CORREIA, Pedro Miguel Alves Ribeiro; SANTOS, Susana Isabel da Silva; BILHIM, João Abreu de Faria (2017), "Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime" *Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. XXXIII, pp. 95 - 113
DOI: 10.21747/08723419/soc33a5

Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime

Pedro Miguel Alves Ribeiro Correia
Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa
Centro de Administração e Políticas Públicas

Susana Isabel da Silva Santos
Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa
Centro de Administração e Políticas Públicas

João Abreu de Faria Bilhim
Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa
Centro de Administração e Políticas Públicas

Resumo
O problema da gestão e das políticas públicas em matérias de cibersegurança e cibercrime não tem sido alvo de um programa de investigação empírica à altura da sua importância e atualidade. Neste texto são apresentados os resultados de um estudo empírico sobre as perceções dos cidadãos portugueses face a esta temática. Os resultados colocam a descoberto uma aparente contradição: apesar de as perceções dos cidadãos acerca das dimensões independentes do modelo proposto serem favoráveis, as perceções acerca da ação do Estado em matérias de cibersegurança e cibercrime não o são.

Palavras-chave: perceção; segurança tecnológica; políticas públicas.

Proposal of explanatory model for the perceptions on public policies and management in matters of cybersecurity and cybercrime

Abstract
The problem of public policies and management in matters of cybersecurity and cybercrime has not been the subject of an empirical research program that can live up to its importance and actuality. In this paper the results of an empirical study on the perceptions of Portuguese citizens on this theme are presented. The results uncover an apparent contradiction: despite the fact that perceptions of citizens regarding the independent dimensions of the model are favorable, the perceptions about the States' action in matters of cybersecurity and cybercrime are not.

Keywords: perception; technology security; public policy.

CORREIA, Pedro Miguel Alves Ribeiro; SANTOS, Susana Isabel da Silva; BILHIM, João Abreu de Faria (2017), "Proposta de modelo explicativo das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime" *Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. XXXIII, pp. 95 - 113

Proposition de modèle explicatif pour les perceptions sur la gestion et politiques publiques en matière de cyber-sécurité et cybercriminalité

Résumé

Le problème de la gestion et des politiques publiques en matière de cyber-sécurité et cybercriminalité n'a pas fait l'objet d'un programme de recherche empirique qui peut vivre jusqu'à son importance et l'actualité. Dans cet article, les résultats d'une étude empirique sur les perceptions des citoyens portugais à ce sujet sont présentés. Les résultats dévoilent une contradiction apparente : malgré le fait que les perceptions des citoyens concernant les dimensions indépendantes du modèle sont favorables, les perceptions au sujet de l'action de État en matière de cyber-sécurité et cybercriminalité ne sont pas.

Mots-clés: perception; sécurité de la technologie; politiques publiques.

Propuesta de modelo explicativo de las percepciones sobre la gestión y políticas públicas en materia de ciberseguridad y crímenes informáticos

Resumen

El problema de la gestión y políticas públicas en materia de ciberseguridad y crímenes informáticos no ha sido objeto de un programa de investigación empírica a la altura de su importancia y actualidad. En este trabajo se presentan los resultados de un estudio empírico sobre las percepciones de los ciudadanos portugueses sobre esta cuestión. El resultado coloca a descubierto una aparente contradicción: a pesar de percepciones favorables de los ciudadanos sobre las dimensiones independientes del modelo, las percepciones acerca de la acción del Estado en materia de ciberseguridad y crímenes informáticos no lo son.

Palabras-clave: percepción; seguridad de la tecnología; políticas públicas.

1. Introdução e referencial teórico

A segurança cibernética constitui um dos principais desafios para os Estados em matéria de Segurança. Segundo os números dos últimos anos[1], a criminalidade informática tem vindo a aumentar consideravelmente, sendo possível extrapolar que, dentro de cerca de uma década, possa atingir mais de 10% da totalidade dos crimes cometidos em Portugal (Correia e Jesus, 2016). Este padrão parece não só resultar das múltiplas e inovadoras possibilidades e especificidades intrínsecas ao meio digital, mas também de uma permuta instrumental e espacial, do meio físico para o meio digital, que tem vindo a resultar num imperativo crescente de combate ao crime e manutenção da segurança em meio informático (Goodman, 2015). A disseminação das tecnologias de informação e comunicação, associada ao fenómeno das grandes

[1] Estatísticas Oficiais da Justiça, disponíveis em www.siej.dgpj.mj.pt.

bases de dados (*bigdata*), resultam numa enorme fragilidade, transversal não só à normal atividade dos Estados (particularmente nas comunicações G2G e G2C), mas também das empresas e dos próprios indivíduos.

O enquadramento teórico contemporâneo da administração pública, resultante, em parte, da evolução de modelos mais antigos como o da administração burocrática de Weber, permitiu o desenvolvimento de um conjunto de novas correntes de pensamento entre as quais se destaca a governança (Hill, 2005). Segundo Kettl (2000), a governança está assente num conjunto de princípios de que se destacam a produtividade, a orientação para a prestação de serviços, a descentralização, as políticas públicas e a responsabilização. É sob a égide dos princípios supracitados que a governança se caracteriza como uma teoria de cariz multidisciplinar, que aborda a contratação externa em mercado livre, procurando explicar a articulação da ação de entes públicos e privados, com foco na eficácia das políticas públicas e tendo como objetivo final a satisfação do cidadão (Frederickson *et al*., 2012).

