Direito Penal Cibernético

Você vai estudar conceitos fundamentais do direito contemporâneo, como direito penal cibernético, compliance, Lei Anticorrupção e lavagem de dinheiro.

Prof. Maurício Tamer

Propósito

Compreender o direito penal aplicado à realidade das tecnologias da informação – ou seja, o direito penal cibernético –, os ilícitos dessa realidade, as principais técnicas aplicadas, os crimes em espécie, o compliance e seus fundamentos, a Lei Anticorrupção e a lavagem de dinheiro é fundamental a estudantes e profissionais da área.

Preparação

Antes de iniciar o conteúdo, tenha em mãos o Código Penal e a Lei Anticorrupção.

Objetivos

- Identificar os principais fundamentos e princípios do direito penal cibernético.
- Descrever compliance, compliance digital, Lei Anticorrupção e crime de lavagem de dinheiro.

Introdução

Neste conteúdo, propomos um estudo sobre o direito penal cibernético com base nos principais fundamentos e princípios do direito penal. Para isso, analisaremos os artefatos implementados nessa dinâmica e as principais técnicas e estudaremos os crimes em espécie mais relevantes.

Analisaremos ainda o compliance, seu conceito e seus principais fundamentos – a saber: autorregulação regulada, governança corporativa, responsabilidade social e ética empresarial – e o que pode vem a ser compliance digital.

Por fim, nosso estudo avançará para a compreensão dos principais pontos da Lei Anticorrupção e do crime de lavagem de dinheiro.

O que é o direito penal cibernético?

Conheça, neste vídeo, a definição de direito penal cibernético, com destaque para os seus princípios mais relevantes: legalidade, anterioridade da lei penal e culpabilidade. Não perca!

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

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.

Compreender essa atribuição do direito penal é absolutamente necessário para que a aplicação de suas normas às tecnologias da informação seja feita da forma certa e com as devidas expectativas alinhadas. Afinal, não são poucas as vezes em que muitas condutas fazem surgir argumentos sobre impunidade.

Comentário

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. Nesse sentido, embora haja divergências, os mesmos princípios jurídicos associados ao direito penal – parte geral são aplicados ao direito penal cibernético. Assim, parece razoável dizer que o direito penal cibernético não possui autonomia científica para se distanciar daquilo que é conhecido como direito penal.

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

- Princípio da legalidade
- Princípio da anterioridade da lei penal
- Princípio da culpabilidade

Vejamos, a seguir, mais detalhes sobre um deles.

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:

Constituição Federal de 1988		Código Penal
“Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (Art. 5º).	⊗	“Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” (Art. 1º).

Na essência, a lei é a fonte imediata do direito penal. Na prática, isso significa que não existe a caracterização de crime sem que o ato ou a omissão esteja previsto em lei – isto é, o texto oriundo de um processo legislativo regular.

Claus Roxin (1997) observa que:

> Um Estado de Direito deve proteger o indivíduo não apenas por meio do Direito Penal, mas também deve protegê-lo do Direito Penal. Em outras palavras, o sistema jurídico não deve apenas ter métodos e meios adequados para a prevenção do crime, mas também impor limites ao uso do poder punitivo, para que o cidadão não fique desprotegido e à mercê de intervenções arbitrárias ou excessivas [...] Diante disso, o princípio da legalidade, [...] serve para evitar uma pena arbitrária e não calculável, sem lei ou baseada em uma lei imprecisa ou retroativa.
>
> —
>
> (Roxin, 1997, p. 137)

Aníbal Bruno (2003) também afirma:

> O Direito Penal distingue-se, no quadro do Direito Positivo, pela importância dos bens jurídicos que tutela e pela gravidade da sua sanção. Tem por isso de revestir-se, mas que qualquer outro, de condições de certeza e precisão, que a lei em particular é que lhe pode assegurar. A fonte imediata do Direito Penal é a lei, a sua fonte formal, em que se fundamenta o seu sistema, que é, assim, muito mais rígido e fechado do que o dos outros ramos do Direito.
>
> —
>
> (Bruno, 2003, p. 121)

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.

Assim, um dos maiores dilemas do direito penal cibernético está vinculado ao alcance das interpretações da lei em relação às tecnologias. Veja os exemplos a seguir.

A subtração de dados caracteriza crime de furto?

Os dados seriam coisa alheia móvel, nos termos do art. 155, CP?

A destruição de arquivos pode caracterizar crime de dano?

