Hackers, Hacktivistas e *Whistleblowers*: o caso português.

José Pedro Arruda [I]
http://orcid.org/0000-0002-0873-7918

[I] *Instituto Superior de Economia e Gestão, Portugal.*
Doutorando em Sociologia pela Universidade de Coimbra.

http://dx.doi.org/10.1590/1981-5344/3869

Apresenta-se uma reflexão de base empírica sobre o fenómeno do hacktivismo em Portugal. A partir de uma abordagem assente nos princípios da *Grounded Theory*, o artigo procura ilustrar o processo reflexivo que conduziu a investigação, assente num trabalho de netnografia, que serviu como base de descoberta para novos atores e lugares de observação. Tendo como primeiro foco de atenção as atividades *online* conotadas com grupos portugueses associados ao coletivo *Anonymous*, parte-se para uma tentativa de definir conceitos e práticas referentes ao *hacking*, hacktivismo, ciberativismo e *whistleblowing*. Este esforço alicerça-se em exemplos empíricos, procurando um cruzamento de diferentes posicionamentos e perspetivas face aos fenómenos em questão, envolvendo hacktivistas, polícias e investigadores em cibersegurança.

Palavras-chave: *Anonymous; hackers; hacktivismo, ciberativismo; whistleblowers.*

Hackers, Hacktivists and Whistleblowers: the Portuguese case.

Presented herein is an empirical reflection on the phenomenon of hacktivism in Portugal. Adopting a Grounded Theory approach, this article seeks to illustrate the reflexive process that oriented the investigation, based on a work of netnography, which served as the basis for the discovery of new actors and places of observation. Having as the first focus of attention the online activities of some Portuguese groups associated with the collective Anonymous, it develops to an attempt to define concepts and practices regarding hacking, hacktivism, cyber-activism and whistleblowing. This effort is based on empirical examples, looking for a cross-referencing of different standpoints and perspectives on these subjects, involving hacktivists, police officers and cybersecurity researchers.

Keywords: *Anonymous; hackers; hacktivism; cyber-activism; whistleblowers.*

Recebido em 24.02.2019 Aceito em 31.05.2021

1 Introdução

Este artigo consiste numa tentativa de sedimentar reflexivamente um somatório de materiais empíricos relacionados com o fenómeno do hacktivismo, que fui recolhendo ao longo dos últimos dois anos. Em fevereiro de 2017, fui contratado como bolseiro de investigação para o projeto "Policiamento e Imaginários Urbanos: Novos Formatos de Segurança em Cidades do Sul"[1], com o objetivo de desenvolver um trabalho de recolha etnográfica sobre novas práticas de vigilantismo e de "policiamento sombra", nomeadamente através do ciberespaço. Tais práticas remetem quase instantaneamente para os denominados grupos hacktivistas, com os *Anonymous* a surgirem como expoente máximo do mediatismo que estes coletivos alcançaram na última década. Tratando-se de um fenómeno relativamente desconhecido para mim, enquanto investigador e utilizador pouco entusiasta dos novos mecanismos de comunicação, procurei entrar paulatinamente nas práticas e problemáticas relacionadas com este tipo de atividade. O texto que aqui se apresenta convida o leitor a reconstituir este percurso de aprendizagem reflexiva,

1 Ref.ª: FAPESP/19989/2014, projeto financiado pela Fundação para a Ciência e a Tecnologia (FCT) e pelo Fundo de Amparo à Pesquisa do Estado de São Paulo (FAPESP), tendo decorrido em simultâneo em Portugal (SOCIUS/ISEG) e no Brasil (UNICAMP).

acompanhando as hipóteses, ilações, dúvidas e considerações que fui experimentando.

Desde a sua génese, este estudo procurou ser fundamentado numa investigação empírica, desenvolvendo-se a partir desta e não de um enquadramento teórico previamente definido. Assim, seguiram-se os preceitos metodológicos da *Grounded Theory* (GT), inicialmente formulada por Barney Glaser e Anselm Strauss (1967), que procura gerar teorias a partir da investigação, em vez de testar hipóteses construídas *a priori*. Esta abordagem enfatiza o trabalho de campo e a necessidade de explicar em pormenor o que acontece em algumas situações práticas, no mundo quotidiano. Ora, tendo em conta que as práticas que caracterizam o hacktivismo decorrem essencialmente no ciberespaço, este foi, desde logo, o terreno de observação preferencial para a realização da pesquisa empírica. Apesar de limitado pela falta de conhecimentos técnicos que me permitissem aceder aos lugares onde os *hackers* habitualmente operam, sitos na denominada *dark web*, assim como entender alguns dos conceitos por eles utilizados, procurei acompanhar as atividades mais públicas e visíveis dos hacktivistas. Desenvolveu-se um trabalho de netnografia (Kozinets, 2010) em diversos *sites*, fóruns e páginas de redes sociais, em particular no *Facebook*, identificados com os *Anonymous* e outros grupos hacktivistas. A expectativa era a de descortinar algumas das suas práticas 'ocultas' através da sua faceta mais acessível, nomeadamente pela forma como estes grupos se apresentam publicamente.

No entanto, a proposta da GT de fazer *tabula rasa* do conhecimento construído, como se o investigador pudesse esvaziar-se de si mesmo, além de ser impraticável, tornar-se-ia inconsequente, já que qualquer teoria assim fabricada não poderia ser incorporada em pesquisas futuras. Isso conduziu àquilo que passou a ser entendido como a GT *de segunda vaga*. Autores como Bruno Hildenbrand reconhecem que trabalhos prévios fornecem uma codificação de conceitos e práticas que podem servir às novas pesquisas, ao mesmo tempo que permitem o reconhecimento de certas matrizes estruturais, que se alteram de forma mais lenta: "No entanto, mesmo esses elementos da sociedade que se movem mais lentamente não podem ser simplesmente assumidos numa perspectiva de teoria fundamentada. Nós vemo-los como uma fração, que pode ser relevante, mas não tem necessariamente de ser. Eles constituem uma hipótese"[2] (Hildenbrand, 2007, p. 551 – tradução do autor). No caso que aqui se apresenta, as hipóteses com que abordei inicialmente o campo derivaram sobretudo do trabalho empírico desenvolvido pela antropóloga Gabriella Coleman (2016), cuja leitura constituiu um primeiro contacto mais detalhado e reflexivo com as atividades dos *Anonymous*.

2 "Yet even these more slowly moving elements of society cannot be simply taken as assumed in a perspective of grounded theory. We see them as a frame, which can be relevant, given this hypothesis, but need not necessarily be. They have the status of hypothesis" (texto original)

2 Em busca dos *Anonymous* portugueses

Coleman realizou um vasto trabalho de campo, ao longo de vários anos, acompanhando as atividades *online* (e não só) dos *Anonymous* durante um dos períodos de maior atividade do grupo nos Estado Unidos da América (EUA), entre 2008 e 2013. Logo no título do seu livro, a autora assume que uma das principais dificuldades em caracterizar um grupo como os *Anonymous* prende-se com as suas "muitas faces". Nesta obra, procura demonstrar o processo, acidentado e quase caótico, que transformou um pequeno grupo de utilizadores dispersos de um *site* recreativo (*4chan*) num grupo hacktivista mundialmente famoso. De uma forma extremamente linear, pode dizer-se que o grupo nasceu de uma forma de atuação que visava exclusivamente o divertimento - o "*lulz*", corruptela de LOL (*Laughing Out Loud*) – passando progressivamente a assumir algumas lutas político-ideológicas e uma missão cívica. Contudo, isto não aconteceu repentinamente nem de forma harmoniosa. Foi uma improvável sucessão de acontecimentos, assim como de decisões, disputas e cisões internas, que possibilitou essa transformação. Além disso, a própria devoção ao anonimato e estratégias de ação camufladas torna a análise do grupo particularmente difícil. "Apesar de toda a vida social e todos os movimentos políticos serem complexos e de difícil abordagem, a associação dos *Anonymous* com a multiplicidade, o secretismo e os estratagemas torna o seu estudo e compreensão especialmente difíceis" (Coleman, 2016: 366). Quando comecei a debruçar-me sobre o caso dos *Anonymous* em Portugal, estava já à espera de encontrar muita desta complexidade e ambiguidade estrutural.

Comecei por acompanhar algumas plataformas *online* associadas aos *Anonymous* e outros grupos hacktivistas que fizessem referência a Portugal ou utilizassem a língua portuguesa. O ponto de partida para a análise destes grupos no ciberespaço foram as suas páginas na rede social *Facebook*. Encontrei várias páginas que se identificavam com os *Anonymous*, mesmo limitando a busca às que assumem explicitamente a sua nacionalidade. Foram selecionadas algumas para uma observação mais detalhada, seguindo o critério da sua popularidade, patente no número de seguidores de cada página: #Anonymous Legion Portugal (44.500 seguidores[3]); #Anonymous Portugal (8.400); #Anonymous PORTUGAL (132.000); #Hackers Portugal (41.900; #Anonymous Portugal Internacional (124.900); #CyberTeam (4.500); #Tugaleaks (159.600). Estas foram as páginas mais escrutinadas, em virtude de os objetivos da pesquisa se focarem nas atividades destes grupos em Portugal. Porém, dado o internacionalismo do movimento, também foram monitorizadas, de forma menos sistemática, algumas páginas internacionais de hacktivistas, como a #Anonymous (6.065.000 seguidores), #LulzSec (44.600) e

3 Dados de Fevereiro de 2018. Valores arredondados.

#WolfSec (3.500). A análise estendeu-se ainda a um site português (https://anonymous.com.pt/), um blogue (http://anonymouspt.blogspot.pt/) e a um fórum de discussão no IRC (*Internet Relay Chat*, protocolo de comunicação utilizado na Internet), disponibilizado pelo sistema TOR, nomeadamente nos canais #anonymousportugal e #oplusofonia.

Esta primeira abordagem foi fundamental para perceber de que forma estes grupos se veem a si mesmo e como querem apresentar-se publicamente. Por exemplo, no blogue #Anonymous Portugal, os seus autores afirmam que "os *Anonymous* não são um movimento típico. É um conjunto de ideias e um esforço de muitas pessoas para a defesa de causas diversas, mas comuns a todos os que se identificam com o coletivo". Sintetizam que "na sua essência, os ideais dos Anonymous centram-se na liberdade, privacidade, justiça e igualdade, e visam contrariar, de forma activa, o controlo que o governo nos impõe". Logo aqui, os propósitos do grupo e o "conjunto de ideias" que invocam começaram a tornar-se ambíguos, do ponto de vista analítico. Conceitos como "liberdade, privacidade, justiça e igualdade" são vagos e subjetivos, obedecendo a valores e ideias superficiais comummente aceites. Tal como já esperava, não verifiquei a existência de princípios ideológicos ou de organização político-social que permitam estruturar um modelo de ação, capaz de garantir uma defesa efetiva dessas ideias e valores.

No mesmo blogue, o grupo publica o seu manifesto[4], onde começam por dizer: "Cidadãos Portugueses, nós somos os *Anonymous* Portugal. Trazemos esta mensagem até vós, para dar a conhecer uma Ideia". Essa "ideia" acaba por não ser apresentada de forma clara em nenhum ponto do documento. Porém, o grupo revela algumas das suas intenções: "Este movimento irá servir para expor não só a corrupção, como também queremos criar uma imprensa totalmente livre em Portugal, trazendo as notícias que não são censuradas pelos editores que possuem interesses, ou são pressionados por empresas e governo". Em seguida, fazem um apelo à união e à coesão do grupo, entre si, e também face a outros "movimentos cívicos", não identificados: "iremos tentar trabalhar em conjunto com os outros movimentos cívicos em Portugal, pois está na altura de alguma coesão nacional". Justificam essa pretensão, dizendo que "muitas vozes com gritos de guerra diferentes soam a uma salva de pólvora seca, enquanto algo mais organizado e com uma agenda comum será muito mais eficaz e atingirá melhor o alvo". No entanto, esta postura parece, de certa forma, contrariar a natureza desestruturada e dispersa dos *Anonymous*. Será, então, igualmente importante atentar em alguns dos "princípios fundamentais" pelos quais o grupo diz guiar-se:

4 https://docs.google.com/document/d/1778QpelluSYxEPgj0XVZHcjuEoZ6zZQVXAuBy29dLtU/edit

1) O nosso bem-estar coletivo deve vir em primeiro lugar; O movimento depende da unidade local, da solidariedade e da comunicação forte de outros movimentos em todo o mundo. 2) Para o nosso propósito comum existe apenas uma autoridade - Consciência Coletiva - que se manifesta através de nossas ações e reações a eventos locais e globais. Não há um líder neste movimento, somos a progressão coletiva de ideias para fazer um mundo melhor. Essas ideias podem ser vinculadas a pessoas, mas nenhum grupo pode governar nem reclamar a propriedade sobre essas ideias. 3) O único requisito para ser membro é um desejo de começar a pensar e estar juntos como Um, para um mundo melhor. (...) 4) Assim como cada grupo de ação está para o movimento, também o movimento deve ser autónomo, salvo em assuntos que afetem o movimento global como um todo, e a sua progressão […] 8) O movimento em si, deve ser organizado em contacto constante com a comunidade, local e global e podemos pelo processo democrático confiar funções de gerenciamento de projeto a pessoas experientes nas suas áreas. Eles podem ter a experiência relativa que poderia ajudar o movimento como um todo […] 12) UNIDADE é o fundamento de todos os nossos princípios, e temos de ser constantemente lembrados de colocar os princípios acima das personalidades. Resolução de conflitos dentro do grupo deve ser feito de forma decisiva, com ações acordadas por consenso e cortesia com respeito pelo processo de consciência coletiva do movimento.

O que mais se realça destes princípios é uma grande insistência em conceitos como "unidade", "consciência coletiva" e "consenso", em detrimento do individualismo e das personalidades individuais. Aliás, o próprio nome do grupo baseia-se na ideia de anonimato, do desaparecimento do indivíduo em função do coletivo, que deve reger-se sempre por consensos, sejam eles locais ou globais. Mas, sendo os *Anonymous* um somatório tão díspar de personalidades (qualquer pessoa pode juntar-se ao grupo, de forma permanente ou ocasional), como se consegue essa unidade, tendo por base apenas alguns princípios e ideias mais ou menos vagos, sem uma estrutura organizada, uma liderança legitimada e sistemas próprios de regulação? Estes princípios evocam o modelo "democrático" de participação, atendendo à participação igualitária dos seus membros na busca de consensos, aparentemente atingidos pela vontade das maiorias. Porém, este funcionamento parece assemelhar-se mais a um modelo anarquista, sem estruturas centralizadoras de poder e definindo a própria adesão e o tipo de ação a desempenhar consoante a operação (ou "op", usando a terminologia do grupo) em causa. É por isso importante olhar também para as atividades que estes grupos vão realizando e partilhando publicamente, nomeadamente nas suas páginas do *Facebook* - até porque o blogue em questão não é atualizado desde 2016. Essencialmente, para perceber se essas atividades correspondem à imagem e aos princípios com que o grupo se auto-retrata.

3 *Anonymous* nas redes sociais

No referido acompanhamento de diversas páginas de *Facebook*, ao longo dos meses, algumas tendências começaram a evidenciar-se, nomeadamente os ecos que estas fazem umas das outras, pela partilha de conteúdos comuns. Assim, parecem existir, pelo menos, duas fações principais dentro dos *Anonymous* portugueses, que atuam como dois diferentes aglomerados na difusão dos conteúdos: as páginas #TugaLeaks, #Anonymous PORTUGAL e #Hackers Portugal revelam uma forte tendência para partilharem conteúdos entre si; por outro lado, essa tendência encontra-se também, com menos intensidade, entre as páginas #Anonymous Legion Portugal, #Anonymous Portugal e #Anonymous Portugal Internacional, embora esta última se dedique quase exclusivamente a conteúdos internacionais (externos ao território português). Procurarei caracterizar genericamente as atividades de cada um destes aglomerados. Já a página #Cyberteam, que foi também monitorizada, parece refletir uma postura e um tipo de intervenção substancialmente diferente das anteriores, pelo que merece uma análise própria. Apesar de ter bastante menos relevância, a nível de seguidores, que as restantes páginas, essas diferenças tornam-na relevante, já que ilustram outras formas de usar o *hacking*.

As páginas #Anonymous PORTUGAL e #TugaLeaks, além de partilharem de forma sistemática o mesmo conteúdo, fazem-no também utilizando exatamente o mesmo texto introdutório. Ou seja, não se trata realmente da partilha de uma postagem, mas de duas postagens exatamente iguais em ambas as páginas. Mesmo ocasionais gralhas que surgem no texto repetem-se em ambas as páginas, o que sugere um autor comum, que utiliza a técnica de "*copy/paste*" nesta atividade. A intensidade de publicações de ambas as páginas é elevada, geralmente com várias postagens por dia. Porém, a repetição de conteúdos é também muito frequente, sendo habitual encontrar-se o mesmo *post* em dias consecutivos e, por vezes, até repetido no próprio dia. Isso não acontece com todas as publicações, mas com algumas, não se descortinando um critério pelo qual isso acontece. Apesar do nome de uma das páginas, os conteúdos publicados não se tratam verdadeiramente de "leaks". Não são reveladas informações nem documentos secretos. Em vez disso, trata-se de notícias, habitualmente de cariz um tanto polémico ou revelador de más práticas institucionais, que foram já publicadas noutros órgãos. O que é acrescentado são pequenos textos introdutórios, que visam predispor o leitor a assumir uma posição, de forma bastante ostensiva, face aos conteúdos exibidos. Estes textos tendem a ser curtos, pouco elucidativos e substancialmente superficiais, sendo muito frequente terminarem com frases bombásticas, escritas em maiúsculas e apelando à revolta e à denúncia, como "PARTILHA ESTA VERGONHA, DENUNCIA!!!", ou "DENUNCIA ESTA CORJA!!!".

Os alvos preferenciais destas páginas são as instituições de poder nacionais, sobretudo os partidos políticos com representação parlamentar, tribunais, forças de segurança e organismos do Estado e repartições públicas. Essencialmente, visam denunciar aquilo que entendem ser más práticas por parte de instituições estatais, injustiças sociais, casos ou indícios de corrupção e decisões políticas contestáveis. Porém, a forma como o fazem é habitualmente superficial e tendenciosa, indicando logo na apresentação o que deve o leitor pensar, e sem mostrar interesse em elucidar, aprofundar ou abrir espaço à reflexão e ao debate. Outro tipo de conteúdo frequente é a divulgação de truques informáticos. Neste caso, os conteúdos provêm quase exclusivamente da página #Hackers Portugal, que se concentra sobretudo em questões técnicas, nomeadamente na revelação de *softwares* úteis e gratuitos destinados a aumentar a segurança e privacidade na *internet*. Essas dicas não parecem destinar-se exclusivamente a *hackers* ou informáticos, mas ao público em geral. Na maioria dos casos, trata-se de *softwares* ou técnicas de encriptação de dados, de garantir maior privacidade ou anonimato *online* e de proteção de dados pessoais. Há outros temas também recorrentes nesta página, tradicionalmente ligados à cultura *hacker*, como as criptomoedas, videojogos e *sites* para *download* de filmes e séries. Neste processo, também são reveladas necessariamente algumas técnicas de *hacking*, nem que seja com o aparente propósito de ajudar as pessoas a protegerem-se delas. Um chavão discursivo muito utilizado nesta página é o "partilha com os teus amigos", revelando uma certa solidariedade cooperativa.

Por seu turno, as páginas #Anonymous Legion Portugal, #Anonymous Portugal e #Anonymous Portugal Internacional utilizam uma estratégia comunicacional substancialmente diferente das anteriores. E também o seu âmbito de ação parece ser diferente. Para começar, será importante referir que estas páginas parecem estar fortemente vinculadas ao *site* https://anonymous.com.pt, partilhando muitos dos seus conteúdos, com hiper ligações que remetem para o mesmo. As suas postagens não costumam ter textos introdutórios e, como tal, pode dizer-se que terão menos predisposição para direcionar a opinião dos leitores. O seu âmbito é também mais alargado, não se concentrando em assuntos nacionais, mas também abrangendo temas da atualidade a nível internacional. Como já foi dito, a página #Anonymous Portugal Internacional foca-se mesmo de forma exclusiva em assuntos internacionais, fazendo regularmente partilhas de páginas de dimensão global como a #Anonymous, #LulzSec e #WolfSec. Além disso, estas páginas não se limitam à publicação de notícias sobre questões político-sociais, ambientais ou ligadas ao ciberativismo. Elas recorrem regularmente à publicação de "mêmes" de teor ideológico/ filosófico, que abrangem dois temas principais: 1) reflexões existencialistas sobre a

condição humana, em que o indivíduo é apresentado tendencialmente como subjugado por um sistema opressor e injusto que restringe e controla as suas opções de vida; 2) o papel dos *Anonymous* enquanto defensores da Humanidade e da justiça social, como guerreiros vigilantes ao serviço das populações.

Ao contrário do blogue anteriormente analisado, o *site* https://anonymous.com.pt, que 'alimenta' estas páginas, continua a ser diariamente atualizado, o que demonstra ser uma plataforma ativa e provavelmente dinamizada por vários colaboradores. Além de secções que remetem para fóruns e salas de chat nacionais e internacionais entre membros da comunidade, o *site* divide-se em 5 secções principais, que correspondem também aos temas que preenchem as suas páginas de *Facebook*: a) Portugal e b) Internacional, que revelam notícias e informações sobre políticas que possam ter impactos sociais (tendencialmente negativos) relevantes, assim como casos de corrupção ou indícios de corrupção, acidentes, desastres naturais, conflitos armados e mesmo alguns *fait-divers*/ curiosidades; c) *Cybersecurity*, que serve para difundir informações sobre *softwares* úteis e técnicas de proteção da privacidade; d) *Environment*, que se concentra não só em questões ambientais, como também em atividades suspeitas ilícitas de grandes organizações internacionais, como a *Monsanto*, o Vaticano ou mesmo de sociedades secretas que se movem nos bastidores do poder (remetendo amiúde para teorias da conspiração dificilmente prováveis); e) *Anonymous*, que não se foca tanto nas atividades do grupo, mas sobretudo na forma como este se vê a si próprio, através dos tais mêmes que também se encontram nas referidas páginas do *Facebook*.

Atividades bem diferentes deste tipo de ativismo no ciberespaço são aquelas levadas a cabo pelo grupo "Cyberteam Portugal". Através da sua página do Facebook, os mesmos apresentam-se como "miúdos dos 10 aos 17 anos", assumem-se como "*black hats*" (*hackers* que não se regem por princípios éticos, mas em benefício próprio) e parecem operar simultaneamente em Portugal e no Brasil. A sua postura é assumidamente rebelde e provocadora: publicam os ataques que fazem, que assumem e assinam orgulhosamente (geralmente trata-se de *defacing* de *sites*); lançam ameaças mais ou menos vagas, incluindo à própria *Google*; sugerem desafios aos seus seguidores – exemplo: "Desafie-nos a invadir uma grande plataforma! (Não importa o alvo!)". Provocam repetidamente as autoridades, com uma postura de "apanhem-nos se puderem". Porém, a forma muitas vezes ambígua e codificada, pelo uso de uma gíria própria, revela também alguma preocupação ou receio dessas mesmas autoridades. Será talvez incorreto considerar como hacktivismo as atividades publicitadas por esta página. Não há vislumbre de discursos políticos ou ideológicos, nem qualquer presunção de combater pelo bem comum. Aqui, os administradores da página não colocam o coletivo acima

da individualidade. Um deles, que se identifica como "Zambrius", tende a assinar as suas postagens e frequentemente reivindica a autoria de certos ataques. A ideia de anonimato não está aqui presente, pelo menos não na forma idealizada pelos *Anonymous*. O interesse deste coletivo parece ser exclusivamente pelos desafios tecnológicos, pela diversão em fazer algo que nem toda a gente consegue e, até mesmo, pela audácia que é fazer algo perigoso, porque ilegal.

4 *Anonymous* fora das redes

Com o decorrer dos meses, fui sentindo algum desapontamento relativamente às atividades *online* dos *Anonymous* a que conseguia aceder, descortinando poucas ações que pudessem ser consideradas como hacktivismo. Presumi que tal escassez de atividade fosse um dos efeitos da "Operação C4R3T05 (CARETOS)", levada a cabo pela Polícia Judiciária (PJ) face aos *Anonymous*, e que resultou em sete detenções pela prática de crimes informáticos em 2015. em 26 de fevereiro desse ano[5], a Diretoria de Lisboa e Vale do Tejo da PJ revelava que intervieram nesta operação "70 funcionários altamente especializados", visando o apuramento e atribuição de responsabilidades criminais a grupos de cidadãos envolvidos, "de forma reiterada", em "crimes de sabotagem informática ("DDoS"), de dano informático ("*defacing*")" de acesso ilegítimo ("*hacking*") e de acesso indevido ("exfiltração de dados")", que, alegadamente foram "praticados contra diversos sistemas informáticos do Estado Português", e também de "empresas relevantes do sector privado". Na tentativa de compreender melhor a conjuntura em que se encontravam os *Anonymous* portugueses, contactei com alguma insistência os administradores das suas páginas nas redes sociais, com o objetivo de agendar uma entrevista presencial. Na maioria dos casos, não obtive qualquer resposta, e quando esta surgiu, foi quase sempre negativa. A exceção foi Rui Cruz, fundador do órgão de comunicação "Tugaleaks", que foi também um dos detidos no âmbito da "Operação Caretos", algo que havia já revelado publicamente, incluindo em programas televisivos.

Encontrei-me com o Rui Cruz na qualidade de fundador e responsável pelo Tugaleaks, órgão que dá particular destaque a informação sobre hacktivismo e cibersegurança. O objetivo era abordar estes temas, assim como questões mais específicas relacionadas com os *Anonymous*, e mesmo conceitos como *white hats*, *black hats*, cibercrime e *hacking* ético. É importante salientar que em nenhum momento foi assumido, por nenhuma das partes, que Cruz era membro do coletivo *Anonymous*. Apesar disso, não se inibiu de revelar várias informações sobre o grupo, em particular no caso português. Questionei-o sobre a

5 https://www.policiajudiciaria.pt/operacao-c4r3t05-caretos/

aparente falta de atividade do grupo, ao que respondeu que "muita gente ficou com medo por causa do processo "Caretos", que levou muitos *hackers* a tribunal. Mas… eu acho que está adormecido porque, hoje em dia, não há nada de que nos possamos verdadeiramente queixar". Portanto, atribuiu à falta de contestação social que se fazia sentir no país, em outubro de 2017, o aparente "adormecimento" do coletivo, assim como a algum receio face à intervenção policial. Mas essas não serão as únicas razões, pois também considera que "em Portugal, a ideologia está um bocado dividida, não se sabe muito bem quando é que estão juntos, quando é que não estão, que equipas é que formam… Mas, no estrangeiro, principalmente nos EUA, vejo que é um movimento mais coeso, que não só faz coisas digitais como físicas".

Durante a análise às páginas portuguesas dos *Anonymous* no *Facebook*, tinha já notado, como foi referido, uma clara divisão entre pelo menos dois grupos. Essa divisão foi, de certa forma, confirmada por Rui Cruz, que afirmou existirem "rivalidades de grupo", devido ao facto de "os próprios grupos dentro do grupo maior não se darem uns com os outros". Portanto, dentro do próprio coletivo, a proclamada "unidade" que afirmam almejar parece difícil de alcançar. Contudo, a entrevista não se limitou às atividades dos *Anonymous*, tendo enveredado por questões mais abrangentes, relacionadas com a ética e a essência do hacktivismo. Em suma, Cruz confirmou que, dentro deste género de intervenção, os tipos de ataque mais frequentes são "a obtenção de dados e o *defacing*, a alteração de uma página. Porque o primeiro pode depois ser divulgado nos órgãos de comunicação social ou na *internet*, e o segundo é uma marca que fica visível, da passagem daquela pessoa ou grupo por lá, que vai obrigar depois as pessoas a corrigirem o *site*". Reconhece, ainda assim que, sobretudo no segundo caso, a eficácia de tais ataques é de "curto prazo", equiparável a alguém bloquear uma rua, em protesto, durante algumas horas. E considera que a legislação existente é demasiado restritiva, não reconhecendo que algumas práticas classificadas como cibercrime são equiparáveis a protestos legais no mundo físico. Por exemplo, um ataque de negação de serviço (DDoS) "não se pode colocar na categoria de sabotagem informática, porque assim iríamos colocar o direito à manifestação, que está constitucionalmente previsto, numa espécie de bloqueio de estrada ilegal". Por isso, acha que falta "um bocadinho de lógica e meio-termo, na lei".

Relativamente às questões éticas em torno do hacktivismo, Cruz acredita que, ao contrário do que diz a lei portuguesa, o "*hacking* ético" não deveria ser apenas aquele que é autorizado (ou mesmo pago) pelas empresas, mas considerar se uma pessoa "vai para o bem". Ou seja, "se alguém entrar num *site* e descobrir uma falha, a parte entre o ético e o não-ético é se vai conscientemente dar a conhecer essa falha ao dono do *site*, ou se vai utilizá-lo para proveito próprio, alterando o *site*, buscando

informações, *et cetera*". Porém, reconhece que "a versão portuguesa do *hacking* ético", considera que "se não tem uma autorização prévia, estão a cometer um crime". Na sua perspectiva, "ao estarem a cometer um crime, estão também a salvar a empresa de futuras pessoas que não pensem como aquela. Portanto, aí cabe à gestão da empresa achar que aquilo não foi bem legal, mas se eles não apresentarem queixa, têm mais a ganhar do que se apresentarem uma queixa". Caso contrário, considera que será um enorme desperdício de conhecimento: "as empresas devem trabalhar com essas pessoas de forma positiva e não negativa". Até porque "provavelmente, o que os *hackers*, éticos ou não, têm a mais, é tempo. E, se os *hackers* têm tempo, poderão direcionar o tempo deles para aquilo que eles podem realmente fazer de bem para a sociedade".

5 A perspectiva policial

As compreensíveis dificuldades em estabelecer contacto direto com indivíduos assumidos como hacktivistas, conduziu a pesquisa a outros pontos de entrada e ao contacto com outras perspectivas especializadas sobre este tipo de atividade. Nomeadamente, foi contactada a Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica (UNC3T) da PJ, que aceitou conceder-nos uma entrevista presencial, através do seu Inspetor-Chefe, Rogério Bravo. Ora, da perspectiva da polícia, o próprio conceito de "hacktivismo" é desprovido de sentido. Bravo assume frontalmente que "*hacktivista*, para nós, não existe. Isso é uma categoria que podemos tê-la em termos de conceito, mas depois o crime que cometem pode ser ou acesso ilegítimo, ou sabotagem, ou acesso ilícito a informação, por aí fora". E sublinha que a lei é muito clara em relação a isso: "Na lei, a nível da Europa, e em Portugal, por força dessa harmonização a nível da Europa, a coisa está assim: ou há ou não há autorização. Se não há autorização, é crime". E considera que a adoção de "conceitos muito ligados à literatura anglófona, muito com base americana", como "*red hats* e t*iger teams,black hats* e não sei quê", vem apenas acrescentar desinformação, sobretudo para os mais jovens, que podem assim acabar por envolver-se em atividades criminosas.

Curiosamente, embora assumindo posições antagónicas, tanto Bravo como Rui Cruz desvalorizam a distinção entre *white hats* e *black hats*, por motivos diametralmente opostos. Para Cruz, "mesmo um *black hat*, continua a prestar um serviço público ao *site* que é atacado. Porque depois do *site* ser atacado, portanto, depois do dano, vem a recuperação". Nesse sentido, entende que "um ataque, seja *black hat* ou *white hat*, tem sempre, no fim, digamos, um… açúcar, uma coisa positiva, que adocica a amarguez de um ataque". Por seu turno, Bravo sustenta a perspetiva policial de que qualquer ataque não consentido é um crime. E justifica isso pela perigosidade que tal representa para um ou vários sistemas essenciais: "é perigoso quando pessoas com menos de 16 anos, por um

sentimento de pertença a um grupo e pouco informadas quanto aos efeitos ou consequências dos seus atos, participam numa rede de um ataque distribuído e ficam contentes por mandar abaixo um servidor que, por acaso, é de um hospital". Mesmo que a intenção dos autores do ataque não tivesse sido essa, os efeitos podem ser devastadores. E a sua missão, enquanto polícia, deve ser evitar esses danos: "para mim, a missão não é ir atrás deles… era conseguir ter bons programas, estáveis, de prevenção, desviá-los disso, ou pelo menos pô-los a estudar no ramo, para que tivéssemos bons engenheiros no amanhã".

Apesar de o conceito de hacktivismo não fazer sentido do ponto de vista policial, procuramos perceber se, no processo da Operação Caretos, o Inspetor havia denotado algumas componentes de intervenção social ou de ordem ideológica entre os arguidos. A resposta foi peremptória: "Não têm consciência política nenhuma. Vi muito ressentimento. Por famílias fragmentadas, designadamente separação dos pais, muito ressentimento por despedimento dos pais... e, portanto, aqueles ataques a algumas instituições ou partidos seriam uma forma de vingança, digamos assim". E justifica: "uma coisa é o que as pessoas vendem no espaço mediático, é a propaganda que elas podem fazer, a ideia que elas transmitem delas próprias, a mensagem que elas transmitem, e depois a outra é o que nós temos". Perante isso, reforça que não conseguiu entre os supostos hacktivistas descortinar "pessoas com uma consciência política, que saibam definir ou com um mínimo de educação, no sentido político, de saber de onde é que vem o movimento, quem é que o pode ter fundado, quem é que o pode ter alimentado, como era noutros países", para concluir que "têm frases feitas. Era só mesmo o nome, os grupos que se põem nos *tags*, os grupos que se criava no *Facebook*, com determinadas nomenclaturas e que se dizia que se fazia e se apoiava, mas que, na sua opinião, não chegavam para conferir uma base ideológica ou política ao grupo.

A conversa com o Inspetor Rogério Bravo foi também importante para trazer alguma luz sobre a diferença entre cibercrime e criminalidade informática, que é o que geralmente está associado à ideia de *hacking*. Bravo explicou que "cibercrime é todo o crime que acontece no ciberespaço", sendo que "ciberespaço é tudo o que acontece desde o terminal de comunicações, mais as comunicações eletrónicas e suas infraestruturas". Exemplifica com casos concretos: "estamos no OLX e mandamos vir um telemóvel, por 200 euros. Recebemos um tijolo em casa. Foi uma burla. Foi uma burla no ciberespaço. Foi cibercrime". Porém, tal não constitui crime informático, pois isso não afeta quatro princípios fundamentais: confidencialidade, integridade, disponibilidade e não-repúdio dos dados ou da informação. Por outro lado, se estivermos a falar de um *ransomware*, "um *malware* que cifra os dados de um sistema, e ainda por cima aparece uma mensagem a exigir um pagamento… a

integridade foi-se, a disponibilidade também… pelo menos dois princípios foram afetados. É crime informático". Afirma que esta abordagem tem sido eficaz na definição dos tipos de cibercrime. Relativamente ao hacktivismo, a aplicação destes princípios pode também servir para distingui-lo de outras formas de ciberativismo, que não recorrem ao *hacking*.

6 Investigadores em cibersegurança: os *hackers* "do bem"

Em abril de 2018, vários órgãos de comunicação social portugueses fizeram eco da conquista de uma competição internacional que procurava eleger o "*hacker* mais valioso" (*Most Valuable Hacker*) da atualidade, por parte de um investigador português, André Baptista[6], do Centro de Competências em Cibersegurança e Privacidade (C3P) da Universidade do Porto. Algumas semanas mais tarde, tive oportunidade de falar pessoalmente com ele, por ocasião do Congresso *C-Days 2018*, realizado em Coimbra. Combinamos uma entrevista presencial, já que a sua comunicação ali apresentada sobre "técnicas ofensivas" despertou-me interesse, assim como a perspetiva de que "para saber defender, é preciso também saber atacar". No ínicio de julho de 2018, desloquei-me às instalações do C3P para conversar com o André Baptista, começando por questioná-lo sobre o significa, afinal ser um *hacker*. Ele explicou que "um *hacker* é uma pessoa que gosta de ultrapassar limitações de uma forma criativa. Portanto, é como se fosse um *mindset*, é uma forma de pensar". Porém, embora também reconheça que "em Portugal a consciência está a evoluir", o conceito ainda carrega uma conotação tendencialmente negativa: "existe esse conceito de que o *hacker* é um criminoso. Por exemplo, numa entrevista que dei, que depois foi difundida noutros *sites*, eles puseram lá *hashtags*: #*hacker*, #pirataria e mais não sei quê. Pronto, pirataria? Não tem nada a ver com pirataria!". Mas espera ajudar a mudar essa perceção, tendo já afirmado, em várias entrevistas, que "claramente, um *hacker* não é um criminoso".

Como também fora revelado durante o *C-Days*, Baptista integra uma equipa de investigadores que participa regularmente em competições de *hackers*, nomeadamente as chamadas *bug bounties*, em que empresas ou outras entidades oferecem recompensas financeiras (geralmente, bastante avultadas), a quem conseguir penetrar no seu sistema. Atualmente, Portugal tem duas equipas que integram o TOP-100 mundial deste tipo de competição, sendo a outra composta por investigadores do Instituto Superior Técnico, de Lisboa. Baptista acredita que esta abordagem traz grandes benefícios para quem trabalha em cibersegurança: "recompensar quem descobre falhas é um incentivo para

6 https://www.jn.pt/inovacao/interior/o-hacker-mais-valioso-do-mundo-e-portugues-9264625.html

que montes de pessoas estejam a tentar descobrir falhas, de forma gratuita, claro, porque se ninguém descobrir também não se vai pagar nada. Mas sabemos que, pelo menos, alguém tentou". Assim, acredita que esse investimento é extremamente compensador a nível de retorno, "porque não se paga muito, poupa-se recursos e acaba-se por melhorar significativamente a segurança dos sistemas". E, do ponto de vista prático, isso traduz-se em vantagens, pois "quem está a defender não tem o mesmo ponto de vista do que um atacante. Portanto, se eles estão a proteger contra atacantes, têm que se colocar, obrigatoriamente, no lugar deles". Nesse sentido, procurei perceber se, no seu entender, os ataques que não têm intenções maliciosa devem ser criminalizados, mesmo que se trate de um acesso não autorizado. André Baptista responde:

> *É assim, eu acho que não devia ser um crime, se não houver dano. Agora, a lei portuguesa o que diz é "a tentativa é punível". Pá, eu acho que aqui… tem de haver bom senso por parte das empresas e organizações. Porque se alguém está a tentar descobrir falhas no sistema, um bug, porque quer ajudar, ou até porque quer até ganhar uma certa reputação... Por exemplo, se alguém quiser descobrir falhas no governo nem sequer pode tentar! Nem sequer pode tentar. Mas era bom que ele tentasse, porque se ele tentar e descobrir falhas, pode ganhar até reputação junto do governo, pode ganhar um emprego ou... mesmo receber dinheiro por isso. Tem de haver essa consciência por parte das empresas. De acordo com a lei, é punível, mas tem de haver bom senso. Se um investigador descobre uma falha, ou pelo menos anda a tentar, e quem está a analisar percebe que aquilo é uma tentativa de ataque, pode tentar chegar a essa pessoa e dizer: "você está a tentar descobrir falhas aqui? Ou está a tentar prejudicar os nossos sistemas?". Pronto, tentar perceber se está a tentar danificar os sistemas, ou simplesmente a fazer investigação. Isso é complicado, para quem não tem pessoas que sejam boas na área e que percebam. É complicado. Mas, pelo menos, se receberem uma informação de um investigador bem intencionado, que diz "tentei fazer isto e isto, mas foi com intenção de descobrir falhas, para vos ajudar a melhorar os vossos sistemas, sem pedir nada em troca. Claro que, se me quiserem dar...", devem ter a consciência de que essa pessoa esteve a ajudar-nos, porque se fosse outra pessoa a tentar descobrir falhas, ou porque é da concorrência, ou porque nos quer prejudicar, ou roubar dados para fazer blackmailing, era muito pior para nós!*

