V. 12 N. 2
MAI-AGO 2016

ISSN 2317-6172

Revista DIREITO GV

Recebido: 10.03.2015
Aprovado: 04.04.2016

DOI: http://dx.doi.org/10.1590/2317-6172201622

Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas

COMBATING ILLEGITIMATE BANK TRANSFERS THROUGH THE INTERNET IN PORTUGUESE LAW: BETWEEN DOMESTIC EXPERIENCES AND CONCERTED GLOBAL POLICIES

Pedro Miguel Alves Ribeiro Correia[1]
e Inês Oliveira Andrade de Jesus[2]

Resumo
O estudo que conduziu a este artigo atenta na forma como a lei e o direito português proporcionam mecanismos que permitem levar a cabo políticas de combate às transferências bancárias ilegítimas com recurso à Internet. A abordagem metodológica consistiu não apenas numa análise rigorosa do enquadramento jurídico da questão mas também numa análise estatística de dados correspondentes aos crimes de burla informática e nas comunicações registados pelas autoridades policiais. É apresentada argumentação a favor de que as transferências bancárias ilegítimas com recurso à Internet devam ser consideradas fraudes ao invés de burlas, e são apresentados dados que corroboram a ideia de que, nos próximos cinco a dez anos, este problema se tornará muitíssimo relevante para o sistema judiciário e para a sociedade como um todo. Finalmente, e como parte do esforço em prol de uma política internacional concertada, sugere-se que estudos futuros alarguem a investigação da temática apresentada a outras regiões geográficas, de que é exemplo a América do Sul e, em particular, a países com grande proximidade a Portugal, como é o caso do Brasil.

Palavras-chave
Burla informática; transferências bancárias ilegítimas; política de combate; Internet; direito português.

Abstract
The study that led to this article verified how Portuguese law provides mechanisms that allow combat policies on illegitimate bank transfers using the Internet. The methodological approach consisted not only on a rigorous analysis of the legal framework of the issue but also on a statistical analysis of data corresponding to computer and communications fraud crimes registered by the police authorities. It is defended that illegitimate bank transfers through the Internet should be considered a fraud instead of a swindle, as well as presented data supporting the idea that, in the next five to ten years, this problem will become extremely important for the judiciary and for society as a whole. Finally, and as part of the effort for a concerted international policy, it is suggested that future studies extend the research themes here presented to other geographical regions, of which South America is an example and, in particular, to countries with close proximity to Portugal, as is the case of Brazil.

Keywords
Computer fraud; illegitimate bank transfers; combat policy; Internet; Portuguese law.

1 Universidade de Lisboa
Lisboa - Portugal

2 Universidade de Lisboa
Lisboa - Portugal

Introdução

Não obstante os benefícios proporcionados diariamente aos indivíduos das sociedades ocidentalizadas, a sociedade de informação levanta desafios e temores relevantes à segurança e privacidade dos indivíduos (a este respeito ver, por exemplo, Correia e Jesus, 2013; 2014). Na verdade, uma das desvantagens que esta nova sociedade de informação acarreta é, precisamente, a vulnerabilidade dos sistemas e das redes informáticas que a suportam.

Um dos exemplos, particularmente dramático, dessa vulnerabilidade materializa-se nas transferências bancárias pela Internet à revelia dos titulares das contas.

O acesso às contas bancárias através da Internet é um serviço que os bancos passaram a prestar há relativamente pouco tempo (*on line banking*) (FILIPKOWSKI, 2008). Convém clarificar que o termo *e-banking* designa os "bancos virtuais", ou seja, os "bancos que apenas existem na Internet e que não têm balcões em local algum", e que é a expressão *home banking* que concretiza o "acesso por via informática a contas e movimentos em bancos tradicionais" (VERDELHO, 2003, p. 350).

Para Maria Raquel Guimarães, o *home banking* ou banco ao domicílio "veio revolucionar a conceção clássica do modo de funcionamento das instituições bancárias, permitindo aos seus clientes realizar as operações tradicionalmente levadas a cabo nos balcões das suas sucursais nos seus próprios domicílios ou escritórios, com a consequente descentralização dos serviços prestados" (GUIMARÃES, 1999, p. 41-42). Esta autora afirma ainda que

> em todos os sistemas de *home banking* o utilizador tem a possibilidade de realizar operações bancárias em tempo real, na medida em que tem acesso direto ao computador do seu banco, que imediatamente debita ou credita a conta do seu cliente, consoante o sentido das ordens emitidas por este [...] a segurança destes serviços é normalmente garantida através da existência de várias combinações numéricas do conhecimento exclusivo do utilizador, que funcionam como códigos secretos de acesso ao sistema, e que terão que ser marcados no teclado do equipamento utilizado para comunicar com a instituição bancária respetiva [...] no entanto, estes dispositivos de segurança revelam-se por vezes insuficientes, principalmente quando é utilizada uma rede de telecomunicações, na medida em que não é impossível a um terceiro intercetar uma comunicação deste tipo e decifrar os códigos marcados, para posteriormente aceder ao sistema. (GUIMARÃES, 1999, p. 43-44).

Por seu turno, para Rita Coelho Santos, "o '*home banking*' consiste no serviço à distância, prestado por instituições bancárias, que permite aos clientes efetuar, eletronicamente, transferências patrimoniais (entre contas bancárias), a partir de sua casa, mediante o estabelecimento de uma ligação telefônica, via *modem*, entre o seu computador pessoal e o terminal da respetiva entidade financeira" (SANTOS, 2005, p. 195-196). No seguimento, a autora conclui que estes serviços, "a que se acede através de um código de acesso secreto", podem "conduzir a situações

de verdadeira delapidação patrimonial": "são cada vez mais numerosos os casos de 'pirataria informática', caracterizada pelo acesso, mediante apropriação ilegítima da '*password*' alheia, a uma conta bancária de terceiro, a partir da qual se operam transferências eletrónicas de fundos" (SANTOS, 2005, p. 195-196).

Por norma, os burlões informáticos enviam *e-mails* em nome do banco a solicitar dados bancários (*phishing*), nomeadamente, o código de acesso à conta bancária pela Internet, e efetuam, depois disso, transferências monetárias sem a autorização dos titulares das contas. No entanto, em alguns casos, os piratas conseguem mesmo entrar diretamente no acesso à conta pela Internet (*hacking*) (WODA, 2006). Note-se que, nestes casos, as transferências são operadas pelos sistemas bancários legais, havendo, porém, sistemas paralelos e ilegais, como o Hawala (WODA, 2006).

A Internet, oferecendo, designadamente, o anonimato, a celeridade das transações e a possibilidade de atividades transfronteiriças (FILIPKOWSKI, 2008), é o palco ideal para comportamentos ilícitos. As transferências bancárias pela Internet tornaram-se o mecanismo preferido dos agentes criminosos, uma vez que, a par das referidas vantagens, aliam a dificuldade de controlo ao grande número de operações diárias, assim como a falta de uniformidade dos regimes legais à facilidade de blindagem dos dados e à capacidade de obscurecer o usufruto das quantias transferidas (HUGHES, 1992).

Importa, pois, atentar na forma como a lei e o direito proporcionam mecanismos que permitem levar a cabo políticas de combate a estas ilicitudes. Este artigo fez incidir o seu foco no caso de estudo português.

1 Materiais e métodos

A forma como, neste artigo, o tema das transferências bancárias ilegítimas pela Internet foi tratado seguiu duas abordagens metodológicas distintas.

A primeira dessas abordagens consistiu numa análise rigorosa do enquadramento jurídico desta questão à luz do direito português: um caso de estudo. Neste caso de estudo, é dado particular relevo à discussão se este tipo de atividade ilícita deve ser classificada como burla, como é atualmente o caso.

Esta metodologia foi complementada por uma segunda, que se materializou uma análise estatística (descritiva, mas também projetiva) de dados associados aos crimes registados pelas autoridades policiais (Polícia Judiciária, Polícia de Segurança Pública, Guarda Nacional Republicana, Autoridade de Segurança Alimentar e Econômica, Polícia Marítima, Polícia Judiciária Militar, Serviço de Estrangeiros e Fronteiras, e Autoridade Tributária e Aduaneira), em Portugal, com particular destaque para os processos correspondentes ao crime de burla informática e nas comunicações. Foram analisados dados estatísticos referentes a este tipo de crimes entre os anos de 1998 a 2015, inclusive.

Os dados que serviram de base à análise estatística apresentada neste trabalho (bem como

muitíssimos outros dados sobre o sistema judiciário português) foram recolhidos, tratados e disponibilizados a título gratuito pela Direção-Geral da Política de Justiça, do Ministério da Justiça de Portugal, e podem ser encontrados em: www.siej.dgpj.mj.pt.

