Revista Eletrônica de Direito Processual – REDP.
Rio de Janeiro. Ano 16. Volume 23. Número 1. Janeiro a Abril de 2022
Periódico Quadrimestral da Pós-Graduação *Stricto Sensu* em Direito Processual da UERJ
Patrono: José Carlos Barbosa Moreira (*in mem.*). ISSN 1982-7636. pp. 434-457
www.redp.uerj.br

NOVAS TENDÊNCIAS NA INVESTIGAÇÃO DE CRIMES COMPLEXOS EM UM CONTEXTO EUROPEU GLOBALIZADO[1]

NEW TRENDS IN INVESTIGATION OF COMPLEX CRIMES IN A GLOBALIZED EUROPEAN CONTEXT

Federico Bueno de Mata
Professor Titular de Direito Processual da Universidade e Salamanca, Espanha. E-mail: febuma@usal.es

RESUMO: O presente artigo objetiva relacionar o fenômeno dos crimes cibernéticos e os seus desafios em relação ao Direito Processual. Realizar-se-á, nesse contexto, uma análise (i) acerca dos meios de prova mais adequados a esse tipo de crime, bem como (ii) da forma como cada país pode lidar com o assunto nos limites e extensões de sua jurisdição, de modo a realizar investigações que produzam resultados positivos e válidos.

PALAVRAS-CHAVE: Direito Processual Penal espanhol; crimes cibernéticos; investigação tecnológica; Lei Orgânica 13/2015.

ABSTRACT: This article aims to correlate the phenomenon of cybercrime and the challenges related to Procedural Law. It will be analyzed the evidence-finding procedures more adequate for this type of crime. The paper also intends to analyze how each country could deal with this matter within the limits and extensions of its jurisdiction, in order to carry out investigations that produce positive and valid results.

KEYWORDS: Spanish Criminal Procedural Law, cybercrimes; technological investigation; Law 13/2015.

[1] Artigo recebido em 18/10/2021, sob dispensa de revisão.

1. INVESTIGAÇÃO DE CRIMES COMPLEXOS EM UM MUNDO INTERLIGADO

Na Espanha, se olharmos para o último Estudo sobre Cibercrime publicado pelo Ministério do Interior espanhol no ano de 2019[2] podemos ver como o cibercrime é um fenômeno imparável em nosso país. Especificamente, 218.302 casos foram relatados sob investigação, o que representa cerca de 5% do número real de incidentes, e dos quais apenas 30.841 foram resolvidos, o que representa 15,1% dos casos para os quais as investigações foram abertas. Poderíamos assim dizer que alcançar o princípio da legalidade no ciberespaço é utópico, já que em termos globais estaríamos afirmando que os fatos que são esclarecidos são um em cada dez dos que são investigados, ao qual deve ser acrescentada uma enorme porcentagem de casos que não são investigados e que também são realizados em diferentes níveis da Rede. Assim, devemos entender a Rede como um canal multifacetado e multiofensivo, a partir do qual diferentes bens legais individuais e coletivos podem ser atacados ao mesmo tempo, causando danos em um determinado estado e irradiando sua eficácia para sujeitos exponenciais ou coisas localizadas em diferentes partes do mundo.

Assim, o fenômeno do crime online tem uma característica transnacional. Além disso, em tempos recentes, novos conceitos foram acrescentados, tais como a Teia Profunda e a Teia Escura, termos que muitas vezes são confundidos. O primeiro se refere aos dados ocultos do usuário, tudo o que não pode ser visto pelo usuário e que não tem necessariamente que estar associado a tipos de crime. A Dark Web, por outro lado, se referiria ao conteúdo criminoso que é hospedado em sites cujo endereço IP é escondido do usuário, mas que qualquer pessoa pode acessar desde que saiba o endereço específico ou tenha uma espécie de "safe-conduct virtual" para entrar. Muitas vezes estas redes são canais privados para o intercâmbio de arquivos ilícitos ou mesmo redes fechadas de sistemas e estruturas previamente criadas com o propósito de crime. Assim, vemos como o cibercrime, baseado na inclusão de uma rede de computadores para sua execução, está em constante expansão. Sem querer entrar em uma definição terminológica do que pode ser entendido por crimes cibernéticos em sentido estrito ou amplo, pois este é um campo destinado aos criminalistas,

[2] *Estudio sobre la cibercriminalidad en España 2019*, Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Documents/2020/070620-cibercriminalidad.pdf (Fecha de última consulta: 14 de diciembre de 2020).

é importante observar que o crime cibernético não é um crime que possa ser definido em sentido estrito ou amplo[3], mossa tarefa será relacionar este fenômeno com os últimos desafios que esta realidade coloca no nível processual. Especificamente, discutimos como provar este tipo de crime e como a extensão e os limites da jurisdição de cada país podem lidar com este tipo de assunto, pois, como ele aponta corretamente Ortiz Pradillo[4], nos encontramos em uma espécie de ilegalidade informática, onde muitos criminosos hospedam dados eletrônicos fraudulentos em servidores localizados em terceiros países, o que impossibilita o estabelecimento de mecanismos de cooperação processual internacional para acusar com sucesso um determinado crime cibernético a seu suposto autor.

É comum na prática judicial diária que muitos processos acabem sendo arquivados devido a esta questão. Existem obstáculos internacionais à transferência de dados eletrônicos, o que significa que quando contestamos provas desta natureza e pedimos a um servidor estrangeiro as informações completas e autenticadas, a resposta nunca chega ou é negativa por estar localizada em uma jurisdição que não a espanhola e não há acordo bilateral específico sobre a transferência de provas eletrônicas de um país para outro. Certamente, se recorrermos à LOPJ, estaremos falando de uma aplicação preferencial do critério de territorialidade para atribuir jurisdição à Espanha e competência aos tribunais penais: "Os tribunais civis espanhóis ouvirão as reivindicações que surjam em território espanhol de acordo com as disposições dos tratados e convenções internacionais dos quais a Espanha é parte, nas regras da União Européia e na legislação espanhola"; mas estamos realmente em uma encruzilhada, pois estes atos ilícitos têm uma clara projeção extraterritorial.

Dado que o princípio da territorialidade é entendido como estando ligado ao local onde o crime é cometido, os crimes cibernéticos também podem ser entendidos como tendo

[3]. MIRO LLINARES, F., *El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio,* 2012, pág.47. "O crime cibernético é hoje preferível ao crime informático, reconhece-se que ele serve essencialmente para definir uma área particular e específica de risco, a do uso das TICs, para bens jurídicos essenciais, e aceita-se, finalmente, que esta categoria não inclui delitos penais, mas tipologias de conduta que são perigosas para estes bens e caracterizadas pelo uso de redes telemáticas e outros sistemas, terminais e serviços TIC com os riscos que isso implica, que esta categoria não inclui infrações penais, mas tipologias de conduta perigosas para estes bens e caracterizadas pelo uso de redes telemáticas e outros sistemas, terminais e serviços TIC com os riscos que isso implica, é hora de tentar sistematizar, com base nos diferentes critérios existentes, estas tipologias incluídas no cibercrime".