A governança operacionaliza-se através de mecanismos como subsídios, contratos e acordos de cooperação (Milward e Provan, 2000). Rehfuss (1989) aponta como vantagens do recurso à contratualização o acesso a um vasto leque de profissionais especializados e a um mercado genuíno, que permite ao governo obter o melhor produto ao melhor preço. É, neste sentido, que se assume que os padrões desejados de atuação da boa gestão pública passam pela prestação de bens e serviços públicos de qualidade, de forma eficiente, transparente e sustentável. Dito de outra forma, é possível afirmar que a essência desta corrente teórica, governança, se encontra na administração e na implementação de políticas públicas através de redes e parcerias entre governo, empresas e associações da sociedade civil (Pollitt e Bouckaert, 2011).

A estrutura centralizada, altamente hierárquica e focada no cumprimento de leis, deu atualmente lugar a uma estrutura focada no desenvolvimento e eficácia das políticas públicas nas diversas áreas de atuação do Estado (Frederickson *et al*., 2012). Segundo Peters e Pierre (2006) este modelo realça as possibilidades de interação entre diferentes atividades, integradas numa mesma política pública, em diferentes momentos, diferentes locais e através de diversos intervenientes. Por outro lado, pelo seu carácter de multidisciplinaridade, especialização e interação com mercados em livre concorrência, Hay (2002) afirma que a elaboração de políticas públicas compele à consideração daquilo a que se pode dar o nome de variáveis-extra-políticas, isto é, variáveis em que o investigador deve conjugar, além dos fatores políticos, fatores sociológicos, económicos, culturais ou históricos.

Note-se ainda que, segundo Pollitt e Bouckaert (2011), há uma clara distinção

entre o paradigma continental europeu e o paradigma dos países anglo-saxónicos. No modelo europeu, o Estado tem um papel central, com uma forte ação modeladora da conduta da sociedade, sendo que os valores que imperam são os da legalidade e da equidade (Levi-Faur e Vigoda-Gadot, 2004). Já no modelo dos países anglo-saxónicos, precursores da aproximação da administração pública com a privada (Bilhim e Correia, 2016), a presença do Estado é ténue, bastante limitada, enquanto outros agentes sociais assumem funções de relevo (Levi-Faur e Vigoda-Gadot, 2004). Por isso mesmo, em Portugal, onde prevalece o paradigma europeu continental, é notória uma clara transferência dos valores que pautam este dualismo e que se encontram plasmados no próprio *modus operandi* aquando a abordagem da gestão e das políticas públicas: o Estado tem um claro papel interventivo, baseado predominantemente no uso da lei. Os aspetos legais são, como tal, incontornáveis para qualquer modelo que se proponha explicar as perceções sobre gestão e políticas públicas em geral e, em particular, as perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime.

2. O contexto das políticas públicas em matéria de cibersegurança e cibercrime em Portugal

O tema do crime e da justiça criminal tem vindo a ser abordado do ponto de vista das políticas públicas (Peters e Pierre, 2006). No século XX prevaleceu aquilo a que se pode chamar um consenso partidário sobre a melhor forma de lidar com o crime, assente em binómios chave como punir e reinserir (*ex-post*) ou prevenir e orientar (*ex-ante*) (Peters e Pierre, 2006).

Howlett e Ramesh (2009) postulam a existência de três grandes grupos de medidas enquanto instrumentos de políticas públicas. Instrumentos voluntários, que incluem a família e comunidade, organizações voluntárias, e mercados privados; instrumentos combinados, que incluem informação e persuasão, subsídios, e impostos e taxas de utilização; e instrumentos compulsórios, que incluem regulação, empresas do setor público, e provisionamento direto. A pertinência da avaliação das políticas públicas e uma criteriosa escolha dos instrumentos utilizados, em matéria de criminalidade, tendo em conta a relação entre custos e impactos gerados, evidencia a possibilidade de conceber um portfólio de estratégias com altas taxas de retorno de investimento que, inclusive a longo prazo, se podem traduzir em reduções da carga fiscal (Aos *et al*., 2006).

Segundo McGuire e Dowling as especificidades no cibercrime, que se traduzem

em desafios à formulação de medidas fundadas em evidências empíricas, dizem respeito à falta de mecanismos de distinção entre crime *online* e *offline*; à não participação da totalidade de incidentes cibernéticos (quer pelos privados quer pelas empresas) e ao desconhecimento de que certo tipo de atividades constituem crimes; a inconsistências na medição e definição de crime cibernético (ausência de homogeneidade); à natureza global, objetivamente não limitada por fronteiras nacionais; e ao potencial que este tipo de atividades tem para ser realizado em grande escala, resultando eventualmente numa interação entre transgressor-vítimas muito distinta dos padrões convencionais no crime *offline* (McGuire e Dowling, 2013).

Em Portugal, a estratégia atualmente definida no que concerne à segurança do ciberespaço, assenta em seis eixos, associados à estrutura e segurança do ciberespaço, respeitante à coordenação político-estratégica, coordenação das demais estruturas nacionais com o recém-criado Centro Nacional de Cibersegurança (CNCS), desenvolvimento da capacidade de ciberdefesa e da capacidade de resposta a incidentes (nomeadamente através da coordenação com as CSIRT[2]); ao combate ao cibercrime, através da revisão e atualização (periódica) da legislação, e da melhoria das capacidades técnicas e humanas da Polícia Judiciária; à proteção do ciberespaço e das infraestruturas, através de uma maior robustez dos sistemas e da informação associada, e de mecanismos de deteção antecipada de ameaças; à educação, sensibilização e prevenção, através de campanhas, ações de formação, promoção da utilização segura das TIC (nomeadamente nos grupos de risco); à investigação e desenvolvimento, com a promoção, estimulo e apoio à investigação e desenvolvimento do conhecimento necessário à manutenção da segurança informática; e à cooperação entre aliados e parceiros nacionais e internacionais (nomeadamente com CSIRTs, União Europeia e NATO) (Portugal, 2015).

Apesar do crescimento da informação relativa aos perigos e incidentes cibernéticos, e do apelo à manutenção de um ambiente *online* seguro, são poucos os estudos empíricos que avaliam as perceções dos cidadãos nesta matéria, especialmente no que diz respeito a potenciais fatores explicativos das perceções dos cidadãos sobre a ação do Estado em matérias de cibersegurança e cibercrime. É exatamente neste sentido que o presente artigo procura dar o seu contributo.

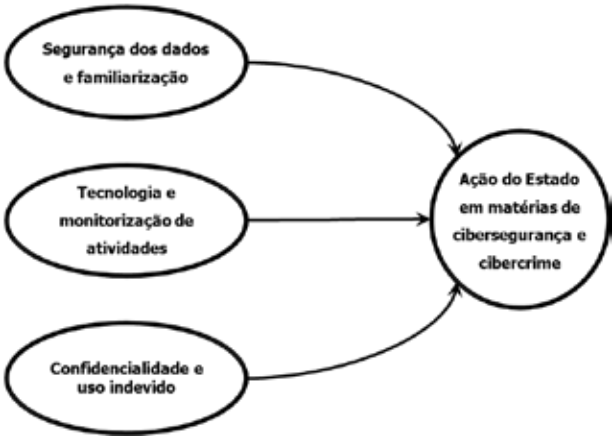
[2] Computer Security Incident Response Team. Para detalhes sobre os objetivos e as equipas da rede nacional, consultar: http://fe02.cert.pt/index.php/rede-nacional-csirt/objectivos e http://fe02.cert.pt/index.php/rede-nacional-csirt/directorio.

3. Modelo de investigação

O enquadramento teórico-conceptual anteriormente apresentado, quando contextualizado na sociedade portuguesa e quando articulado com o tema da ação do Estado em matérias de cibersegurança e cibercrime, permite associar à gestão pública e às políticas públicas, neste particular, um conjunto de conceitos macro, implícita ou explicitamente veiculados, promovidos e/ou garantidos por um conjunto vasto e difuso de valores, padrões de conduta de cidadãos e entidades publicas e privadas, regulamentos e leis, que visam alcançar a cibersegurança e evitar o cibercrime. Como tal, é possível constatar que as perceções dos cidadãos sobre a ação do Estado em matérias de cibersegurança e cibercrime (o *output*) estão intimamente ligadas a conceitos macro como segurança dos dados informáticos, familiarização com as tecnologias, monitorização informática de atividades, e confidencialidade ou uso indevido desses mesmos dados (os *inputs*).

Seguindo esta linha de raciocínio, neste artigo, é proposto um modelo teórico para a formação das perceções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime, que se encontra representado na Figura 1.

Figura 1
Modelo teórico de perceções sobre políticas públicas em matéria de cibersegurança e cibercrime



Fonte: elaboração própria.

No modelo apresentado na figura 1, parte-se do pressuposto que as variáveis latentes segurança dos dados e familiarização; tecnologia e monitorização de atividades; e confidencialidade e uso indevido, influenciam as perceções sobre a ação

do Estado em matérias de cibersegurança e cibercrime. Como tal, foram formuladas três hipóteses de investigação:

H1 – A variável latente segurança dos dados e familiarização tem impacto positivo direto na variável latente ação do Estado em matérias de cibersegurança e cibercrime.

H2 – A variável latente tecnologia e monitorização de atividades tem impacto positivo direto na variável latente ação do Estado em matérias de cibersegurança e cibercrime.

H3 – A variável latente confidencialidade e uso indevido tem impacto positivo direto na variável latente ação do Estado em matérias de cibersegurança e cibercrime.

4. Metodologia

Na investigação empírica, a opção recaiu sobre um inquérito por questionário enquanto instrumento de recolha de dados. Esse mesmo instrumento de recolha de dados incorporou 15 questões: 10 questões de escala referentes a perceções sobre segurança tecnológica e assuntos conexos e cinco questões de caracterização pessoal dos inquiridos.

As questões relativas às perceções sobre segurança tecnológica (e assuntos conexos) tiveram por base a realidade e o contexto português, nomeadamente, fatores como o grau de disseminação da tecnologia, o enquadramento legal e a sofisticação típica dos utilizadores.

A listagem detalhada dos 10 indicadores (ou variáveis de medida) referentes às perceções sobre segurança tecnológica encontra-se no Quadro 1. Neste quadro é possível encontrar as questões colocadas aos inquiridos, a incorporação de conjuntos de indicadores nas quatro variáveis latentes propostas (dimensão segurança dos dados e familiarização; dimensão tecnologia e monitorização de atividades; dimensão confidencialidade e uso indevido; e dimensão ação do Estado em matérias de cibersegurança e cibercrime) e as respetivas fontes e conceitos de referência associados a cada uma dessas questões e dimensões.

Quadro 1
Questões colocadas aos inquiridos, dimensões agregadoras e respetivas fontes e conceitos de referência

Dimensões	Questões colocadas	Fontes e Conceitos Referência
Segurança dos dados e familiarização	SDF 1 – Como classifica o seu entendimento do conceito de "Cibercrime"?	Elaboração própria com base no conceito de cibercrime (União Europeia, 2001; Marques e 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 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 e Jesus, 2013).
Tecnologia e monitorização de atividades	TMA 1 – 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 e Jesus, 2013).
	TMA 2 – Concorda com o uso de sistemas de localização geográfica (vulgo GPS) a fim de localizar pessoas?	Elaboração própria com base no conceito genérico de privacidade; conceito particular: sistemas de localização - GPS (Enge, 1994; Correia e Jesus, 2013).
	TMA 3 – Concorda com a utilização de registos de identificação/horário de entrada/saída?	Elaboração própria com base no conceito genérico de privacidade; conceito particular: registo de entradas e saídas (Portugal, 1998, 2013; Correia e Jesus, 2013).
Confidencialidade e uso indevido	CUI 1 – As entidades públicas, consoante 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 e Jesus, 2013).
	CUI 2 – Considera provável que os seus dados venham a ser usados de forma a prejudica-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 e Martins, 2006).
Ação do Estado em matérias de cibersegurança e cibercrime	AEMCC 1 – Como 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 e Martins, 2006).
	AEMCC 2 – Como 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: adaptado e expandido a partir do trabalho de Correia *et al*., (2017, *in press*).

Por forma a quantificar as 10 variáveis de medida integrantes das quatro variáveis latentes propostas no modelo em análise, foram empregues escalas de Likert com âncoras nos extremos (para o extremo inferior – *nível muito baixo*; extremo superior – *nível muito alto*) e 10 pontos[3], tendo sempre sido garantida aos inquiridos a opção de escolher a resposta *não sabe/não responde*.

Das cinco variáveis de caracterização pessoal dos inquiridos constaram as variáveis: idade, sexo, região de residência (NUTS II), nível de escolaridade e frequência de utilização da internet.

A disponibilização e aplicação do questionário ocorreram em dois formatos, *on-line* e em papel (presencial), entre os dias 6 de julho e 28 de julho de 2015. Durante o período de recolha foram obtidas 1.216 respostas, das quais 1.168 foram consideradas como válidas, consubstanciando uma dimensão amostral que permite calcular a precisão absoluta do estudo como sendo de 2,999% (0,02999)[4]. O grupo de respondentes apresentou uma idade média de 34,03 anos[5]. Dos 1.168 inquiridos, 617 (52,8%) eram do sexo feminino e 546 (46,8%) do sexo masculino (tendo ainda sido registados cinco valores omissos, correspondendo a 0,4%). Quanto à região de residência (NUTS II), 62 respondentes (5,3%) residiam na região Norte, 117 (10,0%) residiam na região Centro, 886 (75,9%) residiam na região de Lisboa, 48 (4,1%) residiam na região do Alentejo, 17 (1,5%) residiam na região do Algarve, 17 (1,5%) residiam na região autónoma dos Açores e 8 (0,7%) residiam na região autónoma da Madeira (tendo ainda sido registados 13 valores omissos, correspondendo a 1,1%). Quanto ao nível de escolaridade, 21 respondentes (1,8%) afirmaram ter até quatro anos de escolaridade, 19 (1,6%) afirmaram ter 5 ou 6 anos de escolaridade, 68 (5,8%) afirmaram ter 7, 8 ou 9 anos de escolaridade, 384 (32,9%) afirmaram ter 10, 11 ou 12 anos de escolaridade, 502 (43,0%) afirmaram ser licenciados, 144 (12,3%) afirmaram ser mestres e 26 (2,2%) afirmaram ser doutorados (tendo ainda sido registados quatro valores omissos, correspondendo a 0,3%). Finalmente, no que concerne à frequência de utilização da internet, 38 (3,3%) afirmaram não utilizar a internet, 27 (2,3%) afirmaram utilizar a internet uma ou duas vezes por semana, 53 (4,5%) afirmaram utilizar a internet 3 a 5 vezes por semana, 671 (57,4%) afirmaram

[3] A opção por escalas de Likert numéricas e por intervalo com 10 pontos garante, face a escalas de cinco ou sete pontos, uma maior variabilidade dos resultados obtidos, garantindo maior qualidade e robustez dos procedimentos estatísticos efetuados. Um tratamento, em maior detalhe, deste tópico, pode ser consultado, por exemplo, em Correia (2012: 140-144).

[4] 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.

[5] Mediana de 32,00 anos; desvio-padrão de 14,22 anos.

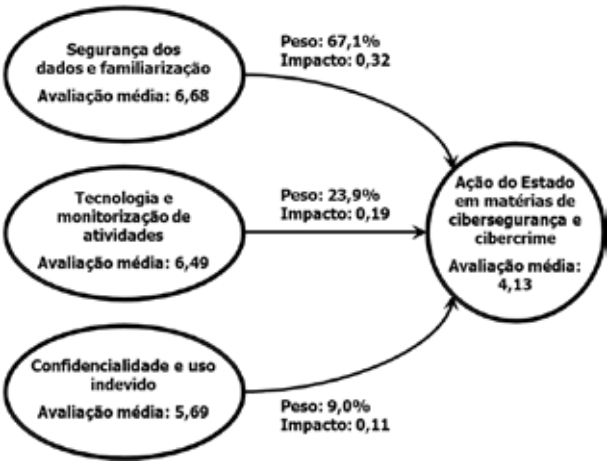
utilizar a internet diariamente e 357 (30,6%) afirmaram utilizar a internet mais de 3 horas, diariamente (tendo ainda sido registados 22 valores omissos, correspondendo a 1,9%).

A formação das quatro variáveis latentes com base nas 10 variáveis de medida associadas às perceções sobre políticas públicas em matéria de cibersegurança e cibercrime, bem como a estimação do modelo proposto na Figura 1 foram realizadas por intermédio da aplicação de um modelos de equações estruturais (metodologia *SEM*), que permitiu a atribuição de um impacto e de um peso à influência de cada dimensão independente (segurança dos dados e familiarização; tecnologia e monitorização de atividades; e confidencialidade e uso indevido) na dimensão dependente (ação do Estado em matérias de cibersegurança e cibercrime)[6].

5. Resultados

A análise da Figura 2 permite concluir que, para o modelo teórico proposto na Figura 1, as avaliações médias das dimensões segurança dos dados e familiarização; tecnologia e monitorização de atividades; confidencialidade e uso indevido; e ação do Estado em matérias de cibersegurança e cibercrime são, respetivamente, 6,68; 6,49; 5,69; e 4,13 pontos.

Figura 2
Resultados do modelo de perceções sobre políticas públicas em matéria de cibersegurança e cibercrime



Fonte: elaboração própria.

[6] Esta metodologia encontra-se descrita de forma mais detalhada em Tenenhaus *et al*. (2005) ou Correia (2012: 162-170). Exemplos de aplicação similar podem ser consultados, por exemplo, em Correia (2013), Correia *et al*. (2013), Correia e Bilhim (2014), ou Correia e Garcia (2015).

Adotando 5,00% como nível de significância, é possível afirmar que o aumento de 1 ponto na avaliação média da variável latente independente segurança dos dados e familiarização teria um impacto direto de 0,32 pontos na variável latente dependente ação do Estado em matérias de cibersegurança e cibercrime, o aumento de 1 ponto na avaliação média da variável latente independente tecnologia e monitorização de atividades teria um impacto direto de 0,19 pontos na variável latente dependente ação do Estado em matérias de cibersegurança e cibercrime, e o aumento de 1 ponto na avaliação média da variável latente independente confidencialidade e uso indevido teria um impacto direto de 0,11 pontos na variável latente dependente ação do Estado em matérias de cibersegurança e cibercrime. A variável latente independente que apresenta maior peso na formação das perceções sobre a variável latente dependente ação do Estado em matérias de cibersegurança e cibercrime é a variável latente independente segurança dos dados e familiarização, com um contributo de cerca de 67,1%, seguida da variável latente independente tecnologia e monitorização de atividades, com um contributo de cerca de 23,9% e da variável latente independente confidencialidade e uso indevido, com um contributo de cerca de 9,0%.

O Quadro 2 apresenta os índices de qualidade do modelo proposto. Tendo como referência os critérios de avaliação da qualidade deste tipo de modelos (Fornell e Cha, 1994; Tenenhaus *et al*., 2005; Karim, 2009), o modelo proposto apresenta um coeficiente de determinação ajustado relativamente baixo, um índice de bondade do ajustamento moderado e Estatísticas de Stone-Geisser (Stone, 1974; Geisser, 1975) globalmente aceitáveis[7].

Quadro 2
Índices de qualidade do modelo explicativos da variável latente dependente ação do Estado em matérias de cibersegurança e cibercrime

Parâmetro	Modelo
R^2	0,162
R^2-*ajustado*	0,161
Índice de Bondade do Ajustamento (*GoF*)	0,329
Estatísticas Q^2 de Stone-Geisser	
SSO	317.273
SSE	90.782
SSE'	363.959
H^2	0,714
F^2	-0,147

Fonte: elaboração própria.

[7] Informações adicionais sobre os parâmetros do modelo (estimativas das médias das variáveis de medida e correlações entre as variáveis latentes) podem ser encontradas no Apêndice, apresentado no final do texto.

O modelo proposto permitiu confirmar a validade amostral de todas as hipóteses avançadas neste texto: H1, H2 e H3[8].

Os dados apresentados na Figura 2 e descritos no texto, complementados pela informação constante do Apêndice, colocam em evidência que, em Portugal, as perceções médias face a qualquer uma das três variáveis latentes independentes consideradas no estudo são favoráveis (sempre superiores a 5 pontos em 10 possíveis), oscilando entre um valor mínimo de 5,69 pontos, relativo à dimensão confidencialidade e uso indevido, e um valor máximo de 6,68 pontos, relativo à dimensão segurança dos dados e responsabilização. Contudo, não obstante os valores favoráveis obtidos ao nível das dimensões independentes do modelo, a dimensão dependente, ação do Estado em matérias de cibersegurança e cibercrime, apresenta um valor médio desfavorável para as perceções, correspondendo a 4,13 pontos. Dignos de relevo são ainda os indicadores SDF 3 (que importância atribui à segurança dos dados dos seus dispositivos digitais), TMA 1 (concorda com a vulgarização do uso da videovigilância em espaços públicos) e SDF 1 (como classifica o seu entendimento do conceito de "Cibercrime"), que apresentam as avaliações médias mais elevadas (as avaliações médias destas variáveis de medida foram, respetivamente, 8,43; 6,98 e 6,72 pontos). Em sentido contrário, destacam-se as variáveis de medida AEMCC 1 (como avalia o seu conhecimento da legislação e dos organismos que, em Portugal, se ocupam da criminalidade informática), AEMCC 2 (como classifica a eficácia da atuação do Estado em matéria de segurança informática) e CUI 1 (as entidades públicas, consoante a sua atribuição, detêm dados dos cidadãos. Qual a importância de estas informações permanecerem confidenciais?), pelos seus valores desfavoráveis (as avaliações médias destes indicadores foram, respetivamente, 4,22; 3,90 e 2,53 pontos).

6. Discussão e conclusões

O principal objetivo da investigação empírica cujos resultados são apresentados neste artigo consistiu em testar a existência de relações de causalidade entre as dimensões relacionadas com a ação do Estado em matérias de cibersegurança e cibercrime (Quadro 1). O modelo de equações estruturais proposto para as relações

[8] Note-se que, no presente estudo, considerou-se a validade amostral como confirmada sempre que se registou um p-valor<0,05 para o impacto direto entre as dimensões em análise. De modo similar, considerou-se a validade amostral como infirmada sempre que se registou um p-valor≥0,05 para o impacto direto entre as dimensões em análise.

causais entre as quatro variáveis latentes utilizadas na pesquisa pode ser encontrado na Figura 1.

