Tema 4

Módulo 1

**O que é o direito penal cibernético?**

É o conjunto das estruturas jurídicas inter-relacionadas. Seu objetivo deixa muito claro quais são as situações concretas em que a violência estatal está legitimada, principalmente devido à restrição da liberdade individual.

O direito penal não é concebido para gerar situações que punirão as pessoas, mas para limitar a ocorrência delas. Toda a sua estrutura de aplicabilidade deve ter essa diretriz, e com as tecnologias não seria diferente.

O direito penal cibernético pode ser compreendido como a leitura de todas as estruturas imersas no uso que a sociedade faz das tecnologias da informação, gerando a **sociedade da informação**.

**Princípios fundamentais**

A principal diferença entre o direito penal e o direito penal cibernético está no fato de que o segundo se aplica às tecnologias da informação.

A seguir, destacamos três princípios que possuem relevância para esse tema:

* Princípio da legalidade
* Princípio da anterioridade da lei penal
* Princípio da culpabilidade

**Princípio da legalidade**

É um dos postulados mais caros – senão, o mais caro – do direito penal brasileiro. Está consagrado na Constituição Federal de 1988 e no Código Penal (CP). Vejamos:

Linha do tempo

O conteúdo gerado por IA pode estar incorreto.

Somente é considerado crime aquilo que a lei diz que é – e tem que ser assim. No entanto, não se pode ignorar a dificuldade de aplicar a lei penal em contextos que envolvem as tecnologias da informação, uma vez que as TIs sempre – ou quase sempre – avançam em velocidade muito maior do que as alterações legislativas.

**Princípio da anterioridade da lei penal**

Parece representar a extensão da lógica e da eficácia do princípio da legalidade. No princípio da anterioridade da lei penal, não só o fato (inclusive os que usaram tecnologias da informação) precisa ser considerado legalmente crime, mas a definição como tal também tem de ser anterior ao ocorrido.

**Princípio da culpabilidade**

Determina que, para se caracterizar como crime, o agente deve possuir consciência atual e vontade de realizar os elementos contidos no tipo penal. Essa lógica estipula que o indivíduo atue, como regra, com dolo ou culpa nas situações em que a lei penal assim determina. Além disso, o princípio da culpabilidade estabelece a vedação da responsabilidade objetiva do agente, isto é, ninguém pode ser punido por um crime se não houver dolo ou culpa.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

**Classificação e nomenclatura**

A nosso ver, a classificação e a nomenclatura mais corretas para serem usadas no contexto do direito penal cibernético são infrações penais cibernéticas ou crimes cibernéticos. Na infração penal, também há a inclusão das contravenções penais.

É comum encontrarmos as expressões crimes informáticos, crimes eletrônicos ou crimes telemáticos. A posição adotada aqui reflete a ideia de que a ciência cibernética é mais abrangente do que as ciências informática e telemática.

Uma imagem contendo Texto

O conteúdo gerado por IA pode estar incorreto.

**Artefatos e técnicas**

Antes de comentarmos os principais crimes em espécie (ou crimes digitais), é importante apresentar as principais técnicas e os artefatos utilizados. Dessa forma, é possível ter uma visão técnica mais apurada do que acontece.

Vírus

Programa de computador vocacionado para alterar ou destruir dados, ou até sistemas – quando possui a capacidade de se espalhar pela rede (worm, por exemplo).

Trojan

Malware ocultado em outro programa, tornando o sistema vulnerável para danificá-lo, administrá-lo ou capturar sua base de dados.

Backdoor

Malware dedicado a burlar os mecanismos de autenticação.

Spyware

Software malicioso dedicado a monitorar o sistema, coletando informações e encaminhando ao destinatário.

Keylogging e screenlogging

Práticas que capturam teclas e telas e encaminham ao destinatário.

Defacement

Pichação e alteração de sites, colocando mensagens de protestos.

Ransomware

Sequestro de dados da empresa.

DDoS (Denial of Service)

Ataque para indisponibilizar algum serviço por sobrecarga.

DNS poisoning

Alteração de endereços de resolução DNS (domain name system) para direcionar o acesso a um site falso ou serviço criado.

Brute force

Técnica para quebrar senhas e sistemas por meio de tentativas a partir de todas as combinações possíveis.

SQL injection

Alteração dos parâmetros ou das instruções executadas sobre o banco de dados por meio da linguagem SQL (structured query language), permitindo o acesso indevido.

SIM Swap

O fraudador, com participação de colaborador da empresa de telefonia (engenharia social), ativa o número de telefone em outro chip (SIM card). Isso é possível a partir das informações pessoais obtidas, por exemplo, por phishing.

Engenharia social e código OTP (one-time-password) ou token

As vítimas são enganadas para fornecer o código de ativação.

**Principais crimes digitais em espécie**

Calúnia e difamação

São descritas nos artigos 138 e 139 do Código Penal.

Art. 138 – Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena – detenção, de seis meses a dois anos, e multa.

§ 1º – Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

§ 2º – É punível a calúnia contra os mortos.

Art. 139 – Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – detenção, de três meses a um ano, e multa.

Elas são consideradas crimes contra a **honra objetiva**, ou seja, o bem jurídico tutelado é a honra objetiva. Nesse sentido, há:

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Ameaça

É prevista no art. 147 do Código Penal:

Art. 147 – Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: §1º – Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

Trata-se de mais um crime cibernético impuro. Basta que alguém ameace outra pessoa de sofrer mal injusto – que não é legalmente devido – e grave, o qual provoque real temor. O crime está caracterizado se isso for feito com o uso de tecnologias (por exemplo, conversas em aplicativos de mensagens instantâneas ou por videoconferências).

Violação de segredo profissional

Trata-se de outro crime muito comum, principalmente em empresas. A violação de segredo profissional pode ser classificada como crime cibernético impuro e está prevista no art. 154 do CP:

Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa.

Quando alguém, que recebeu uma informação em razão do trabalho profissional que exerce, dá acesso a essa informação para pessoas que não poderiam ter, isso é crime e pode causar dano.

Invasão de dispositivo informático

É prevista no art. 154-A do Código Penal, e foi inserida pela [Lei Carolina Dieckmann](https://conteudo.ensineme.com.br/hu/01492/intro?brand=estacio) – Lei Federal nº 12.737/2012 – com redação alterada pela Lei nº 14.155/2021. Sobre o tema, o artigo estabelece que:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

Graças à Lei Carolina Dieckmann, configura-se crime: acessar dispositivo informático (computador, smartphone, tablet, rede de intranet etc.) sem autorização expressa ou tácita do titular do dispositivo (o que caracteriza invasão) – desde que isso tenha acontecido por meio da quebra de um mecanismo de segurança, como senhas e *firewalls* – e com o fim de obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidades para obter vantagem ilícita.

Crimes patrimoniais

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Divulgação de cena de estupro

É prevista no Código Penal:

Art. 218-C – Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática –, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena – reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Será crime, por exemplo, qualquer compartilhamento ou disponibilização, em qualquer plataforma – como sites, blog e aplicativos de mensagens, entre outros –, de fotografia ou vídeo que contenha cena de estupro ou de cena de sexo, nudez ou pornografia sem o consentimento da vítima. Desde 2018, nudes constituem crime se forem repassados sem autorização.

Estupro virtual

Sobre os crimes sexuais, vale mencionar a prática do estupro virtual. O crime de estupro é previsto no Código Penal:

Art. 213. Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso: Pena – reclusão, de 6 (seis) a 10 (dez) anos.

O crime está caracterizado se, de forma virtual e mediante ameaça, qualquer ato libidinoso que satisfaça o desejo do agente criminoso for praticado.

**Bullying e cyberbullying**

Bullying

É definido como intimidar de modo sistemático, individual ou em grupo uma ou mais pessoas, por meio de violência física ou psicológica e de modo intencional e repetitivo. Além disso, não há motivação evidente e é realizado por meio de atos de intimidação, humilhação ou discriminação ou ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais. A pena é de multa, se a conduta não constituir crime mais grave.

Cyberbullying

É classificado como intimidação sistemática por meio virtual. Se for realizado por meio da internet, rede social, aplicativos, jogos on-line ou se for transmitido em tempo real, a pena será de reclusão de dois a quatro anos, e multa, se a conduta não constituir crime mais grave.

Módulo 2

**Compliance: definição e origens**

O compliance surge a partir da evolução histórica do diálogo entre o Estado e o capital. Todavia, ele se estruturou como uma evolução pendular, como veremos a seguir.

**Liberdade versus crises do capitalismo**

No século XIX, a relação entre o Estado e o capital era de marcante liberdade, descentralização e autonomia. O Estado e o seu principal instrumento de estruturação – o direito – cumpriam os papéis que lhes foram atribuídos de assegurar a existência do mercado e de suas respectivas trocas e bens.

Contudo, ao final do século XIX e ao longo do século XX, verificamos as chamadas **crises do capitalismo**, quando houve o estremecimento de suas principais bases estruturantes. Entre elas, podemos citar, em especial:

**Surgimento do direito econômico e do direito penal econômico**

As normas de direcionamento e a natureza marcantemente programática não apresentaram resultados inteiramente satisfatórios. Nesse ponto, e com características de evolução, como a tentativa anterior não funcionou, o Estado adota normas de índole penal para corrigir os desvios dos direcionamentos constitucionalmente postos. Surge, então, o **direito penal econômico**, que também não trouxe os resultados esperados.

Paralelamente, houve a formatação de duas agendas internacionais que potencializaram a ideia do particular, auxiliando o Estado na tarefa de evitar ilegalidades. São elas:

* Combate à corrupção
* Manutenção da saúde de sistemas econômicos e financeiros

**Surgimento do compliance**

De maneira geral, o compliance é uma ferramenta estatal, de estágio avançado, para o intervencionismo econômico. Isso se dá pelo direcionamento da organização e do comportamento do capital, com o objetivo de evitar a destinação de recursos para fins contrários ao direcionamento econômico constitucional. Transfere-se, nesse ponto, a missão de conformidade para o particular, reconhecendo-o em lei pela desorganização, nesse sentido, e por não evitar a ilegalidade.

**Compliance digital**

Compliance digital pode ser compreendido como a tarefa de conformidade imersa em uma realidade permeada por tecnologias da informação, bem como pelas características da sociedade da informação e da quarta revolução industrial. Juntam-se a isso as respectivas normas jurídicas e os desafios e os benefícios que decorrem delas.

-Dados pessoais

O exemplo mais claro de compliance digital na atualidade é o uso de dados pessoais. Graças a eles, as organizações podem fazer uma série de mapeamentos e previsões. Ao mesmo tempo, elas precisam adotar altos padrões de privacidade para se manterem em plena conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

-Blockchain

Outro exemplo ilustra bem a bivalência curiosa que as tecnologias da informação provocam ao compliance, trazendo tanto instrumentos como desafios. Trata-se de blockchain, que explica, de modo prático, o compliance digital, além de ser uma tecnologia extremamente interessante.

Interface gráfica do usuário, Texto, Site

O conteúdo gerado por IA pode estar incorreto.

O blockchain apresenta duas perspectivas de funcionamento:

Vertical ou sequencial

Há uma cadeia de blocos de informação, e cada um contém tanto as sua informação como as de todos os anteriores.

Horizontal ou distributiva

Está em uma malha descentralizada de dispositivos, e cada um tem uma cópia fidedigna da cadeia de blocos.

**Provas digitais**

Blockchain é uma ferramenta poderosíssima na tarefa de conformidade. Um bom exemplo é a sua utilidade para a preservação de qualquer prova digital na rede.

Prova digital

Para preservar uma prova digital, basta confeccioná-la em um documento eletrônico – normalmente no formato .pdf – e inseri-la na rede descentralizada.

Código hash

A informação será validada por todos os dispositivos participantes, e o documento receberá um código hash, isto é, uma sequência alfanumérica.

Integridade e autenticidade

A informação possibilita atestar que o documento está preservado na rede, conferindo integridade e autenticidade à prova digital – dois dos três pilares de validade da prova, ao lado da preservação de sua cadeia de custódia.

Fato consubstanciado

A prova de como aquele conteúdo era no momento da preservação é obtido, provando o fato consubstanciado no documento. Isso é fundamental para qualquer medida jurídica relacionada à pessoa jurídica, como a preservação de fatos que respaldam a demissão por justa causa de alguns empregado.

**Registro de atividades**

O blockchain oferece transparência. A depender da configuração da rede – pública ou privada –, é possível registrar todas as atividades desenvolvidas pela pessoa jurídica e por seus integrantes, de forma perpétua e imutável. Com isso, qualquer pessoa – inclusive, os órgãos oficiais de *law enforcement* (cumprimento da lei) – poderá verificar toda a atividade feita de forma retroativa.

**Riscos**

Apesar de seu caráter instrumental importante, não se pode ignorar que o uso de tecnologia blockchain apresenta riscos à tarefa de conformidade jurídica. Afinal, a mesma ferramenta que permite a preservação probatória e a existência de uma trilha auditável transparente e confiável é aquela que viabiliza a existência dos criptoativos, como o bitcoin.

Estamos falando dos riscos jurídicos de ordem tributária ou mesmo criminal, como as discussões sobre os crimes de evasão de divisas e lavagem de dinheiro. Também podemos pensar nos riscos à proteção de dados que o uso dessa ferramenta pode trazer.

**Fundamentos do compliance**

O conceito de compliance e, especialmente, o de compliance digital estão emconstante evolução, dependendo da verificação contextual e relacional contemporânea. Atualmente, é possível identificar, ao menos, quatro ideias que fundamentam e dão respaldo ao desenvolvimento da tarefa de conformidade. São elas:

* Autorregulação regulada
* Governança corporativa
* Responsabilidade social
* Ética empresarial

**Autorregulação regulada**

A ideia de autorregulação regulada talvez seja a que mais concretize a noção de transferência do Estado para o particular, na tarefa de auxiliá-lo na **prevenção de ilegalidades** ou de práticas que não estão em conformidade com o ordenamento legal.

A organização vai se autorregular com os documentos pertinentes – o que configura a **autorregulação** – e dentro do que o Estado prevê como modelo mais aberto de regulamentação – o que caracteriza o aspecto **regulada**.

**Governança corporativa**

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

**Responsabilidade social**

Representa a ideia de que as organizações não são mais meros agentes executores de suas próprias atividades. Assim, elas se tornam agentes atuantes no desenvolvimento econômico, jurídico, social e coletivo.

**Ética empresarial**

Pode ser entendida como o comportamento da organização e dos agentes que ela representa, que é pautado pelos valores morais e éticos que a coletividade espera ou deseja.

Organização ética é aquela que tem atuação ajustada aos níveis éticos esperados pela sociedade em que está inserida. Desse modo, a ética empresarial se perfaz na conformidade não jurídica da organização e no ajuste aos sistemas de normas éticas e morais socialmente postos.

**Lei Anticorrupção e lavagem de dinheiro**

**Lei Anticorrupção**

A Lei nº 12.846, de 2013, conhecida também como Lei da Integridade Empresarial, Lei Anticorrupção ou Lei da Empresa Limpa, foi promulgada para suprir a lacuna que existia referente ao cumprimento das convenções da OEA, OCDE e ONU, que foram internalizadas pelo Brasil. Trata-se, portanto, de um dos grandes marcos legislativos do compliance no país.

**Objeto**

Em sua ementa, como era de se esperar, a Lei pontua seu objeto: “a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a Administração Pública, nacional ou estrangeira”.