[4] ORTIZ PRADILLO, J.C., *Problemas Procesales de la Ciberdelincuencia*, Madrid, 2013, págs. 30-31. Ele apresenta um trabalho que trata dos principais problemas deste tipo de crime, e apresenta os problemas de obtenção de provas eletrônicas como resultado de medidas de investigação no campo do crime cibernético de um ponto de vista jurídico.

sido cometidos em outras jurisdições, em aplicação da teoria do resultado[5]. Em outras palavras, mesmo que o ataque comece na Espanha, os resultados criminais podem ocorrer em vários países ao mesmo tempo. Isto, por sua vez, gera problemas de jurisdição e a necessidade de novos instrumentos processuais para a cooperação internacional nas etapas de investigação, processo e julgamento, uma vez que muitos países terão opções para iniciar ações ao mesmo tempo, a fim de elucidar os atos cometidos[6].

Neste sentido, a Espanha poderia ter jurisdição se os perpetradores cometessem crimes do território espanhol através do uso da rede como veículo para cometer o crime. Além disso, quando uma das partes prejudicadas, mesmo que o resto esteja em estados diferentes, está em território espanhol. Como última opção, a jurisdição pode ser atraída quando o material recebido estiver em um terminal ou servidor localizado na Espanha. E, é claro, outros princípios também poderiam entrar em jogo, como a extraterritorialidade, se as redes de crimes cibernéticos infringirem qualquer valor supranacional de nosso país em aplicação do critério real sobre a extensão e os limites da jurisdição. Essas opções tendem a ser semelhantes em outros países, especialmente em nível da União Européia, o que levanta claros problemas de jurisdição nos casos em que mais de um país deseja que seus tribunais investiguem um determinado episódio de cibercrime.

Isso economizaria tempo em investigações duplicadas e evitaria investigações duplicadas que afetariam o princípio comum de cooperação *non bis in idem*, enquanto economizaria custos processuais para diferentes países e evitaria que essas distorções

[5] Vid. SÁNCHEZ GARCÍA DE PAZ. I, y BLANCO CORDERO. I, "Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Internet", *La ley digital*, 2002, págs. 1-28.

[6] A este respeito, devemos destacar a posição do FONTESTAD PORTALÉS, quando afirma que "consideramos que a solução para a concorrência de jurisdições no crime informático transfronteiriço não vem da criação deste tipo de organismos supranacionais, mas de algo muito mais simples, como a criação de uma lista de critérios hierárquicos para a determinação de jurisdição internacional em matéria penal, o que por si só reduziria os conflitos de jurisdição, reduziria por si só os conflitos de jurisdição; de fato, poderia evitá-los, já que os Estados saberiam desde o início qual Estado tem mais pontos de conexão com o crime e, portanto, qual tem, digamos, jurisdição preferencial",Vid. FONTESTAD PORTALÉS, L., "Jurisdicción y competencia internacional en materia de ciberdelincuencia", *La globalización del derecho procesal*, Valencia, 2019, págs. 295-332.

Da mesma forma, com relação aos problemas de jurisdição em nível internacional, BUJOSA VADELL afirma que "Não há dúvida de que estamos enfrentando uma realidade extraordinariamente mutável à qual a lei está tentando se adaptar com grande dificuldade. Com dificuldade ainda maior são os métodos tradicionais de resolução de disputas e, especialmente, o principal, que, como era o caso nos tempos medievais, para muitas das reivindicações levantadas, revela-se uma peça de maquinaria incômoda e ineficaz.", Vid. BUJOSA VADELL, L., "Sobre la insoportable levedad de la jurisdicción", *La globalización del derechoprocesal*, Valencia, 2019, pág. 46.

legislativas fossem exploradas por criminosos para cometer crimes cibernéticos em uma área de aparente impunidade. Como indicamos, este problema afeta não apenas a própria acusação, mas também a investigação destes atos criminosos. É por esta razão que os países devem cooperar uns com os outros, facilitando a informação entre os Estados e estabelecendo protocolos para implementar diretrizes para ajudar a decidir sobre a jurisdição e aplicar critérios que favoreçam a investigação de crimes de natureza transfronteiriça.

Em nível europeu, os instrumentos europeus de cooperação judiciária em matéria penal estão configurados para combater a criminalidade em geral e criar um espaço de liberdade, segurança e justiça; cumprindo as disposições do Tratado de Lisboa ou do Tratado da União Européia[7] e baseados no princípio do reconhecimento mútuo das decisões entre os Estados-Membros, percebido desde o Conselho de Tampere como um marco da cooperação judiciária européia. Em linha com este objetivo, entre as instituições europeias que defendem a facilitação destas questões está a Eurojust, uma agência da União Européia com personalidade jurídica própria que realiza um importante trabalho de *soft law* através da publicação de relatórios, diretrizes e manuais, nos quais são dadas recomendações específicas para superar este tipo de situação, com base na criação de Equipes de Investigação Conjunta ou na indicação de critérios de decisão sobre jurisdição aplicável e os critérios a serem seguidos para coordenar uma investigação conjunta em nível processual. O objetivo é reforçar a comunicação plena entre os Estados e que cada um tenha uma série de pontos de contato para coordenar ações conjuntas contra os crimes transfronteiriços e o crime organizado. Além das próprias instituições, temos desenvolvido progressivamente instrumentos de assistência em justiça penal através de um caminho que começou em 1959 com a Convenção Européia de Assistência Mútua em Matéria Penal e foi revitalizado pela Convenção de Assistência Mútua em Matéria Penal entre os Estados-Membros da União Européia de 29 de maio de 2000. Tudo isso se baseia nos princípios da confiança mútua e do reconhecimento mútuo, que posteriormente foram refletidos em instrumentos legais que ajudam tanto a investigar os casos quanto a processá-los através de uma série de textos legais europeus que favorecem a verdadeira aplicação e eficácia do princípio de legalidade e apoio

[7] O artigo 3(2) do TUE estabelece que: "A União oferecerá a seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, no qual seja assegurada a livre circulação de pessoas, em conjunto com medidas adequadas em matéria de controles nas fronteiras externas, asilo, imigração e prevenção e combate ao crime"

à área de segurança, igualdade e justiça, tão avidamente buscada.

2. INSTRUMENTOS E INSTITUIÇÕES EUROPEIAS PARA A PESQUISA DE CRIMES TECNOLÓGICOS COMPLEXOS

Na área de crimes cibernéticos, a UE criou um centro associado à Europol chamado European Cybercrime Center (EC3) há oito anos, especificamente em meados de 2013. Sua criação foi motivada pelo cumprimento da Estratégia de Segurança Interna da União Européia Rumo a um Modelo de Segurança Européia ligado ao Programa de Estocolmo desde 2010 e pelo cumprimento da Convenção do Conselho da Europa de 2001 sobre Cibercrime.

A este respeito, a UE solicitou a criação de instituições específicas para combater o crime cibernético devido a seu perfil transfronteiriço. Esta luta se concentrou na fase de investigação, sabendo que o perigo do anonimato e a ampla disseminação de tais crimes via Internet tornava necessário responder não apenas preventivamente, mas também enfrentar o problema desde o início, por meio de policiais especializados em crimes cibernéticos e que também estavam interligados nos diferentes estados membros. O objetivo seria coletar provas eletrônicas que poderiam ser usadas para acusar os supostos perpetradores de atos criminosos no mundo do *ciberespaço* e assim cumprir os princípios de investigação e legalidade.

