**FUNDAÇÃO GETÚLIO VARGAS**

**ESCOLA DE DIREITO DE SÃO PAULO**

LINCOLN MACHADO DOMINGUES

# INCIDENTES CIBERNÉTICOS LESIVOS E RESPONSABILIDADE PENAL POR OMISSÃO IMPRÓPRIA EM CONTEXTO EMPRESARIAL

São Paulo

2021

**FUNDAÇÃO GETÚLIO VARGAS**

**ESCOLA DE DIREITO DE SÃO PAULO**

LINCOLN MACHADO DOMINGUES

# INCIDENTES CIBERNÉTICOS LESIVOS E RESPONSABILIDADE PENAL POR OMISSÃO IMPRÓPRIA EM CONTEXTO EMPRESARIAL

Projeto de pesquisa apresentado como requisito parcial para aprovação no Mestrado Profissional em Direito Penal Econômico, da Escola de Direito de São Paulo da Fundação Getúlio Vargas.

Orientador: Prof. Dr. Rodrigo de Grandis

São Paulo

2021

## 1. IDENTIFICAÇÃO E APRESENTAÇÃO DO TEMA E DA PROBLEMÁTICA

Independentemente de ter ou não como atividade-fim a coleta e o processamento de dados alheios, companhias têm aperfeiçoado seus mecanismos de uso de dados sobretudo por meio de técnicas de análise preditiva, a qual consiste em uma tecnologia que aprende a partir da experiência gerada por dados e, assim, almeja prever o comportamento futuro de indivíduos a fim de tornar possíveis decisões corporativas mais profícuas.[1]

Cientificamente, tal tecnologia se insere no campo da Ciência de Dados que, embora de diversificada definição, é tida como o segmento científico dedicado a extrair inferências relevantes de dados, por meio de habilidades de programação, matemática e estatística.[2]

É por meio dessa ciência e de suas aplicações que companhias de diversos ramos têm, com suas equipes de cientistas de dados, se valido desse recurso para efetuar valiosas inferências para seus negócios.

A Target, empresa americana do ramo de varejo, é capaz de saber quais clientes estão grávidas a partir de dados relacionados a suas compras presenciais e digitais, bem como de suas interações com a plataforma eletrônica.[3] Já o eHarmony, uma plataforma de relacionamentos, se vale dos dados de usuários para prospectar candidatos amorosos.[4]

Há, além desses, diversos outros exemplos concretos de como empresas têm se valido da interpretação tecnológica de dados para incrementar a performance.

---

[1] SIEGEL, Eric. **Análise preditiva: o poder de prever quem vai clicar, comprar, mentir ou morrer.** Tradução de Wendy Campos. Rio de Janeiro: Alta Books, 2017, p. 13.
[2] BOOKSHEAR, J. Gleen. **Ciência da computação: uma visão abrangente.** Tradução de Eduardo Kessler Piveta. 11. ed. Porto Alegre: Bookshear, 2013, p. 447.
[3] GRUS, Joel. **Data science do zero: primeiras regras com o Python.** Tradução de Welington Nascimento. Rio de Janeiro: Alta Books, 2016, p. 2.
[4] SIEGEL, Eric. **Análise preditiva: o poder de prever quem vai clicar, comprar, mentir ou morrer.** Tradução de Wendy Campos. Rio de Janeiro: Alta Books, 2017, p. 13.

Ocorre que, paralelamente à crescente aplicação da Ciência de Dados e da tecnologia de análise preditiva em contexto empresarial, chamam atenção os também crescentes hackeamentos em detrimento dos dados detidos por empresas.

