CRIMINOLOGIA

- Cibercriminologia

  - *Cyberbullying*
  - *Sextorsão*
  - *Cyberstalking*
  - *Scamming*

Prof. Me. Guilherme Godoy

➢Cibercriminologia

Ciência que estuda a causa dos crimes que ocorrem no ciberespaço e seus impactos no mundo físico.
(Jaishankar apud Sydow, 2021)

Estuda o cibercrime, o comportamento do cibercriminoso, as cibervítimas, as ciberleis e a ciber investigação.

Ciência multidisciplinar que reúne pesquisas de vários campos do saber como criminologia clássica, a vitimologia, a sociologia da informação, a ciência da Internet, a ciência da computação, a estatística, a psicologia e a antropologia, entre outras.
(Sydow, 2021)

- Cibercriminologia

Cibercriminoso (segundo as estatísticas)

Alguém entre 10 e 60 anos, com conhecimentos de língua inglesa, afinidade com informática e alguma habilidade técnica. (Sydow, 2021)

➢Cibercriminologia

Cibervitimologia

Ramo da cibercriminologia que estuda

a forma de comportamento do usuário-vítima,
os ambientes que frequenta virtualmente,
as condutas causadoras de sua própria vitimização,
as estatísticas de vitimização,
a psicologia que leva à vitimização informática,
os modos de ludibriar e sugestionar a vítima,
os métodos de prevenção de tais situações
e até mesmo os gatilhos comportamentais,
entre outros ramos do conhecimento que podem ajudar a identificar a vítima e sua vitimização. (Sydow, 2021)

➢Cibercriminologia

Teoria dos Espaços Transitoriais

Karuppannan Jaishankar, 2008

Premissas:

-Pessoas reprimidas em suas vontades de cometer delitos no espaço físico tem propensão a cometer delitos no ciberespaço, especialmente porque não cometeriam os delitos na vida real pela posição que ocupam e pelo status que gozam;

-A flexibilização da identidade, a anonimidade dissociativa e a ausência de um fator de constrição no ciberespaço estimulam a escolha por delinquir;

➢Cibercriminologia

Premissas:

-Há uma tendência a se importar ao mundo virtual o delito do mundo real pelos ganhos de velocidade, facilidade e abrangência;

-A intermitência do ofensor no ciberespaço e a dinâmica da natureza espaço-temporal da virtualidade fazem com que haja sempre chance de escapar impune do delito;

➢Cibercriminologia

Premissas:

-Há uma dualidade agremiadora, associativa e recrutadora no ciberespaço: existe uma capacidade diferente do usual de reunião no ciberespaço, inclusive de agrupamento de totais estranhos, no intuito de cometerem um delito real. E há uma reunião de pessoas que se conhecem no mundo real que se reunem para delinquir no ciberespaço;

➢Cibercriminologia

Premissas:

-Pessoas introspectivas encontram estímulos no ciberespaço para extravasarem seus sentimentos e, por isso, sentem-se a vontade para agir;

-O conflito de normas internacionais ou a inexistência destas no ciberespaço facilita a ponderação pelo delito informático.

➢Direito Penal Informático

Apesar das denominações que já surgiram (Direito e Tecnologia, Direito Digital, Direito de Tecnologia da Informação, Direito Eletrônico, Ciberdireito, Direito da internet, Direito da Tecnologia, E-Direito, entre outros),

A ciência que estuda a área de tecnologia deve ser denominada de "Tecnologia da Informação (TI)", sendo o ramo de estudo que une as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.

Os estudos do Direito sobre esse contexto trata das mesmas situações, levando à denominação de "Direito Informático", com o sub-ramo "Direito Penal Informático". Na mesma esteira, a nomenclatura "Delitos Informáticos".

Tecnologia

Conjunto de processos, métodos, técnicas e ferramentas aplicados a um campo particular e que servem para utilizar os recursos ou de uma nova forma ou de uma forma mais eficaz.

Virtualidade

É um meio ambiente. A internet é uma das tantas ferramentas existentes nesse ambiente que servem para acessá-lo e modificá-lo.

Deepweb – parcela não indexada da internet

Darkweb – uma parte da deepweb que é utilizada especialmente para a delinquência.

Darknet – segmentos especializados dentro da deepweb que possuem característica de permitir a troca de conteúdo de qualquer natureza sem possibilidade de identificação dos usuários, com arquivos criptografados.

Superexposição (*Oversharing*)

Se cada vez mais estamos dispostos a expor nossas vidas nos sites de redes sociais e compartilhar todo tipo de momento e situação,

não podemos abandonar a cautela para pensar e escolher o que publicar, onde publicar e, principalmente, para quem publicar.

(Safernet)

Rastros Digitais

Além das informações que você publica voluntariamente,

há centenas de dados sobre você que ficam registrados a cada passo (ou clique) que dá online.

(Safernet)

safernet.org.br/

Cooperação:

PFDC Procuradoria Federal dos Direitos do Cidadão · MPF Ministério Público Federal · CNPG · unicef · Secretaria de Direitos Humanos · cgi.br · INHOPE · ins@fe

Parceiros em Projetos:

Google · facebook · vivo · nic.br

➢ *Cyberbullying*

Bullying – assédio
Mobbing – bullying no ambiente de trabalho (assédio moral)

To bully – ameaçar, intimidar

To mob – maltratar

"A brincadeira boba passa a ser *bullying* quando a vítima e o perpetrador deixam de concordar sobre quando a brincadeira deve parar, e passa a haver um desequilíbrio de poder entre eles" (Calhau, 2019).