A própria Convenção sobre Crime Cibernético declarou expressamente no ponto 4.4 que "grupos criminosos têm sido capazes de tirar proveito efetivo da tecnologia". Isto, por sua vez, dificulta a realização de investigações por parte das autoridades responsáveis pela aplicação da lei"; portanto, uma "resposta rápida" aos ataques cibernéticos foi solicitada. Também em 2017, o Conselho da Europa começou a preparar um segundo protocolo adicional à Convenção de Budapeste sobre Cibercriminalidade para um regime de cooperação mais eficiente através da inclusão de garantias e requisitos rigorosos de proteção de dados, que seriam potencialmente aplicáveis em todo o mundo e deveriam ter sido concluídos antes do final de 2020, um assunto que foi finalmente adiado, provavelmente devido ao efeito da pandemia de Covid-19, como exploraremos com mais detalhes no próximo ponto deste estudo. O objetivo deste protocolo é "melhorar o canal tradicional de

cooperação e incluir disposições para a cooperação direta entre as autoridades de aplicação da lei e os prestadores de serviços transfronteiriços, bem como disposições sobre o acesso direto aos dados pelas autoridades de aplicação da lei".

Não devemos esquecer que o papel da lei não é apenas resolver conflitos, mas que ela tem um papel principal anterior na prevenção de conflitos. Isto requer instrumentos focados na inteligência, ou seja, saber prever o que pode acontecer e até mesmo ser capaz de infiltrar de alguma forma as organizações que prevêem estes tipos de ataques a fim de detê-los antes que sejam realizados. É realmente complicado promover instrumentos desta natureza, mas acreditamos que o EC3 através da Europol é um bom exemplo para criar uma espécie de serviço de inteligência coordenado na luta contra o crime cibernético na UE.

Portanto, estamos falando também das funções de *cibersegurança* e *ciberdefesa* e de uma concepção futurista, destinada a investigar crimes cibernéticos de nova geração e ao mesmo tempo a funcionar como uma espécie de plataforma com ramificações que está conectada a agências de segurança nacional e operadores legais ou policiais que se dedicam à mesma coisa em cada um dos países membros. Ela pode ser vista como uma espécie de plataforma cooperativa sobre este assunto, operando principalmente através da Europol, mas que pode ajudar outras instituições já mencionadas neste estudo, tais como a Eurojust. Além dessas tarefas, a Europol, através do EC3, realiza ações coordenadas na área de medidas de investigação através da coordenação e do fortalecimento de equipes de investigação conjuntas entre diferentes estados. Em outras palavras, operadores policiais de diferentes países colaboram em operações cibernéticas com um componente transfronteiriço para investigar crimes cibernéticos de alta tecnologia, pornografia infantil, fraude eletrônica, etc.

Em si mesma, esta tarefa apresenta desvantagens, pois não há harmonização legislativa no nível dos procedimentos de investigação tecnológica na UE, e países como Espanha, Holanda, Alemanha ou França têm suas próprias particularidades quanto ao uso da interceptação de comunicações ou outros métodos mais avançados como a inclusão de vírus espiões ou a infiltração de agentes disfarçados na Internet. Portanto, é necessário agir com um princípio de garantias preventivas absolutas a fim de não comprometer o resultado da investigação de um ponto de vista geral.

Sem ir mais longe, uma das operações mais conhecidas ativadas pelo EC3 através de equipes de investigação conjuntas foi o caso Sweetie, que ao mesmo tempo reflete algumas

deficiências adicionais no caso da Espanha. Neste caso, estamos falando da aplicação da inteligência artificial como uma diligência investigativa, uma questão que não está regulamentada na Espanha, mas que tem feito progressos significativos nos Países Baixos.

Entre a Holanda, sua organização em favor dos direitos humanos das crianças Terre des hommes (Terra dos Homens) e a Europol, através de uma menina criada pela inteligência artificial, foi possível atrair mais de 20.000 pedófilos em todo o mundo entre 2013 e 2014, por isso já era uma estratégia coordenada graças ao EC3 e a todas as suas operações. Se transferíssemos a execução das medidas para nosso país, nos depararíamos com um problema que certamente teria obstáculos legais e problemas de reconhecimento judicial na Espanha devido à falta de regulamentação deste tipo de tecnologia na época. Desta forma, vemos um exemplo claro da infiltração de agentes na Internet coordenados pelo EC3, cujo objetivo é reunir provas eletrônicas com o objetivo final de torná-las válidas para provar um crime cibernético específico e que, por sua vez, seriam válidas em diferentes Estados Membros.

Assim, cada país tem sua própria regulamentação sobre o uso de medidas de investigação, seus princípios norteadores para sua autorização e uma modalidade particular de execução, bem como características para a concessão de decisões judiciais para sua concessão, etc. que devem ser validados para que as provas sejam eficazes e para que princípios suficientes sejam respeitados a fim de garantir sua cobrança válida e preservar a custódia efetiva. Portanto, é interessante explorar a medida das Equipes de Investigação Conjunta (EIC), na qual os estados envolvidos, através de suas agências policiais autorizadas, fazem um acordo prévio e um ato de constituição do escopo das medidas de investigação a serem adotadas. O EC3 realiza assim um importante trabalho de inteligência criminal e de informação e também ajuda através da análise operacional e da coordenação pessoal e instrumental entre os estados para combater o crime cibernético transfronteiriço de alta tecnologia. Em última análise, facilita a conexão entre as agências de aplicação da lei, o meio acadêmico, o setor privado e outras partes interessadas preocupadas com a segurança das redes. Com tudo isso, concluímos que o próprio objetivo é obter provas eletrônicas para acreditar os fatos ligados a certos crimes cibernéticos através de procedimentos de investigação tecnológica; por isso, apresentaremos aqueles regulamentados no sistema espanhol, que podem ser transferidos para o resto do mundo.

3. PROCEDIMENTOS DE PESQUISA TECNOLÓGICA NO CONTEXTO ESPANHOL

O progresso tecnológico no início do novo século tem sido um fator revulsivo em todas as áreas da sociedade, incluindo o setor jurídico. O direito não pode ficar à margem da evolução das novas tecnologias da informação, pois os novos meios de comunicação constituem um novo ponto de referência fundamental a ser levado em conta pelo Estado de Direito para saber como conciliar os direitos e interesses dos cidadãos com os avanços tecnológicos. Atualmente, estamos vendo como os cidadãos estão exigindo cada vez mais a intervenção do judiciário, que, ao não responder rapidamente às exigências dos cidadãos, está gerando uma percepção geral na sociedade da lentidão do sistema judiciário espanhol e do número de deficiências que ele possui.

As inovações tecnológicas podem mudar muitos aspectos do atual sistema judiciário espanhol, mas para que isso seja possível, precisaríamos do consenso e da vontade comum de todos os poderes do Estado, convertendo assim o Judiciário em um poder moderno e próximo da sociedade atual. Desta forma, não estaria ultrapassado em comparação com outros países europeus e seu valor e importância para o judiciário aumentaria. Tudo isso nos leva a considerar a introdução desses avanços de forma meticulosa, tentando sempre garantir cem por cento dos direitos dos cidadãos, para que todos possam ter acesso ao sistema judicial e obter uma decisão fundamentada dos tribunais, sem permitir que sofram a indefensabilidade por não lhes permitir exercer todos os poderes legalmente reconhecidos no artigo 24 de nossa Constituição, garantindo assim a proteção judicial efetiva de seus direitos.

Estas necessidades de modernização do sistema judiciário, graças às novas tecnologias, já vêm sendo exigidas há anos por instituições e profissionais ligados ao mundo do direito, embora seja graças à Lei 18/2011 sobre a aplicação de novas tecnologias na Administração da Justiça, cuja aplicação entrou em pleno vigor a partir de 2016, que a questão ganha importância capital. Por outro lado, desde que o esboço do futuro Código de Processo Penal veio à luz em 2012, tem havido muita expectativa e debate sobre o novo sistema de investigação criminal que se pretende propor, deixando praticamente todo o

projeto em esquecimento. Mesmo assim, foi considerado um bom momento para cristalizar as mudanças propostas como resultado da Lei 18/2011, a fim de adaptar nosso sistema processual às novas tecnologias. Por esta razão, e observando a necessidade imperativa de empreender mudanças para modernizar a justiça e adaptá-la à nova realidade tecnológica, foi aberto um novo debate sobre a aprovação, em um curto período de tempo, de reformas na pesquisa tecnológica no campo criminal. Assim, três anos após o Projeto de Código de Processo Penal ter introduzido conceitos tecnológicos altamente controversos, que geraram discussões doutrinárias, vemos como o legislador canaliza essas mudanças para um novo texto legal que começou a ser debatido no final de 2014 e finalmente se tornou um Projeto de Lei em 20 de março de 2015, após passar com sucesso por vários procedimentos parlamentares. Ela é agora finalmente ratificada como Lei 13/2015, que entrou em vigor no início de dezembro do mesmo ano, com exceção das seções um, três, quatro, cinco e seis do artigo único, que entraram em vigor em 1 de novembro de 2015.

Desta forma, estamos falando em dar cobertura legal a diferentes procedimentos de investigação que servem para investigar crimes cibernéticos de forma a oferecer garantias, e que também estão ligados a crimes complexos. Assim, os assuntos que sofreram mudanças após a reforma são: a interceptação de comunicações telefônicas e telemáticas, a captura e gravação de comunicações orais e imagens através do uso de dispositivos eletrônicos, o uso de dispositivos técnicos para rastreamento, localização e captura de imagens; e finalmente, a busca de dispositivos de armazenamento de informações em massa. Uma série de medidas investigativas que serão descritas abaixo e que abrem a porta para o uso de figuras tão controversas como drones, agentes infiltrados na Internet ou vírus controlados à distância. Todas as garantias processuais são respeitadas com a introdução dessas novas medidas, estaríamos diante de uma clara violação dos diferentes direitos fundamentais daqueles potencialmente sob investigação e, em suma, o fim sempre justifica os meios? Estas e outras questões serão abordadas ao longo deste documento.

3.1. Interceptação das comunicações

Na Espanha, a questão da interceptação das comunicações sempre foi um tema muito debatido devido à controvérsia gerada pelo sistema de investigação integral SITEL, o

Sistema Integral de Interceptação de Comunicações Eletrônicas; um sistema informático que oferece uma "espionagem completa" das comunicações eletrônicas. Graças a este sistema, um extenso material probatório eletrônico é obtido com base na interceptação e gravação digital de conversas via telefones celulares ou dispositivos eletrônicos, tanto em formato oral quanto em escrita digital, que devem ser apresentados posteriormente em um determinado julgamento. Assim, a STS de 13 de março e 5 de novembro de 2009 descreveu o funcionamento do SITEL[8] como um programa dedicado à obtenção de provas eletrônicas; especificando ao mesmo tempo na STS de 19 de dezembro de 2008 e na STS de 30 de dezembro de 2009, que as provas eletrônicas obtidas graças a este instrumento não são apenas conversas digitais, mas também documentos eletrônicos que vão desde o conteúdo de um SMS até dados específicos de um GPS[9]. Isto demonstra a força prática e jurisprudencial desta evidência também nestes crimes. Graças a ferramentas informáticas específicas como a citada aqui, é possível esclarecer crimes de sabotagem informática, divulgação de segredos ou interceptação de comunicações.

Mesmo assim, até hoje não tínhamos um regulamento que abrangesse o amplo espectro das comunicações que a SITEL poderia interceptar, nem uma lei orgânica que endossasse seu uso. Para resolver este vácuo legal, nos referimos à jurisprudência estabelecida pelo TC sobre escutas telefônicas em numerosas normas e extraímos delas os requisitos mínimos para interceptação, o que significava que estávamos nos movendo em uma área claramente marcada por uma incerteza legal palpável.

Agora, com a regulamentação dada na Lei, vemos como qualquer tipo de interceptação é permitida através de sistemas de interceptação integral, através do telefone ou qualquer outro meio ou sistema de comunicação telemática, lógica ou virtual, de modo que qualquer aplicação oferecida por um Smartphone seria coberta pelo artigo acima mencionado. Tudo isso para reunir novos tipos de mensagens derivadas de certos APPs, como o WhatsApp, dando assim substância a outras formas de comunicação telemática que carecem de tratamento regulatório no direito processual.

Trata também da questão da detenção e abertura de correspondência escrita e

[8] Vid. GIMENO SENDRA, V., "La intervención de las comunicaciones*", Diario La Ley, Nº 7192*, Sección Doctrina, 9 Jun. 2009.
[9] STS (Sala de lo Penal, Sec. 2.ª) de 19 diciembre 2008.

telegráfica, atualizando assim o art. 579 LECrim, onde seu âmbito de aplicação material é limitado, ao mesmo tempo em que regulamenta os períodos máximos de duração e as exceções à necessidade de autorização judicial de acordo com uma doutrina jurisprudencial consolidada, de modo que equacionamos a abertura no terreno físico e virtual graças à comparação entre cartas e e-mails.

Este artigo foi altamente criticado em sua versão original quando ainda estava na fase de anteprojeto, pois previa a prorrogação das circunstâncias excepcionais em que o Ministro do Interior, ou o Secretário de Estado da Segurança, poderia ordenar a interceptação das comunicações sem autorização judicial prévia, desde que fossem consideradas crimes graves, por meio de uma cláusula com conteúdo jurídico indeterminado. O texto do qual previa que as comunicações poderiam ser interceptadas sem autorização judicial em "outros crimes que, em virtude das circunstâncias do caso, podem ser considerados particularmente graves, e há razões bem fundamentadas que tornam essencial a interceptação das comunicações".

Após a interceptação, o juiz encarregado da investigação do caso deveria ser informado da adoção desta medida dentro de um prazo máximo de 24 horas, e seria este juiz que, dentro de um prazo máximo de 72 horas após ter sido informado de tal decisão, teria que ratificá-la ou revogá-la de forma fundamentada. Com esta medida, estaríamos claramente violando o direito fundamental ao sigilo das comunicações, bem como o direito à privacidade, desde que seja utilizado para crimes graves cometidos através de ferramentas informáticas ou qualquer outra tecnologia de informação ou telecomunicação, ou seja, com uma pena de pelo menos três anos de prisão... tudo isto nos colocaria numa situação em que a conduta ilícita dos cidadãos que ocorre com certa regularidade na Internet, como downloads ilegais de séries ou filmes, poderia ser objeto de investigação.