O Quadro 3 e os Quadros 4 e 5 (estes últimos constantes do Apêndice apresentado no final do texto) permitem afirmar que as medidas e os índices de qualidade do modelo apresentam evidências estatísticas de um ajuste razoável.

Em termos de resultados, o modelo de equações estruturais (Figura 2) revela coeficientes de impacto estatisticamente significativos para níveis de significância de 0,05 (p-valores todos inferiores a 0,05)[9]. Assim sendo, foram confirmadas as validades amostrais das três hipóteses inicialmente avançadas: H1, H2 e H3. Por isso mesmo, pode ser considerada como válida a seguinte afirmação: as perceções dos cidadãos sobre as variáveis latentes segurança dos dados e familiarização; tecnologia e monitorização de atividades; e confidencialidade e uso indevido têm impacto direto e positivo nas perceções dos cidadãos sobre a variável latente ação do Estado em matérias de cibersegurança e cibercrime.

É possível concluir, pelo acima exposto, que o modelo para as perceções sobre a ação do Estado em matérias de cibersegurança e cibercrime, avançado neste texto, é globalmente válido, não obstante os ganhos futuros que possam vir a ser obtidos em termos da sua qualidade e robustez. Os resultados consubstanciam-se ainda na validade do modelo de medida para as perceções face à ação do Estado em matérias de cibersegurança e cibercrime, composto por 10 indicadores (Quadro 1), contributo original deste trabalho e que teve por base considerações sobre a realidade Portuguesa, conceitos de referência constantes da literatura académica, e a legislação nacional e europeia sobre esta temática (Enge, 1994; União Europeia, 2001; Marques e Martins, 2006; Mullins, 2007; Correia e Jesus, 2013; Jonhson, 2015; Portugal, 1998, 2009, 2012, 2013, 2015).

Foi também possível tornar evidente que, apesar das perceções médias favoráveis obtidas nas dimensões independentes (segurança dos dados e familiarização: 6,68 pontos; tecnologia e monitorização de atividades: 6,49 pontos; e confidencialidade e uso indevido: 5,69 pontos), a dimensão dependente ação do Estado em matérias de cibersegurança e cibercrime não goza de níveis de perceção favoráveis por parte dos cidadãos (4,13 pontos). O mesmo é dizer que os inquiridos se encontram globalmente pouco satisfeitos com a ação do Estado em matérias de cibersegurança e cibercrime. Ora, se as perceções médias dos cidadãos face às variáveis latentes associadas à

[9] Efetivamente, os coeficientes de impacto continuam válidos mesmo que em vez dos habituais níveis de significância de 5,00%, sejam considerandos níveis de significância tão restritivos como 0,10%, o que reforça a robustez e confiança no modelo proposto.

segurança dos dados e familiarização; à tecnologia e monitorização de atividades; e à confidencialidade e uso indevido são todas favoráveis e a perceção dos cidadãos face à ação do Estado em matérias de cibersegurança e cibercrime não espelha esses resultados, é possível conjeturar quanto à existência de um enviesamento conjuntural das perceções no sentido de uma apreciação pouco objetiva da gestão pública e das políticas públicas nestas matérias. De outra forma, seria difícil compreender por que motivo cidadãos que avaliam positivamente questões ligadas à segurança dos dados, familiarização com as tecnologias, monitorização informática de atividades ou confidencialidade dos dados, seriam os mesmos que avaliam aspetos gerais ligados à atuação do Estado em matérias de cibersegurança e cibercrime de forma desfavorável.

De uma forma mais abrangente e genérica, os resultados decorrentes desta investigação permitem que profissionais e académicos dedicados às questões da gestão pública e das políticas públicas possam, ao aplicar o modelo proposto ou um modelo similar neste alicerçado, avaliar as dinâmicas relevantes para a construção das perceções dos cidadãos face à ação do Estado em matérias de cibersegurança e cibercrime, dando desta forma o seu contributo para o progresso e evolução da performance e da qualidade da gestão e das políticas públicas nesta nova e crescentemente relevante área de atuação do Estado. Sem dúvida que a governança dos aspetos relacionados com a segurança tecnológica, isto é, a relação entre o Estado e os cidadãos em matérias de segurança tecnológica, num contexto cada vez mais caracterizado pela prevalência do *hollow state*, continuará a assumir, e cada vez mais, relevância sociológica.

A principal preocupação teórico-metodológica que deverá ser tida em conta em estudos futuros está diretamente associada ao valor obtido para o coeficiente de determinação ajustado do modelo (0,161). Este valor pode ser interpretado como a percentagem da variabilidade do fenómeno da perceção da ação do Estado em matérias de cibersegurança e cibercrime que é explicada pelo modelo: 16,1%. Como tal, é possível afirmar que cerca de 83,9% da variabilidade deste fenómeno está relacionada com fatores (variáveis de medida e/ou variáveis latentes) que não foram consideradas no modelo analisado neste texto. Por isso mesmo, propor novas variáveis de medida que possam teoricamente justificar inclusão no modelo apresentado, propor o agrupamento dessas novas variáveis de medida em variáveis latentes que complementem as variáveis latentes propostas neste artigo e proceder à sua validação empírica com vista à melhoria da percentagem da variabilidade do fenómeno que é explicada, devem ser as prioridades de qualquer estudo futuro sobre esta temática.

Sugere-se ainda que investigações futuras sobre estas matérias permitam

conseguir um acompanhamento continuado do fenómeno relativo às perceções dos cidadãos face à ação do Estado em matérias de cibersegurança e cibercrime, particularmente através da recolha de dados de forma regular e periódica, de preferência com recurso a amostras com maior dimensão e representatividade.

Finalmente, sugere-se a adaptação e aplicação, quer do modelo de medida, quer do modelo estrutural, a estádios de desenvolvimento tecnológico e realidades sociojurídicas distintas da portuguesa, de que são exemplos especialmente relevantes os contextos existentes em países da América Latina como o Brasil, que partilham ligações históricas e sociológicas mais intensas com Portugal.

Referências bibliográficas

AOS, Steve; MILLER, Marna; DRAKE, Elizabeth (2006), *Evidence-based public policy options to reduce future prison construction, criminal justice costs, and crime rates*. Olympia, Washington State Institute for Public Policy.

BILHIM, João Abreu de Faria; CORREIA, Pedro Miguel Alves Ribeiro (2016), "Diferenças nas perceções dos valores organizacionais dos candidatos a cargos de direção superior na Administração Central do Estado", *Sociologia*, *Revista da Faculdade de Letras da Universidade do Porto*, Vol. XXXI, pp. 81-105.

CORREIA, Pedro Miguel Alves Ribeiro (2012), *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*, Tese de Doutoramento em Ciências Sociais (Especialidade em Administração Pública), Lisboa, Instituto Superior de Ciências Sociais e Políticas da Universidade Técnica de Lisboa.

- (2013), "Igualdade de género no Ministério da Justiça em Portugal: Evidências estatísticas de igualdade homem-mulher na lealdade laboral", *Direitos Fundamentais & Justiça*, 7 (23), pp. 121-130.

CORREIA, Pedro Miguel Alves Ribeiro; BILHIM, João Abreu de Faria (2014), "A antiguidade na organização e a satisfação laboral dos colaboradores do Ministério da Justiça em Portugal: Evidências de uma relação em forma de L e não em forma de U", *Revista de Economia e Administração*, 13 (2), pp. 159-177. doi: 10.11132/rea.2014.872.

CORREIA, Pedro Miguel Alves Ribeiro; GARCIA, Bruno Cardoso (2015), "Administração hospitalar em Portugal: Evidências estatísticas de igualdade homem-mulher nas percepções sobre os sistemas de avaliação de desempenho", *Revista Latino-Americana de Geografia e Gênero*, 6 (1), pp. 127-139. doi: 10.5212/Rlagg.v.6.i1.0009.

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de (2013), "O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana", *Direito, Estado e Sociedade*, 43, pp. 135-61.

- (2016), "Combate às Transferências Bancárias Ilegítimas pela Internet no Direito Português: Entre as Experiências Domésticas e Políticas Globais Concertadas", *Revista Direito GV*, 12 (2), pp. 542-563.

doi: 10.1590/2317-6172201622

CORREIA, Pedro Miguel Alves Ribeiro; MOREIRA, Maria Faia Rafael; GARCIA, Bruno Cardoso (2013), "Igualdade de género no Ministério da Justiça em Portugal: evidências estatísticas de diferenças homem-mulher na satisfação laboral", *Scientia Ivridica*, 62 (333), pp. 569-590.

CORREIA, Pedro Miguel Alves Ribeiro; SANTOS, Susana Isabel da Silva; CORREIA, Maria do Céu Alves Ribeiro Figueiredo (2017, *in press*), "Perceções sobre Cibersegurança e Privacidade em Portugal: Evidências Estatísticas de Igualdade e Desigualdade de Género", *Revista Latino-Americana de Geografia e Género*, 8 (1).

ENGE, Per (1994), "The global positioning system: Signals, measurements, and performance", *International Journal of Wireless Information Networks*, 1 (2), pp. 83-105. doi: 10.1007/BF02106512

FORNELL, Claes; CHA, Jaesung (1994), "Partial least squares", *in* Richard Bagozzi (ed.), *Advanced Methods of Marketing Research*, Cambridge, England, Blackwell.

FREDERICKSON, George; SMITH, Kevin; LARIMER, Christopher; LICARI, Michael (2012), *The public administration theory primer*, USA: Westview Press.

GEISSER, Seymour (1975), "The Predictive Sample Reuse Method with Applications", *Journal of the American Statistical Association*, 70 (350), pp. 320-328. doi: 10.1080/01621459.1975.10479865

GOODMAN, Marc (2015), *The future crimes*, UK, Transworld Publishers Ltd.

HAY, Colin (2002) , *Political analysis: A critical introduction*, Basingstoke, Palgrave.

HILL, Michael (2005) , *The public policy process* (4.ª ed.) , England, Pearson Education.

HOWLETT, Michael; RAMESH, M. (2009) , *Studying public policy: policy cycles and policy subsystems* (3.ª ed.), UK, Oxford University Press.

JOHNSON, Thomas A. (2015), *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*, Missouri: CRC Press.

KARIM, Jahanvash (2009) , "Emotional labor and psychological distress: Testing the mediatory role of work-family conflict" , *European Journal of Social Sciences*, 11 (4), pp. 584-598.

KETTL, Donald (2000), *The global public management revolution*, Washington, Brookings Institution Press.

LEVI-FAUR, David; VIGODA-GADOT, Eran (ed.) (2004), *International public policy and management*, New York, CRC Press.

MARQUES, Garcia; MARTINS, Lourenço (2006), *Direito da informática*, Coimbra, Almedina.

MCGUIRE, Mike; DOWLING, Samantha (2013) *, Research report 75*, London, Home Office.

