

- Costa, T. O. D. (2007). *Avaliação Institucional - uma ferramenta para o sucesso da instituição educacional*, in: COLOMBO, Sónia Simões (Editora Artmed). *Gestão Educacional - uma nova visão*. Porto Alegre: Editora Artmed.
- Fialho, J. Silva, C. A. e Saragoça, J. (2013) *Formação Profissional - Práticas Organizacionais, Políticas Públicas e Estratégias de Acção*. Lisboa: Edições Sílabo.
- Graceffi, V. (2012) *Planeamento e Execução do T & D*. In: BOOG, Gustavo e BOOG Madalena (Coord). *Manual de treinamento e desenvolvimento, processos e operações*. São Paulo: Editora Pearson.
- Instituto Médio de Ciências Policiais (2010). *Relatório Anual*. Luanda: IMCP.
- Instituto Superior de Ciências Policiais e Criminais (2012). *Plano de Desenvolvimento Institucional*. Luanda: ISPCP.
- Instituto Superior de Ciências Policiais e Criminais (2013). *Relatório Anual*. Luanda: ISPCP.
- Lapilli, É. M. (2010) *Gestão de Pessoas em Organizações Empreendedoras*. Brasil: Editora Pandion. Volume 5.
- Madeira, M. C. (2011). *Professor Universitário - Aprimorando o Desempenho*. São Paulo: Editora Sarvier.
- Malschitzky, N. (2011) *Pessoas e Gestão - Uma Parceria Sustentável*. São Paulo: Actual editora.
- Oliveira, D. P. R. (2011). *Administração Estratégica na Prática - A Competitividade para Administrar o Futuro das Empresas*. 7ª Edição. São Paulo: Atlas Editora, Lda.

3.

Fundamentos Criminológicos do Risco Informático

Waldemar Paulo da Silva José³

RESUMO

O presente artigo de como finalidade de abordar as alterações paradigmáticas que temos vindo a observar nas sociedades pós-modernas, parte delas são provenientes dos efeitos da globalização, da disseminação do computador e da Internet. Para esse estudo utilizou-se a pesquisa bibliográfica, e alguns sites, os mesmos permitiram explorar temáticas sobre o risco e a criminalidade informática apresentando características de um acto ilegal de carácter transnacional que o distanciam do crime tradicional e o aproxima de um crime não convencional ou, de um novo tipo, de um bem jurídico difuso, atendendo que torna complexo o processo de individualização e responsabilização do autor do facto e de seus participantes. O *know-how* tecnológico avançado e o equipamento tecnológico especializado são exigidos tanto para executar as acções lícitas e ilegais, como para poder enfrentá-las, impedi-las e persegui-las efectivamente, uma vez que apresentam problemas de jurisdição ao transcender as acções cometidas nas fronteiras

³ Doutorado em Ciências Jurídicas, pela Universidade de Havana-Cuba, Pós-graduado em Criminalística, pelo Instituto Superior del MININT "Eliseo Rodríguez - Capitán San Luis, Licenciado em Ciências Policiais pelo Instituto Superior de Ciências Policiais e Segurança Interna, Portugal.

nacionais e podendo causar seus efeitos em todas as latitudes do mundo, o que exigiu o apelo das organizações a nível internacional em unir forças para a sua prevenção e combate, envolvendo o desenvolvimento de políticas de segurança de cada nação, em que predomina um desequilíbrio a favor do exercício do poder punitivo em detrimento das garantias individuais, como o direito à liberdade de comunicação, expressão e privacidade.

Palavras – Chave: Fundamentos Criminológicos; Riscos Informáticos.

Introdução

As sociedades actuais estão condicionadas e determinadas pelo surgimento da cultura do risco, devido o constante desenvolvimento das ciências que contribuem com ordenações que facilitam o seu surgimento, particularmente, as tecnologias de informação e comunicação, que por sua vez, tem favorecido o processo de globalização mundial, assim como o surgimento e consolidação do delito ou crimes transnacionais.

O processo de globalização supracitado tem favorecido a destruição dos pilares basilares, a partir dos quais se concebeu, tradicionalmente, as sociedades, como uma unidade territorial coesa, em torno de instituições políticas e de governo, o que afecta, consideravelmente, a histórica unidade do Estado e da Nação, pressupostos fundamentais para a existência de crise na ideologia filosófica do Estado Nação.

Na nova sociedade, o seu papel prende-se com o facto de se desenvolver empresas transnacionais, organismos nacionais e internacionais, que são autênticos protagonistas e principais actores

de uma economia organizada à escala mundial.⁴ Este processo implica que, praticamente, quase todos os fenómenos que sucedem no mundo limitam suas repercussões a um espaço geopolítico concreto.

A interdependência de sistemas tem-se verificado em todos os aspectos da sociedade, desde os económicos até aos humanos, políticos ou culturais. Como consequência deles, tem surgido a chamada "sociedade- vermelha", amplamente tratada por Castells,⁵ no que se refere ao carácter imediato das relações, fundamentada nos avanços tecnológicos (em especial as telecomunicações), ocupando um lugar essencial. A sociedade moderna da informação domina, de modo primordial, as inter-relações do sujeito com o meio que o rodeia, mas entende-se isto, não como seu contexto mais directo e concreto, senão como o total das sociedades industrializadas que têm acesso às ditas telecomunicações, sem esquecer que as transferências da informação são hoje dirigidas aos países mais desenvolvidos.