2 Resultados

2.1 Enquadramento jurídico português: aspetos gerais

No direito português (PORTUGAL, 2015), estas transferências bancárias não consubstanciam crimes de furto (artigo 203º do Código Penal), abuso de confiança (artigo 205º do Código Penal) ou roubo (artigo 210º do Código Penal). Na verdade, as quantias monetárias transferidas não encaixam no conceito de coisa móvel, não se preenchendo, por isso, os tipos patrimoniais clássicos referidos.

O furto, o abuso de confiança e o roubo exigem, com efeito, a subtração ou a apropriação de uma coisa móvel. Ora, a moeda escritural, objeto da transferência bancária, não é uma coisa que pode, por natureza, ser subtraída ou apropriada. Trata-se de uma forma de moeda impalpável, intocável e intangível, concretizada em dados informáticos com valor econômico. Na verdade, "o patrimônio já não se esgota no domínio das coisas corpóreas ou materializáveis, fungíveis ou não": "a *res* volatizou-se" (SANTOS, 2005, p. 21-22).

Note-se que as transferências bancárias ilegítimas pela Internet também não preenchem o tipo legal de burla, segundo o qual (artigo 217º, n. 1, do Código Penal) "quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa" (PORTUGAL, 2015).

Atentando nos casos em que os burlões enviam um *e-mail* a pedir os dados bancários do titular da conta e, depois de saberem o código de acesso à conta bancária através da Internet, transferem uma quantia monetária sem a sua autorização, verifica-se que o elemento típico consistente na prática, pelo burlado, de atos causadores de prejuízo patrimonial não está preenchido. Na verdade, o *e-mail* enviado sob a capa do banco pode ser considerado como um facto provocado astuciosamente. Além disso, o titular da conta é efetivamente induzido em erro por esse *e-mail*. No entanto, não é a cedência do código de acesso pelo titular, mas antes a transferência pelo burlão que provoca o prejuízo patrimonial. Logo, o crime de burla não se mostra completo. Pode ainda afirmar-se que os computadores não são suscetíveis de erro ou engano, uma vez que essa é uma característica especificamente humana.

O crime de burla surgiu para penalizar as formas de captação do alheio através de meios ardilosos. Em face da utilização dos computadores e da Internet, o legislador sentiu necessidade de introduzir um novo tipo de crime: o crime de burla informática (artigo 221º, n. 1, do Código Penal). Não é difícil, portanto, entender o acesso ilegítimo a contas bancárias

através da Internet e as transferências de dinheiro realizadas por esse meio à revelia dos titulares das contas como preenchendo o referido crime (PORTUGAL, 2015).

2.2 Enquadramento jurídico português: aspetos históricos

O problema da delinquência informática foi abordado, pela primeira vez, no Projeto da Comissão de Revisão do Código Penal, em 1990. A ata n. 39 da Comissão de Revisão relata o debate sobre o tema (PORTUGAL, 1993).

Figueiredo Dias, que iniciou a discussão com "a questão fundamental (e prévia) sobre a qual a Comissão teria que tomar posição" – a criação ou não, no Código Penal, de tipos de crimes informáticos, defendeu, primeiramente, "que a criminalidade informática deveria ser objeto de uma lei especial, não devendo ser prevista pelo Código qualquer nova incriminação neste domínio" (PORTUGAL, 1993, p. 453). José Manuel Meirim, portador da posição do Procurador-Geral da República, Manso Preto e Costa Andrade pronunciaram-se no mesmo sentido, entendendo que os crimes informáticos deveriam constar de legislação extravagante. Lopes Rocha e Ferreira Ramos, seguindo o mesmo entendimento, destacaram o facto de esta matéria integrar o direito penal econômico, pelo que não deveria ser incluída no Código Penal, mas consagrada em lei especial. Sousa e Brito, por seu turno, entendeu que existia "um tipo suficientemente esclarecido para merecer a inclusão no Código – a burla informática" (PORTUGAL, 1993, p. 453). No seguimento deste entendimento, sublinhou-se que "na atual Reforma foi aceite como política orientadora a não necessidade extrema de inserir no Código toda a incriminação de mancha de não punibilidade existente", adotando-se "a via da convivência do Código Penal com legislação penal avulsa", e apelou-se a "um debate alargado, inclusive na sede própria, Assembleia da República", uma vez que as instâncias políticas devem estar cientes da "necessidade de intervenção legislativa neste domínio" (PORTUGAL, 1993, p. 453-454). Após esta primeira discussão, Figueiredo Dias concluiu que o Código Penal não deveria conter "articulados esgotantes sobre a criminalidade informática", que "esta decisão deve ser comunicada às instâncias políticas dado haver toda a vantagem (e mesmo urgência) em que se preparem as medidas legislativas necessárias" e que "houve uma sugestão para integrar a burla informática nos crimes patrimoniais" (PORTUGAL, 1993, p. 454).

Na segunda fase do debate, o mesmo Figueiredo Dias "manifestou que não se oporia à consagração da burla informática" e lançou a discussão sobre a "questão da receção" deste tipo de crime (PORTUGAL, 1993, p. 455). Sousa e Brito, que propôs a inclusão da burla informática no Código Penal, "observou que ao recolher este tipo não o faz no quadro da criminalidade informática, mas sim como uma espécie de burla, para a qual não existe incriminação ao contrário do que já ocorre quer na Alemanha quer na Áustria" (PORTUGAL, 1993, p. 455).

A comissão acabou por consagrar este tipo de crime no Código Penal.

2.3 Crime de burla informática: um problema de enquadramento jurídico?

A Lei n. 109/91, de 17 de agosto, Lei da Criminalidade Informática, aprovada em 1991,

acolheu os principais ilícitos informáticos, mas deixou de fora o crime de burla informática (PORTUGAL, 1991). Este crime só viria a ser previsto em 1995 no Código Penal (PORTUGAL, 1995). Em 2009, a grande reforma legislativa que culminou com a aprovação da Lei n. 109/2009, de 15 de setembro, Lei do Cibercrime (PORTUGAL, 2009), não contemplou este tipo de crime, que continua no Código Penal, com a mesma previsão típica.

Na verdade, o artigo 2º, alínea 1, da Lei n. 35/94, de 15 de setembro, que autorizava o governo a rever o Código Penal, estabelecia o objetivo de "introduzir novos tipos de crime, face à revelação de novos bens jurídicos ou de novas modalidades de agressão ou de perigo ou à necessidade de respeitar compromissos internacionais assumidos ou em vias de o serem, como [...] a burla informática" (PORTUGAL, 1994). Ora, este tipo de ilícito foi efetivamente introduzido pela reforma de 1995, levada a efeito pelo Decreto-Lei n. 48/95, de 15 de março. Este diploma legal apresentou "um conjunto significativo, se bem que limitado, de propostas de neocriminalização", como a burla informática, e destacou a opção de "deixar fora do Código Penal a punição de muitas condutas cuja dignidade penal é hoje já pacífica e consensual, mas que razões de técnica legislativa aconselham que constituam objeto de legislação extravagante" (PORTUGAL, 1995), como é o caso da criminalidade informática. Com a reforma de 1998, levada a cabo pela Lei n. 65/98, de 2 de setembro, o artigo 221º, que tinha como epígrafe burla informática e previa no n. 1 este tipo de ilícito, foi epigrafado de burla informática e nas comunicações, sendo adicionado um n. 2 para consagrar este último tipo de burla (PORTUGAL, 1998).

A Lei da Criminalidade Informática, que viria a ser aprovada em 1991, não acolheu o crime de burla informática, um tipo indiscutivelmente informático (PORTUGAL, 1991). Este tipo só seria consagrado no Código Penal, em 1995, apesar do preâmbulo do diploma da reforma se inclinar para a inclusão fora do mesmo (PORTUGAL, 1995). Esta inserção tem gerado uma grande discussão na doutrina, havendo opiniões contra e a favor. Contudo, parecem avolumar-se os argumentos que indiciam que a inserção da burla informática no Código Penal foi um erro do legislador, mantido até aos dias de hoje.

Durante aproximadamente quatro anos, não existiu qualquer norma incriminadora para as manipulações informáticas com repercussões patrimoniais. Além disso, de 1995 em diante, a burla informática, ao ser inserida no Código Penal, não ficou sujeita ao regime geral de responsabilidade das pessoas coletivas e equiparadas. Isto implicou, pelo artigo 11º do Código Penal então em vigor (PORTUGAL, 1995), a exclusão dessa responsabilidade. Apesar de o artigo 11º do Código Penal ter sido alterado pela Lei n. 59/2007, de 4 de setembro (PORTUGAL, 2007), anulando as críticas relativamente ao diferente regime de responsabilidade dos crimes informáticos, realce-se que este regime permaneceu inalterado durante doze anos. Até 2007, a responsabilidade das pessoas coletivas e equiparadas estava excluída, pelo que havia uma grande falha na punibilidade da burla informática e uma incongruência e desadequação das leis penais. Podemos até afirmar que a inserção "desatenta" da burla informática no Código Penal provocou "cisões arbitrárias" no ordenamento penal português (MENDES, 2003, p. 396).

Já em 1990, a Comissão de Revisão do Código Penal apontava para a criação de uma lei especial para os crimes informáticos (PORTUGAL, 1993). No entanto, foi defendido que a chamada burla informática deveria ser inserida no Código Penal, uma vez que era uma "espécie de burla", mas esta exceção carece de fundamento, pois, como se irá demonstrar de seguida, a burla informática não deve ser considerada como uma subespécie desse crime basilar.

2.4 Crime de burla informática: enquadramento alternativo

É importante notar que a burla informática, para além de ser um crime informático, é um crime pertencente ao direito penal econômico, pelo que faria todo o sentido a sua consagração num diploma avulso e com um regime de responsabilidade penal dos entes coletivos. Na verdade, é compreensível a posição de Lopes Rocha quando defende que

> a burla informática, como os restantes crimes informáticos, é frequentemente obra de agentes que pertencem à categoria criminológica do *col blanc* ou do *white-collar*, cujos comportamentos não raro se desenvolvem no interior das sociedades e empresas, enquanto seus órgãos ou representantes, atuando em nome delas e no interesse coletivo. (ROCHA, 1993, p. 70).

Por outro lado, tal como foi referido, a razão apontada para a inserção da burla informática no Código Penal prende-se com o facto de esta ser uma "espécie de burla". No entanto, a burla informática não é uma verdadeira burla, uma vez que não segue o *iter criminis* da burla clássica nem adota os seus elementos essenciais. Isto porque a burla informática não contempla a astúcia, o erro ou engano e a prática de atos pelo burlado, exigidos na burla tradicional. A ideia de que a burla informática não constitui uma verdadeira burla é reforçada pelo teor dos trabalhos preparatórios da reforma de 1995 do Código Penal (PORTUGAL, 1995), e o próprio desenho legal da burla informática evidencia que não se está perante uma verdadeira burla. Apesar do *nomen iuris*, da inserção sistemática, do bem jurídico protegido e da moldura penal apontarem para a qualificação da burla informática como uma "espécie de burla", reitera-se que não se trata de uma burla em sentido próprio e técnico. O mesmo é dizer que o crime de burla informática traz muitas especificidades que o descaracterizam totalmente como uma espécie de burla, não devendo ser assim qualificado.

Este entendimento é defensável, não obstante o bem jurídico protegido ser, primacialmente, o patrimônio. Este, apesar de ser o bem jurídico protegido em primeira linha, não é o único a ser tutelado: a burla informática também protege o regular funcionamento dos sistemas e das redes informáticas.

A própria denominação do ilícito não é a mais correta. Deveria ter-se acolhido a designação: fraude informática. Esta mesma designação foi reiterada na Convenção sobre Cibercrime, recentemente ratificada por Portugal e que dá corpo à nova Lei do Cibercrime (PORTUGAL,

2009). Não só a designação de fraude informática seria mais sensata, como este tipo de crime estaria melhor enquadrado nesta recente lei.

2.5 Crime de burla informática: detalhes e especificidades

A burla informática é um novo tipo de crime que, por isso mesmo, não se coaduna com a designação de "espécie de burla". Entre a burla e a burla informática não poderá haver nenhuma relação de especialidade, uma vez que a burla informática não acolhe os elementos típicos essenciais da burla tradicional. Com efeito, nas relações de especialidade, o tipo especial espelha o tipo fundamental, contendo um elemento adicional que o especializa. Ora, na burla informática, o que temos são elementos totalmente inovadores.

Seja como for, a burla informática adota o nome de burla e está no Código Penal no título respeitante aos crimes contra o patrimônio. Entrando na caracterização propriamente dita do crime de burla informática plasmado no artigo 221º, n. 1, do Código Penal (PORTUGAL, 2015), e começando pelo bem jurídico protegido, saliente-se que a generalidade da doutrina portuguesa defende que o bem jurídico protegido é o patrimônio. O crime de burla informática, previsto nesse mesmo artigo do Código Penal, está inserido no Título II da Parte Especial, que acolhe os crimes contra o patrimônio, e dentro deste Título, no Capítulo III, que reúne os crimes contra o patrimônio em geral. Daí deriva a tendência para considerar o patrimônio globalmente considerado como o bem jurídico protegido. Quanto à noção de patrimônio entenda-se, para efeitos desta discussão, o "conceito jurídico-penal": "[...] conjunto de todas as 'situações' e 'posições' com valor econômico, detidas por uma pessoa e protegidas pela ordem jurídica ou, pelo menos, cujo exercício não é desaprovado por essa mesma ordem jurídica", e "[...] merecedoras de tutela à luz da particular teleologia do direito criminal" (COSTA, 1999, p. 279-282).

Porém, este tipo de crime também visa tutelar um interesse coletivo. O crime de burla informática protege não só o patrimônio, mas também o regular funcionamento dos sistemas e das redes informáticas. Este entendimento também tem sido defendido por alguma jurisprudência (Acórdão do Supremo Tribunal de Justiça, 30-3-2000, processo 00P3101, Rel. Leal Henriques; Acórdão do Supremo Tribunal de Justiça, 14-7-2004, processo 04P3287, Rel. Santos Carvalho; Acórdão do Supremo Tribunal de Justiça, 6-10-2005, processo 05P2253, Rel. Simas Santos; Acórdão do Tribunal da Relação de Lisboa, 3-5-2007, processo 10042/06-5, Rel. Ana Sebastião). Efetivamente, "existem normas relativamente às quais, não obstante a sua localização sistemática, se reconhece protegerem bens jurídicos diversos daqueles que identificam a sua concreta integração no Código Penal" (SANTOS, 2005, p. 217). Além disso, "poderá um só tipo legal proteger 'especialmente', mais do que um bem jurídico" (Acórdão do Supremo Tribunal de Justiça, 6-10-2005, processo 05P2253, Rel. Simas Santos, p. 10). Logo, não é de estranhar que as novas tecnologias também sejam tuteladas pelo preceito em análise.

Na verdade, as transferências bancárias ilegítimas pela Internet visam dados informáticos com valor patrimonial, designadamente, as novas formas de moeda escritural e eletrônica. Os

dados informatizados com valor econômico são, assim, o novo bem jurídico e o novo objeto do crime, imaterial e de tipo informático.

A norma do artigo 221º, n. 1, do Código Penal (PORTUGAL, 2015), prevê um crime comum, pelo que "pode ser cometido por qualquer pessoa, não obstante a sua prática encontrar-se socialmente referenciada a indivíduos com particulares conhecimentos técnicos" (SANTOS, 2005, p. 239). Carlos Gameiro, entendendo que a figura dos "piratas informáticos" traz associada alguma experiência e investimento na área tecnológica, defende que "agressores com conhecimentos técnicos limitados" também podem "efetivar ataques cada vez mais bem-sucedidos", pois "estão disponibilizadas muitas ferramentas com fácil consulta e execução" (GAMEIRO, 2007, p. 130). Também Jaime Fernandes afirma que "podem ser suficientes conhecimentos rudimentares de informática"; para além disso,

> se é certo serem a maioria dos sujeitos ativos destes crimes oriundos ou relacionados com o próprio ambiente em que a fraude decorre [...], não é menos verdade que a utilização da informática, com a suscetibilidade que proporciona de manipulação de dados à distância, pode fazer surgir situações criminais em que o agente seja absolutamente estranho ao mesmo. (FERNANDES, 1990, p. 49).

Afigura-se como razoável a posição de que os burlões informáticos possuem, na sua maioria, conhecimentos técnicos aprofundados, não só para praticarem o ilícito, mas também para limparem o rasto do mesmo. Na realidade, o processo das fraudes é camuflado e os criminosos dificilmente são identificados. Não obstante, o desenho legal do ilícito permite o seu cometimento por qualquer pessoa, pelo que o crime em análise é, indiscutivelmente, um crime comum.

Nos termos do artigo 13º e do artigo 221º do Código Penal (PORTUGAL, 2015), a burla informática é um crime doloso, não admitindo punição a título de negligência. Além disso, é um crime intencional, que exige a verificação de uma intenção específica de enriquecimento ilegítimo. Isso mesmo está bem explanado num aresto do Tribunal da Relação de Lisboa (Acórdão do Tribunal da Relação de Lisboa, 24-1-2007, processo 5990/2006-3, Rel. Pedro Mourão). Quanto ao enriquecimento, este "pode traduzir-se num aumento patrimonial, na diminuição de débitos ou na poupança de despesas" (SANTOS, 2005, p. 266). Joana Rita Ferreira acrescenta que o enriquecimento ilegítimo corresponde "objetiva ou subjetivamente a qualquer direito" (FERREIRA, 2001, p. 53). Saliente-se, não obstante, que a norma incriminadora prescreve a intenção de enriquecimento ilegítimo, mas não exige a verificação de um efetivo enriquecimento para a consumação do crime, pelo que este se considera perpetrado no momento em que ocorre o prejuízo patrimonial. A burla informática é, por isso, um crime de resultado parcial ou cortado. Este é também o entendimento da jurisprudência portuguesa (Acórdão do Tribunal da Relação de Coimbra, 15-5-2002, processo 1318/02, Rel. Barreto do Carmo; Acórdão do Supremo Tribunal de Justiça, 20-9-2006,

processo 06P1942, Rel. Henriques Gaspar; Acórdão do Tribunal da Relação de Lisboa, 24-1-2007, processo 5990/2006-3, Rel. Pedro Mourão; Acórdão do Supremo Tribunal de Justiça, 5-11-2008, processo 08P2817, Rel. Henriques Gaspar).

Na realidade, a burla informática é um crime de dano, que pressupõe a efetiva lesão do patrimônio, e um crime material ou de resultado, que exige a verificação de um prejuízo patrimonial. Este entendimento tem sido frequentemente expresso, em Portugal, na jurisprudência (Acórdão do Tribunal da Relação de Coimbra, 15-5-2002, processo 1318/02, Rel. Barreto do Carmo; Acórdão do Tribunal da Relação de Lisboa, 24-1-2007, processo 5990/2006-3, Rel. Pedro Mourão; Acórdão do Supremo Tribunal de Justiça, 5-11-2008, processo 08P2817, Rel. Henriques Gaspar).

Por conseguinte, as vítimas deste crime são as pessoas que suportam tal prejuízo, podendo coincidir ou não com a entidade titular do sistema informático. Há um atentado direto ao patrimônio: o agente utiliza o material informático para executar o crime, sem a mediação de outra pessoa em estado de erro ou engano. Isso mesmo está explicado num aresto do Tribunal da Relação de Coimbra (Acórdão do Tribunal da Relação de Coimbra, 15-5-2002, processo 1318/02, Rel. Barreto do Carmo). Assim, na burla informática, não há qualquer artifício fraudulento, uma vez que o crime é perpetrado por intermediação de um sistema informático que, como é óbvio, não se consegue enganar. Só os seres humanos são suscetíveis de engano, pelo que não é coerente atribuir essa suscetibilidade a uma máquina.

Saliente-se, adicionalmente, que o crime em análise é de execução vinculada. Na verdade, a norma incriminadora procede a uma enumeração dos modos de cometimento do ilícito. No entanto, a cláusula geral inserta no final dá aos modos previstos um carácter meramente exemplificativo. Logo, o meio informático é vinculado, mas o modo de comissão fica na discricionariedade do agente. Isso mesmo está plasmado em vários arestos (Acórdão do Tribunal da Relação de Coimbra, 15-5-2002, processo 1318/02, Rel. Barreto do Carmo; Acórdão do Tribunal da Relação de Lisboa, 16-3-2004, processo 9743/2003-5, Rel. Pulido Garcia; Acórdão do Supremo Tribunal de Justiça, 12-7-2006, processo 06P2032, Rel. Santos Cabral; Acórdão do Supremo Tribunal de Justiça, 20-9-2006, processo 06P1942, Rel. Henriques Gaspar; Acórdão do Supremo Tribunal de Justiça, 5-12-2007, processo 07P3864, Rel. Santos Monteiro; Acórdão do Supremo Tribunal de Justiça, 5-11-2008, processo 08P2817, Rel. Henriques Gaspar).

Por outro lado, a corrente doutrinal segundo a qual a interferência no resultado de tratamento de dados é a consequência necessária dos modos de execução do crime descritos na norma, e não uma das formas de comissão do crime afigura-se como sustentável. Na realidade, a estruturação incorreta de programa informático, a utilização incorreta ou incompleta de dados, a utilização de dados sem autorização e a intervenção por qualquer outro modo não autorizada no processamento são as formas de cometimento do crime que levam à interferência no resultado de tratamento de dados. Esta interferência não é um modo de perpetrar o ilícito, a par com as outras formas, mas o corolário dessas formas. Este entendimento parece ser

adotado pelo Supremo Tribunal de Justiça quando afirma que "a perspetiva geral de enquadramento do tipo remete, especificamente, para a interferência e a intromissão ilegítimas, abusivas ou intencionalmente incorretas em dados e/ou programas informáticos" (Acórdão do Supremo Tribunal de Justiça de 20-9-2006, processo 06P1942, Rel. Henriques Gaspar, p. 9; Acórdão do Supremo Tribunal de Justiça, 5-11-2008, processo 08P2817, Rel. Henriques Gaspar, p. 10).

A primeira modalidade é a estruturação incorreta de programa informático. Esta manipulação do programa informático

> [...] consiste na modificação da totalidade ou de parte das operações lógicas que o integram, por forma a que as novas instruções não coincidam com as inicialmente concebidas pelo seu titular ou determinem resultados não previstos, objetivamente contrários aos fins do respetivo programa [...] pode concretizar-se na sua total ou parcial reestruturação, no aditamento, alteração ou supressão de fases do programa, na introdução de novas instruções (por forma a evitar o exame do sistema de segurança ou a permitir a realização de determinadas operações, contrárias aos comandos do programa original), na alteração das condições de validade do controlo ou na alteração do '*running time*' do programa [...] (SANTOS, 2005, p. 244-245).

Esta autora sublinha que "a referência expressa à 'estruturação incorreta de programa', a par do 'uso de dados incorretos ou incompletos', apenas cumpre uma função de aclaração do texto da norma, pois os programas traduzem-se, igualmente, em um conjunto de dados" (SANTOS, 2005, p. 246).

A segunda modalidade típica de cometimento do crime de burla informática é a utilização incorreta ou incompleta de dados: "[...] pode consistir no aditamento, na alteração ou na supressão de dados, bem como na introdução de dados que deveriam ser submetidos ao tratamento informático ou, não obstante a sua introdução, não são sujeitos à necessária laboração". Os dados incorretos são definidos como "[...] aqueles que não se encontram conformes à verdade, isto é, dados que não traduzem, ou traduzem erroneamente, a realidade dos factos a que respeitam" e os dados incompletos como "[...] aqueles que, não obstante encerrarem um conjunto verdadeiro, não permitem reconhecer, de modo suficiente, a realidade [...] que representam, porquanto não a refletem inteiramente" (SANTOS, 2005, p. 246-247). A autora alerta ainda que "os dados que constituem o objeto da ação do agente podem encontrar-se armazenados no interior do sistema informático ou em memória externa, funcionalmente ligada a determinado sistema informático" (SANTOS, 2005, p. 247-248).

O terceiro modo de execução previsto no artigo 221º, n. 1, do Código Penal (PORTUGAL, 2015) é a utilização de dados sem autorização. Esta "consiste no uso de dados cujo acesso se encontra vedado a terceiros ou em violação dos limites dos poderes de utilização

conferidos, verificando-se um aproveitamento da disponibilidade daqueles para executar operações não permitidas" (SANTOS, 2005, p. 253). Note-se que

> a utilização não autorizada de dados verifica-se nos casos de uso ilegítimo, por terceiro, de "caixas-automáticas", do sistema de "*telebanking*" ou "*home banking*" ou dos designados "*POSs*", através dos quais, mediante a utilização do código de acesso pessoal alheio, se efetua indevidamente um pagamento ou realiza uma transferência monetária, ultrapassando o crédito do titular do cartão, ou o saldo disponível da respetiva conta bancária, consoante as circunstâncias concretas do caso (SANTOS, 2005, p. 256).

A quarta e última modalidade típica de cometimento do crime de burla informática é a intervenção por qualquer outro modo não autorizada no processamento de dados. Rita Coelho Santos volta a frisar que "o legislador" quis "evitar lacunas de punibilidade", introduzindo, por isso, esta "cláusula de segurança" que é "[...] uma fórmula suficientemente ampla, com significado residual, aí se incluindo outras formas de manipulação informática não subsumíveis às previsões alternativas anteriores, ou cuja subsunção resultaria duvidosa, face aos princípios da tipicidade e da segurança jurídica" (SANTOS, 2005, p. 258-259). Algumas condutas que podem ser incluídas nesta cláusula aberta abrangem: "a interferência no processo mecânico do sistema informático (manipulação de consola)" ou "do *hardware*"; "a conduta do agente que aciona uma 'caixa-automática' através de um programa de computador ilegalmente obtido para esse efeito"; "as interferências não autorizadas no sistema informático [...] operadas diretamente ou através de um sistema telemático"; "as interferências no sistema informático que não correspondem à intromissão direta nos dados (expressamente contemplada pela fórmula legal), mas que neles se repercutem, em termos de alterar o resultado que se observaria se não ocorresse a referida manipulação"; "as interferências em sistema telemático que permitam aceder a um determinado sistema informático de tratamento e/ou armazenamento de dados ou que permitam intervir diretamente sobre os dados ('em trânsito'), destinados a integrar determinado sistema informático" (SANTOS, 2005, p. 259-260). Esta autora também chama a atenção para o facto de a Internet poder consistir um meio através do qual é possível interferir, de modo não autorizado, no processamento de dados.

Frise-se que existe uma relação de causa-efeito ou de causalidade: a manipulação informática tem que ser a causa adequada da interferência no resultado de tratamento de dados e esta interferência tem que ser a causa do prejuízo patrimonial. A lei, no desenho típico do crime, prescreve que o agente interfira no resultado de tratamento de dados. Ora, essa interferência só poderá ocorrer na fase de entrada dos dados. As manipulações que ocorram na fase de saída não constituem burlas informáticas, mas sim burlas clássicas.

Quanto à questão da admissibilidade da burla informática por omissão, é meritório o entendimento de que este ilícito pode ser cometido por omissão, desde que sobre o agente

recaia um dever jurídico que pessoalmente o obrigue a evitar o resultado, nos termos do artigo 10º, n. 2, do Código Penal (PORTUGAL, 2015).

Caso seja possível provar a intenção específica de enriquecimento ilegítimo, o efetivo prejuízo patrimonial e a interferência no resultado de tratamento de dados através de uma das modalidades típicas, o agente pode ser punido, alternativamente, com uma pena de prisão até três anos ou com uma multa. No entanto, como defendido anteriormente, esta norma incriminadora, além de proteger o patrimônio, tutela, de forma colateral, o bom funcionamento dos sistemas e das redes informáticas. Por este motivo, considera-se válido o entendimento que a moldura penal deveria ser alargada.

A burla informática prevista no n. 1 do artigo 221º (PORTUGAL, 2015) é um crime semipúblico. Por conseguinte, o início do procedimento criminal depende da apresentação de queixa do ofendido ou de outra pessoa a quem a lei confira esse direito, nos termos dos artigos 113º a 116º do Código Penal (PORTUGAL, 2015) e do artigo 49º do Código de Processo Penal (PORTUGAL, 2014). Note-se ainda que o n. 3 do artigo 221º (PORTUGAL, 2015) consagra a punibilidade da burla informática na forma tentada e que a norma do n. 5 do artigo 221º (PORTUGAL, 2015) prevê a burla informática qualificada. Uma burla informática qualificada é um crime público, ou seja, o procedimento criminal não está condicionado, na sua tramitação, em momento algum, por atos de outros sujeitos processuais. Assim, o Ministério Público pode promover o processo penal ao abrigo do artigo 48º do Código de Processo Penal. Este entendimento já foi defendido pelo Supremo Tribunal de Justiça (Acórdão do Supremo Tribunal de Justiça, 24-9-1998, processo 98P556, Rel. Sá Nogueira).

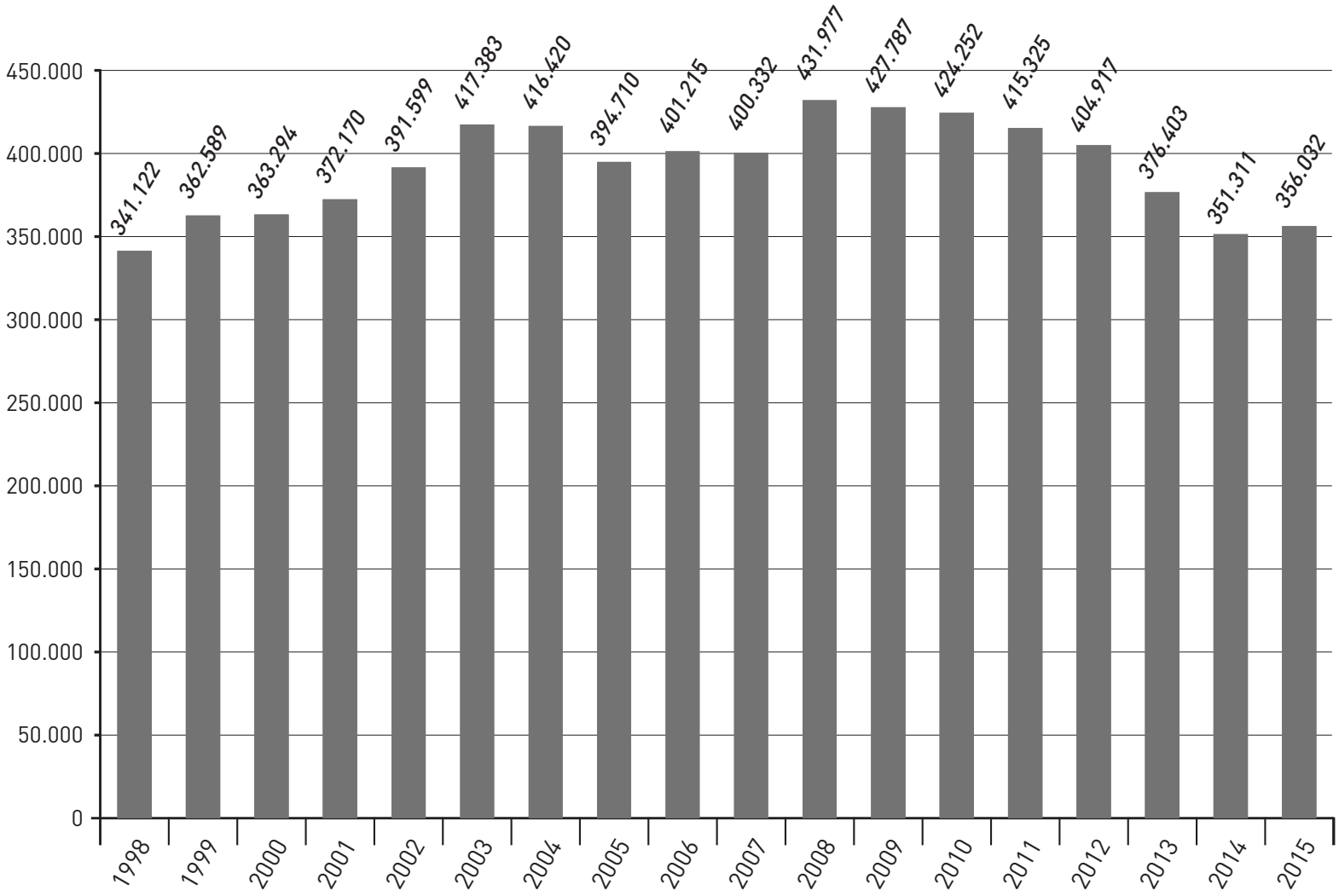
Esta análise dos detalhes e especificidades do preceito em análise termina com a constatação de que o seu último número determina a aplicação do regime plasmado no artigo 206º (PORTUGAL, 2015). Ora, de acordo com este preceito, nos casos de restituição ou reparação, o tribunal pode decretar a extinção da responsabilidade criminal ou a atenuação especial da pena.

2.6 Crime de burla informática: potencial bomba relógio com relevo social

A importância e o relevo social de um adequado enquadramento jurídico das transferências bancárias ilegítimas pela Internet tornam-se particularmente notórios quando se observa a evolução dos crimes de burla informática e nas comunicações ao longo dos últimos anos e o potencial impacto que o crescimento deste fenômeno pode acarretar para o funcionamento do sistema judiciário como um todo.

A Figura 1 apresenta a evolução do número de crimes registados pelas autoridades policiais, em Portugal, entre os anos de 1998 e 2015.

FIGURA 1 – **Número de crimes registados pelas autoridades policiais, em Portugal, 1998 a 2015**

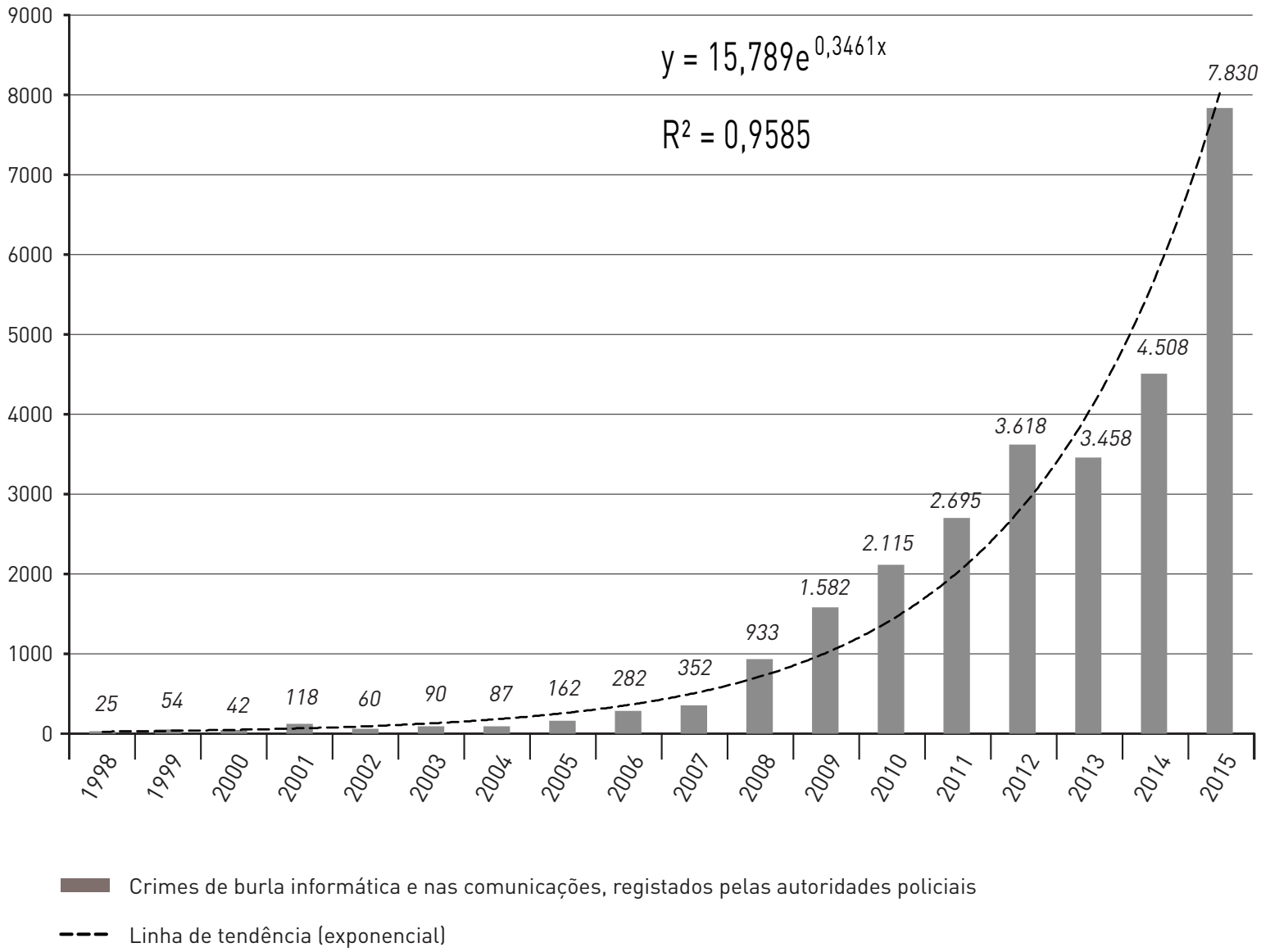


Fonte: elaboração própria com base em dados da Direção-Geral da Política de Justiça, Ministério da Justiça de Portugal.

É possível observar uma tendência para a estabilidade dos valores em que, apesar das flutuações periódicas, se registou um aumento muito moderado de cerca de 4,4% entre os valores correspondentes ao ano de 1998 e os valores correspondentes ao ano de 2015. De facto, face ao máximo registado em 2008, o número de crimes registados, em 2015, diminuiu cerca de 17,6%. Esta diminuição dos crimes registados é uma boa aproximação para o fenômeno de fundo, em curso na sociedade portuguesa ao longo dos últimos 10 anos, e que consiste numa redução gradual mas persistente da criminalidade em geral.

Porém, a realidade associada aos crimes de burla informática e nas comunicações, registados pelas autoridades policiais, no mesmo período, conta uma história bem diferente (Figura 2).

FIGURA 2 – **Número de crimes de burla informática e nas comunicações registados pelas autoridades policiais, em Portugal, 1998 a 2015**



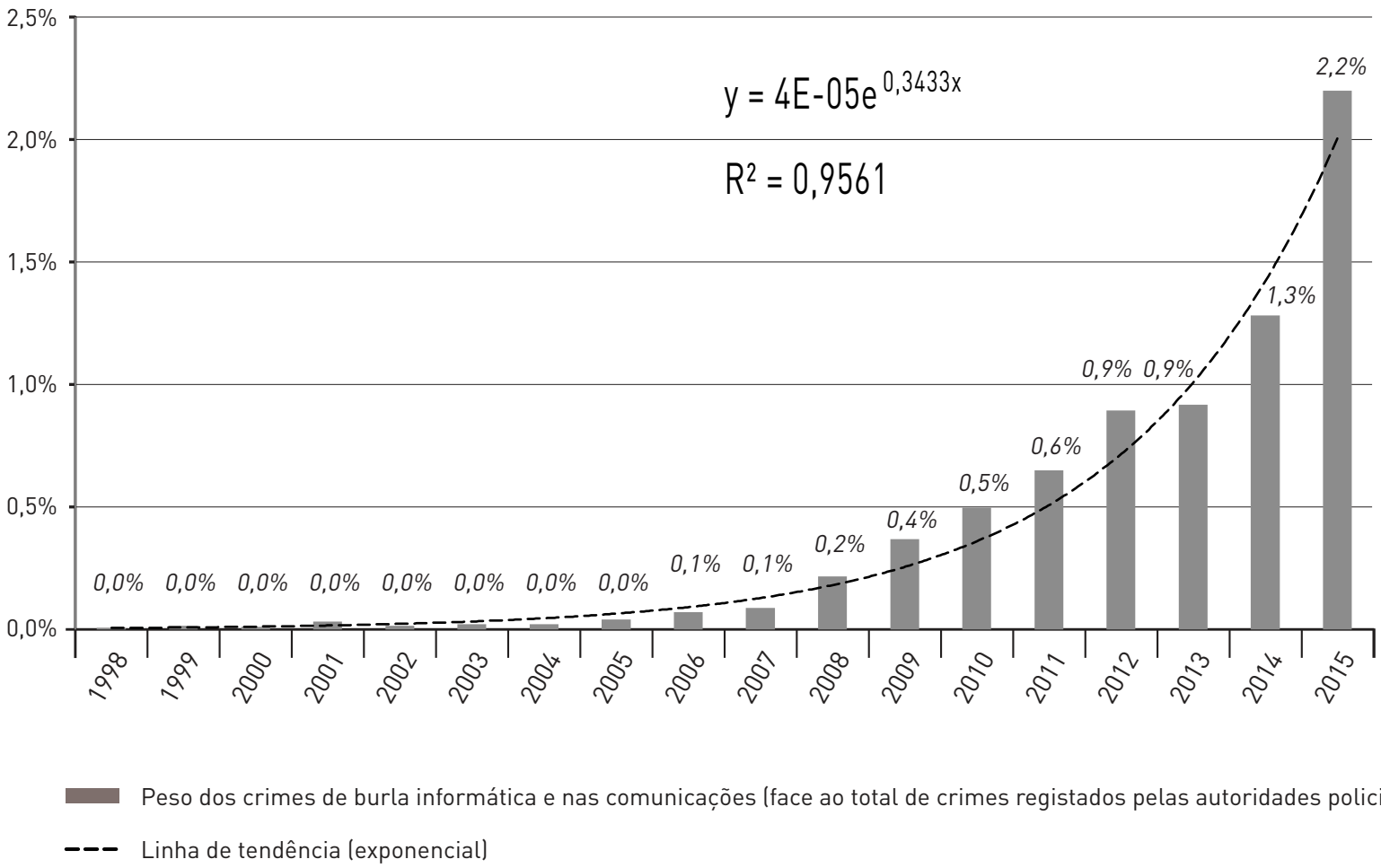
Fonte: elaboração própria com base em dados da Direção-Geral da Política de Justiça, Ministério da Justiça de Portugal.

Apesar de o volume de crimes ser ainda relativamente reduzido, é possível verificar um crescimento muitíssimo intenso deste tipo de crimes ao longo dos últimos anos. O número de crimes de burla informática e nas comunicações registados pelas autoridades policiais, em 2015, foi 312 vezes superior ao valor registado em 1998 (um aumento de 31220%). Este valor ilustra, de forma categórica, o motivo pelo qual o fenômeno é bem aproximado por uma linha de tendência exponencial (algo que é deixado bem claro por um coeficiente de determinação (R^2) de 0,9585) associada a um aumento que ronda os 40% ao ano.

A convergência dos fenômenos ilustrados nos gráficos 1 e 2: tendência continuada para o decréscimo da criminalidade geral e tendência para o crescimento explosivo do crime de burla

informática e nas comunicações (respetivamente), redundam num efeito também exponencial de crescimento do peso deste tipo particular de processos (Figura 3).

FIGURA 3 – **PESO DOS CRIMES DE BURLA INFORMÁTICA E NAS COMUNICAÇÕES REGISTADOS PELAS AUTORIDADES POLICIAIS, EM PORTUGAL, 1998 A 2015**



Fonte: elaboração própria com base em dados da Direção-Geral da Política de Justiça, Ministério da Justiça de Portugal.

Este aumento de peso pode facilmente ser entendido como um aumento da relevância social das questões associadas à burla informática e nas comunicações, como é o caso das transferências bancárias ilícitas pela Internet. De um valor infinitesimal e perfeitamente negligenciável, em 1998, passou-se a um valor mensurável de 2,2% em 2015. Apesar de, em termos absolutos, o aumento ser nominalmente reduzido (aumento de 2,2 pontos percentuais), em termos relativos trata-se de um aumento que ronda os 30008,4%. Este valor pode ser entendido como uma medida do ganho de importância que o problema assumiu na sociedade portuguesa contemporânea.

Discussão e conclusões

Nas transferências bancárias pela Internet à revelia dos titulares das contas, o agente, com a intenção de obter uma vantagem patrimonial ilegítima, prejudicando o titular da conta, interfere no resultado de tratamento de dados através da utilização de dados bancários sem autorização, pelo que se preenche o crime de burla informática.

A doutrina portuguesa pouco tem abordado estas novas formas de defraudar o patrimônio alheio. Para a jurisprudência, este tipo de crime não é totalmente desconhecido. Na realidade, o Tribunal da Relação de Coimbra já foi chamado a pronunciar-se sobre a legalidade do levantamento do sigilo bancário no caso de transferências bancárias ilegítimas pela Internet (Acórdão do Tribunal da Relação de Coimbra, 2-6-2009, processo 325/08.7JALRA-A.C1, Rel. Fernando Ventura). O tribunal, numa perspetiva de ponderação dos interesses conflituantes, decidiu que o banco terá que revelar a identificação dos titulares da conta e os movimentos ulteriores à transferência. Na página três desse mesmo aresto, o Tribunal da Relação de Coimbra defende que o crime de burla informática atinge "a sua consumação com o crédito na conta beneficiária da transferência".

No ordenamento jurídico-penal português, a burla informática é um crime econômico que usa as novas tecnologias de informação e comunicação. É um crime econômico, porque encaixa no perfil da criminalidade económica. E é um crime informático, na exata medida em que usa a informática no cometimento do facto ilícito.

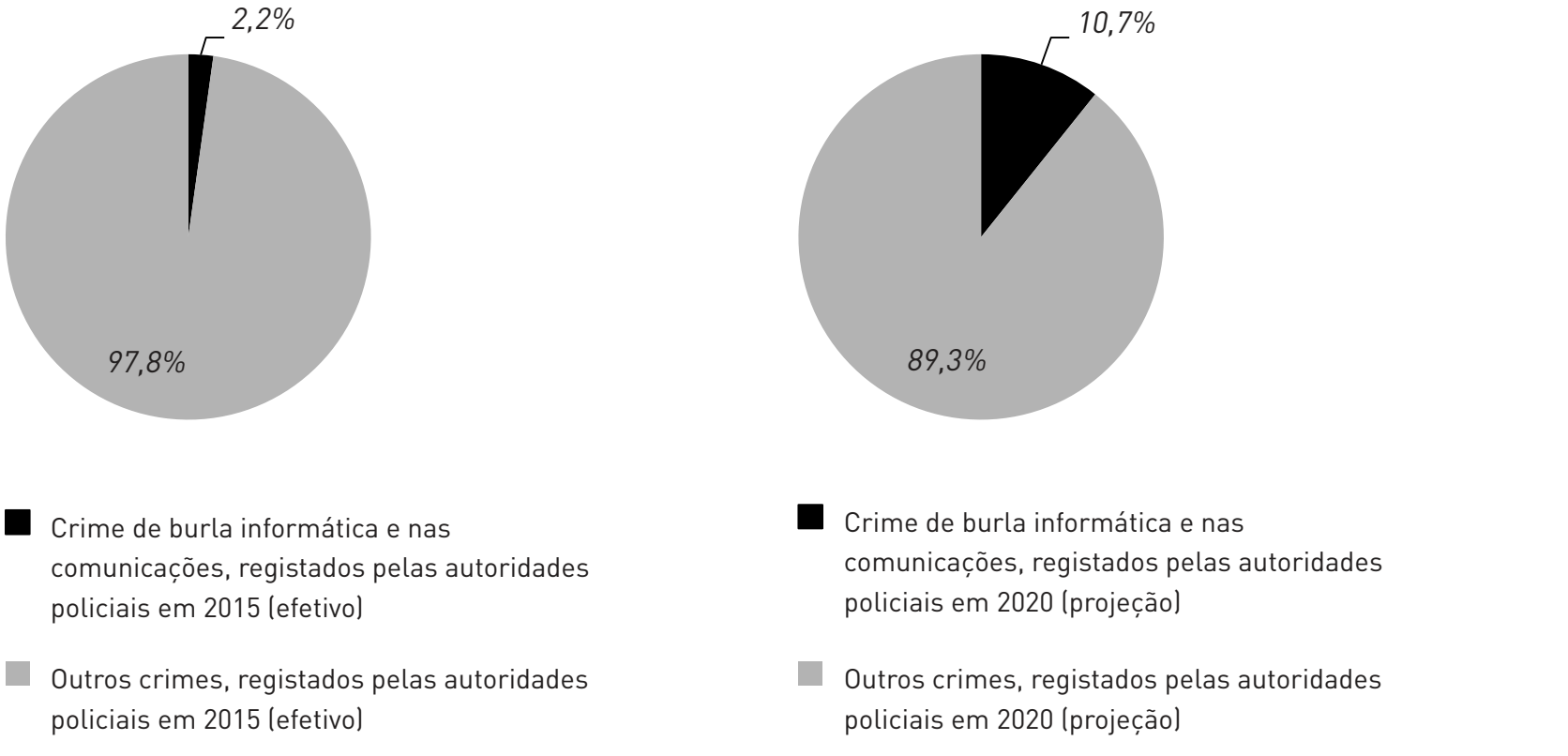
É defensável que este crime deveria ter sido incluído na Lei da Criminalidade Informática, em 1991 (PORTUGAL, 1991), e que deveria estar, atualmente, na Lei do Cibercrime (PORTUGAL, 2009). Também é sustentável que este mesmo crime deveria ser identificado com a figura da fraude, ao invés de ser denominado de burla, uma vez que não acolhe os elementos deste tipo clássico, não constituindo uma burla em sentido próprio.

Não obstante, em Portugal, a burla informática foi inserida no Código Penal (PORTUGAL, 2015) como uma "espécie de burla". É este o quadro legal em vigor, tendo sido o objeto do estudo apresentado neste artigo. É possível interpretar a previsão legal constante do n. 1 do artigo 221º do Código Penal, respeitante à burla informática e nas comunicações (PORTUGAL, 2015), como protetora do patrimônio, mas também do regular funcionamento dos sistemas e das redes informáticas. É de sublinhar que o patrimônio, que é o bem jurídico e o objeto do crime, é incorpóreo e intangível, uma vez que se concretiza em dados informatizados com valor econômico. De acordo com a norma incriminadora, a burla informática é um crime comum, doloso e intencional. Além disso, é um crime de dano, material ou de resultado parcial ou cortado, e de execução vinculada. Mais ainda, há uma relação de causalidade entre a manipulação informática e a interferência no resultado de tratamento de dados e entre esta interferência e o prejuízo patrimonial: a consumação dá-se com o crédito na conta beneficiária da transferência.

Conclui-se, pois, que não há erro ou engano nem qualquer artifício fraudulento que levem a atos causadores de prejuízo por parte da vítima e que possam levar a considerar que esta foi burlada.

Ao problema do enquadramento jurídico adequado, acresce a questão do peso crescente deste tipo de atividades ilegais. Usando a tendência identificada na evolução do peso relativo dos crimes de burla informática e nas comunicações no total de crimes registados pelas autoridades policiais (Figura 3), e assumindo um cenário conservador (isto é, um cenário em que, ao contrário do que se verificou entre 2008 e 2015, o número total de crimes registados, se mantém constante em vez de decrescer), é possível efetuar uma projeção do peso que este tipo de crimes representará num futuro não muito distante. A análise da Figura 4 permite verificar que em apenas 5 anos (isto é, tão cedo quanto 2020), o peso deste tipo de crimes superará já os 10% (estimando-se um aumento entre 2015 e 2020 de cerca de 8,5 pontos percentuais).

FIGURA 4 – **Peso do crime de burla informática e nas comunicações no total de crimes crimes registados pelas autoridades policiais, 2015 (valor efetivo) e 2020 (valor projetado)**



Fonte: elaboração própria.

O forte crescimento estimado para o peso deste tipo de crimes peca, provavelmente, por defeito. Isto porque, não só se tem verificado na sociedade portuguesa uma tendência para o decréscimo dos demais tipos de crime, tal como referido anteriormente, como acima de tudo, a hegemonia crescente da sociedade de informação e dos sistemas e das redes informáticas que lhes estão associadas, e das quais a sociedade está cada vez mais dependente para sobreviver,

traz implícito um crescimento deste tipo de fenômenos ilícitos a uma escala que atualmente não é possível conceber e que escapa a qualquer projeção, por mais cuidado que nesta se incuta. Seja como for, a tendência para que este tipo de crime adquira um peso cada vez mais dominante parece incontornável: um sinal dos tempos.