O estupro virtual existe e é possível de ocorrer?

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.

Exemplo

Em relação às tecnologias, podemos considerar à criação do crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, por meio do art. 218-C, incluído no Código Penal por meio Lei nº 13.718/2018. Todas as condutas anteriores à publicação da Lei, que ocorreu em 25 de setembro de 2018, ainda que descritas no art. 218-C do Código Penal, não caracterizam crime.

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.

Tais ideias trazem consequências relevantes para as tecnologias da informação. Observe.

Crimes dolosos

A maioria dos crimes que envolvem as tecnologias da informação são de natureza dolosa. Desse modo, é necessário demonstrar esse elemento em todas as situações concretas.

Culpabilidade

A culpabilidade e a vedação da responsabilidade objetiva fazem os passos probatórios ganharem muita relevância. Por exemplo, não basta identificar a conexão de internet de onde partiram os atos de uma fraude. A perícia oficial dos equipamentos utilizados também é necessária.

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. Acompanhe.

1
Informática
Estuda e desenvolve os mecanismos dedicados ao armazenamento, à transmissão e ao processamento da informação de forma eletrônica e automatizada.

2
Telemática
Constitui o estudo mais específico da transmissão da informação por meio eletrônico, trabalhando paralelamente à informática.

3
Cibernética
Seria a ciência que engloba a informática e a telemática (em linhas gerais).

Parece mais adequado falar em **crimes cibernéticos**, uma vez que as condutas costumam englobar tanto os dispositivos eletrônicos como os meios de conectividade entre eles.

Há, ainda, outra classificação importante:

Crimes cibernéticos puros ou próprios

Têm como bem jurídico tutelado – aquilo que a norma penal busca proteger com a legitimação da violência estatal – os próprios mecanismos informáticos ou cibernéticos. Como exemplo, temos o crime de invasão de dispositivo informático, previsto no art. 154-A do CP.

Crimes cibernéticos impuros ou impróprios

Têm outros bens jurídicos tutelados. Nesse caso, as tecnologias da informação representam um novo modus operandi ou uma nova forma de praticar a conduta. São exemplos o crime de estupro virtual (art. 213, CP), o crime de ameaça (art. 147, CP) e o estelionato (art. 171, CP).

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.

1
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).

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

3 Backdoor
Malware dedicado a burlar os mecanismos de autenticação.

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

5 Keylogging e screenlogging
Práticas que capturam teclas e telas e encaminham ao destinatário.

6 Defacement
Pichação e alteração de sites, colocando mensagens de protestos.

7 Ransomware
Sequestro de dados da empresa.

8 DDoS (Denial of Service)
Ataque para indisponibilizar algum serviço por sobrecarga.

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

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

11 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.

12 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.

13 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

Assista ao vídeo e conheça os principais crimes digitais, suas características mais relevantes e seu modo de funcionamento.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Feitas as considerações sobre o direito penal cibernético e as principais técnicas utilizadas na prática, passaremos a relacionar os principais crimes digitais – ou seja, as condutas mais comuns na prática – às possíveis penas.

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:

Calúnia

Se alguém é acusado de uma prática criminosa.

Difamação

Se há a acusação de fato desabonador, mas que não constitui crime.

Tanto a calúnia como a difamação podem ser cometidas pelos meios digitais, como postagens em mídias sociais, criação de sites falsos ou alteração de conteúdos de sites verdadeiros – ou *defacement*. Para isso, basta que se ataque a honra objetiva da vítima, o que possibilita que elas sejam classificadas como crimes cibernéticos impuros ou impróprios.

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).

O Superior Tribunal de Justiça admite a existência desse tipo de crime, como pode ser visto no exemplo a seguir:

> “Ameaças de ex-namorado a mulher via Facebook. [...] Ameaças realizadas em sítio virtual de fácil acesso. Suposto autor das ameaças residente nos Estados Unidos da América. Crime à distância. Facebook. Sítio virtual de fácil acesso. [...]
>
> —
>
> (STF, CC 150.712-SP, Rel. Min. Joel Ilan Paciornik, por unanimidade, julgado em 10/10/2018, DJe 19/10/2018)

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.

Exemplo

O empregado que encaminha documentos por e-mail ou outros meios para terceiros, como a concorrência.

Invasão de dispositivo informático

É prevista no art. 154-A do Código Penal, e foi inserida pela **Lei Carolina Dieckmann** – Lei Federal nº 12.737/2012 – com redação alterada pela Lei nº 14.155/2021. Sobre o tema, o artigo estabelece que:

Lei Carolina Dieckmann

Trata-se de um marco na legislação brasileira contra crimes cibernéticos. Ela foi promulgada em 2012, após a invasão do computador de Carolina Dieckmann, em 2011, o que resultou no vazamento de fotos íntimas da atriz. A pena varia de reclusão de um a seis anos e multa de R$ 5.000,00 a R$ 15.000,00. Contudo, a pena pode ser aumentada de 1/3 a 2/3 se o crime for cometido com violência ou grave ameaça à pessoa ou se a vítima for menor de 14 anos.

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.

Observa-se que o bem jurídico tutelado principal é a própria **higidez** dos dispositivos cibernéticos, e, por isso, é ela caracterizada como exemplo de crime cibernético puro ou próprio por excelência. Essa situação ocorre muito em incidente de segurança da informação, quando um agente externo, ao violar uma camada externa, acessa a base de dados da empresa.

Homem tentando acessar o notebook com login e senha.

Crimes patrimoniais

São muito comuns na realidade cibernética e são caracterizados, normalmente, pelas chamadas **fraudes**, que tanto podem ser:

Furto mediante fraude

Segundo o Código Penal, o furto cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento similar, será qualificado, com a previsão de pena de reclusão de quatro a oito anos e multa.

Se o crime for praticado contra idoso ou vulnerável, a pena pode aumentar de um terço até o dobro. E, se for praticado com o uso de servidor de informática mantido fora do país, a pena pode aumentar de um a dois terços.

Estelionato

De acordo com o art. 171, §§ 2º-A, 2º-B e 3º, do CP, a pena do estelionato será reclusão de quatro a oito anos e multa, quando a vítima for enganada e fornecer informações por meio de redes sociais. Anteriormente, o estelionatário (isto é, o indivíduo que engana alguém e causa-lhe prejuízo para obter vantagem ilícita) podia ser punido com reclusão de um a cinco anos e multa.

Assim como no furto qualificado, a pena para estelionato via meio eletrônico é aumentada se for utilizado servidor fora do território nacional ou se o crime for praticado contra idoso ou vulnerável. Quando o estelionato for praticado por meio de depósito, emissão de cheques sem fundos transferência de valores, a competência será definida pelo local de domicílio da vítima.

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.

Exemplo

O agente que, depois de ter conversas consensuais com uma vítima casada, ameaça contar ao cônjuge a situação, a menos que a vítima grave vídeos de nudez.

Bullying e cyberbullying

Acompanhe, neste vídeo, o que é o bullying e o cyberbullying, suas principais características e como funciona a responsabilização penal de ambos.

Conteúdo interativo

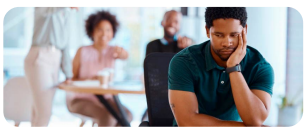
Acesse a versão digital para assistir ao vídeo.

A Lei nº 14.811, de 2024, promoveu alterações significativas no Código Penal, na Lei dos Crimes Hediondos e no Estatuto da Criança e do Adolescente (ECA), criminalizando, por exemplo, as práticas de bullying e cyberbullying.

A norma inclui a tipificação das duas práticas no Código Penal. Vejamos.

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.

A Lei nº 13.185, de 2015, que instituiu o Programa de Combate à Intimidação Sistemática, já previa o bullying, mas não estabeleceu punição específica para esse tipo de conduta. Assim, ela apenas obrigava escolas, clubes e agremiações recreativas a assegurarem medidas de conscientização, diagnóstico, prevenção e combate à violência e à intimidação sistemática.

Verificando o aprendizado

Questão 1

Sobre a função do direito penal e de seus princípios, assinale a alternativa correta.

A

O direito penal, sobretudo se aplicado às tecnologias da informação, representa a estruturação normativa vocacionada à punibilidade dos agentes.

B

Quanto às tecnologias da informação, a anterioridade da lei penal possibilita interpretar que a conduta só é considerada crime se a tecnologia envolvida for desenvolvida antes da existência de lei penal.

C

O princípio da legalidade exige a consciência e a vontade do agente direcionadas à conduta criminosa.

D

O princípio da culpabilidade exige a consciência e a vontade do agente direcionadas à conduta criminosa.

E

O princípio da culpabilidade exige a existência de lei prévia definindo o fato como crime.

A alternativa D está correta.

O princípio da culpabilidade, além de vedar a responsabilidade objetiva do agente, exige que ele tenha vontade de atuar de forma ilícita e consciência da ilegalidade.

Questão 2

A respeito dos principais crimes em espécie, é plenamente correto dizer que:

A

O estelionato ocorre se o poder de vigilância da vítima é afastado pela conduta do agente, e ele subtrai a coisa.

B

O conhecido golpe do WhatsApp, quando alguém se passa pelo dono do número para conseguir dinheiro de parentes e amigos, é um exemplo de estelionato.

C

O conhecido golpe do WhatsApp, quando alguém se passa pelo dono do número para conseguir dinheiro de parentes e amigos, é um exemplo de furto mediante fraude.

D

O crime de difamação na internet ocorre com a acusação da vítima sobre a prática do crime.

E

O crime de estupro, por sua natureza, exige a presença física do agente e da vítima no mesmo ambiente.

A alternativa B está correta.

No golpe do WhatsApp, após assumir o controle da conta da vítima, o agente passa a enganar seus contatos, exigindo o pagamento de valores, o que caracteriza o crime de estelionato.

Compliance: definição e origens

Confira, neste vídeo, a análise da evolução histórica de compliance, até o surgimento do compliance digital. Não perca!

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

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:

1914 - 1918

Primeira Guerra Mundial
Tropas alemãs em uma trincheira durante a Ofensiva de Aisne, 1918.

1929

Crise da Bolsa de Nova York
Multidão em frente a um banco no início da Grande Depressão, 1929.

1939 - 1945

Segunda Guerra Mundial
Prisioneiros no campo de concentração de Buchenwald, 1938 - 1941.

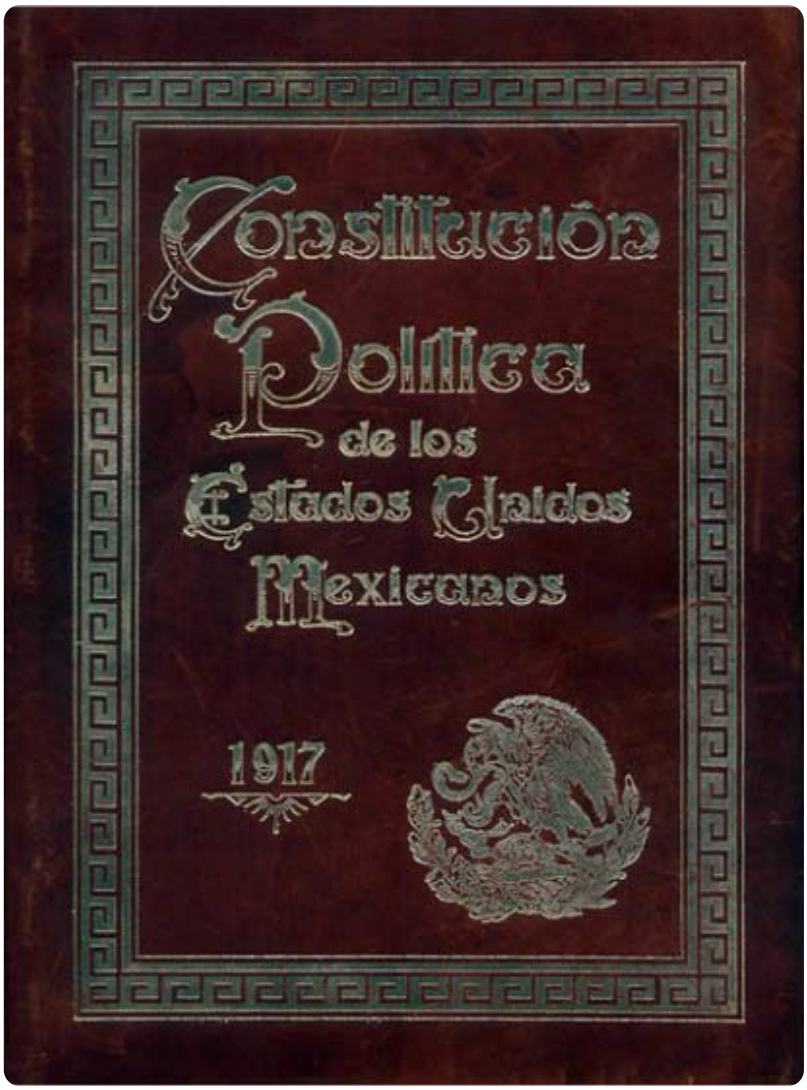
O Estado, nesse período, entende que sua posição de isolamento (ou de não intervenção) não era mais funcional. Ele propõe uma mudança de postura, que implicava o início da participação ativa do Estado na economia.

Quando falamos em participação ativa, identificamos a mudança do papel do Estado na economia com atuação clara no direcionamento econômico. Para tanto, mais uma vez, o Estado se vale de sua técnica mais especializada: **o direito**.

Surgimento do direito econômico e do direito penal econômico

As mudanças ocorridas no mundo todo no final do século XIX e na primeira metade do século XX marcam a fase de surgimento e evolução do **direito econômico**, especialmente quando as diretrizes são traçadas no próprio seio constitucional.

Capa da constituição de Weimar, de 1919.



Capa original da Constituição Mexicana, de 1917.

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

Considerando que tanto o direito econômico como o direito penal econômico não foram totalmente efetivos, o Estado passou a buscar outra opção capaz de assegurar o melhor direcionamento econômico e a diminuição da prática de ilícitos.

Comentário

No Brasil, a Lei nº 12.846/2013 – conhecida como Lei da Integridade Empresarial, Lei Anticorrupção ou Lei da Empresa Limpa – se destaca como grande marco legislativo.

Surgimento do compliance

Palavra de origem inglesa, que significa cumprir, obedecer, satisfazer ou atender a uma imposição, compliance representa um passo na relação entre Estado e capital – marcada, agora, por uma nova forma de controle, que conta diretamente com a participação do particular. Para tanto, o Estado, mais uma vez por meio do direito, passa a prever sanções para os particulares, especialmente para as pessoas jurídicas que não se organizam para evitar ilegalidades.

> 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.

As práticas de compliance são destinadas a garantir que o particular esteja em conformidade com as normas que regem sua atividade. Portanto, essas práticas têm por vocação criar e manter um ambiente de ajuste normativo pleno.

Compliance digital

Assista ao vídeo e entenda o que é compliance digital e blockchain, passando pelas provas digitais e pelos registros de atividades.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Para entender o que é compliance digital, é preciso compreender o que significa o termo **digital** e, em seguida, agregá-lo a compliance. Assim, poderemos avançar e fazer novos questionamentos, como:

O que há de diferente entre o compliance não digital e o digital? Em que medida o termo digital altera a conformidade exercida pelo particular?

A resposta para as duas perguntas parece ser algo que temos estudado e que se apresenta como a grande diferença entre os tipos de compliance: as **tecnologias da informação**. São elas que, inclusive, justificam a denominação compliance digital. Desse modo, entender o que esse termo significa é compreender as mudanças que essas tecnologias provocam no exercício da tarefa de conformidade jurídica pelas empresas.

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.

Os meios digitais, nesse contexto, ora são instrumentos da tarefa de conformidade ora são objetos específicos de preocupação e busca de ajuste ao sistema normativo. Veja alguns exemplos a seguir:

Círculo contendo símbolos de regulação, conformidade e leis.

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.

Blockchain

Pode ser compreendido como uma rede descentralizada de terminais eletrônicos – na maioria, computadores –, distribuída pelo mundo e interligada pela internet. É uma rede *peer-to-peer*, em que cada usuário disponibiliza seu dispositivo, de forma voluntária, em prol da malha descentralizada de dispositivos. Cada dispositivo representa a imagem de um nó ou de um ponto de intersecção da rede.

Acompanhe mais detalhes a seguir!

Armazenamento eletrônico tradicional

Os dados são salvos e armazenados em dispositivos ou servidores centralizados. Os serviços de nuvem (ou *cloud*) também funcionam dessa maneira.

Rede peer-to-peer

As informações armazenadas ou transmitidas (dados) não estão concentradas em um único dispositivo ou servidor, mas dispostas de forma compartilhada por todos e em todos os dispositivos.

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.

A seguir, confira alguns exemplos de como utilizar a ferramenta na atualidade.

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. A seguir, veja um passo a passo para a execução deste exemplo.

1

Prova digital

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

2

Código hash

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

3

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.

4

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.

Desse modo, é possível demonstrar a implementação prática dos programas de compliance e afastar a responsabilização de personagens empresariais em diversas situações concretas.

Exemplo

Imagine-se na prática de algum crime relacionado à atividade empresarial que você exerce. O histórico de atividades registrado na rede blockchain pode ser fundamental para afastar a responsabilização penal por omissão dos dirigentes envolvidos, se as medidas adotadas estiverem disponíveis. Nessa perspectiva, o blockchain é uma importante ferramenta na prestação de contas.

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.

Moedas 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

Confira, neste vídeo, os fundamentos do compliance e compreenda as ideias que os respaldam.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

O conceito de compliance e, especialmente, o de compliance digital estão em constante 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

Vamos conhecer melhor cada um desses fundamentos!

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**.

Comentário

Na lógica das tecnologias da informação, é necessário mencionar a LGPD, que traz ideias mais abertas de regulação, uma vez que ela não é capaz de detalhadamente regular todas as possibilidades de tratamento de dados pessoais. Cabe à empresa se autorregular para implementar os conceitos na prática e por meio de documentos internos, como: códigos de conduta, política de privacidade e política de segurança da informação, entre outros.

Governança corporativa

Pode se apresentar como um sistema coordenado de ideias. Nesse sistema, por meio de mecanismos e princípios, a governança estrutura e orienta a gestão e as atividades das organizações. No Brasil, destacam-se:

- Código brasileiro de governança corporativa – Companhias abertas.
- Instrução nº 480, de 2009, da Comissão de Valores Mobiliários (CVM).
- Código de melhores práticas de governança corporativa, do Instituto Brasileiro de Governança Corporativa (IBGC), de 2015.
- Governança Cooperativa (2008), do Banco Central, que aborda os mecanismos de governança nas cooperativas de crédito.

Não há uma fórmula ou um modelo estanque de governança. O que existe é a ideia de que o aperfeiçoamento da estrutura e da gestão estarão alinhados ao próprio modelo de negócio e à atividade desenvolvida.

Isso parece possível de ser conferido a partir da lógica da governança como sistema. Se a governança diz respeito à melhor estrutura e gestão, o aprimoramento desses dois pilares passa pela compreensão de como eles se apresentam na atividade desenvolvida.

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.

Trata-se da ideia das organizações socialmente participativas, isto é, empresas preocupadas com o desenvolvimento coletivo e que demonstram, concretamente, essa preocupação.

Empresário apresentando à equipe de trabalho o projeto que envolve proteção ao meio ambiente.

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

Veja, neste vídeo, aspectos importantes da Lei Anticorrupção e do crime de lavagem de dinheiro, que são relevantes em um ambiente de conformidade empresarial. Não perca!

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

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".

Seu artigo 1º vai além, pois dispõe que a responsabilização será objetiva e que se aplicará a toda formatação empresarial de pessoa jurídica.

Responsabilização

O artigo 2º da Lei Anticorrupção reafirma a natureza objetiva da responsabilização, sinalizando que ela será caracterizada se a prática de atos lesivos contra a administração pública for verificada e se eles forem em benefício da pessoa jurídica, exclusivamente ou não.

Desse modo, basta que o nexo causal entre a postura – comissiva ou omissiva – da pessoa jurídica e o ato lesivo à administração pública estejam presentes, independentemente de qualquer verificação de culpa da pessoa jurídica.

A opção do legislador foi evitar que as dificuldades da comprovação da culpa da pessoa jurídica e suas diversas possibilidades de entendimento dogmático e prático relativizassem a força sancionatória da lei. Embora existam entendimentos diferentes, a Lei Anticorrupção é clara ao estabelecer que a responsabilização é **administrativa** e **civil**, e não penal.

Ainda no âmbito da responsabilização, é interessante indicar que a Lei Anticorrupção põe a salvo e separa a responsabilidade das pessoas naturais ou físicas que tenham participação comissiva ou omissiva nos atos ilícitos, o que será apurado na compreensão correta das respectivas culpabilidades.

Nesse ponto e no âmbito da própria responsabilidade administrativa e civil, a necessidade da **dupla imputação** ou da **heterorresponsabilidade** se afasta. Isso significa que a pessoa jurídica é responsável, independentemente da responsabilização concreta das pessoas naturais envolvidas.

Juiza batendo o martelo.

Condutas e sanções

Na sequência, a Lei nº 12.846/2013 relaciona as condutas que, se realizadas, fazem surgir o direito subjetivo do Estado de aplicar as sanções administrativas – os chamados **atos lesivos à administração pública**. Eles são elencados no art. 5º dessa lei e, mais uma vez, indicam a propensão do texto legal para facilitar a comprovação da postura da pessoa jurídica, na tentativa de evitar percalços concretos e apurar a efetiva responsabilidade.

É por isso que não são previstas apenas posturas que têm verbos típicos que indicam a existência de um efetivo prejuízo à administração ou a obtenção do benefício ilícito. Também são previstas posturas que perfazem a tentativa de que isso ocorra ou que, de alguma forma, representam um dos passos para o ato lesivo.

O artigo 6º prevê as sanções administrativas cabíveis. Confira!

- Multa, no valor de 0,1% a 20% do faturamento bruto do último exercício anterior ao da instauração do processo administrativo em que a infração é apurada, e em valor nunca inferior à vantagem auferida, quando essa puder ser estimada.
- Publicação extraordinária da decisão administrativa condenatória.

As sanções podem ser aplicadas isoladamente ou de forma cumulativa. Além disso, a pessoa jurídica fica responsável por reparar o dano causado. No caso da multa, caso o faturamento bruto não possa ser usado como critério, a multa respeitará o valor mínimo de R$6.000,00 e o valor máximo de R$60.000.000,00.

Atenção

Do ponto de vista financeiro e, sobretudo, para a reputação da pessoa jurídica, as sanções são muito significativas e importantes. Isso justifica a preocupação sensível das empresas no Brasil com a tarefa de conformidade após a promulgação da lei.

Lavagem de dinheiro

Para as empresas, em matéria de conformidade, a prática e o crime de lavagem de dinheiro são uma das preocupações mais consistentes.

Segundo Badaró e Bottini (2016), a ideia de lavagem de dinheiro é do ato ou da sequência de atos “praticados para mascarar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores e direitos de origem delitiva ou contravencional, com o escopo último de reinseri-los na economia formal com aparência de licitude.” (p. 29).

A ideia principal é a de que há valores oriundos de infrações penais, e eles precisam ser aproveitados na economia formal. Assim, atos de lavagem de dinheiro são adotados para que a origem delitiva dos valores não seja percebida, e eles possam ser aproveitados como se fossem lícitos.

A expressão lavagem de dinheiro foi inicialmente empregada, segundo Badaró e Bottini (2016):

> [...] pelas autoridades norte-americanas para descrever um dos métodos usados pela máfia nos anos 30 do século XX para justificar a origem de recursos ilícitos: a exploração de máquinas de lavar roupas automáticas. A expressão foi usada pela primeira vez em um processo judicial nos EUA em 1982, e a partir de então ingressou na literatura jurídica e em textos normativos nacionais e internacionais.
>
> —
>
> (Badaró; Bottini, p. 29)

No Brasil, o crime é previsto no art. 1º da Lei nº 9.613/1998. Confira:

> Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. Pena: reclusão, de 3 (três) a 10 (dez) anos, e multa.
>
> § 1º Incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:
>
> I – os converte em ativos lícitos;
>
> II – os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimenta ou transfere;
>
> III – importa ou exporta bens com valores não correspondentes aos verdadeiros.
>
> § 2º Incorre, ainda, na mesma pena quem:
>
> I – utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal;
>
> II – participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos nesta Lei.

A seguir, acompanhe elementos relevantes na caracterização do crime de lavagem de dinheiro.

Valores ocultados

É importante dizer que os valores ocultados ou dissimulados devem ser provenientes de infração penal antecedente, ou seja, de crimes ou contravenções penais. Portanto, eles dependem da conexão causal com o ilícito anterior. Não há lavagem sem infração penal antecedente.

Distanciamento do bem

Deve ficar claro que o agente ocultou os valores ou dissimulou sua existência. Em outras palavras, o agente fez o movimento de "distanciamento do bem de sua origem maculada" (Badaró; Bottini, 2016, p. 119).

Verificando o aprendizado

Questão 1

Um dos principais fundamentos contemporâneos do compliance é o conceito de autorregulação regulada. Desse modo, podemos afirmar que a autorregulação regulada:

A

é sinônimo de compliance, traduzindo-se na própria tarefa de conformidade em si considerada.

B

é responsável por caracterizar o posicionamento das organizações como agente de transformação social.

C

volta-se à reunião de ideias consistentes para a melhor gestão da empresa.

D

caracteriza-se pela ideia de complementação dos modelos regulatórios estatais, por meio da qual a organização se autorregula internamente a partir do quadro normativo da empresa.