À sombra deste processo globalizador, tem surgido uma sociedade em que a multiplicidade de recursos e opções se encontra à ordem do dia. Não obstante, do mesmo modo que se tem verificado um aumento substancial das potencialidades dos sistemas informáticos, tem-se produzido, também, a expansão dos riscos derivados delas.⁶

⁴ DIEZRIPOLES, José Luis. "De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado". En: Revista Electrónica de Ciencia Penal y Criminología, BECK, Ulrich. La sociedad del riesgo. Hacia una nueva modernidad, Paidós, Barcelona, 1998, p. 8.

⁵ CASTELLS, Manuel. La era de la información. Economía, sociedad y cultura, Alianza editorial, Madrid, 1999, p. 2.

⁶ JIMÉNEZ DÍAZ, María José. "Sociedad del riesgo e intervención penal". En: Revista Electrónica de Ciencia Penal y Criminología. No. 16-08, p. 9. Disponible en: http://criminologia.ugr.es/rocp/16/rocp16_08.pdf. Fecha de consulta 12 de abril de 2015.

Apesar de tudo, há que ter em conta que o risco como tal, é exclusivamente uma percepção social, surge a partir do momento em que é reconhecido socialmente; pelo seu carácter social, não existe nenhum comportamento livre deste; mas na tomada de decisão, torna-se numa determinação singular, fundamentada na própria ideia de risco.

A percepção de risco implica necessariamente um juízo de valor: em primeiro lugar, identifica-se a situação inicial e depois analisa-se e ajulza-se para saber se existe algum perigo. A definição de risco implica a avaliação negativa das possíveis consequências do facto analisado, o que indica que o risco tem uma forte e fundamental componente subjectiva, pelo que, não é possível distinguir entre risco e a sua percepção, já que vem sendo o mesmo sentido.

O perigo inerente que se encontra implícito na ideia de risco é permanente⁹, mas as consequências negativas seriam iguais ou inclusive piores se a tivéssemos identificado como potencialmente prejudiciais.

A apreciação de risco induz que este só existe desde uma perspectiva do indivíduo, todavia não é assim desde o ponto de vista real, no entanto, sua existência como perigo, não está condicionada à percepção e ao conhecimento humano. A percepção dos riscos nunca se fará de forma emparelhada à dimensão real do mesmo¹⁰. A familiaridade de uma situação, como o uso frequente de computadores na vida pessoal ou empresarial, provoca que

⁹ BECK, Ulrich. Las sociedades del riesgo, Paidós, Barcelona, 1998, p.39.

¹⁰ MARTINEZBLANCO, María Gracia; FERNÁNDEZPÉREZ, María José; MARCÓARBONES, María. "Problemas conductuales relacionados con el uso de internet: un estudio exploratorio", *Anales de psicología*, Vol. 18, Nº 2, diciembre 2002, pp. 273-288.

se minimizem os possíveis danos posteriores ao considerá-los reconhecidos e, portanto, totalmente controlados.¹¹

A familiaridade e a proximidade geram e criam a confiança¹² que nem sempre corresponde com a situação real de perigo desta forma, ignoram-se ou excluem-se aqueles que nos são mais comuns, bem como aqueles extraordinariamente pouco frequentes.¹³

A existência de entidades humanas e os indivíduos que as dirigem, através de suas decisões, são os últimos culpados da maioria dos riscos sociais de hoje, não havendo dúvida de que o próprio conceito de risco está intimamente ligado ao do conceito de responsabilidade.

Toda a análise e gestão de riscos têm como consequência uma eleição, na qual, vistos os seus posteriores resultados, deve comportar necessariamente as responsabilidades das referidas consequências¹⁴, jogando um papel transcendental respectivo ao uso consciente e responsável das tecnologias de informação e comunicação.

A natureza de muitos riscos actuais (sobretudo, os de natureza tecnológica, em que está presente a informática) acentua o grave

¹¹ LOMBARTE BEL, Silvia. El uso de las Tecnología de la Información y las Comunicaciones reduce realmente la vulnerabilidad social en los jóvenes? Universidad de Barcelona. Disponible: http://campus.usab.es/~teoriaeducacion/rev_numero_06/n6/art_lombarte.htm. Fecha de consulta 12 de marzo de 2016, p.3.

¹² CASTELLS, Merce. La era de la información. Economía, sociedad y cultura, Alianza, Madrid, 1998, p. 57.

¹³ DOUGLAS, Mary. La aceptabilidad del riesgo según las ciencias sociales, Paidós, Barcelona, 1996, p.67.

¹⁴ LÓPEZ CERERO, José Antonio y LUJÁN LÓPEZ, José Luis. Ciencia y política el riesgo, Alianza, Madrid, 2000, p. 106.

problema de responsabilidade existente nas sociedades actuais. Ainda assim, não se trata somente de questões de responsabilidade pessoal ou não, no entanto, torna-se difícil não assumir a culpa, senão, tão-somente defini-la, devido ao que a grande maioria dos riscos actuais são consequências directa e indirecta, de uma acumulação de factores.¹⁶

Seja como for, a imputabilidade de responsabilidades torna-se extremamente difícil, por não haver alternativa, desde que, como disse LÓPEZ CERZCOY LUJÁN LÓPEZ¹⁶, para que ele aconteça, deve existir dois factores: o primeiro, a previsibilidade, isto é, o conhecimento preciso das consequências que obterá uma acção e o segundo, o agente a que se possa atribuir a dita consequência e responsabilidade.