Assim, nos depararíamos com uma medida não proporcional que foi duramente criticada pelo Conselho Geral do Judiciário[10] em dezembro de 2014 e que fez com que o texto fosse suavizado do Anteprojeto de Lei para o Projeto de Lei, para usá-lo apenas em casos de terrorismo e que foi finalmente aprovado em 5 de outubro. Por outro lado, o que se

[10] Vid. http://www.diariodenavarra.es/noticias/mas_actualidad/nacional/2015/01/11/cgpj_plantea_dudas_las_escuchas_telefonicas_sin_autorizacion_judicial_190686_1031.html (Fecha de consulta: 14 de mayo 2015)

mantém é a sucessiva extensão das intercepções de comunicações com um período máximo de dois anos, uma questão que ainda nos parece desproporcional, embora seja sempre necessário considerar a motivação e cada caso específico. Mesmo assim, acreditamos que teria sido mais apropriado não estabelecer períodos máximos ou mínimos e deixar uma seção abstrata referindo-se à gravidade e natureza da suposta infração sob investigação; caso contrário, nos encontramos com medidas "temporárias" que são excessivamente prolongadas no tempo, o que é uma contradição em si mesmo[11]. Isto é dito no Art. 588 ter g. quando diz que: "a duração máxima inicial da interceptação, que será calculada a partir da data da autorização judicial, será de 3 meses, prorrogável por períodos sucessivos da mesma duração até um período máximo de 2 anos". Da mesma forma, esta extensão também pode ocorrer não apenas em relação ao tempo, mas também em relação à busca de outros dispositivos ou sistemas de computador por razões de urgência, o que, como Ortiz Pradillo[12] indica, quando ainda estávamos falando de um Projeto de Lei:

> "reintroduz a urgência como uma exceção à autorização judicial prévia para examinar o conteúdo de dispositivos de computador, algo que não estava expressamente incluído na proposta de 2011 e que só foi indicado para o exame de dispositivos apreendidos fora de casa e após uma decisão do Ministério Público na proposta de 2013."

Isso significa que esta questão está ligada à figura da descoberta do acaso eletrônico. Assim, a última questão controversa é a dos achados do acaso, que também é tratada na Lei 13/2015. É bastante normal que quando uma busca é feita em um computador, telefone celular ou qualquer outro dispositivo que consista em uma infinidade de arquivos de computador, há descobertas de provas eletrônicas para as quais não há uma autorização judicial expressa. Portanto, o primeiro problema que pode surgir aqui é delimitar a extensão da ilegalidade das provas derivadas das provas principais, para as quais não há autorização judicial expressa e que, portanto, foram obtidas em violação, no caso de provas eletrônicas,

[11] Artigo 588b d. Pedido de autorização judicial. O pedido de autorização judicial deve conter, além dos requisitos referidos no artigo 588b, os seguintes requisitos referido no artigo 588ab, o seguinte: (a) a identificação do número do assinante, terminal ou etiqueta técnica, (b) a identificação da conexão que é objeto da intervenção; ou (c) os dados necessários para identificar os meios de telecomunicação em questão. Artigo 588b d. Pedido de autorização judicial. O pedido de autorização judicial deve conter, além das exigências referidas nas alíneas b) e c) do artigo 588a, as informações necessárias para identificar os meios de telecomunicação em questão. Artigo 588a(b), o seguinte: (a) identificação do número do assinante, terminal ou etiqueta técnica, (b) a identificação da conexão que é objeto da intervenção; ou (c) os dados necessários para identificar os meios de telecomunicação em questão.

[12] ORTIZ PRADILLO, J., http://juancarlosortizpradillo.blogspot.com.es/2015/05/reforma-penal-y-control-judicial-en-la.html?spref=fb (Fecha de consulta: 22 de mayo de 2015)

do direito fundamental à privacidade, inspecionando material privado para o qual não houve permissão precisa[13].

Devemos partir do fato de que detectamos que parte da doutrina se confundiu um pouco com a limitação desta figura, confundindo em muitos casos as provas derivadas de provas inicialmente ilegais, em outras palavras, as provas que podem ser encontradas após uma busca telefônica sem autorização judicial prévia, com as "descobertas fortuitas", que seriam o surgimento de novos atos criminosos não incluídos na decisão judicial autorizando a medida de interceptação eletrônica, que surgem à luz da investigação que está sendo realizada. Como a López-Barajas Perea[14] corretamente aponta, a questão está centrada em detectar a extensão da proibição de avaliação de material probatório obtido ilegalmente em um determinado processo. A conseqüência direta das provas obtidas em violação aos direitos fundamentais é a proibição de avaliar o resultado probatório, que pode até levar à absolvição do acusado, portanto será necessário delimitar a extensão desta proibição e se ela também pode afetar as provas derivadas ou os achados eletrônicos casuais. Mas, uma vez levantada a questão, onde devemos estabelecer o limite para tal proibição? Ao estudar as escutas telefônicas, acreditamos que uma vez que o juiz tenha conhecimento da descoberta acidental de um ato criminoso diferente daquele sob investigação, a solução dependerá de se este ato constitui um crime relacionado ao inicialmente sob investigação, ou seja, se existe uma conexão entre os dois, ou, ao contrário, se é um crime totalmente autônomo e independente. Neste sentido, Bañuls Gomez, com quem concordamos, pensa que no primeiro caso, deveria ser emitida uma ordem judicial ampliando o escopo da escuta e a investigação deveria continuar no mesmo caso; ao contrário, no segundo caso, o juiz deveria, após reexaminar as questões de proporcionalidade e competência, emitir uma autorização judicial expressa permitindo a continuação da escuta e iniciar o caso apropriado após deduzir o testemunho correspondente; assim, uma investigação diferente seria iniciada, embora com um ponto de partida comum[15].

[13] CAPELLETTI, M. "Eficacia de pruebas ilegítimamente admitidas y comportamiento de la parte", *La oralidad y las pruebas en el proceso civil*, Buenos Aires, 1972, pág. 137.
[14] LOPEZ BARAJAS PEREA, I. *La intervención de las comunicaciones electrónicas,* Madrid, 2011, págs. 227-227.
[15] BAÑULS GOMEZ, F. "Las intervenciones telefónicas a la luz de la jurisprudencia más reciente" en el Portal Web Noticiasjurídicas.com, Febrero 2007, disponible en http://noticias.juridicas.com/articulos/55-Derecho%20Penal/200702-981932563274752514.html (Fecha de consulta: 18 de diciembre de 2014).

Portanto, nossa solução a este respeito seria transferir este poder de decisão ao juiz para que ele determine se deve ou não ser dado valor probatório verdadeiro a este resultado inesperado que inicialmente não corresponde ao propósito original da diligência, mas que, em nossa opinião, se não for valorizado, deixaria um crime impune. Isto também está incluído na Lei 13/2015 ao tratar das conclusões, mesmo afirmando que a decisão tomada pelo juiz a este respeito servirá de orientação para o restante das medidas de investigação tecnológica e cujos resultados poderão ser utilizados em processos subsequentes, desde que as garantias processuais e os direitos fundamentais da parte investigada sejam respeitados. Caso contrário, estaríamos lidando com uma violação da lei e o artigo 11.1 da LOPJ entraria em jogo, segundo o qual "as provas obtidas direta ou indiretamente violando direitos ou liberdades fundamentais não serão eficazes"; ou, em outras palavras, a interceptação de uma comunicação pessoal realizada sem as garantias que a legitimam torna-se nula e sem efeito e, conseqüentemente, não pode ser usada como prova.

3.1.1. Uso de dispositivos técnicos de rastreamento, rastreamento e imagem

Esta seção começa com um artigo 588 *quater* a, que, a priori pode parecer futurista, mas que na verdade está comprometida com uma tipologia aberta com a evolução da tecnologia nos anos futuros em mente, permitindo à Polícia Judiciária obter e registrar imagens da pessoa sob investigação por qualquer meio técnico quando esta se encontra em local ou espaço público, se isso for necessário para facilitar sua identificação, para localizar os instrumentos ou efeitos do crime ou para obter dados relevantes para o esclarecimento dos fatos. Com tudo isso, o catálogo de meios técnicos utilizados é estendido ao infinito com o único objetivo de garantir que a legislação não caia na obsolescência tecnológica com o passar do tempo. Ao nos referirmos a dispositivos em estradas públicas ou outros espaços abertos, temos claramente uma regulamentação que protege o uso de drones como ferramentas de investigação pela Administração Espanhola de Justiça[16].

O drone, entendido como um veículo aéreo não tripulado (doravante UAV), é uma

[16] Vid. NADAL GÓMEZ, I., "La litigiosidad que se nos viene encima: cuestiones procesales al hilo de la aparición de «drones» en nuestros cielos", *Diario La Ley*, Nº 8507, Sección Doctrina, 25 de Marzo de 2015, pág 2.

aeronave que voa sem tripulação. Em outras palavras, estamos lidando com o uso de inteligência artificial que pode ser usada pela CFSE para investigar crimes, tirando fotografias ou interceptando ou pirateando comunicações, ou mesmo como medida de proteção contra uma variedade de ataques, pois eles podem não apenas capturar imagens, mas também podem tirar imagens termográficas ou usar técnicas de reconhecimento biométrico para identificar pessoas. Duas variantes foram desenvolvidas: algumas são controladas a partir de um local remoto, enquanto outras voam de forma autônoma com base em planos de vôo pré-programados, utilizando sistemas de automação dinâmica mais complexos. Assim, há drones que também podem ser sistemas autônomos que podem operar sem intervenção humana. Agora imagine estas ferramentas sendo utilizadas pelos juízes para conduzir um reconhecimento judicial.

O reconhecimento judicial é um meio de prova pelo qual o juiz se desloca para um determinado lugar fora das instalações do tribunal para ter contato direto com o material probatório. Por exemplo, quando ele tem que ir ver um prédio em ruínas ou tem que fazer um exame de um menor fora do tribunal para que sua entrada nas instalações do tribunal não envolva uma vitimização secundária. Ele poderia usar um drone para se movimentar? Devemos concentrar nossos estudos futuros na observação e estudo das possibilidades legais que a aplicação de drone para esses fins implicaria. Até agora, a Espanha tinha um marco legal para os UAVs na Lei 18/2014, de 15 de outubro, sobre medidas urgentes para o crescimento, competitividade e eficiência, onde eram regulamentados em sua sexta seção, referindo-se especificamente às "aeronaves civis pilotadas remotamente", mas sua utilização para fins de investigação é, no momento, apenas coberta por esta Lei. Por outro lado, se os drones são destinados a espaços abertos, de forma semelhante, mas em terrenos privados, teríamos faróis de rastreamento GPS ou dispositivos de geolocalização. Bem, será que esses dispositivos violariam algum direito fundamental? Se entendemos a privacidade como um espaço interior estranho ao olhar de estranhos e seguimos a jurisprudência constitucional que configura o direito à privacidade pessoal como um espaço vital onde o indivíduo desenvolve sua liberdade pessoal reservada a partir do conhecimento dos outros, vemos que ela não entra em confronto com a tecnologia GPS. Assim, pode-se ver claramente que os dispositivos telemáticos de localização não infringem este direito; eles apenas limitam a liberdade do indivíduo diante de uma pessoa ou espaço físico, restringindo assim sua liberdade, mas

nunca sua privacidade[17].

Por todas estas razões, atualmente na Espanha parece difícil negar as possibilidades de utilizar a vigilância eletrônica como meio de facilitar o acesso ao terceiro grau, à liberdade condicional e até mesmo para substituir numerosos casos de prisão preventiva sem que as pessoas questionem a violação dos direitos fundamentais; mesmo assim, no caso de pulseiras, será sempre necessária uma autorização judicial para seu uso. Uma questão diferente é a do uso de UAVs em espaços abertos, ou dispositivos de escuta em espaços fechados, pois seu uso deve atender a certos padrões de necessidade e proporcionalidade, que devem ser justificados pelo juiz em cada caso específico. Finalmente, como no caso da interceptação de comunicações, estas medidas de rastreamento e localização têm uma duração máxima de três meses a partir da data de sua autorização, embora o juiz possa, excepcionalmente, estender sua utilização até um máximo de dois anos; portanto, as críticas da seção anterior também seriam aplicáveis a este tipo de procedimento.

3.1.2. Captura e registro de comunicações orais através do uso de dispositivos eletrônicos

Aqui, a lei trata de duas questões distintas, mas muito diferentes: dispositivos de escuta e agentes infiltrados na Internet. Duas questões que perseguem o mesmo objetivo, mas que são suficientemente importantes para não serem regulamentadas na mesma seção e dão origem a preceitos independentes e amplamente espaçados dentro da Lei de Processo Penal espanhola[18].

Se olharmos para os dispositivos de escuta ou microfones, podemos ver que eles podem ser colocados tanto fora como dentro de casa ou em espaços fechados. Esta é uma questão muito controversa quando falamos da esfera privada, pois prevemos o impacto que ela pode ter sobre os direitos fundamentais das pessoas sob investigação, já que em um espaço privado esta medida pode ter efeitos colaterais sobre as pessoas que vivem com as pessoas sob investigação e que nada têm a ver com o ato criminoso que está sendo

[17] LYON, David, *El ojo electrónico. El auge de la sociedad de vigilancia*, Madrid, 1995, p. 91.
[18] O agente disfarçado é regulamentado no Artigo 282a(6) e (7). enquanto que a captura e gravação de comunicações orais através do uso de dispositivos eletrônicos é coberta pelo artigo 588.

investigado, restringindo também a privacidade ou a inviolabilidade da casa das pessoas que vivem com a pessoa sob investigação[19].