➢ *Cyberbullying*

Legislação Federal

Lei 13.185/2015 – instituiu o programa de combate à intimidação sistêmica (*bullying*)

Lei 13.277/2016 – instituiu o 7 de abril como dia nacional de combate ao *bullying* e à violência na escola

Lei 13.663/2018 – alterou a Lei de Diretrizes e Bases da Educação para incluir a promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura de paz entre as incumbências dos estabelecimentos de ensino

➢ *Cyberbullying*

Cyberbullying (assédio virtual ou *bullying* virtual) – utilização de meio eletrônico como instrumento de agressão no *bullying* (Calhau, 2019).

➢ *Cyberbullying*

Tipos:

1- Assédio (ofensa repetida)
2- *flaming* (trocar mensagem *on-line* de conteúdo hostil e/ou agressivo)
3- difamação (ferir a honra)
4- despersonalização (agressor se faz passar pela vítima)
5- trapaças (busca-se atingiros relacionamentos sociais da vítima)
6- uso de informações pessoais (espalhar informações pessoais confidenciadas a amigos)
7- exclusão ou *cyberostracismo* (vítima bloqueada por contatos e impedida de enviar mensagens instantâneas ou *e-mails*)
8- exposição indevida (fotografias e/ou vídeos comprometedores de uma vítima são postados *on-line*)

(Débora Carpenter e Christopher J. Ferguson *apud* Calhau, 2019)

- Sextorsão informática

Sextorsão
Sexo + extorsão

Boletim da ONU (2002) – Medidas Especiais para Proteção contra Exploração Sexual e Abuso Sexual.

➢Sextorsão informática

Principais elementos facilitadores:

-Uso frequente de redes sociais e outros métodos de comunicação on-line, dispositivos particularmente móveis;
-Tendência a se envolver em comportamentos on-line arriscados, ou seja, fazer upload de dados pessoais, vídeo ao vivo, bate-papo na web e amizade com estranhos;
-Quantidade significativa de tempo gasto on-line todos os dias;
-Participação confortável em comunicações/interações sexuais on-line;
-Ingenuidade interpessoal (por exemplo, vulnerabilidade social, carência juvenil) ou técnica (segurança on-line);
-Ausência / mau controle dos pais.

(David Lester apud Sydow, 2021)

- Sextorsão informática

Tipos penais próximos:

-Assédio sexual (art. 216-A)
-Violência sexual mediante fraude (art. 215, CP)
-Estupro (art. 213, CP)
-Constrangimento ilegal (art. 146, CP)

➢ *Cyberstalking*

Não é adequado dizer que trata-se do *stalking* realizado por meio eletrônico (Sydow, 2021)

Pode ser chamado de "importunação insidiosa informática" (Sydow, 2021)

O delinquente dessa modalidade de delito possui maior periculosidade porque:

-Sua conduta não enfrenta limites geográficos
-Sua conduta não enfrenta limites temporais
-A conduta admite automatização gerando incômodo potencializado, ubíquo e constante
-A conduta admite que terceiros pratiquem a importunação auxiliando o agente
-O delinquente oculta-se em véus de anonimidade já apresentados tanto nos ecudos de falsas contas, como com falsos nomes
-A virtualidade permite que a conduta nessa modalidade vá se alastrando para os círculos de contato e convívio, prejudicando em cadeia usuários afins e pessoas de relacionamento. (Sydow, 2021)

➢ *Scamming* (Estelionato por meio virtual)

To scam – enganar alguém

Scammer – estelionatário que age no meio virtual, que se utiliza de armadilhas e golpes construídos especialmente para uso na virtualidade e com o intuito de obter vantagens patrimoniais.

A escolha é feita pelo potencial alastrador, pela grande multiplicação, pelo número de vítimas atingidas e pela velocidade de retorno. (Sydow, 2021)

➢*Scamming* (Estelionato por meio virtual)

Argumentos comuns para convencer o usuário a ser vitimizado:

- Fatos tristes
- Oportunidade única
- Fatos de utilidade pública
- Fatos geradores de curiosidade

(Sydow, 2021)

➢ *Scamming* (Estelionato por meio virtual)

Social engineering – popularmente traduzida como engenharia social, mas sendo um termo mais adequado "engenhosidade social".

Na ciência política, trata-se de técnica de criação de nova forma de pensamento ou comportamento a partir de uso de técnicas científicas de propaganda.

Em Segurança da Informação, o termo refere-se ao fato de os sistemas de informação serem operados por seres humanos, fazendo com que sejam falíveis.

Com isso, uma boa história com razoável verossimilhança e capacidade de convencimento faz com que a maior parte das falhas sejam geradas por seres humanos ludibriados e os golpes sejam aperfeiçoados. (Sydow, 2021)

Referências Bibliográficas

CALHAU, L. B. (2019). ***Bullying* – O que você precisa saber – Identificação, prevenção e repressão**. 5ª Ed. Belo Horizonte: Editora D'Plácido.

MPMG (2017). **Navegar com segurança: por uma internet mais segura, ética e responsável**. 4ª Ed. Disponível em <https://www.mpmg.mp.br/comunicacao/producao-editorial/cartilha-navegar-com-seguranca.htm#.YVOKCD9KiDI>. Acesso aos 28.set.2021.

SAFERNET BRASIL. Disponível em <safernet.org.br>. Acesso aos 28.set.2021.

SYDOW, S. T. (2021). **Curso de Direito Informático – Parte Geral e Especial**. 2ª Ed. Salvador: Editora Jus Podivm.