Clusters de Percepções sobre cibersegurança e cibercriminalidade em Portugal e as suas implicações para a implementação de políticas públicas nesse domínio

Clusters of perceptions about cybersecurity and cyber criminality in Portugal and their implications for the implementation of public policies in that domain

Pedro Miguel Ribeiro Alves Correia[1]
Susana Isabel da Silva Santos[2]
João Abreu de Faria Bilhim[3]

Resumo

Neste texto são abordadas questões relativas à definição e implementação de políticas públicas em matéria de cibersegurança e cibercrime em Portugal. Os principais objetivos consistem na identificação de *clusters* de percepções dos cidadãos face à atuação do Estado, nesta problemática, e na análise das implicações da existência desses agrupamentos para as políticas públicas. Foi utilizada uma amostra constituída por 1.168 inquiridos. A aplicação sucessiva de análises estatísticas (modelo de equações estruturais, análise fatorial de componentes principais e análise de *clusters* através do método hierárquico) permitiu identificar cinco *clusters* de cidadãos com sensibilidades diferenciadas face aos instrumentos de políticas públicas. Sugere-se que estudos futuros repliquem e aprofundem esta investigação nos países de língua portuguesa e que seja dada ênfase ao papel do dualismo legalidade-moralidade no mecanismo de formação das percepções dos indivíduos.

Palavras-chave: Políticas Públicas. Cibersegurança. Cibercriminalidade. Estado. Portugal.

[1] Doutorado em Ciências Sociais na Especialidade de Administração Pública pela Universidade Técnica de Lisboa (UTL). Professor de Administração Pública no Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa (ULisboa). Consultor da Direção-Geral da Política de Justiça do Ministério da Justiça de Portugal. Coordenador do Observatório Nacional de Administração Pública (ONAP). Investigador Integrado no Centro de Administração e Políticas Públicas (CAPP). *E-mail*: pcorreia@iscsp.ulisboa.pt
[2] Mestranda em Gestão e Políticas Públicas pelo Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa (ULisboa). *E-mail*: susanaissantos@gmail.com
[3] Doutor em Ciências Sociais na Especialidade de Sociologia pela Universidade Técnica de Lisboa (UTL). Investigador Integrado do Centro de Administração e Políticas Públicas (CAPP). *E-mail*: bilhim@iscsp.ulisboa.pt

Abstract

This text addresses issues relating to the definition and implementation of public policies on matters of cyber security and cybercrime, in Portugal. The main objectives are the identification of clusters of citizens' perceptions towards the State action, concerning this subject, and the analysis of the implications of the existence of such groups for public policy. A sample of 1,168 respondents is used. The successive application of statistical analysis (structural equations model, factor analysis of principal components and cluster analysis using the hierarchical method) allowed the identification of five clusters of citizens with differentiated sensitivities regarding public policy instruments. Future studies, it is suggested, should replicate and deepen this research in Portuguese-speaking countries and greater emphasis should be given to the role of the legality-morality dualism in the individuals' perceptions shaping mechanism.

Keywords: Public Policy. Cybersecurity. Cyber criminality. State. Portugal.

Introdução

A atividade dos serviços de informações conheceu desenvolvimentos importantes na Europa durante os séculos XVIII e XIX. Inicialmente, teve por base os intuitos de defesa militar e de segurança interna como instrumentos de guerra ou como forma repressiva de manutenção de regimes políticos (CARVALHO, 2009). Atualmente as tecnologias de informação e comunicação (TIC) funcionam como catalisador de informação, negócios e suporte tecnológico de serviços e infraestruturas, quer no setor público, quer no setor privado. Este paradigma, marcado pela vulgarização de aparelhos digitais, pela informatização de dados e pelo funcionamento em rede, resulta numa convergência de fatores que favorecem o surgimento de ocorrências ilícitas ou criminosas.

A fragilidade destas estruturas coloca em risco não só o funcionamento da administração pública (por exemplo, na comunicação interministerial ou nas plataformas *on-line* para utilização pelo cidadão), mas também a segurança no setor empresarial e dos próprios indivíduos. As consequências da criminalidade associada a este tipo de sistemas pode ter, inclusivamente, implicações ao nível dos sistemas fiduciários (ANDERSON et al., 2013). Posto isto, torna-se imperativo que o Estado, naquilo que é a sua jurisdição em segurança, garanta não só a proteção dos seus próprios sistemas e estruturas, mas também a utilização segura das novas tecnologias por parte dos seus cidadãos (NUNES, 2012).

A abordagem do cibercrime, segundo a lógica das teorias de governança, respeita a multiplicidade de agentes e instituições, sejam eles públicos ou privados, que participam na elaboração e execução de políticas públicas com vista ao combate deste fenômeno. Esta realidade representa um reinventar da ação do Estado e contribui para o estabelecimento de novos paradigmas no que diz respeito a questões como a *accountability* e a satisfação dos cidadãos.

O cibercrime, sendo um tema relativamente recente, apesar das projeções que indiciam que este irá assumir, nos próximos anos, um peso proeminente no total de crimes praticados (CORREIA; JESUS, 2016), reúne ainda poucos estudos, sobretudo no que diz respeito aos tópicos da ação e das funções do Estado. É particularmente evidente a ausência de estudos sobre as percepções dos diversos grupos de utilizadores, de acordo com as suas características sociodemográficas e a utilização que fazem dos sistemas de informação. Sendo reconhecidamente importante perceber que fatores melhor explicam as percepções dos indivíduos nesta matéria, este estudo visa abordar o cibercrime, tendo como moldura teórica a governança e as políticas públicas. Depois de uma definição cuidadosa das dimensões que impactam a percepção dos cidadãos portugueses relativa à performance do Estado nestas matérias, a investigação empírica realizada procurou segmentar os participantes em agrupamentos relevantes para a definição e implementação de políticas públicas no domínio da cibersegurança e cibercriminalidade.

O cibercrime reúne ainda poucos estudos, sobretudo no que diz respeito aos tópicos da ação e das funções do Estado.

1 Enquadramento Conceitual

Da evolução de correntes, como a burocrática de Weber ou a *new public management*, desenvolveram-se um conjunto de novas vertentes teóricas, entre as quais se salienta a governança (HILL, 2005). Segundo Stoker (1998), a governança se refere a um conjunto complexo de instituições e intervenientes que, autônomos *per si*, atuam de forma concertada. Com o

acentuamento do esbatimento da fronteira entre os setores público e privado, surgem e ganham relevo novas ferramentas e técnicas de gestão, como as parcerias, e o diálogo permanente entre governo, sociedade civil organizada e os próprios cidadãos (STOKER, 1998; FREY; CZAJKOWSKI, 2005). Segundo esta perspectiva conceitual, a abordagem dos problemas de forma abrangente e alargada é a única forma eficiente de atuar, dada a incapacidade de uma única entidade, seja pública ou privada, reunir conhecimento e recursos suficientes para enfrentar os problemas sociais e econômicos de forma unilateral (KOOIMAN, 1993).

Por sua vez, a autonomia de cada um destes agentes é indispensável para que seja possível atingir uma rede eficaz, eficiente, mais próxima do contexto e do próprio cidadão. Assim, a atuação dos vários agentes vai para além da mera influência latente, sendo que estes passam realmente a desempenhar funções antes reservadas à administração pública (STOKER, 1998). A revisão das formas tradicionais de atuação dá ao governo o desafio de "liderar o processo em vários momentos, mas também partilhar, delegar e interagir" (FISCHER, 1996, p. 15).

Para Shearing (1992), o controle do crime diz respeito à preservação da paz, isto é, à manutenção de um Estado Social que garanta a proteção das pessoas e dos seus bens. Para este autor, o combate da criminalidade diz respeito a todas as ações que permitem alcançar esse nível de Estado Social. Essa definição pressupõe, à semelhança da elaboração de políticas públicas orientadas pela lógica da governança, que a responsabilidade no combate ao crime não diz somente respeito ao Estado, mas à atuação de múltiplas entidades e agentes sociais. Para Oliveira (2010), esta atuação tanto diz respeito às práticas formais quanto informais de controle social.

A governança reconhece, pois, não uma alteração nas funções e nas atribuições do Estado, mas antes uma alteração no seu *modus operandi*: a operacionalização passa a se fazer articulada com entidades privadas, nomeadamente através de subsídios, contratos e acordos de cooperação (MILWARD; PROVAN, 2000). Segundo Rehfuss (1989), essa configuração permite ao Estado aceder a um leque de profissionais especializados e a um mercado genuíno (sublinhe-se, concorrencial), permitindo obter os melhores produtos/serviços aos menores custos.

Em Portugal, [...] o Estado tem um claro papel interventivo, baseado no uso da lei.

Marques (2007) afirma que a Governança associa à boa gestão pública valores como a transparência, a responsabilidade e a integração, associando ainda, ao nível dos recursos humanos, valores e virtudes como a liderança, a integridade e o compromisso.

Todavia, há que salientar a distinção entre o paradigma continental europeu e o paradigma dos países anglo-saxônicos (POLLITT; BOUCKAERT, 2011; BILHIM; CORREIA, 2016). No paradigma europeu, o Estado tem um papel central, com forte presença e influência na sociedade, sendo que os valores que imperam são os da legalidade e equidade (LEVI-FAUR; VIGODA-GADOT, 2004). No paradigma dos países anglo-saxônicos, precursores da aproximação entre a administração pública e privada, a presença do Estado é menor, sendo muitas funções deixadas a cargo de outros agentes sociais e da própria sociedade civil.

Em Portugal, onde prevalece o paradigma europeu continental, é notória a transferência dos valores que pautam essa mundividência para a própria forma de atuação e de abordagem à gestão e às próprias políticas públicas: o Estado tem um claro papel interventivo, baseado no uso da lei.

2 O Quadro das Políticas Públicas em Matéria de Cibersegurança e Cibercrime em Portugal

Segundo Cárdenas et al. (2010), duas razões parecem explicar o crescimento do cibercrime: (1) os ganhos potenciais crescentes e (2) as multas e penalizações mais baixas, quando comparadas às aplicadas aos crimes tradicionais. Segundo os autores, o cibercrime é mais conveniente, lucrativo e menos dispendioso e arriscado do que o crime dito mundano.

No decorrer do século XX, surge uma duplicidade de consensos sobre a melhor forma de lidar com o crime e com a justiça criminal. Uma das correntes defendia a abordagem convencional baseada em punir e reinserir (intervenção *ex-post*), ao passo que a outra corrente defendia que a criminalidade deveria ser abordada através da prevenção e orientação (*ex-ante*) (PETERS; PIERRE, 2006). Mais recentemente, o problema da criminalidade tem sido abordado sob o ponto de vista das políticas públicas (PETERS; PIERRE, 2006). Howlett, Ramesh e Perl (2009) mencionam a existência de três grandes conjuntos de opções enquanto instrumentos das políticas públicas (QUADRO 1):

QUADRO 1 – Instrumentos de políticas públicas

Instrumentos Voluntários	Instrumentos Combinados	Instrumentos Compulsórios
Família e Comunidade	Informação e Sensibilização	Regulação
Organizações Voluntárias	Subsídios	Empresas do Setor Público
Mercados Privados	Impostos e Taxas de Utilização	Provisionamento Direto

FONTE: Howlett, Ramesh e Perl (2009, adaptado)

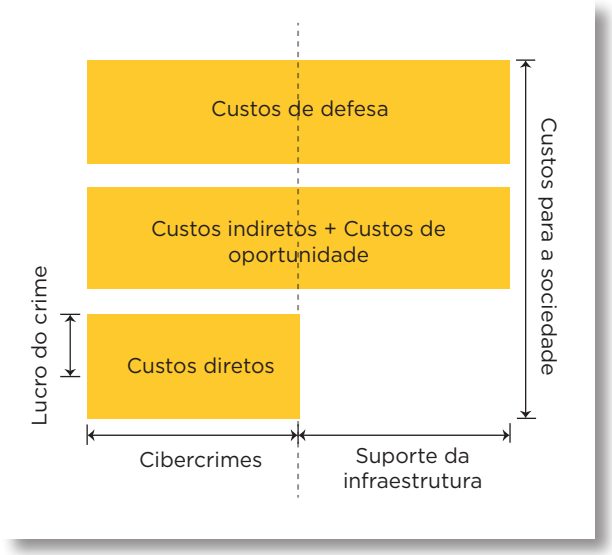
No que diz respeito à prevenção enquanto instrumento de políticas públicas de combate à cibercriminalidade, esta era tida tão somente, numa primeira fase, como o atuar nas causas que estão na origem da motivação criminal. Nessa lógica, as medidas a serem aplicadas passavam exclusivamente pelos tratamentos médicos, psiquiátricos e pelas reformas sociais (OLIVEIRA, 2010). Já nos anos 1970, acrescenta-se ao fator motivação criminal o fator ocasião, ou seja, a ideia de que algumas situações favorecem a ocorrência do crime. Por conseguinte, surge a denominada prevenção situacional (CUSSON, 1988, p. 253), que se propõe a eliminar as oportunidades de cometer crimes, tornando-os mais difíceis, mais arriscados e menos lucrativos. Exemplos de prevenção situacional de crimes usuais, fazendo com que o ato criminal seja mais arriscado, passam pelo planejamento urbano, a iluminação pública ou as câmeras de videovigilância (OLIVEIRA, 2010).

A escolha dos instrumentos a serem utilizados em cada caso particular deve levar em conta as suas especificidades, nomeadamente a natureza do problema e o seu contexto, tendo sempre em consideração os custos das medidas e o impacto gerado. Este raciocínio permite conceber um portfólio de estratégias eficientes com altas taxas de retorno de investimento (AOS; MILLER; DRAKE, 2006).

No que diz respeito à elaboração de políticas públicas para o combate do crime informático, McGuire e Dowling (2013) apontam certas especificidades deste tipo de crime que se materializam em desafios a partir do recolhimento de dados empíricos: dificuldade na distinção entre crime *on-line* e *off-line*; entidades, públicas e privadas, não participam da totalidade de incidentes; ausência de homogeneidade na mensuração e classificação de incidentes; natureza global do cibercrime (não é, objetivamente, limitado por fronteiras nacionais); frequentemente a relação transgressor-vítima é muito diferente dos padrões convencionais do crime *off-line*.

O cibercrime em contraste com os crimes fisicamente consubstanciados (pelo menos parte destes) tem especificidades que resultam em configurações diferentes das demais formas de crime, nomeadamente, no que diz respeito ao seu impacto econômico. Os custos associados ao cibercrime, quer para as empresas (privadas e públicas) ou para o resto da sociedade, podem ser desdobrados em três categorias: custos diretos, custos indiretos e de oportunidade, e custos de defesa (FIG. 1).

FIGURA 1 – Custos do cibercrime



FONTE: Anderson et al. e Ponemon Institute (2013; 2015, adaptado)

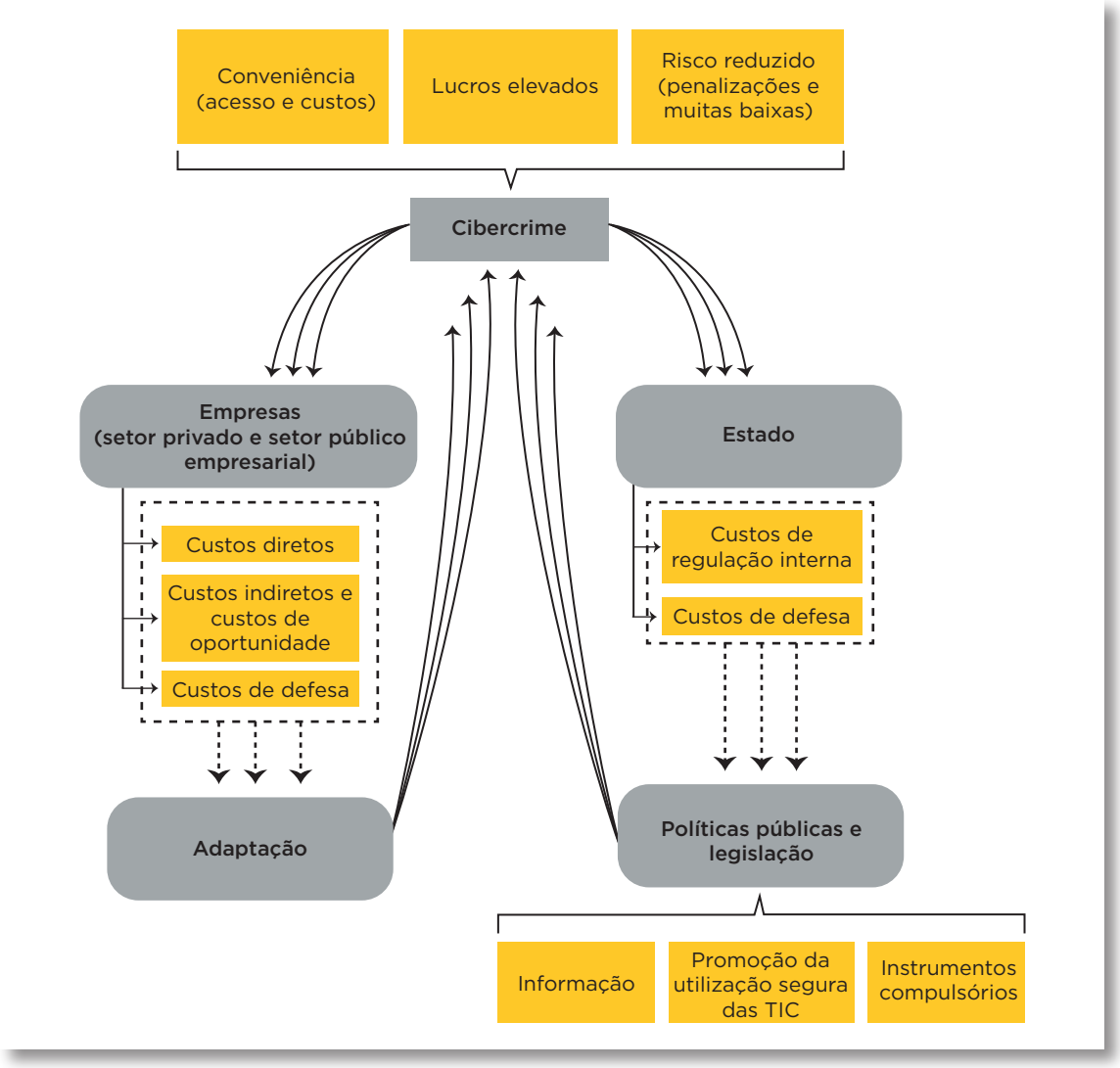
Os custos diretos incluem, por exemplo, valores extraídos das contas das vítimas. Os custos indiretos incluem custos para restaurar os sistemas, a perda de confiança nas empresas ou nos sistemas eletrônicos (o que se traduz em perdas de receitas) e custos de oportunidade associados, por exemplo, ao tempo em que lojas *on-line* ou *softwares* institucionais estão inoperacionais. Já os custos de defesa incluem os valores gastos com antivírus, detectores de fraude ou processos judiciais (ANDERSON et al., 2013; PONEMON INSTITUTE, 2015).

Em Portugal, a estratégia de abordagem da segurança no ciberespaço passa pelo foco em seis eixos (PORTUGAL, 2015): coordenação político-estratégica das várias estruturas nacionais (nomeadamente as Computer Security Incident Response Team ou CSIRT[4]) com o Centro Nacional de Cibersegurança (CNCS), no desenvolvimento de capacidades técnicas de ciberdefesa e cibersegurança; revisão e atualização periódica da legislação e melhoria das capacidades técnicas e humanas da Polícia Judiciária; maior robustez dos sistemas e da informação, e a introdução de mecanismos de detecção antecipada de ameaças; educação, sensibilização e prevenção, através de campanhas, ações de formação e promoção da utilização segura das TIC (nomeadamente nos grupos considerados de risco, como as crianças e os idosos); investigação e desenvolvimento, através de estímulos e apoios; e cooperação entre entidades nacionais e internacionais, nomeadamente entre as CSIRTs, a União Europeia e a North Atlantic Treaty Organization (NATO).

Contudo, independente do continente, do conjunto de países ou do país sobre o qual qualquer análise particular incida, os padrões observados são comuns e os desafios colocados às sociedades são partilhados a nível global. Num mecanismo de *feedback* sem fim discernível, os agentes do cibercrime procuram tirar vantagem das falhas existentes nos sistemas dos Estados e das empresas que, por sua vez e respectivamente, elaboram/implementam políticas públicas e se adaptam, obrigando os perpetradores de cibercrime a reagir e evoluir (FIG. 2).

[4] Para detalhes sobre os objetivos e as equipes da rede nacional, consultar: http://fe02.cert.pt/index.php/rede-nacional-csirt/objectivos e http://fe02.cert.pt/index.php/rede-nacional-csirt/directorio.

FIGURA 2 – Esquema síntese do cibercrime



FONTE: Os autores (2016)

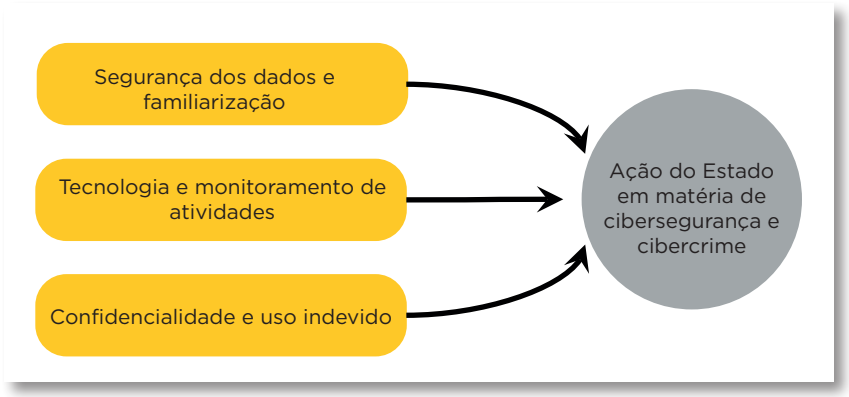
Este artigo procura, pois, com base nos conceitos atinentes a estes mecanismos, criar agrupamentos homogêneos de cidadãos (*clusters*) em função das suas percepções face à forma como o Estado define e implementa políticas públicas em matéria de cibersegurança e cibercrime. O objetivo adquire particular relevo na medida em que os *clusters* assim gerados permitem discriminação positiva ao nível da escolha das políticas públicas mais eficientes para cada grupo de cidadãos.

3 Modelo de Investigação

A promoção de um conjunto de valores, os padrões de conduta dos cidadãos, das entidades públicas e privadas e os regulamentos e leis que visam promover o uso seguro do ciberespaço sugerem a existência de

três macroconceitos implícita ou explicitamente vinculados à percepção dos cidadãos sobre a ação do Estado relativamente ao tema em análise. É possível constatar que a apreciação da ação do Estado em matérias de cibersegurança e cibercrime (*outcome*) está intimamente relacionada com os conceitos de segurança dos dados e familiarização com a tecnologia, o monitoramento digital das atividades e a confidencialidade ou uso indevido desses mesmos dados (FIG. 3).

FIGURA 3 – Modelo teórico de percepções sobre políticas públicas em matéria de cibersegurança e cibercrime



FONTE: Correia et al. (no prelo, adaptado)

4 Metodologia

Na investigação empírica optou-se por recolher os dados através de um inquérito por questionário. Esse mesmo instrumento de recolhimento de dados incorporou 15 questões: dez questões de escala referentes à cibersegurança e assuntos conexos (como supracitado) e cinco questões de caracterização pessoal.

As questões de escala relativas às percepções dos inquiridos tiveram por base a realidade e o contexto portugueses, nomeadamente fatores como o grau de difusão tecnológica, enquadramento jurídico e sofisticação dos utilizadores.

A listagem detalhada das variáveis de medida encontra-se no QUADRO 2. Neste quadro é possível observar as questões colocadas aos inquiridos, a agregação de conjuntos destas questões nas quatro variáveis latentes propostas (segurança dos dados e familiarização; tecnologia e monitoramento de atividades; confidencialidade e uso indevido; e ação do Estado em matérias de cibersegurança e cibercrime) e os respectivos conceitos e fontes relativas a cada um dos indicadores e dimensões.

QUADRO 2 – Questões colocadas aos inquiridos, dimensões agregadoras e respectivas fontes e conceitos de referência Continua

Dimensões	Questões colocadas	Fontes e Conceitos
Segurança dos dados e familiarização (SDF)	SDF 1 – Como você classifica o seu entendimento do conceito de **Cibercrime**?	Elaboração própria com base no conceito de cibercrime (UNIÃO EUROPEIA, 2001; MARQUES; MARTINS, 2006).
	SDF 2 – Sente-se familiarizado com a noção de **Cibersegurança**?	Elaboração própria com base no conceito de cibersegurança (JOHNSON, 2015; PORTUGAL, 2015).
	SDF 3 – Que importância você atribui à segurança dos dados dos seus dispositivos digitais?	Elaboração própria com base no conceito genérico de privacidade. Conceito particular: dados e dispositivos digitais (PORTUGAL, 2009; CORREIA; JESUS, 2013).

QUADRO 2 – Questões colocadas aos inquiridos, dimensões agregadoras e respectivas fontes e conceitos de referência Continua

Dimensões	Questões colocadas	Fontes e Conceitos
Tecnologia e monitoramento de atividades (TMA)	TMA 1 – Você concorda com a vulgarização do uso da videovigilância em espaços públicos?	Elaboração própria com base no conceito genérico de privacidade. Conceito particular: videovigilância (PORTUGAL, 2012; 2013; CORREIA; JESUS, 2013).
	TMA 2 – Você concorda com o uso de sistemas de localização geográfica (vulgo GPS) para localizar pessoas?	Elaboração própria com base no conceito genérico de privacidade. Conceito particular: sistemas de localização - GPS (ENGE, 1994; CORREIA; JESUS, 2013).
	TMA 3 – Você concorda com a utilização de registros de identificação/horário de entrada/saída?	Elaboração própria com base no conceito genérico de privacidade. Conceito particular: registro de entradas e saídas (PORTUGAL, 1998; 2013; CORREIA; JESUS, 2013).
Confidencialidade e uso indevido (CUI)	CUI 1 – As entidades públicas, consoantes a sua atribuição, detêm dados dos cidadãos. Qual a importância de estas informações permanecerem confidenciais? (Escala invertida)	Elaboração própria com base no conceito genérico de privacidade. Conceito particular: dados pessoais (PORTUGAL, 1998; 2013; CORREIA; JESUS, 2013).
	CUI 2 – Você considera provável que os seus dados venham a ser usados de forma a prejudicá-lo ou para favorecer terceiros (por exemplo economicamente)?	Elaboração própria com base no conceito genérico de crime informático. Conceito particular: fraude informática (UNIÃO EUROPEIA, 2001; MARQUES; MARTINS, 2006).
Ação do Estado em matéria de cibersegurança e cibercrime (AEMCC)	AEMCC 1 – Como você avalia o seu conhecimento da legislação e dos organismos que, em Portugal, se ocupam da criminalidade informática?	Elaboração própria com base no conceito genérico do conhecimento da legislação e entidades de serviço público. Conceito particular: cibercrime (UNIÃO EUROPEIA, 2001; MARQUES; MARTINS, 2006).
	AEMCC 2 – Como você classifica a eficácia da atuação do Estado em matéria de segurança informática?	Elaboração própria com base no conceito genérico de eficácia. Conceito particular: segurança do ciberespaço (MULLINS, 2007; PORTUGAL, 2015).

FONTE: Correia et al. (no prelo)

De forma a quantificar as dez variáveis de medida integrantes das quatro variáveis latentes propostas no modelo em análise, foram aplicadas escalas de Likert com âncoras nos extremos (para o extremo inferior – nível muito baixo; extremo superior – nível muito alto) e dez pontos[5], sendo que foi garantido aos inquiridos a opção de escolha **não respondeu/não sabe**.

Das variáveis de caracterização pessoal utilizadas no inquérito, foram constatadas: idade, gênero, região de residência (segundo NUTS II), nível de escolaridade e frequência de utilização da internet.

A disponibilização e aplicação do questionário ocorreu em dois formatos, *on-line* e presencial (em papel), entre os dias 6 de julho e 28 de julho de 2015. Durante o período de recolhimento foram obtidas 1.216 respostas, das quais 1.168 foram consideradas como válidas,

[5] A opção por escalas de Likert numéricas e por intervalo com dez pontos garante, face às escalas de cinco ou sete pontos, uma maior variabilidade dos resultados obtidos, garantindo maior qualidade e robustez dos procedimentos estatísticos efetuados. Um tratamento, mais detalhado, deste tópico pode ser consultado, por exemplo, em Correia (2012, p. 140-144).

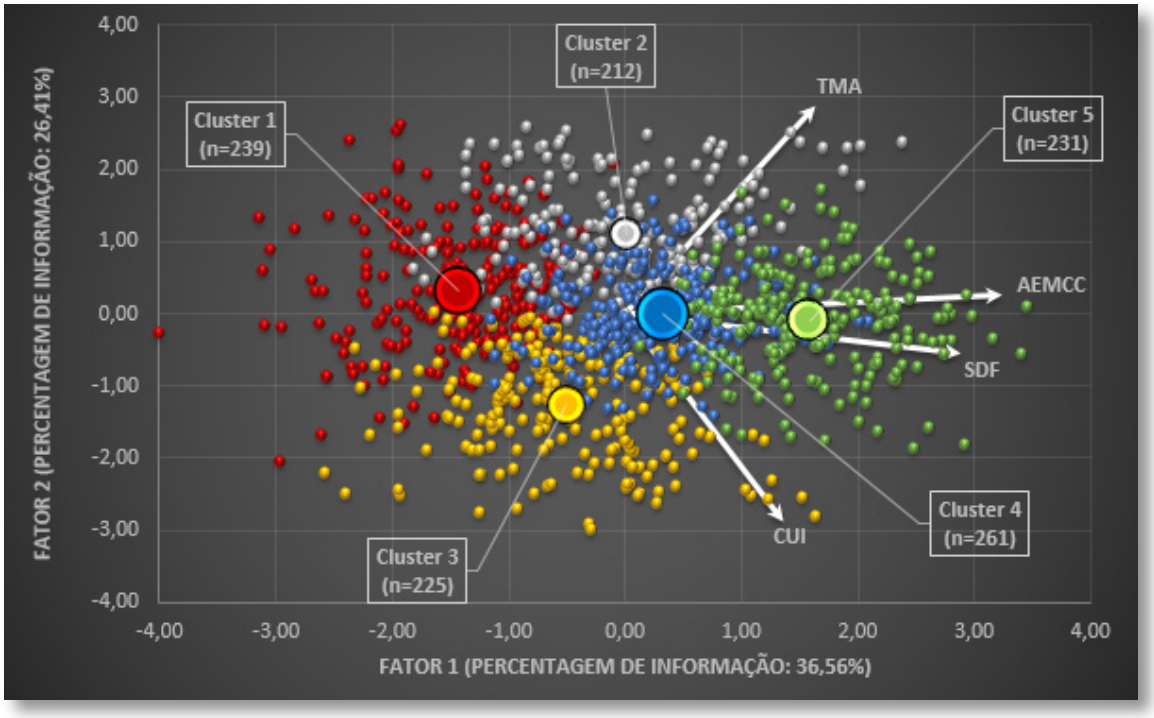
consubstanciando uma dimensão amostral que permite calcular a precisão absoluta do estudo como sendo de 2,999% (0,02999)[6].

Optou-se pela utilização do algoritmo PLS Path Modeling para a modelização e cálculo dos resultados das equações estruturais associadas ao modelo teórico proposto (FIG. 2). Foi com base nos *scores*, para cada respondente em cada uma das quatro dimensões ilustradas na FIG. 2, que se realizou a análise fatorial de componentes principais, a qual serviu de base à análise de *clusters* (método hierárquico), cujos resultados são apresentados neste artigo como foco principal. As análises foram realizadas com a versão 6.5 do *software* SPAD (Système Pour Analyse de Données).

5 Resultados

A análise de *clusters* organizou os indivíduos em cinco agrupamentos, cuja dispersão pode ser encontrada no GRÁF. 1.