A sociedade actual encara as novas tecnologias e o desenvolvimento acelerado das comunicações e da informática, enfrentando os riscos identificados em diferentes pontos de vista: do ponto de vista global e do ponto de vista individual, na qual, a cada um corresponde, particularmente, uma ideia e o respectivo argumento ou juízo de valor.¹⁷

¹⁶ Según lo señala otros autores como BRUNNER, COUSIÑO y VALENZUELA, este tipo de procesos se encuentran operando globalmente y afectan la totalidad de los procesos de modernización, donde un rol fundamental lo desempeñan el constante desarrollo de las tecnologías de la información y las comunicaciones, por las graves consecuencias que puede ocasionar su inadecuado uso. Cfr. BRUNNER, José Joaquín, *Globalización cultural y postmodernidad*, Volumen I, Fondo de Cultura Económica, México, 1998, p. 8; COUSIÑO, Carlos y VALENZUELA Emilio, "Polifización y Monetización en América Latina".

¹⁶ LÓPEZ CERZCO, José Antonio y LUJÁN LÓPEZ, José Luis, Ob. Cit. P.136.

¹⁷ Idem. p.136.

O acto mais proeminente da sociedade globalizada diz-nos que não é impossível controlar os riscos. Cada vez mais, os actos realizados numa parte do mundo encontram-se inter-relacionados de maneira directa com o resto do planeta; e, portanto, cada vez mais internacionalizam-se e tornam-se transfronteiriços, tanto os que surgem num determinado lugar como os que surgem em outros lugares mais distantes, não havendo, a partida, a possibilidade de se dar o devido tratamento a estas novas situações de perigo de forma isolada.

Hoje é inquestionável dizer-se que as acções correctas que a sociedade, no geral, se baseia em suas actuações são potencialmente perigosas, pois estas actuações têm a ver com os avanços tecnológicos e científicos. A exposição a estes riscos acontece de forma constante na maior parte do mundo, principalmente nas sociedades da informação, onde há uma interconexão constante entre continentes em tempo real.¹⁸

Este estado de coisas torna necessário examinar e avaliar qualquer um dos problemas que surgem de forma global e interactiva como parte de um sistema sociocultural complexo, onde o crime é uma das suas componentes e também um fenómeno social ao qual a Criminologia e o direito penal tem que se adaptar e, acima de tudo, encontrar formas de enfrentar efectivamente os riscos impostos pela sociedade da informação e pelas comunicações, que podem ser identificados como risco informáticos.

¹⁸ En cuanto al futuro, como dice LÓPEZ BARJA DE QUIROGA, la sociedad actual no es una sociedad del coche o la radio, con un planteamiento individual e independiente del objeto o de la persona; es la sociedad en la que sus actividades están aforadas por las nuevas tecnologías de la información profundamente vinculadas o interrelacionadas. LÓPEZ BARJA DE QUIROGA, Jacobo, "La protección penal de los programas de ordenador". En: Revista del poder judicial, n° 88, Dialnet, 2000, p. 11.

No que diz respeito à tecnologia informática, o risco geralmente é apenas representado como uma ameaça, determinando o grau de exposição à ocorrência de uma perda (por exemplo, o risco de perda de dados devido a falhas no disco, vírus informáticos, etc.). A Organização Internacional de Padronização (ISO-27005: 2008) define um risco tecnológico como: "a probabilidade de uma ameaça se materializar, usando a vulnerabilidade existente de um activo ou um grupo de activos, gerando-lhe perdas ou danos".

Os riscos informáticos referem-se à incerteza da possível ocorrência de um evento relacionado à ameaça de danos em relação aos bens ou serviços informáticos, tais como equipamentos informáticos, periféricos, instalações, projectos, programas informáticos, arquivos, informações, dados confidenciais, entre outros.¹⁹

3.2. Enfoque do Delito Informático

A nova e questionada denominação de delitos informáticos expressa perfeitamente a preocupação com um novo tipo de crime que surgiu com a existência dos primeiros sistemas informáticos, nos quais esses eram os meios ou o objectivo do crime.

Como diz Wall²⁰, "a geração de crimes que nos interessam não está mais preocupada em ter como o elemento característico a ser executado a partir de computadores, mas pelo facto de que tais sistemas informáticos estão conectados em um campo de

comunicação transnacional-universal, o ciberespaço, sendo nesse novo "lugar" em que, a partir de qualquer espaço físico localizado em qualquer nação, podem ser cometidos infracções que possam afectar, em diferentes lugares e simultaneamente, bens jurídicos tão diversos como património, privacidade, liberdade e intimidade sexual, honra dignidade pessoal, segurança do Estado, livre concorrência, entre muitos outros²¹.

Em primeiro lugar, o crime informático, do ponto de vista da criminologia, foi categorizado como uma encarnação da delinquência económica²², mas rapidamente reconheceu outro espaço quando começou a representar uma ameaça à esfera privada do cidadão²³.

Na criminalidade informática, independentemente do propósito do infractor informático persegue, seja económico, político ou ideológico, social ou pessoal, de uma perspectiva fenomenológica, agrupam-se os comportamentos que provocam crimes que só poderiam ser realizados pela existência do ciberespaço ou Crime

²¹ CLOUGH, Jobs. *Principles of Cybercrime*, Cambridge University Press, Cambridge, 2010, p. 4-6.

²² THIEDEMANN, Klaus. *Wirtschaftsstrafrecht und Wirtschaftskriminalität*, Vol. 2, Hamburg, 1976, p. 148; SIEBER, Ulrich, *Ob. Cit.*, p. 188.

