
CYBER
ACADEMY
FEBRABAN

Crimes Cibernéticos

Definição e Classificação

Nos moldes do que foi anteriormente comentado, decidimos utilizar o termo “crimes cibernéticos” para definir os delitos praticados por intermédio de dispositivos informáticos (computadores, notebooks, celulares etc.) conectados ou não à internet. Atualmente é comum a prática de crimes no ambiente de nuvem, sendo que, inclusive nesses casos, estamos diante de crimes cibernéticos considerando que são utilizados dispositivos informáticos para acessar esse ambiente. Além dessa questão, apenas para fins didáticos, apresentamos uma classificação para as denominadas “condutas indevidas praticadas por dispositivos informáticos”. Essas “condutas indevidas praticadas por computador e/ou dispositivos móveis” podem ser divididas em “crimes cibernéticos” e “ações prejudiciais atípicas”.

Tipos de Crimes Cibernéticos

A espécie “crimes cibernéticos” subdivide-se em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. As “ações prejudiciais atípicas” são aquelas condutas, praticadas por intermédio de dispositivos informáticos, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade. Por exemplo, o indivíduo que invade o computador de um conhecido sem o objetivo de obter, adulterar ou destruir dados ou informações não será indiciado nem preso, pois esses fatos não são criminosos, por não se adequarem ao art. 154-A do Código Penal (nova redação pela Lei nº 14.155/2021). Por outro lado, o causador do transtorno pode ser responsabilizado na esfera civil, como, por exemplo, ser condenado a pagar indenização em virtude dos danos morais/materiais produzidos. Conforme anteriormente mencionado, os “crimes cibernéticos” se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Com relação aos crimes cibernéticos “abertos”, são aqueles que podem ser praticados da forma tradicional ou por intermédio de dispositivos informáticos,

ou seja, o dispositivo é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. Dentre os tipos penais abarcados nesta modalidade estão, por exemplo, crimes contra a honra, ameaça, furto mediante fraude, estelionato, falsificação documental, falsa identidade, extorsão, tráfico de drogas etc.

Já os crimes "exclusivamente cibernéticos" são diferentes, pois eles somente podem ser praticados com a utilização de dispositivos informáticos. Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate-papo na Internet, previsto no art. 244-B, § 1º, do Estatuto da Criança e Adolescente (Lei nº 8.069/1990). Também são exemplos os crimes de interceptação telemática ilegal (art. 10 da Lei nº 9.296/1996), interceptação ambiental de sinais ilegal (art. 10-A da Lei nº 9.296/1996), invasão de dispositivo informático (art. 154-A do Código Penal), divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (art. 218-C do Código Penal), imagens de abuso infantil por meio do sistema de informática/telemática (arts. 241-A, 241-B e 241-C da Lei nº 8.069/1990), registro não autorizado da intimidade sexual (art. 216-B do Código Penal), a alteração do art. 122 do Código Penal, dobrando a pena quando a instigação ou indução ao suicídio ou automutilação ocorrem por meio da Internet (Lei nº 13.968/2019), a previsão do crime de stalking, do art. 147-A (Lei nº 14.132/2021), e as alterações/inclusões nos arts. 155, § 4º-B (furto mediante fraude por meio de dispositivo eletrônico ou informático) e 171, § 2º-A (fraude eletrônica), promovidas pela Lei nº 14.155/2021.

A lógica da criminalidade no ambiente virtual leva a intensificação dos delitos de caráter passional (como crimes contra a honra, ameaça, bullying etc.), das fraudes financeiras (estelionato, furto, extorsão e falsificação documental) e dos delitos de caráter sexual (registro e divulgação de cenas de sexo e/ou pornográfica, estupro etc.). As circunstâncias delitivas levam à necessidade de analisar caso a caso e buscar seu enquadramento à legislação penal vigente.

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN