

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE
NAS RELAÇÕES DE CONSUMO**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, globalização e responsabilidade nas relações de consumo [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Caio Augusto Souza Lara; Edith Maria Barbosa Ramos; Sinara Lacerda Andrade Caloche – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-593-4

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito e globalização. 3. Responsabilidade nas relações de consumo. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO

Apresentação

DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO I

Os artigos contidos nesta publicação foram apresentados no Grupo de Trabalho DIREITO, GLOBALIZAÇÃO E RESPONSABILIDADE NAS RELAÇÕES DE CONSUMO I durante o IX Encontro Virtual do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, realizado nos dias 22 a 26 de junho de 2026, que teve por tema geral “Constituição, Processo e Justiça Judicial: o papel da jurisdição constitucional na efetivação de Direitos”. Trata-se da nona experiência de encontro virtual do CONPEDI em mais de três décadas de existência.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central grupo. Essa temática traz consigo os desafios que as diversas linhas de pesquisa jurídica enfrentam no tocante ao estudo dos referenciais teóricos do Direito do Consumidor e temáticas conexas. Os trabalhos apresentados no grupo de trabalho evidenciaram a centralidade das novas vulnerabilidades nas relações de consumo contemporâneas, especialmente diante da intensificação da vida digital, da economia de dados e da expansão de práticas comerciais cada vez mais sofisticadas.

Em um primeiro eixo, destacaram-se pesquisas voltadas à proteção da personalidade, à tutela de crianças, adolescentes, idosos e consumidores analógicos, bem como aos riscos

crédito fácil, fintechs, conciliação, dever de informação e termos de ajustamento de conduta, indicaram a urgência de se repensar os instrumentos de prevenção e solução de conflitos, sobretudo diante de práticas mercadológicas que estimulam o consumo imediato, ampliam a assimetria informacional e agravam a situação de consumidores jovens, idosos, de baixa renda ou emocionalmente expostos a estímulos digitais intensivos.

Em um segundo eixo, o grupo de trabalho aprofundou a reflexão sobre algoritmos, plataformas digitais, responsabilidade civil, governança regulatória e sustentabilidade nas relações de consumo. As discussões sobre capitalismo de vigilância, publicidade algorítmica, contratos invisíveis, termos de uso, precificação dinâmica, cibercrimes e proteção do consumidor turista apontaram para a necessidade de revisão dos parâmetros clássicos de responsabilização, uma vez que as plataformas digitais atuam não apenas como intermediárias, mas como agentes econômicos capazes de estruturar escolhas, direcionar comportamentos, explorar dados pessoais e produzir novas formas de dependência e assimetria.

Ao mesmo tempo, os trabalhos voltados à evolução histórica do Código de Defesa do Consumidor, aos princípios fundamentais da matéria, à competência legislativa, à governança global e à obsolescência programada permitiram situar os desafios atuais em uma perspectiva mais ampla, conectando a proteção consumerista à sustentabilidade, ao direito à informação, à regulação transnacional e à crítica da sociedade de consumo.

A análise conjunta dos temas revela um campo jurídico em transformação, no qual a defesa do consumidor precisa dialogar com tecnologia, ética, economia comportamental, proteção de dados, meio ambiente e políticas públicas. Assim, o grupo de trabalho demonstrou que o Direito do Consumidor permanece como instrumento essencial de promoção da dignidade humana, mas deve ser continuamente atualizado para responder aos impactos da digitalização, da financeirização do consumo, da exploração algorítmica e da crise socioambiental contemporânea.

Prof. Dr. Caio Augusto Souza Lara

Prof. Dr.^a Edith Maria Barbosa Ramos

Prof. Dr.^a Sinara Lacerda Andrade Caloche

O CIBERCRIME COMO ESCOLHA RACIONAL: A LUCRATIVIDADE DOS CRIMES DIGITAIS NAS RELAÇÕES DE CONSUMO À LUZ DO CDC

CYBERCRIME AS RATIONAL CHOICE: THE PROFITABILITY OF DIGITAL CRIMES IN CONSUMER RELATIONS UNDER THE BRAZILIAN CONSUMER PROTECTION CODE

Fabiano Ferreira Lopes ¹

Sarah Linhares Marques ²

Resumo

O crescimento dos crimes cibernéticos no Brasil reflete uma transformação estrutural das relações de consumo na sociedade em rede, conforme descrita por Castells. O presente artigo analisa, por meio da Teoria da Escolha Racional de Gary S. Becker e da Análise Econômica do Direito (AED), em que medida o sistema normativo brasileiro — em especial o Código de Defesa do Consumidor (CDC), a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet — é capaz de alterar o cálculo econômico do criminoso digital. A pesquisa adota abordagem qualitativa com revisão bibliográfica e análise legislativa. A partir da fórmula beckeriana de utilidade esperada do crime, demonstra-se que a baixa probabilidade de identificação e punição do agente torna o cibercrime uma atividade racionalmente lucrativa. A assimetria informacional, nos termos de George Akerlof, amplifica a vulnerabilidade do consumidor digital, exposto ao information overload e à sofisticação tecnológica do criminoso. Conclui-se que o CDC, ao prever a responsabilidade objetiva dos fornecedores, atua de forma indireta sobre o cálculo do criminoso, sem, contudo, alcançar a neutralização efetiva de sua lucratividade. O enfrentamento eficaz do cibercrime exige a articulação entre incentivos negativos — aumento da probabilidade de punição por meio de investimentos tecnológicos — e incentivos positivos às empresas para o fortalecimento da segurança digital, superando a lógica meramente reparatória.

Palavras-chave: Cibercrime, Teoria da escolha racional, Código de defesa do consumidor, Assimetria informacional, Análise econômica do direito

General Data Protection Law (LGPD), and the Civil Rights Framework for the Internet — is capable of altering the economic calculation of the digital criminal. The research adopts a qualitative approach based on bibliographic review and legislative analysis. Drawing on Becker's expected utility formula for crime, the study demonstrates that the low probability of identifying and punishing offenders makes cybercrime a rationally profitable activity. Informational asymmetry, in George Akerlof's terms, amplifies the vulnerability of digital consumers, who are exposed to information overload and the technological sophistication of criminals. The study concludes that the CDC, by establishing strict liability for suppliers, acts indirectly on the criminal's cost-benefit calculation, without, however, effectively neutralizing its profitability. Effective responses to cybercrime require the combination of negative incentives — increasing the probability of punishment through technological investment — and positive incentives for companies to strengthen digital security, moving beyond a purely compensatory legal logic.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Rational choice theory, Consumer protection code, Informational asymmetry, Economic analysis of law

1 INTRODUÇÃO

Desde o século XX, a sociedade vem se tornando cada vez mais tecnológica, com o uso da internet e mecanismos de telecomunicações. Concomitantemente, cresce o número de crimes que acompanharam as evoluções da sociedade, gerando uma nova preocupação: os crimes cibernéticos. O surgimento desse tipo penal demonstrou vulnerabilidades sofridas pela sociedade em rede, e analisar a vulnerabilidade sofrida por grupos específicos da sociedade frente a essa nova tipificação penal envolve não apenas segurança pública, mas traz à tona principalmente fragilidades econômicas.

A migração dos crimes tradicionais para o meio digital revela um novo panorama de fragilidades que afeta tanto o ser humano individualmente quanto a coletividade na sociedade atual. Se anteriormente o roubo, a fraude ou a difamação aconteciam em ambientes físicos e bem definidos, atualmente essas práticas se expandem para o ciberespaço, em que os limites são incertos e a sensação de proteção é aparente e ilusória. A sociedade em rede, caracterizada pela intensa troca de informações e pela interdependência tecnológica, torna-se mais suscetível a ameaças invisíveis e de difícil controle.

Ademais, essa realidade traz reflexões e implicações na área do direito, pois a realocação dos crimes reais para o ambiente digital não é apenas uma mudança de cenário de atuação, mas uma reconfiguração profunda das relações de poder e vulnerabilidade. Essa transposição altera o sistema de custos e benefícios, pois no ambiente digital o "custo" de cometer um crime (risco de ser pego + severidade da pena) cai drasticamente, tornando a ação mais lucrativa para o criminoso. É exatamente nessa equação que reside o problema central desta pesquisa: em que medida o sistema de proteção do consumidor, previsto no Código de Defesa do Consumidor (CDC), é capaz de alterar o cálculo econômico do criminoso digital, à luz da Teoria da Escolha Racional?

A relevância do questionamento se evidencia nos dados empíricos disponíveis. O 19º Anuário Brasileiro de Segurança Pública (Fórum Brasileiro de Segurança Pública, 2025) registrou crescimento de 7,8% na taxa de estelionato em 2024, ao passo que o painel de estatísticas do Conselho Nacional de Justiça aponta apenas 51.793 casos resolvidos diante de 2,2 milhões de boletins de ocorrência. Esses números revelam, na prática, a baixa probabilidade de punição que sustenta a lucratividade do cibercrime e que justifica a análise proposta neste trabalho. Tais informações também poderão configurar-se como instrumento de promoção e defesa dos direitos humanos, fomentando discussões e reflexões acerca das possíveis violações

que se manifestam no âmbito digital.

Na sociedade em rede, o espaço virtual amplia as possibilidades de dano, fragmenta as responsabilidades e impõe ao Estado o dever de modificar e atualizar a proteção jurídica dos cidadãos nesses ambientes. Atualmente, apesar dos avanços legais que merecem ser reconhecidos, como a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014), essas normas ainda possuem alcance efetivo limitado. Portanto, a vulnerabilidade digital é o reflexo da vulnerabilidade social e o enfrentamento desse fenômeno exige não apenas novas leis, mas uma nova cultura de cidadania digital.

Um estudo nessa temática auxilia na análise de como o direito tem se inserido nesse novo mundo da tecnologia, além das aplicações de políticas públicas voltadas a essa temática. De acordo com Gico (2012), a Análise Econômica do Direito, por meio de seu caráter consequencialista, busca não apenas analisar de forma abstrata a violação da norma, mas entender a eficiência da mesma na dinâmica prática. Inserida no contexto do consumidor digital, essa análise configura um instrumental que permite entender a dinâmica do mercado digital e identificar suas falhas, além de avaliar como mudanças normativas podem aprimorar a segurança e a efetividade das relações de consumo. Os dados obtidos poderão ainda constituir importantes contribuições para a elaboração de novas normativas e para a análise da efetividade das políticas públicas atualmente vigentes.