²³ THIEDEMANN, Klaus. *Poder económico y delito*, Ariel, Barcelona, 1986, p. 122; SIEBER, Ulrich. *The International Handbook...*, *Ob. Cit.*, p. 57; HERNÁNDEZ DÍAZ, L., "Aproximación a un concepto de Derecho penal informático", en *Derecho penal informático*; DE LA CUESTA ARZAMENDI, J. L. (Dir.), *Cizur Menor, Civitas, España*, 2010, pp. 35 - 42; ROMERO CASABONA, Carlos Manuel. *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información*, Duendesco, Madrid, 1988, p. 28. Al respecto, Ruiz VADILLO, estima que "si partimos por vía de hipótesis de que existe una delincuencia específica informática necesitada de una cierta autonomía, esta ha de insertarse en el más amplio capítulo de la criminalidad de los negocios". Más adelante, el mismo autor considera tres las zonas hacia las que se dirige la delincuencia económica: la patrimonial, el espionaje y la intimidad de las personas. RUIZ VADILLO, E., *Ob. Cit.*, p. 66.

¹⁹ SILVA SÁNCHEZ, José María. *La expansión del Derecho penal. Aspectos de la Política criminal en las sociedades post industriales*. Edisofer, Madrid, 2011, p. 23.

²⁰ WALL, David. *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2007, p. 44.

informático puro, tais como *hacking*, ataques, infecções de *malware*, utilização das técnicas de *Phishing*, *Salami*, *Trojan Horse*, *Spyware* etc.

Também incluem crimes que têm uma modalidade tradicional de comissão no espaço físico e hoje exibem uma modalidade concreta de execução no ciberespaço, entre as quais destacam-se ciborfraudes de diferentes naturezas, ciber-abuso sexual a menores, cyberbullying, cyberstalking, entre muitos outros.

Dentro dessas formas peculiares de execução criminal, também inclui aqueles cuja ilegalidade é caracterizada pela proibição de transmissão ou disseminação de conteúdo, como a pornografia infantil, a transmissão oral ou a disseminação de mensagens de ódio racial, ciberterrorismo, pirataria intelectual na Internet, etc.

As primeiras aproximações da Criminologia ao fenómeno da criminalidade informática centralizaram-se na discussão sobre as motivações do delinquentes informático, talvez por causa da atractividade desse sujeito que perpetrava crimes usando o conhecimento adquirido de tecnologia da informação e telemática, no entanto, não foi identificado com o protótipo tradicional assumido para cada delinquentes, por apresentar um perfil criminológico peculiar, mas também porque a Criminologia, naquele período, focalizava-se na compreensão de determinantes do comportamento do sujeito criminal e suas modalidades.

Hoje, o foco mudou e, enquanto estudos criminológicos interessantes foram desenvolvidos sobre crime informático em que são tratadas teorias criminais, tais como a do autocontrolo²⁴,

²⁴ HIGGINS, George. "Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy?" En: University of Louisville, USA, Primavera, Vol. 2, United States, 2004; HIGGINS, George y FELL, Brian "Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States" En: Social Science Computer Review, Nº 25, United States, 2007, p. 339.

tornada de decisão racional²⁵, aprendizado social²⁶, controlo social²⁷ ou rotulagem, uma grande parte desses estudos que tentam entender o crime informático e definir suas características particulares ao serem realizadas no ciberespaço levam em consideração a "abordagem" da oportunidade e, mais especificamente, a teoria da COHEN e FELSON;

Referências Bibliográficas

Blasco Lucía. *Qué es el peligroso juego de "La ballena azul" y por qué preocupa a las autoridades*. BBC Mundo. Disponible: <http://www.bbc.com/mundo/noticias-39721105>. Fecha de consulta: 17 de mayo de 2001.

Castells, Manuel. *La era de la información. Economía, sociedad y cultura*, Alianza editorial, Madrid, 1999, p. 2.

Castells, Manuel. *La era de la información. Economía, sociedad y cultura*, Alianza, Madrid, 1998, p. 57.

Clement San Juan, Victor. *Sociedad del riesgo, producción y sostenibilidad*, Dialnet, ISSN 0210-2862, Nº 82, 2006, p. 121.

²⁵ BEEBE, Nicole. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security". En: Proceedings of the 2005 Software Conference, Las Vegas, NV, December 2005.

²⁶ YOUNG, Robert y ZHANG, Lixuan. "Factors Affecting Illegal Hacking Behavior". En: Americas Conference on Information Systems, (AMCIS) Proceedings, Omaha, Francia, 2005, Disponible: <http://www.waisel.a.snet.org>. Fecha de consulta: 12 de julio de 2016. Miró Linares, Fernando. "En el ciberespacio. Aplicación y Desarrollo de la Teoría de las Actividades Cotidiana para la prevención del cibercrimin". En: Revista Electrónica de Ciencia Penal y Criminología, Nº 13-07, España, 2011, p. 7.

²⁷ SVENSSON, Jörgen y BANNISTER, Frank. "Pirates, sharks and moral crusaders: Social control in peer-to-peer networks". En: First Monday Peer Reviewed Journal on the Internet, Vol. 9, Nº 6 – 7, junio, 2004, p. 1.

Díezripollés, José Luis. *De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado*. En: *Revista Electrónica de Ciencia Penal y Criminología*,

Del Pino Acurio, Santiago, *Delitos informáticos. Generalidades: Correlación carácter transnacional de esta nueva forma de delincuencia estíma, que: "La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003*, Disponible: www.oas.org/juridico/spanish/cyb_ocu_delitos_inform.pdf 13 de marzo de 2017.

Desireé Jaimovich. *Ciber delitos: cuáles son los más peligrosos y qué medidas de precaución tomar*. Disponible: <http://www.infobae.com/tecnologia/2016/07/31/ciberdelitos-cuales-son-los-mas-peligrosos-y-que-medidas-de-precaucion-tomar>.

Jiménez Díaz, María José. *Sociedad del riesgo e intervención penal*. En *Revista Electrónica de Ciencia Penal y Criminología*. Nº. 16-08, p. 9. Disponible en: <http://criminol.ugr.es/recpc/16/recpc16-08.pdf>. Fecha de consulta 12 de abril de 2015.