**Responsabilização**

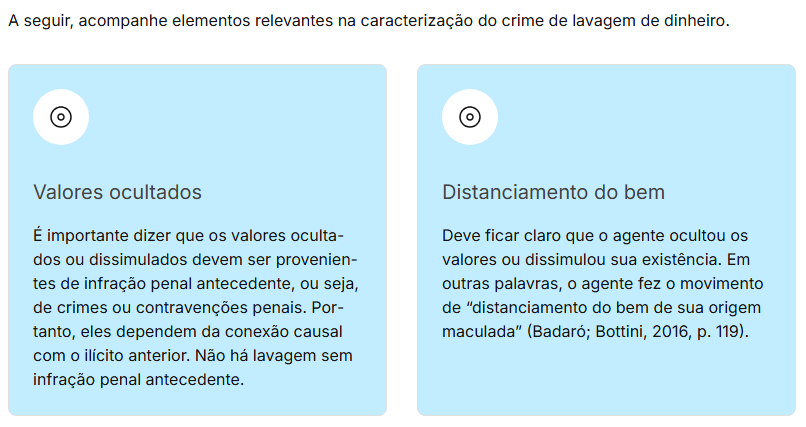
A Lei Anticorrupção estabelece a responsabilização objetiva das pessoas jurídicas por atos lesivos contra a administração pública, independentemente da comprovação de culpa. Basta a existência de um nexo causal entre a conduta da empresa e o dano causado. A responsabilidade é administrativa e civil, não penal. Além disso, a lei separa a responsabilização da empresa da de pessoas físicas envolvidas, afastando a necessidade de dupla imputação.

**Condutas e sanções**

A Lei nº 12.846/2013 define atos lesivos à administração pública, listados no art. 5º, incluindo não apenas condutas que causem prejuízo ou benefício ilícito, mas também tentativas e etapas para a concretização desses atos. O art. 6º prevê sanções administrativas, como multa de 0,1% a 20% do faturamento bruto ou valores entre R$6.000,00 e R$60.000.000,00, além da publicação da decisão condenatória. As penalidades podem ser cumulativas, e a empresa deve reparar o dano causado. O impacto financeiro e reputacional dessas sanções reforça a importância da conformidade para as empresas.

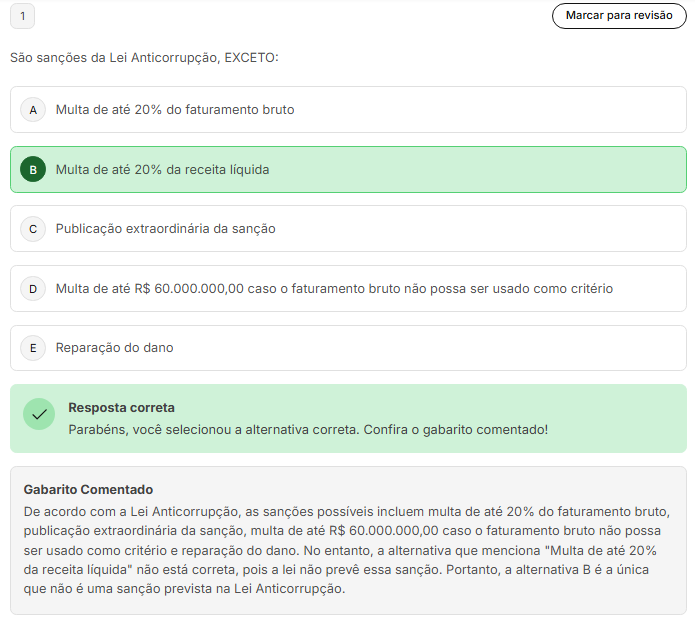
**Lavagem de dinheiro**

A lavagem de dinheiro é uma das principais preocupações das empresas em matéria de conformidade. Segundo Badaró e Bottini (2016), consiste em atos para ocultar a origem ilícita de bens, valores ou direitos, permitindo sua reinserção na economia formal com aparência de legalidade. O termo surgiu nos EUA, nos anos 1930, e foi usado juridicamente pela primeira vez em 1982. No Brasil, o crime está previsto no art. 1º da Lei nº 9.613/1998, punindo com reclusão de 3 a 10 anos e multa quem ocultar ou dissimular a origem de bens ilícitos, convertê-los em ativos legais ou usá-los na atividade econômica.



**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

****

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**

**Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.**