Por todas estas razões, a lei, mais uma vez, só permite sua utilização para crimes graves, crimes cometidos dentro de um grupo ou organização criminosa, bem como para delitos terroristas, além de exigir uma motivação específica baseada no fato de que, graças à instalação destes dispositivos, dados essenciais de relevância probatória podem ser obtidos racionalmente para o esclarecimento dos fatos e para imputar sua comissão ao presumível perpetrador. Da mesma forma, o juiz deve fazer menção específica ao local ou instalações que devem ser objeto de vigilância. A outra medida que é rotulada na exposição de motivos como uma ferramenta para capturar comunicações em canais fechados, assim como para gravar imagens ou conversas, é a do agente disfarçado na Internet. Uma figura que vem sendo utilizada há algum tempo na Espanha, e que necessitava de reforma e atualização urgentes, a fim de dar-lhe a cobertura legal urgente de que necessitava e pôr fim às brechas legais em torno de suas ações. Assim, o artigo 282 bis LECrim incorporaria duas novas seções referentes à utilização de uma identidade baseada no engano em "canais fechados de comunicação", bem como lhe daria o poder de "enviar arquivos ilegais por si só por causa de seu conteúdo e analisar os algoritmos associados a esses arquivos ilegais". Duas questões altamente controversas que agora vamos comentar. Quanto ao primeiro deles, o cenário em que o agente infiltrado deveria atuar, pensamos que seria um bom momento para ampliar a lista de casos em que um agente pode intervir, incluindo crimes cometidos através da Internet relacionados a vítimas particularmente vulneráveis, para que possam atuar em operações contra a pedofilia e o intercâmbio de material pornográfico ou ciberterrorismo, e ao mesmo tempo contra crimes que ocorrem através de redes sociais.

Quanto ao fato de só ser permitido agir em canais fechados, devemos levantar uma nova crítica. Na aprovação final, afirma-se textualmente que só é estabelecido para canais fechados, pois se entende que para canais abertos, por sua própria natureza, não é necessário. Não concordamos com esta afirmação na lei, pois acreditamos que estaríamos deixando de fora todo conteúdo de computador de natureza aberta, como fóruns, blogs, chats ou redes

[19] A medida pode ser executada mesmo quando afeta outras pessoas que não a pessoa sob investigação, desde que de outra forma a utilidade da vigilância seja significativamente reduzida ou haja indicações bem fundamentadas da relação dessas pessoas com a pessoa sob investigação e os fatos que são objeto da investigação.

sociais com conteúdo público.

Só poderia ser usado para canais fechados, como mensagens privadas em redes sociais ou fóruns restritos, o que o torna muito próximo do infrator e limita seus poderes, tendo que lidar muito de perto com o suposto infrator devido à própria natureza desses tipos de canais. Como forma de neutralizar este escopo de ação reduzido, com o qual não concordamos, o legislador espanhol opta por dar a ele mesmo o poder de compartilhar arquivos ilegais para que a pessoa que está investigando tenha confiança nele e possa conseguir uma infiltração eficiente. Da mesma forma, rejeitamos completamente este poder, pois acreditamos que não pode haver engano a qualquer preço, portanto os princípios da necessidade e proporcionalidade devem ser sempre levados em consideração, respeitando sempre os princípios e garantias processuais e os Direitos Fundamentais de qualquer pessoa, incluindo os dos supostos perpetradores. A justificativa para o engano utilizado pelo agente disfarçado reside em uma questão de política criminal, que vem a justificar as conseqüências desvalorizáveis que seu uso implica. A solução é dada por uma ponderação de valores, na qual o valor da "eficácia" é dado preponderância, no sentido de que se quisermos lutar eficazmente contra este crime oculto, a melhor maneira e a opção ideal é infiltrar a pessoa desta forma para conseguir uma situação mais favorável para a sociedade. Assim, estamos escolhendo uma solução que traga mais segurança e bem-estar para a sociedade como um todo e que alcance a justiça, um objetivo-chave em um Estado de Direito.

Então, que modus operandi defenderíamos para que o agente infiltrado seja capaz de se infiltrar efetivamente? Foi proposto que o material criminal de antigas batidas fosse trocado, o que não concordamos, pois acreditamos que a ofensa continuaria a ser cometida pelos agentes e que os direitos das vítimas seriam minados. Neste caso, optaríamos por permitir a troca de "material camuflado criado ad hoc", por isso nos referimos, por exemplo, à troca de material pornográfico no qual atores e atrizes pornográficas de idade legal aparecem como menores ou em tweets ou ameaças criadas contra pessoas fictícias para criar confiança na pessoa sob investigação. Nesses casos, tanto as ações do agente quanto o próprio material seriam enganosos sem realmente perpetrar qualquer ato repreensível contra qualquer pessoa ou qualquer valor legal ou bem. Acreditamos firmemente que o legislador deveria ter repensado esta figura, pois conceder ao agente o poder de trocar material ilícito com a pessoa sob investigação poderia levar a uma acusação pela defesa da indução ao crime

pelo próprio agente, com a qual a investigação poderia tornar-se nula e sem efeito ao considerar que o agente infiltrado se tornou um agente provocador, ao "dar à luz o germe criminoso[20]" sobre a pessoa sob investigação e ao utilizar a comissão de crimes como ferramentas de investigação. A este respeito, o texto final da lei estabelece que "será necessária uma autorização especial (seja na mesma decisão judicial, com motivação separada e suficiente, ou em outra diferente) para trocar ou enviar arquivos ilícitos em razão de seu conteúdo no curso de uma investigação", mas ainda não faz nenhuma declaração sobre a terminologia de "arquivo ilícito", uma questão que exigimos em trabalhos anteriores e que terá sua reflexão no final deste estudo.

3.1.3. Registro de dispositivos de armazenamento em massa

A busca de dispositivos é um dos procedimentos mais controversos regulamentados na Lei 13/2015, pois por um lado contempla referências à inspeção de dispositivos de armazenamento em massa, ou seja, servidores de organizações criminosas, bem como o uso de vírus espiões para realizar uma busca remota de dispositivos eletrônicos. Entre as questões a serem destacadas, a nova lei permite o acesso a informações de dispositivos eletrônicos apreendidos fora da residência da pessoa sob investigação, desde que arquivos ou dados armazenados em outros equipamentos que estejam de alguma forma conectados ao equipamento inicial sejam obtidos. Esta opção, devido à sua seriedade, foi especialmente projetada para crimes complexos. Desta forma, a Polícia Judiciária poderia até mesmo, em casos urgentes em que um interesse constitucional legítimo pudesse ser apreciado, realizar a interceptação e mesmo o exame direto do conteúdo sem autorização judicial, informando imediatamente o juiz e, em qualquer caso, dentro de um prazo máximo de 24 horas da ação realizada, a forma como foi realizada e seu resultado. O juiz, como nos casos anteriores, terá um período de 3 dias para autorizar ou negar a interceptação. Desta forma, o legislador

[20] STS de 14 de julio de 2000 que afirma que um crime provocado "é entendido como aquele que ocorre em virtude da indução enganosa de uma pessoa específica, geralmente um membro das Forças de Segurança que, desejando prender suspeitos, incita aqueles que não tinham intenção anterior de cometer o crime a fazê-lo, dando assim origem a intenção criminosa em um caso específico, um crime que não teria ocorrido se não fosse por tal provocação, embora por outro lado sua execução complexa fosse praticamente impossível devido à intervenção planejada ab initio da força policial".

impede a implementação da teoria do fruto da árvore envenenada nas evidências obtidas e joga com a teoria da conexão da antijurisdição[21], para discernir se a evidência reflexiva é válida ou não. Esta teoria tem sido defendida e aplicada pela doutrina e jurisprudência desde os anos 80, e endossada por decisões mais recentes como a STS 739/2009, segundo a qual a nulidade só deve afetar as ações realizadas no processo que tenham uma conexão causal ou legal, desde que a ordem de autorização judicial não tenha sido prorrogada. Da mesma forma, em termos de duração, por ser uma medida tão invasiva, é a mais curta das reguladas, pois está estipulado que terá uma duração máxima de um mês, prorrogável por períodos iguais até um máximo de 3 meses. Em segundo lugar, como no Rascunho do Código de Procedimentos Espanhol de 2013, o uso de vírus de *spyware* para o controle ou gerenciamento remoto do equipamento do investigado também é mantido, como foi contemplado no Rascunho do Código de Procedimentos Espanhol de 2013, pois ao falar abstratamente de "instalação de software" o tipo de vírus a ser usado pela polícia judiciária não é especificamente definido, deixando no ar a natureza maliciosa do vírus de computador, embora ao nos referirmos ao controle e gerenciamento remoto tudo nos leva a acreditar que se trata de um *spyware* de natureza zumbi.*[22]*.

Após várias questões mais ou menos discutíveis, o regulamento estabelece um preceito no qual adota a frase "os fins justificam os meios" para garantir o bom fim da diligência, estabelecendo que:

> "As autoridades e agentes encarregados da investigação podem ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados informáticos nele contidos que forneça as informações necessárias, desde que isso não resulte em um ônus desproporcional para a parte afetada, sob pena de incorrer no delito de desobediência".

[21] DE URBANO CASTRILLO, E., define a conexão da ilegalidade "como uma relação entre o meio de prova ilegal e a prova-espelho, suficientemente forte para nos permitir considerar que a ilegalidade original do primeiro transcende o segundo, a ponto de provocar sua sanção invalidante". Portanto, quando esta forte relação existe, é produzida a "contaminação" da prova reflexa, que também seria afetada pela ilegalidade da primeira e, portanto, seria igualmente nula e nula. Neste sentido, para uma melhor compreensão e sua relação com as TIC, devemos nos referir a dois exemplos: um em que esta relação de conexão é cumprida e outro em que não é. Foi assim que se pronunciou DE URBANO CASTRILLO en el artículo electrónico "La desconexión de antijuridicidad en la prueba ilícita", http://www.legaltoday.com/opinion/articulos-de-opinion/la-desconexion-de-antijuridiciad-en-la-prueba-ilicta (Fecha de consulta: 2 de marzo de 2015).

[22] Vid. VELASCO NUÑEZ, E., *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid, 2010, págs. 131-137, explica o que significa um vírus de natureza zumbi, onde você infecta um terminal e pode usá-lo à vontade sem que a pessoa que o possui perceba qualquer mudança.

O termo "qualquer pessoa" tem dois efeitos negativos imediatos. Em primeiro lugar, desvaloriza ou reconhece como insuficiente o treinamento técnico da polícia judiciária em termos de investigação policial, quando existem unidades específicas com membros com anos de especialização que foram treinados para esse fim e estão em constante reciclagem e treinamento, de modo que em termos de publicidade e imagem externa não acreditamos que isso nos faça bem e, em segundo lugar, que perfil essa pessoa tem? Quando falamos de qualquer pessoa, a identidade dessa pessoa não está definida; estamos falando de um engenheiro informático profissional? Ou, pelo contrário, abre a porta para o recrutamento de hackers agindo de forma antiética ou mesmo criminosa? Estes perfis poderiam ser possíveis, pois o regulamento só proíbe a colaboração da pessoa investigada ou acusada, pessoas que estão isentas da obrigação de testemunhar por razões de parentesco, bem como aquelas que, de acordo com o art. 416.2 LECRim, que indica que o advogado do réu não pode testemunhar em virtude do sigilo profissional em relação aos fatos que seu cliente lhe confiou na qualidade de advogado de defesa. Portanto, podemos ver como os processos estão se polêmicizando com diferentes questões até chegar a um zênite com as medidas contempladas para a busca de dispositivos, caracterizados por uma invasão feroz de diferentes direitos fundamentais de potenciais suspeitos, razão pela qual a motivação do juiz deve exigir um acréscimo de justificativa, com base em razões de necessidade que devem ser levadas em conta na investigação de crimes complexos.

REFERÊNCIAS:

ÁLVAREZ DE NEYRA KAPPLER, S. "Los descubrimientos casuales en el marco de una investigación penal", *RIEDPA*, nº 2 Mayo, 2011.

BAÑULS GOMEZ, F. "*Las intervenciones telefónicas a la luz de la jurisprudencia más reciente*" en el Portal Web Noticiasjurídicas.com, Febrero 2007, disponible en http://noticias.juridicas.com/articulos/55-Derecho%20Penal/200702-98193256327475 2514.html (Fecha de consulta: 18 de diciembre de 2014).

BUENO DE MATA, F. "Ciberterrorismo: Tratamiento penal y procesal del terrorismo del futuro", *Segundo Libro INCIJUP*, 2014.

BUENO DE MATA, F. "*El uso de spyware como diligencia de investigación en España: ¿inmoralidad necesaria*?", Ponencia presentada al XX Congreso Iberoamericano de Derecho e Informática, Costa Rica, 2014.

BUENO DE MATA, F. "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?", El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito, 2013.

BUENO DE MATA, F. *Prueba electrónica y proceso 2.0*. Valencia, 2014.

CAPELLETTI, M. "Eficacia de pruebas ilegítimamente admitidas y comportamiento de la parte", *La oralidad y las pruebas en el proceso civil*, Buenos Aires, 1972.

DE URBANO CASTRILLO en el artículo electrónico "La desconexión de antijuridicidad en la prueba ilícita", para la revista electrónica LegalToday, disponible en http://www.legaltoday.com/opinion/articulos-de-opinion/la-desconexion-de-antijuridiciad-en-la-prueba-ilicta

DELGADO MARTÍN, J., "La criminalidad organizada*" Comentarios a la LO 5/99, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilícito de drogas y otras actividades ilícitas grave,* Barcelona, J. M. Bosch, 2001.

GIMENO SENDRA, V., "La intervención de las comunicaciones*" Diario La Ley, Nº 7192,* Sección Doctrina, 9 Jun. 2009.

LOPEZ BARAJAS PEREA, I. *La intervención de las comunicaciones electrónicas,* Madrid, 2011.

LÓPEZ CABRERO, G., "Penas cortas de prisión. Medidas sustitutivas" en *Poder judicial*, 2ª Época. Núm. 40, octubre-diciembre de 1995.

LYON, David, *El ojo electrónico. El auge de la sociedad de vigilancia*, Madrid, 1995.

NADAL GÓMEZ, I., "La litigiosidad que se nos viene encima: cuestiones procesales al hilo de la aparición de «drones» en nuestros cielos", Diario La Ley, Nº 8507, Sección Doctrina, 25 de Marzo de 2015.

ORTIZ PRADILLO, J., http://juancarlosortizpradillo.blogspot.com.es/2015/05/reforma-penal-y-control-judicial-en-la.html?spref=fb (Fecha de consulta: 22 de mayo de 2015)

VELASCO NUÑEZ, E., *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid, 2010.