Lombarte Bel, Silvia. *El uso de las Tecnología de la Información y las Comunicaciones reduce realmente la vulnerabilidad social en los jóvenes?* Universidad de Barcelona. Disponible: http://campus.usal.es/~teoriaeducacion/rev_numero_06/n6.art.lombarte.htm. Fecha de consulta 12 de Marzo de 2016, p.3.

López Cerezo, José Antonio y LUJÁN LÓPEZ, José Luis. *Ciencia y política el riesgo*, Alianza, Madrid, 2000, p. 106.

Linares, Fernando. "En el ciberespacio. Aplicación y Desarrollo de la Teoría de las Actividades Cotidiana para la prevención del ciberdelito". En: *Revista Electrónica de Ciencia Penal y Criminología*,. Nº 13-07. España. 2011, p. 7.

Marcóarbonos, María. *Problemas conductuales relacionados con el uso de internet: un estudio exploratorio*, *Anales de psicología*, Vol. 18, Nº 2, Diciembre 2002, pp. 273-298.

Silva Sánchez, José María. *La expansión del Derecho penal. Aspectos de la Política criminal en las sociedades post industriales*. Edisofer, Madrid, 2011, p. 23.

Svensson, Jörgen y Bannister, Frank. *Pirates, sharks and moral crusaders: Social control in peer-to-peer networks*. En: *First Monday Peer Reviewed Journal on the Internet*, Vol. 9, Nº 6 – 7, junio, 2004, p. 1.

Thiodemann, Klaus. *Wirtschaftsstrafrecht und Wirtschaftskriminalität*, Vol. 2, Hamburg, 1976, p. 148; SIEBER, Ulrich, *Ob. Cit.*, p. 188.

Young, Robert y ZHANG, Lixuan. "Factors Affecting Illegal Hacking Behavior". En: *Americas Conference on Information Systems, (AMCIS) Proceedings*, Omaha, Francia, 2005, Disponible: <http://www.aiselaisnet.org>. Fecha de consulta: 12 de julio de 2015. Miró

3.3. Carácter Transnacional

É comum nos estudos criminológicos realizados hoje associar o carácter transnacional de um crime e, consequentemente, de quem executa o crime transnacional organizado, tão bem reconhecido na Convenção de Palermo de 2000, normativo de alcance mundial que uniformizou do nível substantivo e processual as formas de investigação, persecução e julgamento dos delinquentes ligados à criminalidade organizada e que cometem actos criminosos de especial gravidade que podem afectar bens jurídicos difusos, supranacionais, etc.

Diante dessa retórica, eles atribuem o de "transnacional" à criminalidade informática devido à sua gravidade especial, considerada com base nos marcos criminais abstractos previstos nos tipos criminais que foram regulamentados em diferentes países. No entanto, argumenta-se que esta condição não deve depender do exposto acima, mas fundamentalmente, deve ser considerada como tal, pelo alcance dos ataques informáticos e o número de vítimas que se podem atingir em diferentes latitudes em tempo real. Paralelamente a isso, pode-se acrescentar que o delinquente informático, geralmente, apresenta como perfil uma acção criminal individual e em raras ocasiões se identifica como membro de uma organização criminosa, integrada por duas ou mais pessoas com propósitos semelhantes.

O delinquente informático e, conseqüentemente, o crime informático, hoje, atingem uma dimensão de acção criminal do delito transnacional e transcultural, devido à sua estrutura básica e à disponibilidade global dos seus serviços, visto que é muito fácil enviar *e-mails* ou ficheiros com conteúdos ilegais ou maliciosos aos destinatários de vários países, mesmo quando o remetente inicial e o destinatário final estão no mesmo país ou onde o remetente ou destinatário usam um serviço de correio electrónico fornecido por um provedor localizado fora do país.

Por exemplo, alguns dos mais conhecidos provedores de serviços de correio electrónico gratuito têm milhões de usuários em todo o mundo, que podem estar sujeitos a ataques cibernéticos de outro país, reforçando a dimensão transnacional do cibercrime.

Além do exposto, pode-se resumir que a criminalidade informática apresenta características de um acto ilegal de carácter transnacional que o distanciam do crime tradicional e o aproxima de um crime não convencional ou, de um novo tipo, atendendo que

torna complexo o processo de individualização do autor do facto e de seus participantes.

O *know-how* tecnológico avançado e o equipamento tecnológico especializados são exigidos tanto para executar as acções ilegais, como para poder enfrentá-las, impedi-las e persegui-las efectivamente, uma vez que apresentam problemas de jurisdição, ao transcender as acções cometidas nas fronteiras nacionais e podendo causar seus efeitos em todas as latitudes do mundo, o que exigiu o apelo das organizações mundiais, com o objectivo de unir forças na comunidade internacional de cada país para a sua luta, pelo qual invocam o desenvolvimento de políticas de segurança de cada nação, em que predomina um desequilíbrio a favor do exercício do poder punitivo em detrimento das garantias individuais, como o direito à liberdade de comunicação, expressão e privacidade.

Um exemplo real do crime transnacional e transcultural da cibercriminalidade, devido à extensão do dano em diferentes latitudes do planeta, onde não só se relacionam pessoas de diferentes países como perpetradores e vítimas, mas também de diferentes continentes, é notada no perigoso jogo virtual *Blue whale*, ou Baleia Azul, que foi expandido pelas redes sociais e causou inúmeras perdas de vidas humanas em vários países.