GRÁFICO 1 – Gráfico de dispersão dos *clusters*

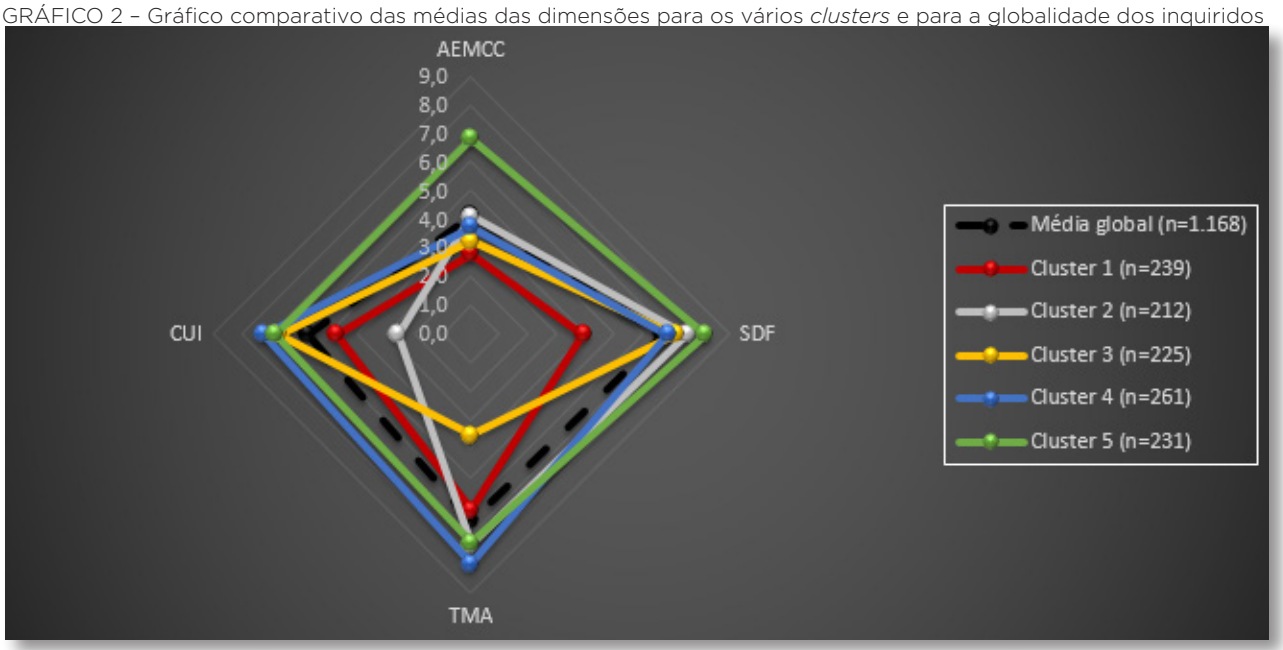


FONTE: Os autores (2016)

É possível observar, no GRÁF. 2, as avaliações médias das dimensões consideradas no modelo de investigação. Além das médias das percepções globais em cada variável, é possível observar a discriminação alcançada pela análise de *clusters*, no que diz respeito às avaliações médias atribuídas pelos inquiridos pertencentes a cada um dos agrupamentos nas suas respostas ao inquérito.

[6] Cálculo efetuado com base na fórmula para a dimensão amostral para proporções; nível de confiança de 95,00% (0,9500); adoção de uma postura metodologicamente cautelosa que assume a existência de um cenário de variância máxima e dimensão populacional infinita.

GRÁFICO 2 – Gráfico comparativo das médias das dimensões para os vários *clusters* e para a globalidade dos inquiridos



FONTE: Os autores (2016)

O *cluster* 1 (composto por 239 observações, que correspondem a 20,5% do total) é constituído por indivíduos com baixa familiarização com os termos cibercrime e cibersegurança. São indivíduos que dão pouca importância à segurança dos dados dos seus dispositivos, têm baixo conhecimento da legislação aplicável e das entidades competentes nesta matéria, pois consideram pouco provável serem alvos de crime informático. É um grupo formado majoritariamente por mulheres (aproximadamente 66,9%) e os seus integrantes avaliam de forma negativa a ação do Estado.

O *cluster* 2 (composto por 212 observações, que correspondem a 18,1% do total) é constituído por indivíduos que, embora se considerem informados sobre os conceitos relacionados com este tipo de criminalidade e concordem bastante com a vulgarização de instrumentos de vigilância, não acreditam que exista algum risco inerente ao uso das tecnologias e, por conseguinte, expressam descrença pela possibilidade de uso criminoso dos seus dados.

O *cluster* 3 (composto por 225 observações, que correspondem a 19,3% do total) é constituído por um grande número de indivíduos jovens (média de idade de 32,4 anos), com formação superior (18,7% com grau de mestre) e que despendem muitas horas por dia na internet (36,9% passam mais de três horas por dia *on-line*). A principal característica deste grupo é a vincada aversão à vigilância. Apesar desta aversão aos instrumentos de vigilância, consideram provável que os seus dados sejam usados de forma incorreta. Apresentam ainda um baixo conhecimento da legislação e das entidades competentes e avaliam a ação do Estado negativamente.

O *cluster* 4 (composto por 261 observações, que correspondem a 22,3% do total) é um grupo majoritariamente constituído por pessoas com nível de ensino secundário (38,7%). Estes indivíduos são entusiastas da cultura de vigilância, mostrando-se muito favoráveis ao aumento destes instrumentos. Evidenciam também percepções que vão no sentido da forte crença na possibilidade de os seus dados serem usados para fins ilícitos. Este grupo avalia a ação do Estado ligeiramente abaixo da média global.

Finalmente, o *cluster* 5 (composto por 231 observações, que correspondem a 19,8% do total de observações) é essencialmente constituído por habitantes da região de Lisboa (82,7%), predominantemente do sexo masculino (54,5%).

Identificam-se como entendedores dos conceitos associados à cibercriminalidade e consideram-se conhecedores da legislação e das entidades competentes. Ponderam a possibilidade de crime informático e não veem inconveniente no aumento da vigilância. Este grupo é um constituído por indivíduos extremamente satisfeitos com a ação do Estado nestas matérias.

Com base nas suas características-chave, cada um dos cinco *clusters* pode ser apelidado, respectivamente, de *cluster* dos cidadãos desinformados; *cluster* dos cidadãos despreocupados; *cluster* dos cidadãos anti-vigilância; *cluster* dos cidadãos pró-vigilância; e *cluster* dos cidadãos satisfeitos com a ação do Estado em matérias de cibercrime e cibersegurança.

Conclusão

O presente trabalho propôs-se a analisar as percepções dos cidadãos no que diz respeito às políticas públicas de cibersegurança.

Recorrendo à análise da literatura, foi possível contextualizar o cibercrime no que diz respeito à sua atratividade: conveniência (fácil acesso e baixo custo), lucros elevados e riscos reduzidos (multas e penalizações mais baixas quando comparadas com os crimes mundanos). Os efeitos destes crimes podem ser divididos naqueles que incidem sobre o setor empresarial (empresas privadas ou públicas) e naqueles que incidem sobre as próprias estruturas do Estado. Os custos causados por esse tipo de crime podem ser classificados como diretos (quando há extração de valores), indiretos e de oportunidade (devido à inoperância dos sistemas). Podem ainda ser classificados como custos de defesa (referentes à detecção, restabelecimento do sistema e medidas de defesa preventivas de novos incidentes). Este paradigma resulta numa dupla necessidade de adaptação, quer por parte das entidades-alvo, de forma a prevenir novos ataques com técnicas mais sofisticadas, quer por parte dos infratores, no sentido de ultrapassarem as contingências e barreiras de segurança crescentes dessas entidades.

A elaboração de políticas públicas para o combate deste tipo de criminalidade assenta, cada vez mais, na governança enquanto teoria de gestão. A governança caracteriza-se por uma série de proposições, das quais se salientam a intervenção de uma multiplicidade de entidades e agentes autônomos *per si*, o esbater das fronteiras público-privado e o uso de ferramentas, como os subsídios, contratos e acordos de cooperação. É segundo estes princípios que as práticas de governança se propõem a facultar à sociedade bens e serviços especializados de uma forma mais próxima dos próprios cidadãos e com menores custos para o Estado. Este tipo de abordagem ao fenômeno da cibercriminalidade é especialmente relevante, dada a hodiernidade da temática e a imperatividade de um elevado *know-how* técnico, especialização e compreensão do contexto particular. Exemplos desta atuação são os CSIRTs, equipes de profissionais em segurança informática, de entidades públicas e privadas, predominantemente dos setores tecnológicos e financeiros, que atuam na prevenção e mitigação de incidentes.

As políticas públicas para o combate do cibercrime estão grandemente condicionadas por determinadas especificidades deste tipo de criminalidade, como a dificuldade de identificação dos perpetradores, a não participação dos incidentes, a falta de homogeneidade na classificação das ocorrências e da sua quantificação, ou a sua natureza além-fronteiras.

A elaboração de políticas públicas para o combate deste tipo de criminalidade assenta, cada vez mais, na governança enquanto teoria de gestão.

Segundo a literatura, os instrumentos passíveis de aplicação na elaboração destas políticas públicas alinham-se ao longo de três grandes vetores: os instrumentos voluntários, que englobam a ação das famílias e a influência dos mercados privados; os instrumentos combinados, que englobam a informação e a formação para a segurança informática; e os instrumentos compulsórios, que englobam a legislação e a regulação (FIG. 2). Tendo em conta a abordagem definida para Portugal, é possível salientar a atuação concertada entre entidades (Polícia Judiciária, CNCS, CSIRTs), o aumento da robustez dos sistemas e do *know-how* técnico ou a revisão periódica da legislação como exemplos de instrumentos de regulação compulsória. Já no que diz respeito aos instrumentos designados como combinados, é possível distinguir um primeiro eixo relativo à informação e ao conhecimento destas temáticas, e um segundo eixo, de natureza mais operacional, relativo à formação para utilização segura das tecnologias de informação e comunicação.

A análise realizada da amostra de cidadãos portugueses, relativa a sua sensibilidade face aos diferentes instrumentos de políticas públicas, permitiu identificar cinco perfis distintos (GRÁF. 1 e GRÁF. 2). A identificação de perfis de cidadãos, em função de suas percepções, reveste-se de particular importância na medida em que permite tornar mais eficaz e eficiente a ação do Estado, uma vez que as políticas públicas podem passar a ser especificamente desenhadas e direcionadas para determinados públicos-alvo, em função das suas idiossincrasias e da sua sensibilidade face ao tema da cibersegurança e do cibercrime.

O QUADRO 3 propõe, com base nos resultados obtidos, aquilo que poderá ser expectável em termos de sensibilidade aos instrumentos de políticas públicas, por parte dos cidadãos pertencentes aos vários *clusters* identificados na análise. Destaca-se, em particular, a associação que é possível estabelecer entre uma elevada satisfação com a ação do Estado e um grupo de pessoas (*cluster* 5) muito informadas sobre estes temas, instruídas sobre os perigos e riscos que existem *on-line* e que conhecem os procedimentos para uma utilização segura das TIC. Destaca-se, ainda, relativa aos restantes *clusters* (1 a 4), a baixa ou muito baixa sensibilidade aos instrumentos compulsórios consubstanciados nas políticas de regulação. Os resultados sugerem ainda que, com exceção do *cluster* 1, os instrumentos combinados (políticas de informação e políticas de utilização segura das TIC) são opções adequadas para a intervenção do Estado nas questões de cibersegurança e cibercrime, com recurso às políticas públicas.

QUADRO 3 – Sensibilidade dos *clusters* aos instrumentos de políticas públicas

	Instrumentos combinados		Instrumentos compulsórios	
	Políticas de informação	Políticas de utilização segura das TIC	Políticas de regulação	Satisfação com a ação do Estado
Cluster 1 – Desinformados	Baixa	Baixa	Muito Baixa	Reduzida
Cluster 2 – Despreocupados	Alta	Muito baixa	Baixa	Reduzida
Cluster 3 – Antivigilância	Alta	Alta	Baixa	Reduzida
Cluster 4 – Pró-vigilância	Alta	Alta	Baixa	Reduzida
Cluster 5 – Satisfeitos com a ação do Estado	Muito alta	Alta	Alta	Elevada

FONTE: Os autores (2016)

Sugere-se que estudos futuros repliquem a abordagem descrita nesta pesquisa de modo a robustecer e refinar as conclusões apresentadas. Em especial, sugere-se que seja dada ênfase adicional ao dualismo legalidade-moralidade, que poderá desempenhar um importante papel na formação das percepções dos indivíduos. Esses exercícios serão particularmente relevantes se levados a cabo noutros contextos, em particular, noutros países de língua oficial portuguesa, como é o caso do Brasil, de modo que seja possível aferir a influência da envolvente sociocultural e econômica nas percepções dos cidadãos sobre as políticas públicas de cibersegurança e contra a cibercriminalidade.

Referências

ANDERSON, R. et al. Measuring the cost of cybercrime. In: BÖHME, R. (Ed.). **The Economics of information security and privacy**. Heidelberg: Springer, 2013. p. 265-300.

AOS, S.; MILLER, M.; DRAKE, E. **Evidence-based public policy options to reduce future prison construction, criminal justice costs, and crime rates**. Olympia: Washington State Institute for Public Policy, 2006. Disponível em: <http://www.wsipp.wa.gov/ReportFile/952/Wsipp_Evidence-Based-Public-Policy-Options-to-Reduce-Future-Prison-Construction-Criminal-Justice-Costs-and-Crime-Rates_Full-Report.pdf>. Acesso em: 20 fev. 2016.

