter por vítima uma pessoa idosa ou vulnerável.

Em qualquer situação, está-se diante do entrelaçamento do Direito Penal com a tecnologia. Pode-se apontar a tipificação do estelionato previsto no artigo 171-A do Código Penal, envolvendo ativos virtuais, como as criptomoedas, com sanção severa, de reclusão, de 4 a 8 anos, e multa, como um avanço peculiar. Afinal, cuida-se de um tipo incriminador necessário, mas que surgiu antes mesmo da operação com ativos virtuais se tornar comum e abrangente no Brasil, demonstrando que o direito penal, por vezes, acompanha mais de perto a evolução tecnológica.

Spacca

Guilherme Nucci, desembargador

Crimes contra a dignidade sexual

Não se olvide, ainda, a *extorsão sexual*, inserida no contexto da invasão de privacidade, em que o agente, conseguindo, de algum modo, foto ou vídeo da vítima, em sua intimidade sexual – mesclando-se com o crime do artigo 216-B (registro não autorizado da intimidade sexual) em muitos casos – alcança indevida vantagem econômica, sob a ameaça de divulgação desse conteúdo na Internet ou distribuição para outras pessoas. Finalmente, ainda no campo da extorsão, encontra-se o *sequestro de dados*, por meio do qual o agente infecta um sistema de dados de empresa, instalando um vírus ou *malware*, bem como qualquer mecanismo apto a criptografar esse conteúdo, tornando-o inacessível até que lhe seja pago um *resgate*, vale dizer, uma vantagem econômica indevida. Não se esgota, por certo, o amplo avanço compassado e ritmado da tecnologia e do crime, viabilizando a atuação do direito penal.

Um dos mais sensíveis cenários das infrações penais em que a tecnologia avançada desponta, grande parte concentrada na navegação pela internet e no uso de redes sociais e aplicativos de mensagens, está concentrada nos crimes contra a dignidade sexual. E, com maior gravidade, contra vulneráveis menores de 18 anos, pois o bem jurídico é complexo, envolvendo não somente a dignidade sexual, mas a formação moral de crianças e adolescentes.

O registro não autorizado da intimidade sexual (artigo 216-B, CP), incluído em 2018, associado à internet e às redes sociais e aplicativos de mensagens, adveio da tutela que se pretende dar à privacidade associada à dignidade sexual, mormente quando se percebeu a lamentável divulgação de fotos ou vídeos de nudez ou de atos sexuais, como decorrência da denominada *pornografia de vingança*. Ilustra-se com o parceiro que, inconformado com o término de um relacionamento amoroso, *vinga-se* da ex-namorada, noiva, cônjuge ou companheira introduzindo na rede mundial de computadores os registros que fez na intimidade do casal. Pode, ainda, enviar a foto ou vídeo, por aplicativo de mensagem, a vários parentes, amigos ou simples conhecidos.

O progresso tecnológico possibilitou a ocorrência do *estupro virtual*, que pode dar-se tanto na forma do artigo 213, quando do artigo 217-A, do Código Penal. Nada impede que, em tempo real, por meio de comunicação digital (telechamada, por exemplo), o agente, mediante grave ameaça, constranja a pessoa com a qual está conectado a se despir e a se tocar, a fim de gerar ato libidinoso (como a masturbação), satisfazendo seu prazer sexual. Essa situação se torna particularmente grave quando envolve criança ou adolescente, configurando o estupro virtual de vulnerável.

No Estatuto da Criança e do Adolescente, há um variado rol de tipos penais incriminadores (artigos 241, 241-A, 241-B, 241-C, 241-D), inseridos em 2008, buscando alcançar a punição de pedófilos, pessoas com transtorno de personalidade parafílico, voltados a ter prazer sexual, dentre outras manifestações, com crianças. Abrange-se, também, a tutela de adolescentes, no tocante à salvaguarda de sua imagem, registrada em qualquer meio (foto, vídeo ou base similar). Esses tipos penais buscam punir quem lida com armazenamento, distribuição de qualquer maneira e produção de imagens de crianças e jovens em cenas de sexo explícito ou pornográficas. Com o avanço tecnológico, algo ampliado pela inteligência artificial, tipificou-se a simulação da participação de criança ou adolescente nessas cenas por meio de adulteração, montagem ou modificação de fotografias, vídeos ou outro formato visual.

Não é demais lembrar que a chamada *pedofilia virtual* é cliente assídua do comércio constante realizado na *deep web*, oculto e dissimulado, difícil de ser localizado, embora envolva atividade investigatória constante das autoridades policiais. Para facilitar a busca de predadores sexuais de infantes, criou-se em 2019 a viabilidade da infiltração *virtual* de agentes policiais (artigo 10-A, Lei 12.850/2013), procurando, na Internet (geralmente, na *deep web*) as organizações criminosas voltadas a crimes sexuais contra crianças e adolescentes.

Considerações finais

Diversos outros tipos penais poderiam ser mencionados para indicar a interligação do Direito Penal e da tecnologia, mas não se pretende esgotar o assunto, vasto pela própria natureza, na exata medida em que o *universo eletrônico* parece cada vez mais ilimitado e, a cada dia, emergem novas técnicas e recursos.

A rede mundial de computadores trouxe a todos os países uma autêntica *revolução* nos campos da informação e da comunicação, com aspectos nitidamente positivos, acompanhado pelos prismas negativos. Em paralelo, caminha o processo penal tecnológico, informatizando processos, digitalizando provas e promovendo atos processuais à distância, o que produz benefícios e malefícios, como expusemos linhas atrás. É preciso acompanhar o avanço tecnológico, sem perder de vista o predomínio da sensibilidade humana no campo jurídico.

Fonte: https://conjur.jumps.com.br/2025-mar-13/penal-processo-penal-e-tecnologia/