O fenómeno criminal da baleia azul está presente em plataformas como *Facebook* ou *Twitter*, *Instagram*, *YouTube*, entre outros, e atinge hoje um número considerável de vítimas de diferentes continentes; há relatos de vítimas na Rússia, Espanha, Colômbia, México, Brasil, entre outros,²³ e consiste numa série de desafios criados em grupos

²³ DEL PINO ACURIO, Santiago, Delitos informáticos. Generalidades. Correlacional carácter transnacional de esta nueva forma de delincuencia estima, que: "La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional,

fechados, em que jovens, preferencialmente, entre 12 e 14 anos, que são convidados a realizar um teste, em cada dia, num período de cinquenta dias²⁰.

A intensidade dos desafios aumenta com a passagem de pedidos, como comer uma certa quantidade de ovos cozidos ou não falar o dia todo com outras pessoas, até ao ponto de se demandar exigências mais macabras, como invocar espíritos ou fazer alguns arranhões na pele sob a forma de uma baleia. Alguns forçam as vítimas a acordar de madrugada para assistir vídeos de terror, cortar o braço com uma navalha ou aproximar-se da borda de um penhasco ou precipício. Finalmente, os jovens são chamados pelos "promotores

que entrón vigor en septiembre de 2003, es el principal instrumento internacional en la lucha contraladelincuencia organizada. (...) endichaconvención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichasregashacen especial mención de los delitos relacionados con la legitimación de activos y los de corrupción. También se mencionan a los llamados "delitos graves" que son de acuerdocon el Art. 2 toda "conducta que constituyaun delito puniblecon una privación de libertad máxima de al menos cuatroaños o con una pena más grave. En el caso de las llamadasinfracciones informáticas todas ellason delitos graves de acuerdo a la definición de la Convención, en tal razón se encuadranensuámbito de aplicación de la convención de conformidad al Art. 3, siempre que dichos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado" Disponible:www.oas.org/juridico/espanish/cyb/eou/delitosInform.pdf13 de marzo de 2017.

²⁰ Vid.¿Cuáles son los 50 retos del mortal juego: "La Ballena Azul"? Disponible: <http://www.metro851.com/301705/cuales-son-los-50-retos-del-mortal-juego-la-ballena-azul/>. Fecha de consulta: 19 de Mayo de 2017. La ballena azul, 50 retos y 130 menores rusos muertos. Disponible: <http://www.laregion.es/articulo/virales/ballena-azul-macabro-juego-ruso-han-muerto-130-menores/30170306193326691945.html>. Fecha de consulta: 19 de Mayo de 2017. La ballena azul, ¿responsable de la ola de suicidios adolescentes en Latinoamérica? Disponible: http://www.elconfidencial.com/mundo/2017-06-10/américa-latina-treinta-muertos-ballena-azul-juego-adolescente-muerte_1380293/. Fecha de consulta: 19 de Mayo de 2017.

sdo jogo", que estão acostumados a ser pessoas com traumas e graves desequilíbrios psicológicos, a cometer suicídio.²¹

Estima-se que este tipo de jogos seja abundante nas redes sociais, não é nem o primeiro nem o último. Na Rússia, como resultado do jogo da baleia azul, de Novembro de 2015 a Abril de 2016, 130 crianças e adolescentes do país suicidaram-se²².

Outro sinal do alcance transcontinental da criminalidade informática está no constante e crescente alcance global de seus efeitos nocivos, pois, de acordo com os relatórios de *PandaLabs*, no último semestre foram colocados no ciberespaço 18 milhões de novos vírus informáticos²³.

Entre os ataques mais frequentemente identificados, o *Ransomware*, também conhecido como cybersequestro de dados, que corresponde a ataques informáticos de *hackers* e *crackers* que criptografam arquivos ou ficheiros e, em seguida, através de um e-mail, por meio de uma chamada ou SMS requerem uma certa quantia de dinheiro ao usuário, para recuperar as informações criptografadas.

²¹ BLASCO Lucia. Qué es el peligroso juego de "La ballena azul" y por qué preocupa a las autoridades. BBC Mundo. Disponible: <http://www.bbc.com/mundo/noticias-38721106>. Fecha de consulta: 17 de mayo de 2017.

²² Vid. Así es el "juego de la ballena azul", que lleva a los jóvenes hasta el suicidio. Disponible: <http://www.antenat3.com/noticias/mundo/asi-juego-ballena-azul-que-lleva-jovenes-suicidio-2017030158b718040cf2884da459caes.html>. Actualizado el 13/04/2017 a las 10:16 horas. Fecha de consulta: 17 de mayo de 2017.

²³ DESIREE Jaimovich. Ciberdelitos: cuáles son los más peligrosos y qué medidas de precaución tomar. Disponible: <http://www.infobae.com/tecnologia/2016/07/31/ciberdelitos-cuales-son-los-mas-peligrosos-y-que-medidas-de-precaucion-tomar/>. Fecha de consulta 16 de mayo de 2017. a sensação de insegurança de sua vítima, que chega a sentir-se completamente invadida a sua privacidade, acto que lhe obriga, de qualquer maneira, a ceder perante o pagamento exigido.

Nos ataques informáticos anteriormente expostos, o usuário escolhido é repetidamente vitimizado, uma vez que, juntamente com a demanda de pagamento de dinheiro para o resgate de seus dados, os criminosos informáticos enviam os dados de IP de conexão, o nome do servidor de internet e até uma foto da casa tirada da *webcam* do próprio internauta, algo que

Este tipo de acto ilegal não obedece a acções de natureza aleatória ou de azar, mas são direccionadas para pessoas e entidades que anteriormente conheciam, manipulam informações sensíveis ou valiosas que se deseja preservar. Esses ataques ou *malwares* são possíveis, precisamente, por causa do nível de interconectividade que existe hoje na nuvem cibernética ou acesso a dados por meio da internet, onde vários sistemas de mensagens estão vinculados para transferir dados à nuvem. Também na nuvem, os sites da empresa são usados para compartilhar informações entre os funcionários no quadro da Internet das coisas e, a partir daí, o hacker ou o cracker pode aceder os dados do usuário ou o servidor onde está a informação.