BILHIM, J.; CORREIA, P. Diferenças nas perceções dos valores organizacionais dos candidatos a cargos de direção superior na administração central do estado. **Sociologia**, Porto, n. 31, p. 81-105, 2016.

CÁRDENAS, A. et al. An economic map of cybercrime. In: THE RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND INTERNET POLICY (TPRC), 37., 2009. Arlington. **Annals...** Arlington: George Mason University Law School, 2010.

CARVALHO, J. S. **Segurança nacional, serviços de informação e as forças armadas**. Intervenção proferida pelo diretor do serviço de informações estratégicas de defesa (SIED). Lisboa: Faculdade de Letras da Universidade de Lisboa, 28 de maio de 2009. Disponível em: < http://www.segurancaedefesa.pt/noticias/009/intervencao_jorge_silva_carvalho_20090528.pdf>. Acesso em: 22 nov. 2016.

CORREIA, P. **O impacto do Sistema Integrado de Gestão e Avaliação do Desempenho da Administração Pública (SIADAP) na satisfação dos colaboradores** – o caso dos serviços do Ministério da Justiça em Portugal. 2012. 549 f. Tese (Doutorado em Administração Pública) - Instituto Superior de Ciências Sociais e Políticas da Universidade Técnica de Lisboa, Lisboa, 2012.

CORREIA, P.; JESUS, I. Combate às transferências bancárias ilegítimas pela internet no direito português: entre as experiências domésticas e políticas globais concertadas. **Revista Direito GV**, São Paulo, v. 12, n. 2, p. 542-563, 2016.

_____. O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana. **Direito, Estado e Sociedade**, Rio de Janeiro, n. 43, p. 135-61, jul./dez. 2013.

CORREIA, P.; SANTOS, S.; BILHIM, J. Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime. **Sociologias**, Porto Alegre. No prelo.

CUSSON, M. **Criminologie actuelle**. Paris: Les Presses Universitaires de France, 1998.

ENGE, P. The global positioning system: signals, measurements, and performance. **International Journal of Wireless Information Networks**, Worcester, v. 1, n. 2, p. 83-105, 1994.

FISCHER, T. Gestão contemporânea, cidades estratégicas: aprendendo com fragmentos e reconfigurações do local. In: FISCHER, T. (Org.). **Gestão contemporânea**: cidades estratégicas e organizações locais. Rio de Janeiro: FGV, 1996, p. 13-23.

FREY, K.; CZAJKOWSKI, S. O município e a segurança pública: o potencial da governança democrática urbana. **Revista de Administração Pública**, Rio de Janeiro, v. 39, n. 2, p. 297-325, mar./abr. 2005.

HILL, M. **The public policy process**. 4th ed. Harlow: Pearson Education, 2005.

HOWLETT, M.; RAMESH, M.; PERL, A. **Studying public policy**: policy cycles and policy subsystems. 3rd ed. Oxford: Oxford University, 2009.

JOHNSON, T. **Cybersecurity**: protecting critical infrastructures from cyber attack and cyber warfare. Missouri: CRC, 2015.

KOOIMAN, J. Social-political governance: introduction. In: KOOIMAN, J. (Ed.). **Modern governance**: new government-society interactions. London: Sage Publications, 1993. p. 1-8.

LEVI-FAUR, D.; VIGODA-GADOT, E. (Ed.). **International public policy and management**. New York: CRC, 2004.

MARQUES, M. Aplicação dos princípios da governança corporativa ao sector público. **Revista de Administração Contemporânea**, Rio de Janeiro, v. 11, n. 2, p. 11-26, abr./jun. 2007.

MARQUES, G.; MARTINS, L. **Direito da informática**. Coimbra: Almedina, 2006.

MCGUIRE, M.; DOWLING, S. **Research report 75**. London: Home Office, 2013.

MILWARD, H.; PROVAN, K. How networks are governed. In: LYNN, C.; HEINRICH, L.; LYNN, L. (Ed.). **Governance and performance**: new perspectives. Washington, D. C.: Georgetown University, 2000.

MULLINS, L. **Management and organisational behaviour**. Harlow: Pearson Education, 2007.

NUNES, P. A definição de uma estratégia nacional de cibersegurança. **Nação e Defesa**, Lisboa, n. 133, p. 113-127, 2012.

OLIVEIRA, A. Crime, controle do crime e governança democrática. **Dilemas**: Revista de estudos de conflito e controle social, Rio de Janeiro, v. 2, n. 5-6, p. 49-78, 2010.

PETERS, B.; PIERRE, J. **Handbook of public policy**. London: Sage Publications, 2006.

POLLITT, C.; BOUCKAERT, G. **Public management reform**: a comparative analysis – new public management, governance, and the Neo-Weberian State. New York: Oxford University, 2011.

PONEMON INSTITUTE. **2015 cost of cyber crime study**: global. Michigan: Ponemon Institute, 2015. Disponível em: <http://www.cnmeonline.com/myresources/hpe/docs/Report_2015_Ponemon_GLOBAL.pdf>. Acesso em: 20 fev. 2016.

PORTUGAL. Lei n. 9/2012. **Diário da República**, Lisboa, I série, n. 39, p. 868-874, 23 fev. 2012.

_____. Lei n. 34/2013. **Diário da República**, Lisboa, I série, n. 94, p. 2.921-2.942, 16 maio 2013.

_____. Lei n. 67/98. **Diário da República**, Lisboa, I série, n. 247, p. 5.536-5.546, 26 out. 1998.

_____. Lei n. 109/2009. **Diário da República**, Lisboa, I série, n. 179, p. 6.319-6.325, 15 set. 2009.

PORTUGAL. Resolução do Conselho de Ministros n. 36/2015. **Diário da República**, Lisboa, I série, n. 113, p. 3.738-3.742, 12 jun. 2015.

REHFUSS, J. **Contracting out in government**: a guide for working with outside contractors to supply public services. San Francisco: Jossey-Bass, 1989.

SHEARING, C. The relation between public and private policing. **Crime and Justice**, Chicago, v. 15, p. 399-434, 1992.

STOKER, G. Governance as theory: five propositions. **International Social Science Journal**, Malden, v. 50, n. 155, p. 17-28, 1998.

UNIÃO EUROPEIA. **Convenção sobre o cybercrime**. Budapeste: Série de Tratados Europeus, 2001. Disponível em: <http://www.dgpj.mj.pt/sections/relacoes-internacionais/copy_of_anexos/convencao-sobre-o/downloadFile/attachedFile_f0/STE_185.pdf?nocache=1200659879.8>. Acesso em: 20 fev. 2016.

- Recebido em: 16/03/2016
- Aprovado em: 20/06/2016