MILWARD, H. Brinton; PROVAN, Keith (2000) , "How networks are governed" , *in* Carolyn Lynn; Laurence Heinrich; Laurence Lynn (eds.), *Governance and performance: New perspectives*, Washington, D. C., Georgetown University Press.

MULLINS, Laurie (2007), *Management and organisational behaviour*, Harlow, Pearson Education.

PETERS, B. Guy; PIERRE, Jon (2006), *Handbook of public policy*, London, SAGE Publications Ltd.

POLLITT, Christopher; BOUCKAERT, Geert (2011), *Public management reform: A comparative analysis – new public management, governance, and the Neo-Weberian state*, New York, Oxford University Press.

PORTUGAL (1998) , "Lei n.º *67/98*" , *Diário da República*, 1.ª *série, 247, 55*36-5546, 26 de outubro de 1998.

PORTUGAL (2009) , "Lei n.º 109/2009" , *Diário da República,* 1.ª série, 179, 6319-6325, 15 de setembro de 2009.

PORTUGAL (2012) , "Lei n.º 9/2012" , *Diário da República.* 1.ª série, 39, pp. 868-874, 23 de fevereiro de 2012.

PORTUGAL (2013) , "Lei n.º 34/2013", *Diário da República*, 1.ª série, 94, 2921-2942, 16 de maio de 2013.

PORTUGAL (2015) , "Resolução do Conselho de Ministros n.º 36/2015" , *Diário da República*, 1.ª série, 113, 3738-3742, 12 de junho de 2015.

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

STONE, M. (1974), "Cross-Validatory Choice and Assessment of Statistical Predictions" , *Journal of the Royal Statistical Society*, 36, pp. 111-147.

TENENHAUS, Michel; VINZI, Vincenzo; CHATELIN, Yves-Marie; LAURO, Carlo (2005) , "PLS path modeling", *Computational Statistics and Data Analysis*, 48 (1), pp. 159-205. doi: 10.1016/j.csda.2004.03.005

UNIÃO EUROPEIA (2001), *Convenção sobre o cybercrime*, Budapest: Série de Tratados Europeus. 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.

Pedro Miguel Alves Ribeiro Correia. (autor de correspondência). Professor do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa (ISCSP-ULisboa), (Lisboa, Portugal). Investigador integrado do Centro de Administração e Políticas Públicas (CAPP, ISCSP-ULisboa) (Lisboa, Portugal). Investigador colaborador do Centro Interdisciplinar de Estudos de Género (CIEG, ISCSP- Ulisboa). Endereço de correspondência: Instituto Superior de Ciências Sociais e Políticas, Rua Prof. Almerindo Lessa, 1300-663 Lisboa, Portugal. *E-mail*: pcorreia@iscsp.ulisboa.pt.

Website:

http://www.degois.pt/visualizador/curriculum.jsp?key=5791094296158620

Susana Isabel da Silva Santos. Mestranda em Gestão e Políticas Públicas no Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa (ISCSP-ULisboa), (Lisboa, Portugal). Investigadora do Projeto Inovação, Gestão, Administração e Políticas Públicas (IGAPP, CAPP, ISCSP-ULisboa) (Lisboa, Portugal). Endereço de correspondência: Instituto Superior de Ciências Sociais e Políticas, Rua Prof. Almerindo Lessa, 1300-663 Lisboa, Portugal. *E-mail*: susanaissantos@gmail.com.

Website:

http://www.degois.pt/visualizador/curriculum.jsp?key=4652581084713291

João Abreu de Faria Bilhim. Professor do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa (ISCSP-ULisboa), (Lisboa, Portugal); Investigador integrado do Centro de Administração e Políticas Públicas (CAPP, ISCSP-ULisboa) (Lisboa, Portugal). Endereço de correspondência: Instituto Superior de Ciências Sociais e Políticas, Rua Prof. Almerindo Lessa, 1300-663 Lisboa, Portugal. *E-mail*: bilhim@iscsp.ulisboa.pt.

Website:

http://www.degois.pt/visualizador/curriculum.jsp?key=6889163091318193

Artigo recebido em 20 de dezembro de 2015. Publicação aprovada em 23 de junho de 2016.

Apêndice

Quadro 3

Estimativas das médias das variáveis de medida

Variável latente		Média	Variável de medida (*)	Pesos normalizados	Correlações	Média
Segurança dos dados e familiarização	6,68	SDF 1	0,43	0,91	6,72	6,72
		SDF 2	0,55	0,95	6,57	6,57
		SDF 3	0,02	0,21	8,43	8,43
Tecnologia e monitorização de atividades	6,49	TMA 1	0,28	0,73	6,98	6,98
		TMA 2	0,33	0,83	6,21	6,21
		TMA 3	0,39	0,82	6,37	6,37
Confidencialidade e uso indevido	5,69	CUI 1 (escala invertida)	0,09	-0,15	2,53	2,53
		CUI 2	0,91	1,00	5,99	5,99
Ação do Estado em matérias de cibersegurança e cibercrime	4,13	AEMCC 1	0,70	0,96	4,22	4,22
		AEMCC 1	0,30	0,64	3,90	3,90

Fonte: elaboração própria; Nota: (*) abreviaturas de acordo com o Quadro 1.

Quadro 4

Correlações entre as variáveis latentes do modelo

Variável latente	Segurança dos dados e familiarização	Tecnologia e monitorização de atividades	Confidencialidade e uso indevido	Ação do Estado em matérias de cibersegurança e cibercrime
Segurança dos dados e familiarização	1			
Tecnologia e monitorização de atividades	0,058	1		
Confidencialidade e uso indevido	0,098	-0,050	1	
Ação do Estado em matérias de cibersegurança e cibercrime	0,341	0,204	0,132	1

Fonte: elaboração própria.