No que concerne a violação de bens jurídicos difusos, como os casos resultantes de ataques em que se usa a informática como meio ou objecto, também foram detectadas casas inteligentes bloqueadas por criminosos informáticos, bem como em sistemas remotos que retiram dinheiro de celulares. Nesse sentido, é apresentado como uma das perspectivas da Internet das coisas, colocar em operação mecanismos suficientes para minimizar a vulnerabilidade a que a informação está exposta hoje, conforme diz Desirée Jaimovitch³⁵, "de acordo com dados da consultoria Gartner até o final do ano, haverá 6,4 bilhões de dispositivos deste tipo conectados (30% a mais que

³⁵ Ibid.

em 2015) e até 2020, 25% dos ataques que as empresas sofrerão estarão relacionados a esses equipamentos.

Hoje, os telefones inteligentes ou os *smartphones* são pequenos centros operacionais de onde tudo pode ser controlado, o que também implica um maior risco, pois, um estranho ao aceder um celular de uma terceira pessoa, pode ter, não só todos os tipos de informações pessoais do usuário, como também, caso o usuário tenha aplicativos relacionados a cartões de crédito, o *hacker* ou *cracker* o terá à sua disposição, uma caixa virtual completamente disponível que poderá manipular à sua vontade.

O incremento do uso de dispositivos pessoais no local de trabalho também é um fenómeno que tem contribuído para o acréscimo do risco informático, como é o caso do efeito *BYOD – Bring Your Own Device*, traga o seu próprio dispositivo, proporciona dilemas, não apenas relacionados à utilização dos dados e ficheiros digitais, mas principalmente no que concerne à segurança das instituições, levando à perda de dados e contaminação da rede corporativa.

Atendendo ao facto de que alguns dos dispositivos a serem utilizados nas organizações são de uso pessoal, é imprescindível determinar a quem se deverá imputar a responsabilidade pelas informações corporativas que, eventualmente, possam ser transferidas e guardadas no equipamento pessoal, ou pelo facto de estar inserido numa rede em que há acesso a conteúdos com um nível elevado de risco informático que possa danificar ou perigar os outros dispositivos.

Como nem todos os usuários de computadores portáteis, telefones inteligentes, e tablets possuem aplicativos de segurança, como antivírus, proporcionam um ambiente de vulnerabilidade a todos

os demais dispositivos, a contraírem vírus, instalação de programas maliciosos, bem como outros *worms*.

Além da infecção por vírus, o próprio ambiente de mobilidade pode fragilizar o processo de autenticação, de acesso à informação, segurança do *hardware* e *software*, bem como pode facilitar o acesso indevido ou o roubo das informações armazenadas nos sistemas.

As ações da criminalidade informática são, necessariamente, a contraposição verificada pelo desenvolvimento dos sistemas de segurança na Internet, que nem sempre são totalmente inacessíveis, uma vez que os profissionais da cibernética que desencadeiam os seus ataques constantemente desenvolvem vírus, *malwares*, ou técnicas de perpetração criminosa, com a finalidade de tornar vulnerável a segurança informática, sobretudo a que se desenvolve na nuvem, ou espaços adequados para transferir e guardar informações digitais, tendo-se tornado hoje como expressão do ciberespaço, um novo cenário onde uma criminalidade especializada comete crimes de natureza diversa.

Conclusão

O processo de inovação tecnológica proporciona inúmeras vantagens à sociedade, mas também acarreta diversos riscos, visto que o homem utiliza essas novas tecnologias para realizar ações direcionadas para o auxílio das suas actividades, assim como para perpetrar ilícitos criminais.

A globalização trouxe inúmeras vantagens do fórum tecnológico, mas o aparecimento deste fenómeno criminal torna-o num dos maiores fracassos da aldeia global. Pelas próprias características do meio, perspectiva-se uma moderna e convidativa forma para a prática de crimes desta natureza, que ocorrem em maior ou menor número em todos os países.

A adequação social de costumes e culturas dos povos, consubstanciada na soberania dos países, não admite que se estabeleça regras legais internacionais uniformes para todos os ordenamentos jurídicos, questão que se tem vindo a verificar no âmbito da criminalidade das tecnologias de informação.

No campo virtual não está delimitado por barreiras, tornando a indefinição de fronteiras um dos grandes problemas para o esclarecimento dos crimes ocorridos neste domínio. Contrariedades nos ordenamentos jurídicos e tratados internacionais de diferentes países e a falta de definição de responsabilidade aos provedores de serviço de Internet são factores que prejudicam ainda mais as investigações policiais e, concludentemente, a punição aos infractores.

As ferramentas de natureza informática, especialmente a Internet, possibilitam a perpetração de diversos ilícitos criminais. O desenvolvimento tecnológico tem proporcionado a possibilidade

de aumentar os chamados crimes comuns, bem como o surgimento de novas condutas criminais ainda não tipificadas no ordenamento jurídico de muitos países, de tal forma que se pode afirmar, sem sombra de dúvida, que os avanços da criminalidade do fórum informático podem crescer na proporção do avanço da tecnologia.