Por tudo isto, e para terminar, cabe uma última nota a sublinhar que este tipo de ilícito é de difícil deteção e prova, pelo que o novo regime processual e de cooperação internacional introduzido pela Lei do Cibercrime (PORTUGAL, 2009) assume uma importância determinante na política de combate às transferências bancárias ilegítimas pela Internet. A política de combate às transferências bancárias ilegítimas tem, necessariamente, de passar a ser um esforço internacional, que ditará, cada vez mais, a troca de informações (HUGHES, 1992), mormente entre as autoridades policiais e judiciárias dos vários países. O tempo confirmá-lo-á.

Como parte desse esforço e dessa política internacional concertada, sugere-se que estudos futuros alarguem a investigação da temática apresentada neste artigo (quer da vertente jurídica, quer da vertente estatística) a outras regiões geográficas, de que é exemplo a América do Sul e, em particular, a países que partilham laços de proximidade com Portugal bastante acentuados, como é o caso do Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

CORREIA, Pedro M. A. R.; JESUS, Inês O. A. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. *Direito, Estado e Sociedade*, n. 43, p. 135-161, 2013. Disponível em: <http://direitoestadosociedade.jur.puc-rio.br/media/43artigo6.pdf>. Acesso em: 18 fev. 2015.

_____. A proteção de dados pessoais no espaço de liberdade, de segurança e de justiça da União Europeia. *Revista Brasileira de Segurança Pública*, v. 8, n. 2, p. 18-30, 2014. Disponível em: <http://www.forumseguranca.org.br/storage/download//rbsp_ed15final-baixa_18.09_.pdf>. Acesso em: 18 fev. 2015.

COSTA, A. M. A. Capítulo III – Dos Crimes Contra o Patrimônio em Geral. In: DIAS, Jorge de F. (Dir.). *AAVV – Comentário Conimbricense do Código Penal, Parte Especial*, n. 2. Coimbra: Coimbra Editora, 1999.

FERNANDES, Jaime N. da S. O crime informático. *Revista de Investigação Criminal*, n. 33, p. 41-56, 1990.

FERREIRA, J. R. *Perspetiva genérica sobre a criminalidade informática no Direito português*. 2001. Tese (Mestrado em Direito) – Universidade de Lisboa, Lisboa, 2001.

FILIPKOWSKI, Wojciech. Cyber laundering: an analysis of typology and techniques. *International Journal of Criminal Justice Sciences*, v. 3, n. 1, p. 15-27, 2008.

GAMEIRO, C. O risco da informação em ambiente eletrónico. In: *AAVV – Estudos de Direito e Segurança*. Coimbra: Almedina, 2007.

GUIMARÃES, Maria Raquel. *As transferências eletrónicas de fundos e os cartões de débito*: alguns problemas jurídicos relacionados com as operações de levantamento de numerário e de pagamento por meios eletrónicos. Coimbra: Almedina, 1999.

HUGHES, Sarah Jane. Policing money laundering through funds transfers: A critique of regulation under the bank secrecy act. *Indiana Law Journal*, v. 67, n. 2, p. 283-330, 1992.

WODA, Krzysztof. Money Laundering Techniques with Electronic Payment Systems. *Information & Security – An International Journal*, v. 18, p. 27-47, 2006.

MENDES, Paulo de S. A responsabilidade de pessoas coletivas no âmbito da criminalidade informática em Portugal. In: *Separata de Direito da Sociedade de Informação*, n. 4. Coimbra: Coimbra Editora, 2003.

PORTUGAL. Lei n. 109/91, de 17 de agosto, que aprova a Lei da Criminalidade Informática. *Diário da República*, I Série-A, n. 188, p. 4202-4205, de 17 de agosto de 1991.

_____. Comissão de Revisão do Código Penal Código Penal / Atas e projeto da Comissão de Revisão. Lisboa: Rei dos Livros, 1993.

_____. Lei n. 35/94, de 15 de setembro, que autoriza o Governo a rever o Código Penal. *Diário da República*, I Série-A, n. 214, p. 5510-5552, de 15 de setembro de 1994.

_____. Decreto-Lei n. 48/95, de 15 de março, que aprova o Código Penal. *Diário da República*, I Série-A, n. 63, p. 1350-1416, de 15 de março de 1995.

_____. Lei n. 65/98, de 2 de setembro, que altera o Código Penal. *Diário da República*, I Série-A, n. 202, p. 4572-4578, de 2 de setembro de 1998.

_____. Lei n. 59/2007, de 4 de setembro, que aprova a vigésima terceira alteração ao Código Penal, aprovado pelo Decreto-Lei n. 400/82, de 23 de setembro. *Diário da República*, 1ª série, n. 170, p. 6181-6258, de 4 de setembro de 2007.

_____. Lei n. 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, transpondo para a

ordem jurídica interna a Decisão Quadro n. 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. *Diário da República*, 1ª série, n. 119, p. 6319-6325, de 15 de setembro de 2009.

_____. Lei Orgânica n. 2/2014, de 6 de agosto, que aprova o Regime do Segredo de Estado, procede à vigésima primeira alteração ao Código de Processo Penal e à trigésima primeira alteração ao Código Penal e revoga a Lei n. 6/94, de 7 de abril. *Diário da República*, 1ª série, n. 150, p. 4074-4078, de 6 de agosto de 2014.

_____. Lei Orgânica n. 1/2015, de 8 de janeiro, que aprova a primeira alteração ao Regime do Segredo de Estado, aprovado pela Lei Orgânica n. 2/2014, de 6 de agosto, e trigésima quinta alteração ao Código Penal. *Diário da República*, 1ª série, n. 5, p. 206-209, de 8 de janeiro de 2015.

ROCHA, M. A. L. A Lei da Criminalidade Informática (Lei n. 109/91 de 17 de agosto) – Génese e Técnica Legislativa. *Legislação, Cadernos de Ciência de Legislação, Informática Jurídica e Direito da Informática*, n. 8, Lisboa, Instituto Nacional da Administração, 1993.

SANTOS, Rita C. *O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos*. Coimbra: Coimbra Editora, 2005.

VERDELHO, Pedro. Cibercrime. In: *AAVV – Direito da Sociedade de Informação*, n. 4. Coimbra: Coimbra Editora, 2003.

Jurisprudência

Acórdão do Supremo Tribunal de Justiça, 5-11-2008, processo 08P2817, Rel. Henriques Gaspar.

Acórdão do Supremo Tribunal de Justiça, 5-12-2007, processo 07P3864, Rel. Santos Monteiro.

Acórdão do Supremo Tribunal de Justiça, 6-10-2005, processo 05P2253, Rel. Simas Santos.

Acórdão do Supremo Tribunal de Justiça, 12-7-2006, processo 06P2032, Rel. Santos Cabral.

Acórdão do Supremo Tribunal de Justiça, 14-7-2004, processo 04P3287, Rel. Santos Carvalho.

Acórdão do Supremo Tribunal de Justiça, 20-9-2006, processo 06P1942, Rel. Henriques Gaspar.

Acórdão do Supremo Tribunal de Justiça, 24-9-1998, processo 98P556, Rel. Sá Nogueira.

Acórdão do Supremo Tribunal de Justiça, 30-3-2000, processo 00P3101, Rel. Leal Henriques.

Acórdão do Tribunal da Relação de Coimbra, 2-6-2009, processo 325/08.7JALRA-A.C1, Rel. Fernando Ventura.

Acórdão do Tribunal da Relação de Coimbra, 15-5-2002, processo 1318/02, Rel. Barreto do Carmo.

Acórdão do Tribunal da Relação de Lisboa, 3-5-2007, processo 10042/06-5, Rel. Ana Sebastião.

Acórdão do Tribunal da Relação de Lisboa, 16-3-2004, processo 9743/2003-5, Rel. Pulido Garcia.

Acórdão do Tribunal da Relação de Lisboa, 24-1-2007, processo 5990/2006-3, Rel. Pedro Mourão.

Pedro Miguel Alves Ribeiro Correia

Doutorado em Ciências Sociais na Especialidade de Administração Pública pela Universidade Técnica de Lisboa (UTL). Licenciado em Estatística e Gestão de Informação pela Universidade Nova de Lisboa (NOVA). Professor do Instituto Superior de Ciências Sociais e Políticas (ISCSP) da Universidade de Lisboa (ULisboa). Coordenador do Observatório Nacional de Administração Pública (ONAP). Investigador integrado no Centro de Administração e Políticas Públicas (CAPP), ISCSP-Ulisboa. Consultor da Direção-Geral da Política de Justiça (DGPJ) do Ministério da Justiça de Portugal.

pcorreia@iscsp.ulisboa.pt

Inês Oliveira Andrade de Jesus

Doutoranda em Administração Pública na Universidade de Lisboa (ULisboa). Mestre em Direito pela Universidade Nova de Lisboa (NOVA). Licenciada em Direito pela Universidade Nova de Lisboa (NOVA). Consultora da Direção-Geral da Política de Justiça (DGPJ) do Ministério da Justiça de Portugal.

ines.o.jesus@dgpj.mj.pt