A presente pesquisa adota abordagem qualitativa, com base em revisão bibliográfica. O corpus analítico foi constituído por obras doutrinárias, artigos científicos e legislações pertinentes ao tema, com destaque para estudos relacionados à Teoria da Escolha Racional, formulada por Gary S. Becker, e à assimetria informacional de George Akerlof, bem como produções voltadas ao Direito do Consumidor e aos crimes cibernéticos. Foram consultadas bases de dados de periódicos científicos, repositórios institucionais e legislação vigente, incluindo o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014), o Código Penal (Decreto-Lei nº 2.848/1940) e a Lei nº 15.397/2026. O método procedimental se desenvolveu a partir das premissas da Teoria da Escolha Racional e da Assimetria Informacional, para verificar se as normas brasileiras vigentes são capazes de interferir no cálculo econômico do criminoso digital.

O presente estudo tem como objetivo geral analisar, com base na Teoria da Escolha Racional e no Código de Defesa do Consumidor, se a normativa legal vigente está sendo

eficiente para prevenir e minimizar os danos causados pelos crimes digitais nas relações de consumo, além de avaliar se as legislações estão cumprindo seu papel de desincentivar o crime, transformando a dinâmica econômica da atividade ilícita e gerando segurança social. São objetivos específicos: examinar a Teoria da Escolha Racional, conforme formulada por Gary S. Becker, aplicada ao comportamento do criminoso digital nas relações de consumo; investigar o papel da assimetria informacional e da vulnerabilidade do consumidor no ambiente digital; e avaliar o Código de Defesa do Consumidor como instrumento de correção de falhas de mercado. O artigo está organizado em três seções temáticas, que tratam, respectivamente, da racionalidade econômica do criminoso digital, da assimetria informacional e da vulnerabilidade do consumidor, e da análise do CDC como mecanismo de intervenção nas falhas do mercado digital.

2 A TEORIA DA ESCOLHA RACIONAL E A RACIONALIDADE ECONÔMICA DO CRIMINOSO DIGITAL

A sociedade é caracterizada por transformações estruturais impulsionadas pelo avanço tecnológico e pela consolidação das redes digitais de informação. Assim, essa revolução informacional deu origem a uma nova forma de organização social em que a comunicação e as relações se estruturam por meio de fluxos digitais.

Segundo Castells (2019), as novas tecnologias da informação não são apenas ferramentas, mas processos que formam uma base tecnológica para a sociedade em rede. O autor descreve a sociedade como um emaranhado de informações interconectadas que formam uma rede global. Entretanto, essa interdependência da sociedade em relação aos fluxos digitais os torna indivíduos e instituições mais vulneráveis a crimes cibernéticos.

A migração dos crimes reais para o ambiente digital, portanto, é consequência direta dessa lógica em rede. A expansão das tecnologias de comunicação promove um ambiente com ações que geram repercussão global, assim as responsabilidades também geram repercussões quanto ao seu gerenciamento e devidas atribuições. Castells (2019) destaca que a internet se tornou parte integrante de nossas vidas e, por estar tão conectada às ações das pessoas, acaba sendo um "terreno" fértil para atos ilegais, como golpes virtuais, invasões a sistemas institucionais e jogos de apostas online.

O crime pode ser agrupado em dois grandes grupos: crimes lucrativos e não lucrativos, e no caso dos crimes digitais que envolvem extorsão de dinheiro, são classificados como crimes

lucrativos (Becker, 1968). E por isso esses criminosos fazem de suas organizações como empresas, que precisam avaliar custos e lucros. No caso dos crimes digitais podemos mencionar como “vantagens”: lucros rápidos, podem alcançar mais pessoas com mais facilidade, atuam sem identificação (anonimato), e possuem um custo menor.

Assim, o criminoso age como um empresário administrando sua empresa, ponderando custos e benefícios, um agente racional. Segundo Becker (1968 apud Shikida; Amaral, 2012, p. 304):

O argumento básico da abordagem econômica do crime é que os infratores reagem aos incentivos, tanto positivos quanto negativos e que o número de infrações cometidas é influenciado pela alocação de recursos públicos e privados para fazer frente ao cumprimento da lei e de outros meios de preveni-los ou para dissuadir os indivíduos a cometê-los. Para os economistas, o comportamento criminoso não é visto como uma atitude simplesmente emotiva, irracional ou anti social, mas sim como uma atividade eminentemente racional.

Assim, os custos do crime digital são reduzidos e, como seres racionais, os criminosos calculam suas atividades de modo que os lucros esperados superem os custos, incluindo o risco de eventual repressão penal, por exemplo.

O modelo de Escolha Racional proposto por Becker (1968) busca entender o crime de uma maneira matemática e incorpora uma relação comportamental através de custos e níveis de algumas variáveis. Acerca do dano, ele traz um cálculo que relaciona o aumento do nível da atividade criminosa (O) com o impacto no aumento do dano (H), na seguinte relação para a atividade “ i ”:

$$H_i = H_i(O_i), \text{ onde } H_i' > 0$$

Ademais, o ganho para o criminoso (G) aumenta com número de ofensas, na seguinte relação:

$$G_i = G_i(O), \text{ onde: } G_i' > 0$$

O custo ou dano líquido para a sociedade é simplesmente a diferença entre o dano e o ganho e pode ser escrito como:

$$D(O) = H(O) - G(O)$$

Se, como parece plausível, os infratores geralmente recebem ganhos marginais decrescentes e causam danos marginais crescentes com infrações adicionais,

$$G' < 0, H' > 0 \text{ e } D'1 = H' - G' > 0, G'' < 0, H'' > 0, \text{ and } D''1 = H''$$

Segundo Becker a utilidade esperada (U) de se cometer um crime seria definida como a soma da renda esperada do crime (Y) e da renda esperada descontada a punição (f):

Em termos gerais: se $U = \alpha X$, com α constante e maior do que zero. A utilidade esperada do crime é:

$$U e = p\alpha(Y - f) + (1 - p)\alpha Y$$

onde p é a probabilidade de punição, dada pela razão das ofensas elucidadas, como apresentado anteriormente.

E, portanto:

$$\partial U / \partial p = \alpha(Y - f) - \alpha Y = -\alpha f,$$

$$\partial U / \partial f = -p\alpha$$

Logo, o aumento de p é mais efetivo em reduzir a utilidade esperada do que o aumento de f se e somente se:

$$\alpha f > \alpha p \text{ ou } f > p \text{ e como } 0 < p < 1, \text{ é plausível assumir que } f > p$$

A função em questão no contexto do cibercrime apresenta a taxa de variação da utilidade em termos de três variáveis, sendo Y a representação do lucro obtido através da conduta ilícita em meio digital; F demonstra o custo da punição sendo materializado no valor da fiança ou por uma estimativa do custo social que a pena privativa de liberdade pode causar ao indivíduo; e por fim a variável P que significa a probabilidade do agente criminoso ser identificado, processado e condenado. Tendo em vista a última afirmação do cálculo, em que chega-se à conclusão que o custo da punição é maior do que a probabilidade de identificação do agente responsável pela conduta ilícita, consequência das limitações estruturais e normativas na identificação e resolução de conflitos dessa natureza.

Concomitante a isso, como Becker (1968) descreve em $0 < p < 1$, se aumentado a probabilidade do agente criminoso ser identificado terá impacto proporcional sobre todo o cálculo do que se apenas aumentarem as sanções, ou seja a variável F se alterada de forma

isolada não tem impacto significativo no resultado do cálculo. Assim, fica claro que o investimento prioritário deve recair sobre os mecanismos de identificação, investigação e responsabilização dos criminosos digitais, e não isoladamente sobre a severidade das sanções.

Em sua descrição matemática, Becker também demonstra a função do dano social através da fórmula $D(O) = H(O) - G(O)$, ela releva a escalabilidade dos crimes digitais, o principal ponto divergente dos crimes tradicionais. Devido ao grande alcance que uma única ação no ambiente digital pode causar, um mesmo site ou mensagem fraudulenta pode gerar diversas fraudes de forma quase simultânea, segundo apontamentos da Federação Brasileira de Bancos (2025, p. 22) o meio digital proporciona “[...] acesso facilitado a inovações e a escalabilidade, a redução de custos”. Assim, o lucro do criminoso (G) aumenta sem que interfira de forma proporcional nos custos operacionais do criminoso. Na equação é adicionada outra variável, que resulta da diferença entre o dano da ação criminosa (H) em ambiente digital e o custo do criminoso (G) tendo como resultado um elevado valor que representa o dano que recai sobre a sociedade.

No contexto dos crimes digitais no Brasil, esses resultados infelizmente negativos sofridos pela população resultam do que Castells (2019) explica como sendo uma das características da sociedade em rede, a massificação do acesso à internet e a interconexão dos fluxos informacionais. Essa facilidade no alcance de diversas pessoas através de uma única ação aumenta os usuários do comércio eletrônico e consequentemente amplia o número de vítimas potenciais. Além disso, é importante frisar que a probabilidade do indivíduo criminoso ser identificado é baixa, por isso as outras variáveis como o custo da operação e da sanção se tornam contornáveis, cabendo portanto investimentos em mecanismos tecnológicos das empresas para que possa ser identificado o autor de ações delituosas.

Portanto, com base nos cálculos matemáticos propostos por Becker, pode-se inferir que o criminoso encontra utilidade nos resultados dessas variáveis. Isso pressupõe que a sanção prevista na norma não é efetivada na realidade, visto que as duas variáveis seriam equivalentes caso a sanção cominada em lei obtivesse eficácia plena. Assim, para a teoria da dissuasão (Becker, 1968) o direito penal tem como função desestimular a prática de atos ilícitos. Pela perspectiva da AED as sanções não podem dar margem para a racionalização de crimes por meio da fixação de “preços” que tornem utilitário a prática de atos ilícitos, mas pelo contrário deve ser uma ferramenta jurídica de plena eficácia que inviabilize essas práticas.

No âmbito do Direito penal, os crimes digitais nas relações de consumo são caracterizados como ilícito e culpável. O Código Penal (Brasil, 1940) em seu artigo 171 prevê a punibilidade para estelionato eletrônico, e no artigo 154-A trata acerca da punição para casos que envolvam invasão de dispositivo informático. Cabe ainda mencionar a Lei nº 15.397 (Brasil, 2026), que majorou as penas para diversos tipos penais, incluindo o cibercrime. Dessa forma, podemos perceber que o problema não é a tipificação do crime, mas o devido cumprimento da punição prevista.

Segundo a teoria do pensamento racional de Becker (1968), a decisão de cometer um crime parte de um cálculo econômico de custos esperados da punição e lucros econômicos advindos da atividade ilícita, eles levam em consideração o valor da fiança de cada tipificação penal e a probabilidade de identificação e aplicação da devida sanção. Assim, a pena só é efetiva se de fato impacta nesse cálculo, e na prática vemos que não é possível. Por isso que crimes desse tipo são tão recorrentes.

3 ASSIMETRIA INFORMACIONAL E VULNERABILIDADE DO CONSUMIDOR NO AMBIENTE DIGITAL

A sociedade informacional vive em um contexto em que as relações de consumo cada vez mais acontecem por meios digitais de informação. Segundo George Akerlof (1970), em uma negociação, ambas as partes envolvidas devem primar pela transparência e comunicação ativa; porém, é possível que uma delas detenha informações relevantes sobre o serviço ou produto que a outra não possui, causando assim um desequilíbrio denominado pelo autor de assimetria informacional, conceito este desenvolvido pelo autor em seu livro “Mercado de Limões”.

Para ilustrar a assimetria informacional, Akerlof (1970, p. 3) se utilizou do princípio dos limões, em que no mercado existem automóveis de qualidade e alguns carros que não são bons, podendo ser por questões de custo benefício, defeitos, problemas esses mascarados pelos vendedores, chamados pela gíria americana de “limões”. O comprador sabe da possibilidade de comprar um carro ruim, por isso prefere pagar por um preço médio, entretanto esse valor não é justo para os vendedores de carros de alta qualidade e por isso eles se retiram do mercado. Nesse caso, o autor aplica a Lei de Gresham (de forma simplificada, acontece quando a moeda ruim expulsa a boa) de forma modificada em que bens de má qualidade (“limões”) expulsem bens de boa qualidade (“pêssegos”) do mercado.

Em um ambiente virtual essa teoria da economia clássica ganha ainda mais potencialidade pois o fraudador age como agente racional se utilizando da assimetria para mascarar “limões” através de sites falsos ou produtos inexistentes. E tendo em vista que o custo de operação no ambiente digital é baixo, a desonestidade é maximizada em decorrência da dificuldade do consumidor de verificar a procedência da sua transação de compra. Vale ainda mencionar, em conformidade com a análise econômica do direito, a aplicação dessa teoria na lógica do mercado afeta toda a cadeia econômica do mercado pois enquanto os “limões” crescem no mercado, o ambiente de venda digital se torna instável e inseguro para o consumidor e para o vendedor.

De acordo com dados do Anuário Brasileiro de Segurança Pública (2025), em 2024 foi registrado um crescimento de 7,8% na taxa de estelionato no Brasil em relação ao ano anterior. Eles ainda apontaram que o estado do Maranhão apresentou o menor registro de casos de estelionato no Brasil, sendo 285,3 crimes por 100 mil habitantes. Outro dado importante, refere-se ao número de elucidação desses casos, em 2024 foram registrados 2,2 milhões de boletins de ocorrência, entretanto a base do CNJ “Justiça em Números” (2025) deu como resolvido apenas 51.793 casos. Além disso, vale também destacar que “[...] dada as dificuldades das vítimas formalizarem as queixas-crime e diante da baixa capacidade de esclarecimento e investigação de crimes no país, os dados acima revelam um grande vetor de impunidade, com o adicional de onerar a vítima com a responsabilidade [...]” (Fórum Brasileiro de Segurança Pública, 2025, p. 110).

Nesse contexto, destaca-se que o volume de casos de fraudes digitais cresceu significativamente nos últimos anos, em contrapartida uma grande parte deles ficaram impunes. Esses dados ilustram a assimetria informacional na prática, pois em um ambiente comercial digital, a falta de informações essenciais torna-o suscetível a ataques, e os dados demonstram que os criminosos estão se aproveitando dessas falhas informacionais para agirem conforme explica a lógica da escolha racional. Acerca disso, a taxa de elucidação apresentada revela que diante da baixa taxa resolutiva os lucros superam seus gastos, tornando esse cálculo um incentivo para a continuidade do delito. Ainda que no estado do Maranhão as taxas tenham se apresentado menores, mas o problema estrutural ainda é visível e persistente.

Ademais as transações ocorrem com mais velocidade, tanto os consumidores quanto alguns fornecedores de produtos e serviços têm dificuldade de verificar a autenticidade das informações, colocando portanto o consumidor em uma posição de vítima em potencial, em

decorrência do seu lugar de vulnerabilidade. No art.4º, I do Código do Consumidor (Brasil, 1990) está expresso que o código leva em consideração a situação de vulnerabilidade que o consumidor se encontra, mas para além dessa função protetiva, é necessário também um olhar crítico que considere o cálculo de custos e benefícios que orienta a atuação do criminoso. Para Akerlof (1970, p. 14), as instituições de neutralização atuam na neutralização dos efeitos de incerteza do mercado. Elas atuam tanto na proteção do consumidor e amparo do mesmo por meio de sanções aos criminosos, além de utilizar de mecanismos que atuem diretamente na dinâmica do mercado, tornando essas transações seguras aos seus consumidores e afetando na lógica de escolha racional dos criminosos.

Outrossim, a assimetria informacional nos casos de crimes digitais expõe o consumidor a uma posição de vulnerabilidade, uma vez que o criminoso domina a tecnologia, a informação e o tempo. O consumidor, que agora se vê como vítima, não tem acesso claro a uma identidade da empresa ou do vendedor, não dispõe de mecanismo de verificação de autenticidade do site e atrelado a essas desvantagens, caso o criminoso limite o tempo de compra o usuário também perde seu tempo de raciocínio. E o criminoso dispõe de conhecimento avançado do ambiente digital, conhece os padrões de consumo do usuário e o principal e controla o tempo de interação com o consumidor.

Portanto isso demonstra que os consumidores são continuamente expostos a um fluxo intenso de informações e publicidade em seus feeds digitais, o fenômeno de *information overload* (Toffler, 1970; Eppler; Mengis, 2004), e por isso não conseguem distinguir sites/informações falsas de verdadeiras. Evidenciando assim falhas do próprio mercado, que ao não regular de maneira efetiva seu ambiente digital torna os consumidores vulneráveis aos comportamentos oportunistas dos criminosos. Por isso que à luz da teoria da escolha racional, quanto maior a vulnerabilidade informacional da vítima, menor o risco para o criminoso. Essa desigualdade informacional não apenas facilita a ocorrência do crime, mas também se torna um incentivo à contínua prática ilícita.

Tendo em vista essa relação, o mesmo golpe pode ser replicado várias vezes com variadas vítimas, assim o retorno do crime aumenta e por se tratar de um crime de difícil identificação o custo esperado da punição permanece baixo, além do mais devido às inovações tecnológicas os custos para operar nesse ambiente são baixos se comparado com outros crimes, como descrito pela demonstração matemática de Becker (1968). Do ponto de vista da AED se

configura como assimetria informacional, prejudicando diretamente o consumidor e o tornando uma mera vítima de uma organização criminosas.

4 O CÓDIGO DE DEFESA DO CONSUMIDOR COMO INSTRUMENTO ECONÔMICO DE CORREÇÃO DE FALHAS DE MERCADO

O ambiente digital foi reconhecido como passível de regulação com o Marco Civil da Internet (Brasil, Lei nº 12.965/2014), na qual foram instituídos os direitos fundamentais, através da garantia da liberdade de expressão e a proteção da privacidade e dos dados pessoais. Além de definir a responsabilização dos agentes envolvidos a fim de garantir a proteção dos dados pessoais dos usuários e a segurança da rede, tornando um ambiente online mais seguro, democrático e regulado.

Além dessa normativa, em 2018 foi instituída a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709), que regula o armazenamento dos dados pessoais dos usuários com base nos direitos fundamentais. Essa normativa possui caráter preventivo, assim ela age sobre o recurso atacado pelos criminosos, no caso os dados pessoais. Assim, através de regras que regulam como deve ser feita a coleta, tratamento e armazenamento dos dados pessoais dos consumidores pelas empresas, a LGPD pretende dificultar as ações fraudulentas através de medidas de segurança no ambiente digital. Nesse sentido, vale mencionar a Autoridade Nacional de Proteção de Dados (ANPD) como a agência reguladora da aplicação das normativas propostas pela LGPD. Cabe à agência monitorar o cumprimento da lei, aumentando o risco regulatório para empresas que negligenciam a segurança dos dados dos usuários através de sanções administrativas.

No caso de crimes digitais envolvendo compra e venda, o Código de Defesa do Consumidor (CDC) também é uma norma de regulação, uma instituição de neutralização (Akerlof, 1970) que pretende equilibrar a balança informativa entre fornecedor e consumidor. Ademais, o CDC também prevê a responsabilidade objetiva, em seus artigos 12 e 14 acerca da responsabilidade objetiva do fornecedor e do prestador de serviço por “defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos” (Brasil, CDC, 1990). Segundo a AED, a responsabilidade objetiva nesses casos recai sobre quem tem o menor custo de evitá-lo, podendo ser bancos, plataformas ou até fornecedores, por exemplo.

A partir da análise econômica do Direito, a atuação da tríplice proteção normativa, CDC, LGPD, ANPD não são apenas normas que protegem o consumidor de possíveis violações a direitos, mas também devem atuar como reguladores das falhas do mercado. O CDC, por exemplo, pode reduzir a assimetria informacional, em seu artigo 6º, III, art. 30 e 31, está previsto que é um direito básico do consumidor à informação adequada e clara. Entretanto, na prática essas previsões legais não são eficientes, pois o criminoso se apropria dessa confiança que o CDC passa ao consumidor para aplicar seus golpes. Entretanto, nesses dois casos o CDC apenas reduz os danos sobre o consumidor, porém não intervém de fato no esquema da assimetria informacional, pois o criminoso não é identificado, os prejuízos são redirecionados e socializados, causando uma manutenção da lucratividade do criminoso.

Na lógica da AED o criminoso digital atua tal qual um empresário econômico, avaliando riscos, benefícios e custos. Então, enquanto o retorno econômico da atividade criminosa superar o custo e os riscos penais, a atividade ilícita continuará sendo uma escolha racional e vantajosa. Assim o CDC ao atuar como corretor de falhas de mercado, busca reduzir esse desequilíbrio redistribuindo prejuízos, entretanto não atua reparando de fato o dano. [...] O objetivo da sociedade é tornar nulo o retorno lucrativo médio do empresário criminoso e/ou aumentar o risco desta atividade [...] (Shikida; Amaral, 2012, p. 317), dessa forma a função do CDC não será apenas reparar falhas de mercado mas desestruturar a viabilidade econômica do crime.

Ao tornar nulo o retorno lucrativo do empresário criminoso Shikida e Amaral (2012) propõe elevar os custos do crime. Aumentar a probabilidade de punição a atividade criminosa ou reduzir a escalabilidade do crime são algumas alternativas para que o risco supere o benefício. Assim, mesmo se não conseguir diminuir os lucros dos criminosos, os riscos devem aumentar para que os crimes digitais se tornem uma atividade ilícita economicamente irracional. Constata-se ainda que o modelo de prevenção e enfrentamento adequado para tal situação, deve seguir os parâmetros postulados por Becker (1968), aumentando a dissuasão não pelo aumento das penas, mas pelo aumento na probabilidade de punição para o indivíduo. Esse aumento se daria através, principalmente, do aumento no investimento em tecnologias que sejam eficazes em identificar o criminoso.

Cabe ainda ressaltar, outra teoria da análise econômica do Direito que explica essa lucratividade do crime e como as normativas corroboram para isso. Segundo Shikida e Amaral (2012), a teoria dos incentivos parte do pressuposto de que as normas não apenas ditam

o que é certo ou errado perante a lei, mas também trazem incentivos, podendo ser positivos ou negativos, que irão moldar a forma como os indivíduos irão agir. Assim, essa teoria mostra que o Direito molda escolhas. Enquanto a teoria da escolha racional explica como o criminoso calcula se uma atividade ilícita é vantajosa ou não, a teoria dos incentivos mostra como as normativas podem alterar esse cálculo.

O cibercrime do consumo pode apresentar alguns incentivos como, por exemplo a assimetria informacional elevada, a baixa probabilidade de punição e a realocação da responsabilidade. O sistema normativo brasileiro tenta contornar esses incentivos através da responsabilização objetiva prevista no CDC, na qual os fornecedores indenizam possíveis danos decorrentes de fraudes digitais. De forma conjunta, a LGPD e a agência fiscalizadora ANPD, objetivam aumentar os custos da execução de ações criminosas por meio de sanções administrativas e obrigações de segurança. Entretanto, no caso dos incentivos negativos podemos citar que a sanção penal não tem aplicação concreta, o Estado tem dificuldade de identificar esses criminosos além dos custos de atividade serem todos difusos. Isso demonstra que o sistema não tem mecanismos para desincentivar o crime, pelo contrário esses incentivos se colocados na balança pelo criminoso a decisão racional será seguir no crime digital.

O CDC também cria incentivos importantes, como as previsões dispostas nos artigos 12, 14, 6º, VI e 18, por exemplo. Ele incentiva os prestadores de serviços a investirem em segurança para seus sites, à reparação rápida do dano causado ao consumidor e redução dos custos de transação do consumidor. Todavia, esses incentivos positivos ainda são pouco explorados na jurisdição brasileira, sendo necessário mecanismos mais eficientes para incentivar as empresas a investirem em segurança digital. Diante disso, cabe ainda mencionar que apesar da aplicação da teoria da dissuasão (Becker, 1968) nas normativas brasileiras ainda assim no que tange o criminoso o CDC não dispõe de incentivos negativos diretos, assim o retorno econômico da atividade ilícita contribui para o expressivo aumento do comportamento oportunista desses criminosos digitais.

Isto posto, no que concerne a questão resolutiva da problemática a teoria da dissuasão, com uma efetiva articulação entre incentivos positivos e negativos na prática consumerista digital traria um enfrentamento eficaz do cibercrime. Pois os incentivos negativos focam em alterar o cálculo racional do criminoso, especificamente no aumento do custo da operação e identificação do responsável, e os positivos, por sua vez, estimula ações de combate

contra essas condutas ilícitas por parte das empresas, assim essa articulação trará efeitos diretos e indiretos.

Portanto, no âmbito digital essa lógica reforça que o enfrentamento dos crimes de consumo não pode se limitar a ações reparatórias nem à ampliação abstrata de sanções penais. É necessário uma transformação institucional que consiga agir diretamente sobre os incentivos econômicos do cibercrime, combinando instrumentos civis, penais e regulatórios. Tendo em vista os dados e explicações apresentadas, o Direito se apresenta como sendo a principal ferramenta de modificação dessa dinâmica, através da AED o objetivo deve ser tornar nulo o lucro do criminoso através do aumento da taxa de risco das atividades ilícitas realizadas em ambiente digital. Assim, quando o custo esperado da punição superar o ganho ilícito é que se alcançará o objetivo apontado por Shikida e Amaral (2012): inviabilizar economicamente o crime e romper a lógica racional que sustenta sua expansão na sociedade informacional.

5 CONCLUSÃO

Diante do exposto, a importância da informação como ferramenta de poder é notável. Conforme Castells (2019, p. 44), “[...] a habilidade ou inabilidade de as sociedades dominarem a tecnologia [...] incorpora a capacidade de transformação das sociedades[...]”. Desse modo, aquele que controla o trânsito de informações, seja um governo, uma empresa ou um hacker, pode moldar atitudes, escolhas e até mesmo dinâmicas políticas. Isso demonstra que os crimes digitais não se limitam a infrações individuais, mas refletem as tensões estruturais da sociedade informacional, em que a segurança, a privacidade e os direitos humanos se tornam bens jurídicos frágeis diante da lógica global das redes.

Nessa perspectiva, a vulnerabilidade sofrida pela sociedade brasileira demonstra essa dualidade entre as tecnologias de informação e a segurança no ambiente digital. Essa tensão entre o real e o virtual exige que sejam implementadas novas formas de controle tanto social quanto digital, além de políticas públicas efetivas. Essa noção de “crimes reais para digitais” traz essa ideia de um delito que antes era meramente físico agora passa ao campo simbólico e informacional, com o dano se perpetuando não apenas por meio da matéria mas agora também pela informação.

Portanto, a lucratividade dos crimes digitais em relações de compra e venda é oriunda do desequilíbrio entre os altos lucros provenientes da conduta ilícita e a baixa probabilidade de

punição efetiva, e essa lógica lucrativa e vantajosa torna essa conduta criminosa como uma escolha racional para o criminoso.

Além disso, cabe ressaltar que segundo a AED, a consequência jurídica prevista no Código do Consumidor apenas beneficia a vítima e minimiza os danos sofridos pelo consumidor, realocando-os para outros agentes que podem custear esses prejuízos sem sofrerem tanto com os custos. Em parte essa realocação é boa, pois o consumidor não sai prejudicado entretanto essas responsabilidades não conseguem alcançar o criminoso, uma vez que ela não interfere no cálculo econômico e racional do crime. Assim, esse esquema continua preservado e se perpetuando, com elevado retorno financeiro e com reduzido custo penal. Sob essa ótica, a intervenção apenas do Código do Consumidor não será eficiente, por isso a necessidade de estratégias penais que apliquem as sanções de forma efetiva a fim de que se tornem incentivos negativos, mudando assim a estrutura do cálculo econômico racional do criminoso.

Sob a perspectiva penal, há normativas que tipificam e prescrevem punições aos criminosos, entretanto esse avanço normativo não é acompanhado de mecanismos eficazes de investigação, identificação e punição dos autores. Por isso, como explica Becker (1968), essas sanções não atingem diretamente o cálculo custo-benefício dessas organizações criminosas, criando assim lacunas estruturais que apenas contribuem para a continuidade da lucratividade dessas condutas ilícitas no ambiente de consumo digital.

Portanto, o CDC ao dispôr acerca da responsabilidade objetiva dos fornecedores, realoca os danos sofridos pelo consumidor às empresas independentemente de comprovação ou não de culpa. Essa lógica incentiva os fornecedores a aumentarem seus investimentos em segurança da informação, autenticação reforçada e mecanismos antifraude. Nesse sentido, apesar dessa prática não punir os criminosos de forma direta mas reconfigura seu cálculo, tornando o ambiente menos vulnerável e com mais custos de operação para o criminoso.

Entretanto, as normativas brasileiras vigentes ainda apresentam limitações no que tange a alteração direta do cálculo econômico do criminoso, pois ela age apenas sobre os fornecedores. Assim, dada a atuação do CDC, anteriormente apresentadas, podemos inferir que ele atua de forma estrutural e indireta, pois ao incentivar a segurança nas plataformas digitais, redução das vulnerabilidades digitais e ampliação da responsabilização em casos de falhas no mercado, diminui a atratividade econômica do cibercrime. Em suma, a partir da AED, tratar

acerca da teoria da escolha racional inserida no contexto do cibercrime é incutir ao direito um papel estratégico, em que normas não apenas sancionem mas redesenhem uma lógica de mercado para que ela se torne segura aos seus usuários.

REFERÊNCIAS

AKERLOF, George A. **The market for “lemons”: quality uncertainty and the market mechanism**. The Quarterly Journal of Economics, v. 84, n. 3, p. 488-500, 1970. Disponível em: https://cies.org.pe/wp-content/uploads/2016/07/akerlof_1970.pdf. Acesso em: 4 nov. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 4 nov. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 4 nov. 2025.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. **Institui a Estratégia Nacional de Segurança Cibernética (E-Ciber)**. Diário Oficial da União: seção 1, Brasília, DF, 6 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 4 nov. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 4 nov. 2025.

BRASIL. Lei nº 15.397, de 30 de abril de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (**Código Penal**), a fim de majorar as penas previstas para os crimes de furto, roubo, estelionato, receptação, receptação de animal e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, bem como para tipificar os crimes de receptação de animal doméstico e de fraude bancária. Diário Oficial da União: seção 1, Brasília, DF, ed. 81, p. 1, 4 maio 2026. Disponível em: <https://in.gov.br/web/dou/-/lei-n-15.397-de-30-de-abril-de-2026-702822674>. Acesso em: 6 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União: seção 1, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 11 maio 2026.

BECKER, Gary S. **Crime and punishment: an economic approach**. Journal of Political Economy, Chicago, v. 76, n. 2, p. 169–217, 1968.
<https://www.jstor.org/stable/1830482?seq=8>

CASTELLS, Manuel. **A Sociedade em Rede**. 17ª ed. São Paulo: Paz e Terra, 2019.

Conselho Nacional de Justiça. **Painel de Estatísticas** – Justiça em Números. Disponível em: <https://justica-em-numeros.cnj.jus.br/painel-estatisticas/>. Acesso em: 11 maio 2026.

Eppler, Martin J. and Mengis, Jeanne(2004)'**The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines**',The Information Society,20:5,325 — 344. Disponível em: <http://dx.doi.org/10.1080/01972240490507974>. Acesso em 11 maio 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2025/09/anuario-2025.pdf> . Acesso em: 11 maio 2026.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Pesquisa Febraban de Tecnologia Bancária 2025**: volume 1. São Paulo: Febraban, 2025. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_01%20-%205.pdf . Acesso em: 11 maio 2026.

GICO, Ivo Jr. **Introdução ao Direito e Economia**. In: TIMM, Luciano Benetti (org.). **Direito e economia no Brasil**. São Paulo: Atlas, 2012. p.1-33.

SHIKIDA, Pery Francisco Assis; AMARAL, Thiago Bottino. **Análise Econômica do Crime**. In: TIMM, Luciano Benetti (org.). **Direito e economia no Brasil**. São Paulo: Atlas, 2012. p. 296-317.