O facto da identificação do infractor ser uma incógnita, a responsabilização criminal e o acesso global das Tecnologias de Informação e de Comunicação, especialmente da Internet, tornou-se num mundo sem fronteiras, contribuem com que o número de prevaricadores dessa natureza de crimes aumenta, apesar dos grandes esforços conjuntos de vários países na prevenção e combate de tais condutas ilícitas.

No domínio do combate e prevenção, deve-se realçar a grande necessidade de se estabelecer acordos de cooperação judicial e policial, com o propósito de existir uma plataforma comum para investigar com maior celeridade os crimes desta natureza cometidos entre os Estados acordantes, visto que alguns crimes atravessam fronteiras de muitos países. A falta de colaboração e cooperação neste domínio incrementa, no seio dos autores dos crimes, o sentimento de impunidade, conferindo-lhe alguma tranquilidade.

A prática de infracções de natureza informática trouxe à criminalidade uma massa de pessoas que em outros meios talvez não fossem capazes de actuarem. A sensação de estar anónimo e impune faz com que muitas pessoas sirvam-se deste meio para obtenção de vantagens que podem não estar directamente ligados ao mesmo instinto para a prática de crimes no mundo físico.

Referências Bibliográficas

- Agustina, S. J. R. (2014). *Victimización en el ciberespacio. Consideraciones victimológicas y victimológicas en el uso de las TIC*. En: Cuadernos de Política Criminal Nº114, III, Época I, diciembre.
- Afonso, R. L. (2002). *Seguridad Informática. Conceptos Generales*. Disponible: campus.usal.es/derinfo/Activ/Jorn02/Pon2002/LARYALSL.p di. Fecha de consulta: 24 de mayo de 2017.
- Alvarez V., M. (2002). *Consideraciones político-criminales sobre la delincuencia informática. El papel del Derecho penal en la red*. Madrid: Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, En: Internet y Derecho penal.
- Basu, S. y Jones, R. (2007). *Regulating cyberstalking*. Rnalof Information, Law and Technology.
- Berson, I. R. (2012). *Grooming cyber victims: The psychosocial effects of online exploitation for youth*. Journal of School Violence.
- Beck, U. (1998). *La sociedad del riesgo*. Barcelona: Editora Paidós.
- Beck, U. (1998). *La sociedad del riesgo. Hacia una nueva modernidad*. Barcelona: Editora Paidós.
- Beebe, N. (2005). *Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security*. Las Vegas: En: Proceedings of the 2005 Software Conference, NV, December.
- Camacho, L. L. (2009). *El delito informático*. Madrid: Editora Aranza-di.

- Morant, V. J. (2013). *Protección penal de la intimidad frente a las nuevastecnologías, Tirant lo Blanch*, Valencia.
- Morillas, C. L. y C. B. M. J. (2009). *Informática y delito. Aspectos penales relacionados con las nuevas tecnologías*. Madrid: Dykinson, 1ª edición XXI, Ed. En: Benítez Ortúzar, I. F.: Reformas del Código Penal. Respuestas para una sociedad del Siglo.
- Lira, A. O. M. (2010). *Cibercriminalidad. Fundamentos de investigación México. Colección Criminalística*. México: Instituto de Ciencias Penales.
- López, O. J. J. (2004). "Intimidad informática y Derecho penal, Derecho a la intimidad y nuevas tecnologías". Madrid: En: Cuadernos de Derecho Judicial, Consejo General del Poder Judicial.
- López, B. Q. J. (2009) *La protección penal de los programas de ordenador*. En: Revista del poder judicial, Nº 88, Dialnet, 2009.
- Ortega, G. A. (2003) "La regulación de Internet". En: Revista de Derecho Informático Alfa-Redi. Núm. 061, Agosto del 2003. Disponible: <http://www.alfa-redi.org/enlinea.shtml>. Fecha de consulta 12 de septiembre de 2017.
- Orts, B. & Roig, T. M. (2008). *Delitos informáticos y delitos comunes cometidos através de la informática*. Valencia: Editora Tirant lo Blanch.
- Patchin, J. W. & Hinduja, S. B. (2006). *Mov ebeyond the schoolyard a preliminary look at cyberbullying*. Youth violence and juvenile justice.
- Reyna, A. L. M. (2016). *La víctima en el delito informático*.

- Disponible: www.alfonsozambano.com/doctrina_penal/reina_alfaro.pdf. Fecha de consulta: 25 de mayo.
- Romero, C. C. M. (1988). *Poder informático y seguridad jurídica*. Madrid: La función tutelar del Derecho penal ante las nuevas tecnologías de la información, Fundesco.
- Romero, C. C. M. (2006). *De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal*. Comares: Editora Granada En: El cibercrimen: nuevos retos jurídico- penales, nuevas respuestas político-criminales.
- Rovira, D. C. E. (2002). *Delincuencia Informática y fraudes informáticos*. Comares: Editora Granada.
- Smith, R. G. P. y Urbas, G. (2004). *Cybercriminal son trial*. Cambridge University Press, Cambridge.
- Turgeman-Goldschmit, O. (2008). *Meanings that Hackers Assign to their Being a Hacker*. En: International Journal of Cyber Criminology. Vol. 2, julio- diciembre, United States.
- Thomas, D. y Loader, B. (2000). *Introduction - Cybercrime: Law enforcement, security and surveillance in the information age*, Routledge, London.
- Ujarre, A. T. Johanna, et al. (2017). *La delincuencia informática. Revista: Caribeña de Ciencias Sociales*. ISSN: 2254-7630. Disponible: <http://www.eumed.net/rev/caribe/2015/10/delincuencia-informatica.html>. Fecha de consulta: 17 de Mayo.
- Will, D. (2007). *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge.