A ação do Estado em matéria de cibersegurança: Estudo de perceções no caso português

La acción del Estado sobre asuntos de ciberseguridad: Estudio de percepciones en el caso portugués

The State's action on cybersecurity matters: Study of perceptions on the Portuguese case

Recebido em 16-12-2016
Aceito para publicação em 12-03-2018

Pedro Miguel Alves Ribeiro Correia

Doutorado em Ciências Sociais (Especialidade em Administração Pública) no Instituto Superior de Ciências Sociais e Políticas da Universidade Técnica de Lisboa, Portugal. Professor no Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa. Investigador Integrado do Centro de Administração e Políticas Públicas. Consultor da Direção-Geral da Política de Justiça do Ministério da Justiça de Portugal. E-mail: pcorreia@iscsp.ulisboa.pt

Susana Isabel da Silva Santos

Licenciatura em Administração Pública da Universidade de Lisboa, Portugal. Mestranda em Gestão e Políticas Públicas da ULisboa. Mestranda em Estatística e Gestão de Informação da NOVA - Universidade Nova de Lisboa. Investigadora Colaboradora no Projeto Inovação, Gestão, Administração e Políticas Públicas (IGAPP) do CAPP-ISCSP-ULisboa. E-mail: susanaissantos@gmail.com

Resumo

Este artigo aborda, tendo como caso de estudo a realidade portuguesa, a problemática das perceções sobre a ação do Estado em matéria de cibersegurança. São apresentados e contextualizados tópicos relevantes sobre a ação do estado e as políticas públicas. É dado ênfase aos problemas associados à privacidade, dados pessoais e bases de dados, bem como ao tema do cibercrime e suas tipologias. São relatados e analisados os resultados da pesquisa empírica realizada às percepções de 1.216 inquiridos. Por fim, é feita uma reflexão acerca da necessidade de incorporar as perceções dos cidadãos na ação do Estado em matéria de cibersegurança, face aos seus anseios de confidencialidade e segurança, à necessidade de consciencialização e uso equilibrado das novas tecnologias digitais, e à necessidade de um melhor conhecimento das leis e de reconhecimento da eficiência do Estado nestes domínios.

Palavras-Chave: Cibersegurança; Cibercrime; Privacidade; Estado; Percepção.

Resumen

Este artículo analiza, basado en el estudio del caso portugués, la problemática de las percepciones sobre el papel del Estado en materia de ciberseguridad. Se presentan y contextualizan temas relevantes sobre la acción del Estado y las políticas públicas. Es dado énfasis a los problemas relacionados con la privacidad, los datos personales y bases de datos, así como al tema de la cibercrimen y sus tipologías.

Se relatan e analizan resultados de una investigación empírica sobre las percepciones de 1.216 inquiridos. Por último, se hace una reflexión sobre la necesidad de incorporar las percepciones de los ciudadanos en la acción del Estado en el campo de la ciberseguridad, dadas sus expectativas de confidencialidad y seguridad, la necesidad de conocimiento y uso equilibrado de las nuevas tecnologías digitales, y la necesidad de un mejor conocimiento de las leyes y de reconocimiento de la eficiencia del Estado en estas áreas.

Palabras Clave: Ciberseguridad; Ciberdelincuencia; Privacidad; Estado. Percepción.

Abstract

This article discusses, based on the Portuguese case study, the problematic of perceptions on the role of the State on cybersecurity matters. Relevant topics on the state's action and on public policies are presented and contextualized. Emphasis in given to problems associated with privacy, personal data and databases, as well as to the cybercrime theme and its typologies. Results from an empirical research on perceptions of 1,216 respondents are reported and analyzed. Finally, a reflection is made on the need to incorporate the perceptions of citizens regarding the state's action in the field of cybersecurity, given their expectations of confidentiality and security, the need for awareness and balanced use of new digital technologies, and the need for a better knowledge of laws and a recognition of the State's efficiency in these areas.

Keywords: Cybersecurity; Cybercrime; Privacy; State; Perception.

Introdução

As tecnologias de informação e comunicação estão hoje perfeitamente consolidadas na rotina das pessoas, assim como no funcionamento de qualquer organização. A transformação e disseminação tecnológica possibilitou ativamente o acesso e partilha de informação, poupando recursos e facilitando processos outrora dispendiosos e extremamente morosos. No entanto, enquanto os media anunciam as últimas novidades em termos de tecnologia e fazem avaliações e *rankings* de aparelhos digitais, são raras as abordagens às temáticas relativas às várias consequências e adaptações necessárias a este fenômeno. Acontece que a lista de "utilizações menos desejadas" das tecnologias de informação e comunicação é extremamente extensa e complexa, relacionando-se estreitamente com a natureza dos dados ou credenciais em causa, e com a natureza do próprio alvo: uma pessoa, uma organização, ou um Estado. Nos dias de hoje, já se afigura incontável o número de incidentes que diariamente, pelas mais diversas técnicas e motivações, consubstanciam crimes cibernéticos.

A cibersegurança será, previsivelmente, um assunto premente ao longo dos próximos anos, da mesma forma que os sistemas de informação e a sociedade da informação dominaram anteriormente. Este enfoque na segurança cibernética verificar-se-á

particularmente naquilo que é a ação do Estado, dada a sua atribuição na defesa e segurança do território e dos cidadãos.

Neste artigo, depois de breves abordagens de enquadramento aos tópicos da ação do Estado, das políticas públicas, da privacidade, dados pessoais e bases de dados, e do cibercrime, são apresentados os resultados de um estudo às percepções sobre a ação do Estado em matéria de cibersegurança em Portugal.

A ação do Estado

O início da organização político-administrativa que hoje conhecemos como Administração Pública remonta à necessidade da organização do Estado para fazer face às exigências sociais, econômicas e políticas e, por via disso, da necessidade de recolha de coletas, de forma a promover a segurança e as obras públicas.

Jorge Miranda (1992) considera que existem sempre duas características comuns e caracterizantes de qualquer função ou atividade do Estado:

- Ser específica ou diferenciada, pelos seus elementos materiais – os resultados que produz – formais – os trâmites e as formalidades que exige – e orgânicos – os órgãos ou agentes por onde corre;
- Ser duradoura – prolonga-se indefinidamente, ainda que se desdobre em atos localizados no tempo que envolvem pessoas e situações diversas.

Ora, a garantia da segurança é uma necessidade coletiva ancestral elementar, quer para regular comportamentos desviantes inerentes à mera existência e coexistência humana, quer no aspecto da coletividade, enquanto agregados de dada circunscrição territorial face às demais. Posto isto, importa diferenciar dois conceitos: o de Defesa Nacional e o de Segurança Interna.

A Defesa Nacional são as ações e políticas que os Estados desenvolvem e aplicam para prevenir ou combater ataques levados a cabo por outros países. Aqui se compreende o assegurar da soberania, da independência e do funcionamento democrático. Já a Segurança Interna, segundo a Lei n.º 53/2008 (PORTUGAL, 2008) que regula esta matéria, é a atividade desenvolvida pelo Estado para garantir a ordem, segurança e tranquilidade públicas,

protegendo bens e pessoas[1]. A Defesa Nacional e a Segurança Interna constituem, talvez, os melhores exemplos de bens coletivos puros, isto é, são serviços disponibilizados pelo Estado, em que todos os utilizadores usufruem da mesma quantidade e nas mesmas condições, sem sequer poder para negar a sua fruição (SANTOS, 2012).

A atividade de informações desenvolveu-se na Europa durante os séculos XVIII e XIX. Inicialmente, assente nos conceitos de defesa militar e de segurança interna como instrumento de guerra ou numa lógica repressiva de manutenção de regimes políticos (CARVALHO, 2009). As Tecnologias de Informação e Comunicação (TIC) funcionam atualmente como catalisadores de informações, negócios, suporte tecnológico de serviços e infraestruturas, quer no sector público quer privado. Esta centralização inclui, por exemplo, os sistemas de informação e comunicação dos governos, das instâncias policiais e militares ou das entidades da Administração Pública. Acontece que os ataques a estas estruturas vitais são relativamente fáceis de realizar e capazes de inviabilizar integralmente os sistemas (NUNES, 2012). Reconhece-se, pois, que o Estado tem uma dupla necessidade de ação uma vez que se verifica:

> (…) a existência de um nível nacional e supranacional de cibersegurança (...) deste modo, o Estado deve] garantir não só a utilização segura do ciberespaço aos seus cidadãos mas também a salvaguarda da sua própria soberania (NUNES, 2012).

Ao "curso de ação por parte de um ou mais atores públicos ou governamentais" (ANDERSON, 1984, como citado em BILHIM, 2008) chamamos políticas públicas. As políticas públicas são diretrizes elaboradas para enfrentar um problema público. Entende-se como problema público "a diferença entre a situação atual e uma situação ideal" (SECCHI, 2011). Dye (2012), definia-as como "whatever goverments choose to do or not do do" sendo que estas não são meras intenções, são, antes, resultantes de *inputs* convertidos, através do processo de decisão, em programas e leis (ROCHA, 2010).

Hill (2005) afirma que existe uma transição entre Governo e Governação, ou seja, de um estado Weberiano (clara separação entre Política e Administração), para um Estado pós-moderno (como citado em ROCHA, 2010). Ou seja, num contexto de descrença no Estado tradicional e com uma tendência para a descentralização, a ação do Estado é hoje percecionada como uma atividade desenvolvida por inúmeras organizações e inúmeros indivíduos, numa estrutura interligada, em analogia a uma rede.

[1] A Lei n.º 59/2015, de 24 de junho constituiu a primeira alteração à Lei da Segurança Interna modificando a composição do Conselho Superior de Segurança Interna (nomeadamente pela inclusão do coordenador do Centro Nacional de Cibersegurança) e à organização e funcionamento da Unidade de Coordenação Antiterrorismo.

Políticas públicas

As políticas públicas assumem uma visão holística de um determinado tema, numa abordagem multidisciplinar em que estão envolvidas áreas como a ciência política, a gestão ou a econometria (SOUZA, 2006). Surgem, contudo, algumas divergências na consideração das políticas públicas. Leonardo Secchi (2011) refere, por exemplo, fatores como a consideração ou não do Estado como único agente criador de políticas públicas, a consideração da ausência de ação como uma opção, ou a contemplação apenas de indicações estratégicas ou também de diretrizes operacionais.

As políticas públicas são transversais às diversas áreas que hoje em dia estão cobertas pela intervenção Estatal, desde a saúde à educação, passando pelo planejamento urbano ou a cibersegurança. Acontece que não existem políticas uniformes a todas as áreas de intervenção, sendo que cada problema exige uma ponderação e resolução específica tendo em conta inúmeros fatores. As políticas públicas têm, ainda, uma conceção complexa uma vez que são indissociáveis do processo político, ao mesmo tempo que o seu desenho, implementação e administração envolve múltiplos atores, objetivos e agendas (FREDERICKSON *et al*., 2012, p. 226).

Embora a formulação de políticas públicas vá depender necessariamente da área a abordar, existem modelos e teorias que permitem analisar o percurso das políticas públicas desde a sua génese, ao mesmo tempo que permitem avaliar a deliberação política que lhes é inerente. Ainda que existam inúmeros modelos e teorias explicativas do processo das políticas públicas, existem algumas teses que a maioria dos autores da especialidade compartilham: a teoria do ciclo público, a teoria da escolha pública, a teoria pluralista/das *networks* e a teoria institucional (ROCHA 2010).

A teoria do ciclo das políticas públicas divide o processo político em diversas fases subsequentes e interdependentes. Diferentes autores têm diversas visões sobre o número de fases do ciclo, mas assumem-se como principais as seguintes: identificação do problema, agendamento, planejamento, implementação, e avaliação (SOUZA, 2006; SECCHI, 2011).

Segundo Sjöblom (1984) a identificação do problema envolve a percepção, a sua definição e delimitação, e a avaliação da hipótese de resolução (SECCHI, 2011). A formação

da agenda política, por sua vez, prende-se com o processo decisório da inclusão e atribuição de importância, ou não, a certas problemáticas, por parte dos governos[2].

O planejamento é a fase em que são definidos os objetivos a alcançar, em que se verificam as possíveis soluções e os seus efeitos (SECCHI, 2011). É nesta fase que são formulados planos estratégicos, considerados os custos e a eficácia das diversas alternativas. Os mecanismos disponíveis para os *policymakers* são, segundo Bobbio (1987), assentes em três formas de poder: econômico, político e ideológico. É destes que derivam os mecanismos de indução de comportamento: premiação, coerção, consciencialização e soluções técnicas (SECCHI, 2011).

A tomada de decisão e implementação das políticas é a fase posterior à consideração dos vários objetivos a atingir, dos métodos possíveis, e da respetiva eficácia e custos.

A pós-implementação segue-se, para finalizar, com a avaliação do efeito gerado pela implementação das políticas em questão.

Atualmente, o processo político relativo à formulação de políticas públicas é tido como baseado na "racionalidade, nos termos da teoria da escolha pública" (BILHIM, 2008, p. 210). A base da teoria da escolha pública (também conhecida como escolha racional) é a fundamentação na análise econômica em prol da resolução de problemas de ordem pública (SANTOS, 2012). Esta teoria assenta em dois pressupostos:

> • Em primeiro, assume que cada indivíduo procura obter a maximização da utilidade, isto é: o indivíduo conhece as suas preferências, consegue ordena-las e escolherá aquela que melhor preencher as suas necessidades pelo menor custo (FREDERICKSON *et al*., 2012). Segundo Anthony Downs (1957, 1967) assume-se que qualquer indivíduo, embora racional, é egoísta, teorema que ficou conhecido como axioma do interesse pessoal (SANTOS, 2012);
>
> • Em segundo, considera que as ações e decisões coletivas são a soma das ações e decisões individuais (FREDERICKSON *et al*., 2012).

Segundo Michael Jensen (1994) as ações humanas baseiam-se na resposta a incentivos, em que os indivíduos escolhem a opção que, para eles, demonstra ser a mais vantajosa. As teorias que se apresentam opostas à da escolha pública supõem um mundo em que os seres humanos atribuem o mesmo nível de utilidade econômica a todas as opções que

[2] A definição da agenda política depende essencialmente de três fatores: a consciencialização do problema e dos seus efeitos nocivos; a construção coletiva da necessidade de o resolver (por exemplo, através do processo eleitoral ou grupos de pressão); e por fim, a atitude dos participantes, quer os evidentes – políticos, partidos, *media* – quer os mais sutis – como por exemplo, os académicos (Souza 2006).

dispõe. Segundo o mesmo autor, esta presunção é inconcebível, impossível de acontecer num estado de naturalidade intelectual "(...) even primitive man faces incentives to cultivate one piece of land rather than another or to choose one path over another" (JENSEN, 1994).

Assim, a teoria da escolha pública prevê que todas as pessoas (inclusive os políticos, supostamente agentes altruístas que defendem o interesse público) se movem por interesses pessoais. Segundo Santos (2012), constituem motivações pessoais as remunerações econômicas, a influência, o poder, ou, no caso dos políticos, a possibilidade de serem reeleitos ou de obter bons cargos uma vez findo o mandato. Segundo Anthony Downs (como citado em ROWLEY e SCHNEIDER, 2004) "parties formulate policies in order to win elections, rather than win elections in order to formulate policies".

A teoria pluralista, ou das *networks*, afirma que as instituições, as estruturas sociais e as particularidades dos indivíduos e grupos, resultam da interação dos indivíduos, dos vínculos e dos relacionamentos que todos estabelecem entre si, numa espécie de rede (SOUZA, 2006).

O institucionalismo, por sua vez, aponta as instituições formais e informais como influenciadoras na conduta pessoal e coletiva. Assim, são os efeitos da interação com as instituições, formais e informais, que moldam a formulação de políticas públicas (CORTES e LIMA, 2012).

Privacidade, dados pessoais e bases de dados

O conceito de privacidade surgiu em 1890, por Samuel Warren e Louis Brandeis, batizado como "o direito de estar só", sendo que só em 1976 é consagrado, na Constituição da República Portuguesa, a primeira lei fundamental, a nível mundial, a consagrar expressamente a proteção de dados pessoais (CORREIA e JESUS, 2013). O conceito de privacidade é, no entanto, um conceito ambíguo, que se prende por um lado com o relativismo cultural e, por outro lado, com a dificuldade de delimitar o âmbito daquilo que é ou não privado. Para Gomes Canotilho e Vital Moreira, a privacidade abrange o "impedir o acesso de estranhos a informações sobre a vida privada e o direito a que ninguém divulgue as informações que tenha sobre a vida privada de outrem" (CORREIA e JESUS, 2013).

O fenômeno das redes sociais é um exemplo de partilha (suponha-se que de forma voluntária) de dados. A mais popular – o *Facebook* – registra 1,49 bilhões de utilizadores

ativos mensalmente[3]. Este fenômeno consiste numa conjuntura de estímulo à partilha de informações pessoais na forma de fotos, vídeos, interesses pessoais e preferências, associada à "panóplia de instrumentos eletrónicos especialmente intrusivos" (CORREIA e JESUS, 2013).

No que diz respeito à recolha de dados nas redes sociais, é particularmente e prontamente evidente o rastreamento das preferências de consumo para fins publicitários. Os anúncios exibidos durante a utilização das próprias páginas e aplicações são especialmente selecionados de acordo com as características e gostos do consumidor, baseados no histórico de páginas acedidas. Segundo Karas (2002), esta recolha pode ser considerada uma forma de monitorização das próprias atividades diárias das pessoas, muito à semelhança do sistema concebido por George Orwell, caracterizado pelo controlo permanente: "(...) the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized" (ORWELL, 2013). À semelhança do romance de Orwell, a ideia de monitorização permanente é muitas vezes associada aos regimes totalitários, mas a verdade é que a revolução tecnológica permitiu a criação de relatos detalhados da vida das pessoas (RICHARDS, 2013).

No que diz respeito às bases de dados governamentais de grande dimensão, a nível europeu, merecem destaque (CORREIA e JESUS, 2014):

- O Sistema de Informação Schengen (SIS1+), criado em 1995, para registrar pessoas e objetos em circulação no espaço Schengen (modernizada em 2013 no SIS II);
- O Eurodac, criado em 2003, para comparação das impressões digitais;
- O Sistema de Informação sobre Vistos (VIS), operacional desde 2011, que facilita o intercâmbio de informações sobre pedidos de vistos.

Pelo menos a nível teórico, estas bases de dados de grande dimensão encontram justificação em superiores interesses, como o combate ao terrorismo e à criminalidade, e foram concebidas para ser utilizadas de forma a obedecer ao princípio da proporcionalidade.

Estudos anteriores demonstram que as sociedades tendem a considerar como "demasiado especulativo" o facto de as suas comunicações serem vigiadas, da mesma forma que estudos sobre os efeitos nocivos da vigilância demonstram que essa mesma vigilância é mal tolerada e, geralmente, as medidas de políticas públicas que os vários governos tentam

[3] Fonte: DMR. Disponível em: <http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/3/> - Acesso em: 23 de setembro de 2015.

implementar raramente resultam em transposições para legislação sobre esta matéria (RICHARDS, 2013).

No que diz respeito à vigilância e às bases de dados governamentais, podem ser enumerados dois perigos especialmente prementes (RICHARDS, 2013):

- A ameaça ao exercício dos direitos civis, por permitir a vigília das leituras, pensamentos e comunicações, não permitindo a chamada "privacidade/liberdade intelectual";
- O efeito da interação entre observador-observado cria uma disparidade que fomenta a discriminação, coerção, chantagem, aplicação seletiva da lei, entre outros efeitos nocivos.

Ainda sobre a vigilância por parte do Estado, Neil Richards afirma que a legislação sobre vigilância deverá assentar em quatro ideias-base (RICHARDS, 2013):

- A ideia de que a problemática da vigilância transcende a separação entre as esferas pública e privada;
- A ideia de que a vigilância secreta é ilegítima;
- A ideia de que a vigilância permanente e total do indivíduo é ilegítima;
- A ideia de que a vigilância deve ser vista como algo nocivo (por fomentar o aumento de comportamentos como os supramencionados).

Com conceções antagônicas, que repudiam inteiramente qualquer tipo de legislação sobre o tema, posicionam-se autores como John Parry Barlow ou Louis Rosseto, que entendem a *web* como um potencial espaço de liberdade numa "visão libertário-anárquica (...) à margem da tirania dos Governos" (FERNANDES, 2012).

Ora, posto isto, importa abordar a privacidade de dois prismas: em primeiro lugar, de que forma a sociedade em que vivemos constitui um sistema (ainda que discreto) como o descrito por Orwell, em que as ferramentas e sistemas de recolha e transmissão de informação personificam o indesejável sistema "dono do corpo e da mente dos cidadãos" (FERNANDES, 2012); em segundo lugar, perceber, num contexto de apologia às redes sociais e aos *reality-shows*, que valor é atribuído pelas pessoas, nos dias de hoje e efetivamente, à sua privacidade.

Cibercrime

O cibercrime compreende os atos ilícitos cuja realização envolve o uso de meios informáticos. Em Portugal, inclui ainda "aqueles em que, não sendo o computador o instrumento principal da atividade ilícita, o meio de realização de prova assume a forma

digital"[4]. A União Europeia considera admissível uma certa discricionariedade na definição de cibercrime, algo que se fica a dever à complexidade, volatilidade e carácter *sui generis* do mundo tecnológico. Não obstante, em 2013, na Diretiva 2013/40/EU (UNIÃO EUROPEIA, 2013), a União Europeia expressa a necessidade de adotar definições e abordagens comuns a todos os Estados-Membros.

Como supramencionado, a Defesa Nacional distingue-se da Segurança Interna. Essa distinção é mantida em matéria cibernética. A ciberdefesa refere-se a um espaço-cibernético português e à proteção de ataques cibernéticos contra o próprio Estado – ciberguerra – e, por isso, está a cargo das Forças Armadas. A ciberguerra consiste no "conflito entre estados dentro e através do ciberespaço, e todas as ramificações que isso possa ter" (KLIMBURG, 2012, p. 17). As restantes formas de cibercrime pertencem ao domínio da Cibersegurança (o cibercrime e o hacktivismo), e estão a cargo das forças de segurança. A ciberespionagem e o ciberterrorismo estão a cargo dos Serviços de Informação. Todas estas formas de delitos estão, desde 2014, a cargo do Centro Nacional de Cibersegurança (CNCS) que, a par do Gabinete Nacional de Segurança (GNS), garante a segurança do ciberespaço e da informação classificada do Estado.

Para abordar de forma mais sistemática as infrações que constituem crimes cibernéticos, a taxonomia do CNCS agrupa os vários atos em oito classes (CENTRO NACIONAL DE CIBERSEGURANÇA, 2012). Classificam-se como "código malicioso" (vulgarmente conhecido por *malware)* os incidentes em que o agente, através do alojamento de uma codificação, ganha total acesso aos sistemas ou softwares infetados, assim como ao hardware a estes associado (JOHNSON, 2015). Da categoria "disponibilidade" fazem parte delitos que condicionam ou impossibilitam o funcionamento de um programa, pelo esgotamento dos recursos (rede, capacidade de processamento, sessões, etc.). São também atos que, intencionalmente ou não, danificam a informação ou evitam a sua transmissão: vandalismo ou disrupção intencional (REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE, 2015). Agrupam-se em "recolha de informação" os crimes de "*scan" e de "sniffing"* (consistem na sabotagem de uma rede com identificação e recolha de dados de navegação dos sistemas ligados a essa mesma rede), ou ainda de *phishing* (em que o utilizador "(…) depois de clicar numa ligação (aparentemente inocente), é levado a introduzir os seus dados pessoais

[4] Fonte: Serviço de Resposta a Incidentes de Segurança da Rede Ciência, Tecnologia e Sociedade. Disponível em: <http://fe02.cert.pt/index.php/recomendacoes/1712-o-que-e-o-cibercrime-mes-europeu-da-ciber-seguranca-2013> - Acesso em: 24 de setembro de 2015.

numa página falsa que se parece muito com a de um sítio legítimo" (JOHNSON, 2015, p. 294 -295). À "tentativa de intrusão" pertencem os delitos em que existe uma tentativa de aceder ao sistema, rede, página pessoal ou e-mail, sendo que a sua efetivação se enquadra na categoria de "intrusão". Note-se que "pequenas intrusões podem resultar em desconfigurações" (MEHAN, 2014, p. 241). Quanto às infrações relacionadas com a "segurança da informação", dizem respeito ao acesso indevido, modificação, ou eliminação de determinadas informações (CENTRO NACIONAL DE CIBERSEGURANÇA, 2012). Esta ameaça foi das primeiras a ser ponderada, estando intimamente relacionada com o advento das grandes bases de dados. Nigel Hawkes (1971) afirma que, ao reunir dados do cidadão, o computador reforça e torna mais eficiente a burocracia. Contudo, já no ano de 1971, o autor previa a necessidade imperativa de regular esta inovação de forma a evitar abusos de poder. A intrusão e acesso à informação podem ser usadas naquilo que se denomina por "ciberespionagem": situação em que, por exemplo, um governo acede a informações mais sensíveis de outro, ou uma empresa acede aos projetos de uma empresa concorrente. Na categoria de "fraude" são considerados os atos em que há uma utilização dos recursos ou do nome de uma instituição, fazendo-se passar por esta. Por fim, designados como "conteúdo abusivo" estão ações como o *spam*, a partilha de conteúdos com direitos de autor e, ainda, a disseminação de conteúdos proibidos por lei (como pornografia infantil e conteúdos pró-violência ou pró-racismo). É ainda contemplada uma classe de "outros incidentes" onde se incluem formas de ataque que não se enquadram nas acima descritas.

Importa realçar neste enquadramento dois conceitos particularmente interessantes quando se fala em cibercrime: *hacker* e *deep web*. O *hacker* é definido como o agente possuidor de *know-how* informático, por intermédio do qual explora as fragilidades do sistema, rede e/ou *software*, o que resulta (sempre) na violação do espaço de liberdade dos utilizadores. Contudo, apesar da conotação negativa que é atribuída ao conceito de *hacker*, existem os chamados "*hackers* de chapéu branco", que procuram assegurar o bom funcionamento dos sistemas, retificando as ações criminosas dos "*hackers* de chapéu preto" (MARTINS, 2012). A *deep web* (ou *web* profunda) é a parcela de informação da internet não acessível através dos *browsers* comuns, muitas vezes ilustrada como a parte submersa de um iceberg. Na *deep web*, um conjunto de fatores[5] favorece o anonimato e a impossibilidade de

[5] Por exemplo, a possibilidade de pagamento em *bitcoins* ou *darkbit* (moeda de troca aceite na *deep web*) e a existência de serviços *bulletproof web-hosting* (prestadores de alojamento de páginas que consentem o não-cumprimento da lei que rege os conteúdos e termos de utilização da internet).

rastreio dos movimentos dos utilizadores, favorecendo, em particular, atividades como o comércio ilegal de drogas, explosivos, órgãos humanos ou serviços como homicídios a soldo (GOODMAN, 2015).

Tendo em conta que, também em matéria de privacidade, dados pessoais e bases de dados, ou em matéria de cibercrime, a ação do estado e as políticas públicas não devem ser concebidas, desenvolvidas e implementadas sem a devida consideração dos cidadãos, estudar as perceções dos mesmos quanto a estes temas afigura-se como uma atividade relevante, fulcral para o entendimento das principais necessidades, preocupações e anseios da população. Seguidamente, são apresentados a metodologia e os resultados do estudo realizado às perceções sobre a ação do Estado em matéria de cibersegurança no caso português.

Metodologia

O questionário utilizado neste estudo, enquanto ferramenta de recolha de dados, foi constituído por 10 questões de escala, relativas às perceções dos inquiridos, e por cinco questões de caracterização pessoal dos mesmos.

A Tabela 1 apresenta, em detalhe, os 10 indicadores referentes às perceções dos inquiridos relativamente à ação do Estado em matéria de cibersegurança.

TABELA 1

Questões colocadas aos inquiridos sobre a ação do Estado em matéria de cibersegurança

As entidades públicas, consoante a sua atribuição, detêm dados dos cidadãos. Qual a importância de estas informações permanecerem confidenciais?
Como avalia o seu conhecimento da legislação e dos organismos que, em Portugal, se ocupam da criminalidade informática?
Como classifica a eficácia da atuação do Estado em matéria de segurança informática?
Como classifica o seu entendimento do conceito de "cibercrime"?
Concorda com a utilização de registros de identificação/horário de entrada/saída?
Concorda com a vulgarização do uso da videovigilância em espaços públicos?
Concorda com o uso de sistemas de localização geográfica (vulgo GPS) a fim de localizar pessoas?
Considera provável que os seus dados venham a ser usados de forma a prejudica-lo ou para favorecer terceiros (por exemplo economicamente)?
Que importância atribui à segurança dos dados dos seus dispositivos digitais?
Sente-se familiarizado com a noção de "cibersegurança"?

Fonte: Correia *et al*. (2017, *in press*).

As 10 questões foram quantificadas numa escala de Likert, numérica, por intervalo, com 10 pontos[6] distintos e com âncoras nos extremos: nível muito alto para o extremo superior e nível muito baixo para o extremo inferior. Note-se ainda que aos inquiridos foi sempre dada, em todas as questões, a oportunidade de assinalar "não sabe/não responde" como opção de resposta.

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

O questionário foi disponibilizado presencialmente e *on-line*, entre os dias 15 de julho e 6 de setembro de 2015. Das 1.216 respostas recolhidas durante esse período, 1.168 foram consideradas válidas. Adotando um cenário de variância máxima e assumindo uma dimensão infinita da população, enquanto parte de uma postura metodologicamente cautelosa, foi determinada (por intermédio da fórmula de cálculo da dimensão amostral para proporções) uma precisão absoluta de 2,999% (0,02999), para um nível de confiança de 95% (0,9500).

Uma vez que se verificou a ausência de propriedades gaussianas nos dados recolhidos, a utilização das médias das variáveis quantitativas não se revela como adequada e, por isso mesmo, não foi possível utilizar o teste de análise de variância (ANOVA). Ao invés, a ausência ou existência de igualdade entre medianas foi testada por recurso ao teste não paramétrico de Friedman para amostras emparelhadas (FRIEDMAN, 1937, 1939, 1940), por não impor condições de normalidade prévias à distribuição dos resultados. Todos os testes estatísticos empregues fizeram uso de um nível de significância de 5,00% (0,0500).

Resultados

A Tabela 2 apresenta os resultados obtidos no que respeita à caracterização pessoal dos inquiridos, nomeadamente, as frequências absolutas e relativas verificadas para cada uma das categorias das cinco variáveis de caracterização.

[6] A opção por uma escala de 10 pontos fica a dever-se à necessidade de garantir uma adequada variabilidade das respostas obtidas. Para uma discussão mais detalhada sobre as vantagens da utilização de uma escala de 10 pontos face a uma escala de 7 ou de 5 pontos, consultar Correia (2012, p. 140-144).

TABELA 2

Resultados de caracterização pessoal da amostra

	Média	Mediana
As entidades públicas, consoante a sua atribuição, detêm dados dos cidadãos. Qual a importância de estas informações permanecerem confidenciais?	8,5	10,0
Que importância atribui à segurança dos dados dos seus dispositivos digitais?	8,4	9,0
Concorda com a vulgarização do uso da videovigilância em espaços públicos?	7,0	8,0
Como classifica o seu entendimento do conceito de "Cibercrime"?	6,7	7,0
Sente-se familiarizado com a noção de "Cibersegurança"?	6,6	7,0
Concorda com a utilização de registros de identificação/horário de entrada/saída?	6,4	7,0
Concorda com o uso de sistemas de localização geográfica (vulgo GPS) a fim de localizar pessoas?	6,2	7,0
Considera provável que os seus dados venham a ser usados de forma a prejudica-lo ou para favorecer terceiros (por exemplo economicamente)?	6,0	6,0
Como avalia o seu conhecimento da legislação e dos organismos que, em Portugal, se ocupam da criminalidade informática?	4,2	4,0
Como classifica a eficácia da atuação do Estado em matéria de segurança informática?	3,9	4,0

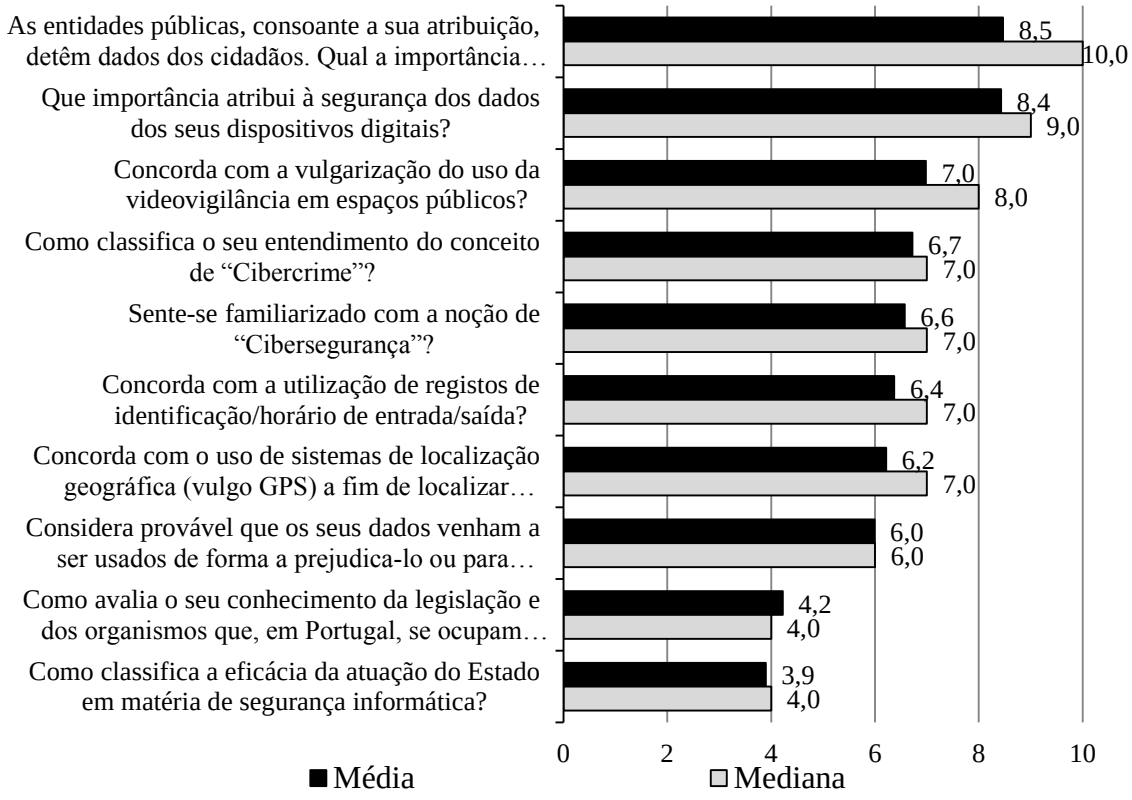
Fonte: elaboração própria com base nos dados recolhidos no estudo.

Note-se que, a par de um número de valores omissos reduzido em todas as variáveis de caracterização, a distribuição feminino-masculino, a nível da variável sexo, se encontra equilibrada, que a amplitude de idades é extremamente abrangente e que todas as categorias de nível de escolaridade, região de residência e frequência de utilização da internet se encontram representadas. Estes valores atestam a robustez da amostra e permitem um grau de confiança adicional nos resultados do estudo.

No que concerne às perceções dos inquiridos no que respeita à ação do Estado em matéria de cibersegurança, matéria central deste texto, é possível efetuar uma leitura, no Gráfico 1, dos respectivos valores das médias e medianas obtidas.

GRÁFICO 1

Médias e medianas das perceções dos inquiridos no que respeita à ação do Estado em matéria de cibersegurança (por ordem decrescente e média e mediana)



Fonte: elaboração própria com base nos dados recolhidos no estudo.

Considerados globalmente, observa-se que os resultados apresentam uma considerável variabilidade. Existem indicadores com valores bastante elevados ao nível das médias e medianas das perceções expressas, e indicadores com valores consideravelmente reduzidos ao nível dessas mesmas médias e medianas. Testar estatisticamente a proximidade ou o afastamento das perceções dos inquiridos face aos vários itens avaliados adquire, por isso mesmo, particular importância. Essa importância é ainda mais potenciada pela formulação e discussão das conjecturas que podem advir das conclusões assim obtidas.

Discussão e conclusões

Como foi dito anteriormente, por impossibilidade estatística de recurso ao teste ANOVA para comparação de médias, optou-se pela utilização do teste não paramétrico de

Friedman (1937, 1939, 1940), que compara os indicadores, ao invés, por recurso às medianas. A aplicação deste teste (χ^2=2.209,14; *p-valor*<0,000) deixa clara a existência de evidências estatísticas em como as medianas dos indicadores utilizados no estudo não são todas iguais.

Ao analisar mais detalhadamente essas evidências, por intermédio de uma comparação *stepwise*, é possível concluir que existem três grupos distintos de indicadores, em função das perceções dos inquiridos: um primeiro grupo, constituído pelos indicadores "As entidades públicas, consoante a sua atribuição, detêm dados dos cidadãos. Qual a importância de estas informações permanecerem confidenciais?" e "Que importância atribui à segurança dos dados dos seus dispositivos digitais?", cujas medianas de 10 e 9 pontos, respetivamente, são as mais elevadas (valores extremamente elevados); um segundo grupo, constituído pelos indicadores "Concorda com a vulgarização do uso da videovigilância em espaços públicos?", "Como classifica o seu entendimento do conceito de 'Cibercrime'?", "Sente-se familiarizado com a noção de 'Cibersegurança'?", "Concorda com a utilização de registros de identificação/ horário de entrada/saída?", "Concorda com o uso de sistemas de localização geográfica (vulgo GPS) a fim de localizar pessoas?" e "Considera provável que os seus dados venham a ser usados de forma a prejudica-lo ou para favorecer terceiros (por exemplo economicamente)?", cujas medianas, entre os 6 e os 8 pontos, se encontram num patamar intermédio (ainda assim considerados valores elevados); e um terceiro e último grupo, constituído pelos indicadores "Como avalia o seu conhecimento da legislação e dos organismos que, em Portugal, se ocupam da criminalidade informática?" e "Como classifica a eficácia da atuação do Estado em matéria de segurança informática?", cujas medianas de 4 pontos são as mais baixas (valores reduzidos). Atente-se, particularmente, na diferença entre os 5 e os 6 pontos entre o primeiro e o terceiro grupo de indicadores.

Assim, é possível concluir que os inquiridos mostram evidências de atribuir extrema importância às questões de confidencialidade e segurança no ciberespaço, ao mesmo tempo que parecem concordar bastante com a utilização de instrumentos como videovigilância, GPS e registros de identificação, afirmando também conhecer razoavelmente os conceitos de cibercrime e cibersegurança. Mostram ainda evidências de considerar que existe uma probabilidade elevada de que venham a ser pessoalmente prejudicados pelo uso indevido dos seus dados. Por fim, e de modo que pode ser considerado algo contraditório, mostram evidências de um reduzido conhecimento da lei aplicável em termos de criminalidade informática e que avaliam o Estado como pouco eficiente nestas matérias.

Tendo em conta o enquadramento inicial sobre a ação do Estado e a elaboração e implementação de políticas públicas, particularmente no que diz respeito a matérias relacionadas com a privacidade, dados pessoais, bases de dados, cibersegurança e cibercrime, os resultados aqui reportados sobre as perceções dos inquiridos deverão ser tidas claramente em consideração. Só dessa forma se afigura como possível uma ação do estado e um conjunto de políticas públicas materializadas em legislação consequente que, ao incorporar as percepções dos cidadãos, consigam responder aos anseios de confidencialidade e segurança da população, reforcem a sua consciencialização e uso equilibrado das novas tecnologias digitais e, com particular interesse para os governos, melhorem o conhecimento que os cidadãos têm das leis associadas e da eficiência do Estado nestes domínios.

Posto isto importa, neste ponto, analisar os principais contributos desta investigação para o tema em apreço. Esses contributos podem ser sumariados em dois tópicos: (1) ficou demonstrada a adequabilidade, para a realidade portuguesa, da escala utilizada para aferir as percepções dos inquiridos sobre a ação do Estado em matéria de cibersegurança e (2) também foi possível demonstrar que os indicadores empregues podem ser agregados, em função dos resultados obtidos, em três agrupamentos estatisticamente distintos (ou dimensões), a que se pode dar os nomes: confidencialidade e segurança; tecnologias e consciencialização e ação do Estado.