E

é sinônimo de ética empresarial, a fim de ajustar a organização aos padrões éticos da sociedade.

A alternativa D está correta.

A autorregulação se caracteriza pela possibilidade de a organização se regular internamente, dentro do espaço de regulação legal determinado pelo Estado.

Questão 2

Sobre a Lei Anticorrupção, é incorreto afirmar que ela dispõe sobre:

A

a responsabilidade da empresa, independentemente da responsabilidade das pessoas naturais envolvidas.

B

a responsabilidade penal da pessoa jurídica.

C

a responsabilidade civil da pessoa jurídica.

D

a responsabilidade por atos lesivos à administração pública.

E

a responsabilidade administrativa da pessoa jurídica.

A alternativa B está correta.

Embora haja entendimentos divergentes e, em alguns momentos, as estruturas sejam similares, a Lei Anticorrupção não traz a responsabilidade penal da pessoa jurídica. Isso, inclusive, seria inconstitucional.

Considerações finais

Vimos os principais fundamentos do direito penal cibernético, compreendendo-o em uma estrutura própria do direito penal. Sua função é limitar o poder de punir do Estado e legitimar o eventual uso de violência. Também estudamos os princípios da legalidade, da anterioridade da lei penal e da culpabilidade.

Apresentamos as nomenclaturas relacionadas e as técnicas e os artefatos mais utilizados na prática dos crimes virtuais. Além disso, analisamos os principais crimes em espécie associados ao uso das tecnologias da informação.

Trabalhamos os conceitos de compliance e compliance digital, conhecemos seus principais fundamentos e a Lei Anticorrupção. Por fim, fizemos algumas considerações sobre o crime de lavagem de dinheiro.

Podcast

Com a palavra, o professor Maurício Tamer, comentando o direito penal cibernético. Aproveite!

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Busque um simulador de Blockchain na internet e veja como ele funciona na prática. Vale a pena conferir!

Veja a entrevista de Pierpaolo Bottini, intitulada **Direito e globalização – lavagem de dinheiro**, disponível na internet.

Leia a Instrução nº 480, de 2009, da Comissão de Valores Mobiliários (CVM).

Leia o documento do Banco Central disponível no site da instituição: **Governança cooperativa**, que aborda os mecanismos de governança nas cooperativas de crédito.

Referências

ALBUQUERQUE, R. C. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

ANDRADE, A.; ROSSETTI, J. P. **Governança corporativa**: fundamentos, desenvolvimento e tendências, São Paulo: Atlas, 2004.

BADARÓ, G. H. **Lavagem de dinheiro**: aspectos penais e processuais penais. 3. ed. São Paulo: Revista dos Tribunais, 2016.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Consultado na internet em: 20 fev. 2021.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Presidência da República, 2013. Consultado na internet em: 20 fev. 2021.

BRASIL. Superior Tribunal Federal. STF. Conflito de competência nº 150.712 - SP (2017/0014052-4) Relator: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 10/10/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 19/10/2018. **Revista Eletrônica de Jurisprudência**, São Paulo, 2017. Consultado na internet em: 20 fev. 2021.

BRUNO, A. **Direito penal**. 5. ed. rev. e atual. Rio de Janeiro: Forense, 2003.

CRESPO, M. X. F. **Crimes digitais**. São Paulo: Saraiva, 2011.

FLORÊNCIO FILHO, M. A. **Culpabilidade**: crítica à presunção absoluta do conhecimento da lei penal. São Paulo: Saraiva, 2017.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. IBGC. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. Consultado na internet em: 20 fev. 2021.

JESUS, D.; MILAGRE, J. A. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MASCARO, A. **Introdução ao estudo do Direito**. 5. ed. São Paulo: Atlas, 2015.

ROXIN, C. **Derecho penal**: la estructura de la teoria del delito. Trad. de la 2. ed. de D. M. L. PEÑA *et al.*. Madrid: Editorial Civitas, S.A., 1997.

SWAN, M. **Blockchain**. Sebastopol: O'Reilly Media, Inc., 2015.

VILA, I. C. **Programas de cumplimiento como forma de autorregulación regulada**. *In*: SÁNCHEZ, J.-M. S.; FERNÁNDEZ, R. M. (coord.).Criminalidad de empresa y compliance: prevención y reacciones corporativas. Barcelona: Atelier Libros, 2013.