A Target, acima citada como empresa que dispõe dos dados de suas clientes para saber quando estas estão grávidas, foi atacada ciberneticamente em 2013, ocasião na qual acabaram sendo expostos dados pessoais e financeiros de 70 milhões de consumidores, o que custou à mencionada companhia – apenas em reembolsos aos clientes lesados – 240 milhões de dólares, isso sem mencionar os danos não patrimoniais causados à empresa e aos clientes.[5]

Em meio a esse e outros cenários, o legislador brasileiro elaborou a Lei n. 13.709/2018 – chamada também de Lei Geral de Proteção de Dados –, a qual, por meio de suas disposições, tem, segundo seu art. 1º, *"o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".*

Para tanto, em seu Capítulo VII – Da Segurança e das Boas Práticas, o aludido diploma legal erigiu uma série de deveres extrapenais relacionados à proteção de dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que possam ocasionar a destruição, perda, alteração, comunicação ou qualquer forma de tratamento ilícito de dados pessoais detidos por pessoa natural ou jurídica de direito público ou privado.

Atentas à realidade[6] e às disposições da Lei Geral de Proteção de Dados e de legislações equivalentes em outros países, diversas empresas passaram a investir em

---

[5] What we learned from infamous hacking incidents. **Maryville University,** Town and Country/EUA, data de publicação não informada, Disponível em: <https://online.maryville.edu/blog/what-we-learned-from-infamous-hacking-incidents/>. Acesso em 12/12/2020.

[6] KUNER, Cristopher et. al. The rise of cybersecurity and its impact on data protection. **International data privacy law,** Oxford/Reino Unido, Volume 7, Número 2, 2017. Disponível em: < https://watermark.silverchair.com/ipx009.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAApwwggKYBgkqhkiG9w0BBwagggKJMIIChQIBADCCAn4GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM39lvvKON-O3bkFWVAgEQgIICT6RLpBga4kkeXO-hrLZEYAHuqKjZ_R7SYF5741Zla18Af1C3HsWH5BGrbaD0Uw5pt2JSMFL1PoCd_qy28X0Ecu7_k63e4KqCLA7nlJpexRtiR9ZwctpT4Gc_hOagKFYLId9y_6WC5lAfW4Hbv_uc8tlLh8Yy1yTO1LzMiC7-deqmPLxvqerwDJvXIm1dNURipl1LD-rsPjx6cABEYb9mGLez1ejz_r8698iCl4TZm4MbwPhSlem8uWjeIbOTadlpvRv7-NhHBaNdn5t-

mecanismos de Cibersegurança, os quais se destinam a promover a defesa de sistemas informáticos, garantir a segurança de componentes físicos de computadores, proteger dados, entre outros.

A relevância que tem sido conferida a investimentos em Cibersegurança tem consequências no rol de profissionais que integram o *C-Level*[7] de empresas, a ponto de diversas organizações terem inserido no rol de executivos a figura do *chief information security officer* – frequentemente referido como CISO –, o qual consiste em um profissional de nível executivo que se dedica, dentre outras, às seguintes atividades:

> *a)* elaboração, revisão e gestão de políticas corporativas de proteção de dados e dos demais recursos cibernéticos e tecnológicos de uma empresa;
>
> *b)* promover, perante o público interno (e, quando necessário, também o externo) da companhia, iniciativas educacionais relativas à boa execução das políticas corporativas de Cibersegurança;
>
> *c)* planejamento de recuperação de ataques cibernéticos e de incidentes correlatos; e
>
> *d)* investigar incidentes de vazamentos de dados.[8]

Ainda que o fenômeno de inserção do *chief information security officer* tenha se iniciado há mais tempo no exterior, tal figura já é vista também em algumas empresas do Brasil[9], as quais, diante dos riscos decorrentes do uso de dados pessoais em suas

---

9tpiB0SyALgB8RbJtvT_d0jrR_YzPKfKABKcrszDoc0opPhFKAbChlngq9dO_tB2h0L5Ye9If8Zqf0S1IRsMqoBAXKjvICZ1QffDqVNsLcfBB8jnNAqKUOeIYEMdNGrTp2MzXlNr6EoVKmcvpepcN8f3eO1eRPrElmByde6EhVL95fdS8UiHo_5HI0bzk5ZMARhYttfkGkCrPgGZ94dtMm4nvUPxEftrQnSlEUcUPxbYUl9kInmxK4f_ZwDU27wMEX5VXtCkWCSIPzKAriJdCVbE1yXO5yw9zw7Q67l1mBkLdZNdbwBOaLGum7XV3kQCEOezDCf_in7mttwbHjFNXt3vffHXB6YBNIINoj1UM3zWiB70xAfRFzi_T2FcMFm11p_rMkwA3XIRoCGPtMFcaiWYD-isoZtotPmfSzr-0j_0Mz_ELZmsyr0_FeffsoMCpbOZAvRoRpIAP_9MQbchW1ZGVoCfnq83Mtkfhfjrxt0V0px_5yO2EFyGkzZgM2d6Fur_IQ>. Acesso em 12.12.2020.

[7] *C-Level* é um termo de origem estadunidense frequentemente utilizado para designar os profissionais que compõem a diretoria executiva de uma empresa.

[8] KARANJA, Erastus; ROSSO, Mark A. The chief information security officer: an exploratory study. **Journal of international technology and information management.** San Bernardino/EUA, Volume 26, Número 2, 06.01.2017. Disponível em: < https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1299&context=jitim>. Acesso em 12.12.2020.

[9] Conforme pesquisa anexa realizada na plataforma LinkedIn.

atividades e dos novos deveres instituídos no ordenamento jurídico pela Lei Geral de Proteção de Dados, têm efetuado investimentos em segurança, assim como tomado cautelas enviesadas a buscar conformidade com o citado diploma legal.

Além do *chief information security officer,* a vigência da Lei Geral de Proteção de Dados e todas essas circunstâncias deram causa ao surgimento de uma outra categoria profissional relacionada às questões de proteção de dados: o *data protection officer,* que tem sido definido como o profissional chamado pela Lei n. 13.709/2018 de *"encarregado"*[10] e, inclusive, tem seu escopo de atuação mínimo definido no art. 41 da citada legislação.

Toda essa situação de coexistência de práticas empresariais que se valem de dados pessoais e de deveres extrapenais de implementação de mecanismos de segurança[11] parece demonstrar que se valer de dados pessoais como prática empresarial pode se mostrar – em sentido penal – perigoso, ainda que não de modo intrínseco.

É que, ao revés de atividades comerciais intrinsecamente perigosas tais como o transporte de passageiros e a fabricação de armamentos, a prática do uso de dados pessoais em contexto empresarial pode se revelar um perigo a partir de atos de organização dos administradores, os quais podem – a partir de falhas na gestão de funções e tarefas relacionadas à proteção de dados – desencadear riscos antes inexistentes, o que poderá fundamentar posição de garantidor em relação a certos administradores.[12]

Como mencionado, diversas empresas já possuem administradores especificamente designados para zelar pelos dados pessoais detidos pela companhia e,

---

[10] CAMPELLO, Tatiana; MAGRANI, Eduardo; CUNHA, Cecília Almada. Encarregado (data protection officer): os dilemas sobre quem escolher. **Jota.** De 14 de dezembro de 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/data-protection-officer-lgpd-dados-14122020>. Acesso em 14.12.2020.

[11] Os quais muitas vezes não se mostram integralmente satisfatórios, o que agrega a tal coexistência alguns incidentes cibernéticos lesivos aos dados pessoais detidos por empresas.

[12] ESTELLITA, Heloisa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017, p. 130.

ainda que não os possuam, poderão ser garantidores originários quaisquer integrantes de órgãos de administração de uma empresa.[13]

Por conta disso, pretende-se analisar a problemática inerente à viabilidade de se afirmar a punibilidade de dirigentes de empresas que se utilizam de dados pessoais para a execução de seus fins sociais, por ocasião da ocorrência de fatos lesivos relacionados a tais dados pessoais em função de condutas omissivas impróprias.

Para tanto, se recorrerá à narrativa de um caso, com algumas variações, a fim de que problemas específicos sejam analisados, já que parece ser inviável apresentar uma única resposta à problemática acima descrita.

Portanto, em circunstâncias fáticas que serão delineadas na dissertação, mas que dirão respeito a fatos com resultados aparentemente delituosos em razão de violação de dados pessoais detidos por empresas, serão exploradas – possivelmente entre outras – as seguintes variações, com o fito de estressar problemas específicos:

| **Variações** | **Alguns problemas específicos inerentes** |
|---|---|
| 1 - Inexistência de diretoria executiva especializada em proteção de dados, mas com profissional de nível gerencial como *data protection officer.* | Imputação a todos os administradores, sob o fundamento de que são igualmente responsabilizáveis. |
| 2 - Existência de diretor executivo especializado em temas de proteção de dados (CISO) e de profissional de nível gerencial como *data protection officer.* | Restrição de imputação, em razão de departamentalização de deveres. |
| 3 - Existência de diretor executivo especializado em temas de proteção de dados (CISO), de profissional de nível gerencial como *data protection officer* e de contratação de bons prestadores de serviço externos na área de Cibersegurança, para os fins de prover soluções de proteção de dados pessoais. | Restrição de imputação, por conta de delegação de deveres. |

[13] ESTELLITA, Heloisa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017, p. 134.

| | |
|---|---|
| 4 - Existência de diretor executivo especializado em temas de proteção de dados (CISO), de profissional de nível gerencial como *data protection officer* e de contratação de maus prestadores de serviço externos na área de Cibersegurança, para os fins de prover soluções de proteção de dados pessoais. | Extensão de imputação, por força de delegação de dever a terceiro inapto. |

## 2. CONCEPÇÕES DOGMÁTICAS PARA A ABORDAGEM DOS PROBLEMAS E ALGUMAS SOLUÇÕES PROPOSTAS

Como dito anteriormente, a problemática básica do trabalho a ser desenvolvido é inerente à viabilidade de se afirmar a punibilidade de dirigentes de empresas que se utilizam de dados pessoais para a execução de seus fins sociais, por ocasião da ocorrência de fatos lesivos relacionados a tais dados em função de condutas omissivas impróprias.

Nesse primeiro ponto, já existe, entre outras, questão que deverá ser abordada dogmaticamente, que diz respeito à medida da relevância penal dos deveres de organização estabelecidos pela Lei Geral de Proteção de Dados em seu art. 46, que dispõe que os agentes de tratamento de dados devem adotar medidas aptas a garantir a segurança dos dados pessoais contra incidentes problemáticos.

Em relação a isso, impende destacar que os deveres previstos na Lei n. 13.709/2018 são de natureza extrapenal e, embora relevantes, não atribuem aos administradores automaticamente a qualidade de garantidores.[14] Por outro lado, são importantes a ponto de denotar indiciária posição de garante, a qual será certamente afirmada a partir do exame de assunção concreta de tal posição e do escopo de atuação do administrador.[15]

Portanto, aparentemente, embora os supracitados deveres extrapenais previstos na Lei Geral de Proteção de Dados não sejam individualmente aptos a conferir aos administradores a posição de garantidores, referidas obrigações dão conta de que, a partir de suas violações de modo omissivo, os dirigentes envolvidos poderão ser responsabilizados criminalmente por omissão imprópria.

---

[14] BOTTINI, Pierpaolo. **Crimes de omissão imprópria.** São Paulo: Marcial Pons, 2018, p. 134.
[15] ESTELLITA, Heloísa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017, p. 145.

Contudo, é justamente pelo fato de tal solução não oferecer resposta completa e de tal resposta depender da análise de especificidades, que se propõe a análise de um caso concreto a ser narrado, com algumas variações.

Na primeira variação, na qual inexiste diretoria executiva especializada em proteção de dados, poderá ser discutida a concepção de que, a rigor, todos os diretores poderão ser responsabilizados, pois, na medida em que o tratamento de dados é uma atividade perigosa a ponto de demandar observância a deveres extrapenais de cuidado, a empresa acaba por se tornar uma fonte de perigo, o qual deve ser prevenido por seus administradores.[16]

Já na segunda variação, na qual há diretor executivo especializado em temas de proteção de dados (CISO), será possível enfrentar a possibilidade de restrição de responsabilidade penal por omissão imprópria ao citado diretor especializado, vez que, quando existe divisão horizontal de funções, normalmente as obrigações de vigilância de cada diretor acabam restritas a cada um de seus escopos de atuação[17], até porque, mesmo nas situações em que um diretor tem conhecimento de que outro poderá incidir em comportamento delituoso, a princípio não se pode deixar de ter em mente que deve ser demonstrada – a partir de circunstâncias concretas – a possibilidade de o diretor alheio agir.[18]

Por fim, no que tange às duas últimas variações, nas quais se está diante de situação na qual há diretoria especializada em temas de proteção de dados (CISO), mas foi contratada – na variação 3 – assessoria externa satisfatória para prestação de serviços de Cibersegurança destinados à entrega de soluções para proteção de dados pessoais e – na variação 4 – tal assessoria não é satisfatória, será possível discutir questões referentes à possibilidade de a delegação de deveres a terceiros ser um fundamento para afastamento de responsabilidade penal dos dirigentes e, além disso,

---

[16] HILGENDORF, Eric; VALERIUS, Brian. **Direito penal: parte geral.** Tradução de Orlandino Gleizer. 2. ed. São Paulo: Marcial Pons, 2019, p. 341.
[17] ESTELLITA, Heloísa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017, p. 166.
[18] REALE JR., Miguel et. al. **Código penal comentado.** São Paulo: Saraiva, 2017, p. 51.

será igualmente possível abordar a viabilidade de se impor ao delegante um dever de seleção adequada do delegado.[19]

De todo modo, essas variações são apenas provisórias e poderão, para os fins de satisfatória abordagem da problemática, ser revisitadas e incrementadas.

[19] ESTELLITA, Heloísa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017, p. 156.

## 3. BIBLIOGRAFIA PRELIMINAR


BOOKSHEAR, J. Gleen. **Ciência da computação: uma visão abrangente.** Tradução de Eduardo Kessler Piveta. 11. ed. Porto Alegre: Bookshear, 2013.

BOTTINI, Pierpaolo. **Crimes de omissão imprópria.** São Paulo: Marcial Pons, 2018.

CAMARGO, Beatriz Corrêa. **A teoria do concurso de pessoas.** São Paulo: Marcial Pons, 2018.

CAMPELLO, Tatiana; MAGRANI, Eduardo; CUNHA, Cecília Almada. Encarregado (data protection officer): os dilemas sobre quem escolher. **Jota.** De 14 de dezembro de 2020. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/data-protection-officer-lgpd-dados-14122020>. Acesso em 14.12.2020.

ESTELLITA, Heloisa. **Responsabilidade penal de dirigentes de empresas por omissão: estudo sobre a responsabilidade omissiva imprópria de dirigentes de sociedades anônimas, limitadas e encarregados de cumprimento por crimes praticados por membros da empresa.** São Paulo: Marcial Pons, 2017.

GRECO, Luís et. al. **Autoria como domínio do fato: estudos introdutórios sobre o concurso de pessoas no direito penal brasileiro.** São Paulo: Marcial Pons, 2014.

GRECO, Luís. **Problemas de causalidade e imputação objetiva nos crimes omissivos impróprios.** São Paulo: Marcial Pons, 2018.

GRUS, Joel. **Data science do zero: primeiras regras com o Python.** Tradução de Welington Nascimento. Rio de Janeiro: Alta Books, 2016.

HILGENDORF, Eric; VALERIUS, Brian. **Direito penal: parte geral.** Tradução de Orlandino Gleizer. 2. ed. São Paulo: Marcial Pons, 2019.

KARANJA, Erastus; ROSSO, Mark A. The chief information security officer: an exploratory study. **Journal of international technology and information management.** San Bernardino/EUA, Volume 26, Número 2, 06.01.2017. Disponível em: < https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1299&context=jitim>. Acesso em 12.12.2020.

KUNER, Cristopher et. al. The rise of cybersecurity and its impact on data protection. **International data privacy law,** Oxford/Reino Unido, Volume 7, Número 2, 2017. Disponível em: < https://watermark.silverchair.com/ipx009.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAApwwggKYBgkqhkiG9w0BBwagggKJMIIChQIBADCCAn4GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM39lvvKON-O3bkFWVAgEQgIICT6RLpBga4kkeXO-hrLZEYAHuqKjZ_R7SYF5741Zla18Af1C3HsWH5BGrbaD0Uw5pt2JSMFL1PoCd_qy28X0Ecu7_k63e4KqCLA7nlJpexRtiR9ZwctpT4Gc_hOagKFYLId9y_6WC5lAfW4Hbv_uc8tlLh8Yy1yTO1LzMiC7-deqmPLxvqerwDJvXIm1dNURipl1LD-rsPjx6cABEYb9mGLez1ejz_r8698iCl4TZm4MbwPhSlem8uWjeIbOTadlpvRv7-NhHBaNdn5t-9tpiB0SyALgB8RbJtvT_d0jrR_YzPKfKABKcrszDoc0opPhFKAbChlngq9dO_tB2h0L5Ye

9If8Zqf0S1IRsMqoBAXKjvICZ1QffDqVNsLcfBB8jnNAqKUOeIYEMdNGrTp2MzXlNr6EoVKmcvpepcN8f3eO1eRPrElmByde6EhVL95fdS8UiHo_5HI0bzk5ZMARhYttfkGkCrPgGZ94dtMm4nvUPxEftrQnSlEUcUPxbYUl9kInmxK4f_ZwDU27wMEX5VXtCkWCSIPzKAriJdCVbE1yXO5yw9zw7Q67l1mBkLdZNdbwBOaLGum7XV3kQCEOezDCf_in7mttwbHjFNXt3vffHXB6YBNIINoj1UM3zWiB70xAfRFzi_T2FcMFm11p_rMkwA3XIRoCGPtMFcaiWYD-isoZtotPmfSzr-0j_0Mz_ELZmsyr0_FeffsoMCpbOZAvRoRpIAP_9MQbchW1ZGVoCfnq83Mtkfhfjrxt0V0px_5yO2EFyGkzZgM2d6Fur_IQ>. Acesso em 12.12.2020.

PUPPE, Ingeborg. **Estudos sobre imputação objetiva e subjetiva no direito penal.** Tradução de Luís Greco et. al. São Paulo: Marcial Pons, 2019.

REALE JR., Miguel et. al. **Código penal comentado.** São Paulo: Saraiva, 2017.

RENZIKOWSKI, Joachim. **Direito penal e teoria das normas. Estudos críticos sobre as teorias do bem jurídico, da imputação objetiva e do domínio do fato.** Tradução de Alaor Leite et. al. São Paulo: Marcial Pons, 2017.

ROXIN, Claus. **Novos estudos de direito penal.** Tradução de Luís Greco et. al. São Paulo: Marcial Pons, 2014.

SCHÜNEMANN, Bernd. **Estudos de direito penal, direito processual penal e filosofia do direito.** Tradução de Adriano Teixeira et. al. São Paulo: Marcial Pons, 2013.

SIEGEL, Eric. **Análise preditiva: o poder de prever quem vai clicar, comprar, mentir ou morrer.** Tradução de Wendy Campos. Rio de Janeiro: Alta Books, 2017.

TAVARES, Juarez. **Teoria dos crimes omissivos.** São Paulo: Marcial Pons, 2018.

What we learned from infamous hacking incidents. **Maryville University,** Town and Country/EUA, data de publicação não informada, Disponível em: <https://online.maryville.edu/blog/what-we-learned-from-infamous-hacking-incidents/>. Acesso em 12/12/2020.