Finalmente, os autores deixam como sugestão, para estudos futuros, a utilização dos três agrupamentos estatisticamente distintos de indicadores, identificados nesta pesquisa, para a construção e utilização de variáveis latentes que possam ser utilizadas em trabalhos que recorram a outro tipo de metodologias, de que são exemplo os modelos de equações estruturais. Sugere-se ainda a repetição desta investigação em novos contextos, por forma a confirmar e reforçar a validade e alcance dos resultados apresentados ao longo deste artigo. Este apelo torna-se ainda mais relevante no contexto dos países lusófonos, como o Brasil, uma vez que a proximidade linguística e cultural pode dispensar a necessidade de adaptação do questionário aplicado.

Referências

ANDERSON, James (1984). *Public policy making*. New York: Holt, Rhinehart & Winston.

BILHIM, João Abreu de Faria (2008). *Ciência da administração*. Lisboa: Universidade Aberta.

BOBBIO, Norberto (1987). *Estado, governo, sociedade – Para uma teoria geral da política*. Brasil: Paz e Terra.

CARVALHO, Jorge Silva (2009). *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.

CENTRO NACIONAL DE CIBERSEGURANÇA (2012). *CERT.PT – Taxonomia*. Portugal: Centro Nacional de Cibersegurança.

CORREIA, Pedro (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). Portugal: Instituto Superior de Ciências Sociais e Políticas da Universidade Técnica de Lisboa.

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

CORREIA, Pedro; JESUS, Inês (2014). "A proteção de dados pessoais no espaço de liberdade, de segurança e de justiça da União Europeia". *Revista Brasileira de Segurança Pública*, 8 (2), 18-30.

CORREIA, Pedro; SANTOS, Susana; CORREIA, Maria (2017). "Perceções sobre cibersegurança e privacidade em Portugal: evidências estatísticas de igualdade e desigualdade de género". *Revista Latino-Americana de Geografia e Género*, 8 (1), in *press*.

CORTES, Soraya; LIMA, Luciana (2012). "A contribuição da sociologia para a análise de políticas públicas". *Lua Nova: Revista de Cultura e Política*, 87, 32-62.

DOWNS, Anthony (1957). *An economic theory of democracy*. USA: Harper & Row Publishers.

DOWNS, Anthony (1967). *Inside bureaucracy*. USA: Little, Brown and Company.

DYE, Tomas (2012). *Understanding public policy*. 14.ª edição. USA: Pearson.

FERNANDES, José (2012). "Utopia, liberdade e soberania no ciberespaço". *Nação e Defesa*, 133, 11-31.

FREDERICKSON, George *et al*. (2012). *The public administration theory primer*. USA: Westview Press.

FRIEDMAN, Milton (1937). "The use of ranks to avoid the assumption of normality implicit in the analysis of variance". *Journal of the American Statistical Association*, 32 (200), 675-701.

_____. (1939). "A Correction: The use of ranks to avoid the assumption of normality implicit in the analysis of variance". *Journal of the American Statistical Association*, 34 (205), 109.
_____. (1940). "A comparison of alternative tests of significance for the problem of m rankings". *The Annals of Mathematical Statistics*, 11 (1), 86-92.

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

HAWKES, Nigel (1971). *A revolução dos computadores*. Portugal: Editorial Verbo.

HILL, Michael (2005). *The public policy process*. 4.ª edição. UK: Pearson Education.

JENSEN, Michael (1994). "Self-interest, altruism, incentives & agency theory". *Journal of Applied Corporate Finance*, 7 (2), 40-45.

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

KARAS, Stan (2002). "Privacy, identity, databases". *American University Law Review*, 52 (2), 393-445.

KLIMBURG, Alexander (Ed.) (2012). *National cyber security framework manual*. Estónia: NATO Cooperative Cyber Defence Centre of Excellence Publications.

MEHAN, Julie (2014). *Cyberwar, cyberterror, cybercrime and cyberactivism*. 2.ª edição. UK: IT Governance Publishing.

MARTINS, Marco (2012). "Ciberespaço: uma nova realidade para a segurança internacional". *Nação e Defesa*, 133, 32-49.

MIRANDA, Jorge (1992). "Funções do Estado". *Revista Direito Administrativo*, 189, 85-99.

NUNES, Paulo (2012). "A definição de uma estratégia nacional de cibersegurança". *Nação e Defesa*, 133, 113-127.

ORWELL, George (2013). *Nineteen eighty-four*. USA: Penguin Classics.

PORTUGAL (2008). "Lei n.º 53/2008, Lei da Segurança Interna". *Diário da República*, 1.ª série, 167, 6135-6141, 29 de Agosto.

REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE (2015). *Medidas de controlo de incidentes de segurança informática – Política de atuação do RCTS CERT para mitigação de impacto de incidentes de segurança informática – Serviço RCTS CERT*. Portugal: Fundação para a Computação Científica Nacional.

RICHARDS, Neil (2013). "The dangers of surveillance". *Harvard Law Review*, 126, 1934-1965.

ROCHA, José Oliveira (2010). *Gestão do processo político e políticas públicas*. Portugal: Escolar Editora.

ROWLEY, Charles; SCHNEIDER, Friedrich (Eds.) (2004). *The encyclopedia of public choice*. USA: Springer.

SANTOS, José Albano (2012). *Economia pública*. Portugal: Instituto Superior de Ciência Sociais e Políticas.

SECCHI, Leonardo (2011). *Políticas públicas: conceitos, esquemas de análise, casos práticos*. Brasil: Cengage Learning.

SJÖBLOM, Gunnar (1984). "Problemi e soluzioni in politica". *Rivista Italiana di Scienza Politica*, 14 (1), 41-85.

SOUZA, Celina (2006). "Políticas públicas: uma revisão da literatura". *Sociologias*, 8, 20-45.

UNIÃO EUROPEIA (2013). "Diretiva 2013/40, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação". *Jornal Oficial da União Europeia*, L 218, 8-14, 14 de Agosto.