Perante este posicionamento, que se pode considerar mais "aberto" do que o da polícia, tentei também averiguar o seu ponto de vista sobre o fenómeno do hacktivismo, que lhe peço para distinguir de outras formas

de ciberativismo: "basicamente, a maior diferença que existe aí é o conceito do *hacking*... é conseguir entrar, por exemplo, num site do *target* que nós achamos que está a fazer alguma coisa injusta e conseguir mudar o *site*. Ou para passar uma mensagem". No geral, o investigador assume uma posição favorável ao hacktivismo, ao nível dos princípios: "a causa é boa porque há muita corrupção e coisas que não se sabem e se souberam devido a esse tipo de movimentos. Agora, esses movimentos, muitas vezes, resultam em atividades ilegais e, depois, a consequente punição dos autores". Porém, não se coíbe de fazer algumas reservas a este tipo de intervenção, nomeadamente no caso dos *Anonymous*, já que estes são "um grupo bastante desorganizado, em si. Desorganizado do ponto de vista em que há pessoas que estão lá e que não sabem o que estão a fazer". E isso pode trazer consequências nefastas: "Um lembra-se de fazer uma coisa qualquer, e entra num site qualquer porque lhe apeteceu, sem motivo político ou ideológico, ou para impor justiça, ou o que seja. Muitas vezes acontece isso: entram num site qualquer só porque sim". No entanto, considera aceitável e até benéfica a intervenção dos hacktivistas em algumas situações, como na denúncia de casos de corrupção ou de pedofilia, ou mesmo no desmantelamento de *sites* que servem como base de recrutamento para grupos terroristas. Nesses casos, afirma até que "há muitos governos que incentivam. Acaba por não ser ilegal, não é? Aquilo é dos terroristas, não é de nenhum governo, não é nenhuma empresa, é dos terroristas, portanto… os terroristas não os vão processar! Por isso, é carta branca: façam o que quiserem!"

Cerca de dois meses depois, voltei ao C3P, desta feita para entrevistar o seu diretor, o Professor Luís Antunes. Questionado sobre a questão do hacktivismo, declara que "se calhar, na questão de princípio até concordo com eles. Depois, é a questão da forma como fazem as coisas para chegar ao objetivo deles. E a forma, eu acho que está errada". Considera que, além de estas atividades constituírem um crime do ponto de vista legal, "do ponto de vista formal, ético e moral, na minha opinião, também é reprovável. Se eles estão a tentar testar uma instituição, contactam a instituição e dizem: olhem, nós gostávamos de os testar". Sublinha que isso é de vital importância porque "não sabemos o que está do outro lado. Pode estar um hospital, pode estar uma universidade, pode estar um Estado. Portanto, o meu conselho aqui tem sido sempre: vamos avisar a instituição, que gostávamos de colaborar, e até podemos fazer isto *pro bono*, só pelo desafio". Contudo, é fundamental a instituição estar avisada, pois "se o sistema de informação for abaixo com os nossos testes, é importante ter do outro lado um profissional pronto para resolver o problema e levantar sistemas. Portanto, a questão do *white hat* que vai fazer os testes com muito boas intenções... pá, ele pode causar problemas sérios à instituição!". E considera que, hoje em dia, não há necessidade de entrar pela via da ilegalidade para aprender técnicas ofensivas, já que "os

concursos que existem, de *hacking*, é precisamente para formação e para estes miúdos… Mas, num cenário controlado".

Do ponto de vista do investigador, este tipo de práticas devia ser implementado, até porque se verifica uma grande escassez de recursos humanos na área da cibersegurança. Mostra-se satisfeito porque "aqueles que temos são muito bons", o que "mostra que a nossa formação está a funcionar", mas são ainda em número insuficiente. Nesse sentido, pensa que as *bug bounties* acabam por ser uma forma atrativa e estimulante de chamar jovens para estas áreas, ao mesmo tempo que os afasta da via da ilegalidade. Diz que ele próprio tem "aconselhado o Estado português a promover um sistema de *bug bounties*", pagando a quem conseguisse encontrar erros nos seus sistemas. Dessa forma, as vulnerabilidades seriam detectadas em ambientes controlados, sem que haja necessidade de um grande investimento a nível de recursos humanos. E considera que o conhecimento das técnicas ofensivas é fundamental, reforçando que "para saber defender, é preciso saber atacar; ninguém sabe defender se não souber atacar". Questionado sobre perigosidade de se ensinar essas técnicas, responde: "muitas vezes somos acusados de estarmos a formar profissionais que, se usarem mal as competências que têm, a coisa corre mal", mas sublinha que "nós, enquanto universidade, temos de formar pessoas com estas competências! O país precisa de pessoas com estas competências. Se elas depois vão fazer um desvio, só temos de saber identificá-las e corrigir esse desvio". Faz mesmo um paralelismo com o serviço militar obrigatório, quando "o país ensinava toda a gente a usar uma arma" e, por conseguinte, "tinha de confiar que estava a dar uma formação ética e moral a essas pessoas, que elas não iam andar para aí aos tiros no meio da rua. Aqui, é a mesma coisa".

7 *Whistleblowers* e libertários: a face mais ativista dos hacktivistas

Ao longo dos meses em que decorreu esta investigação, o trabalho de netnografia, a participação em congressos e conferências sobre cibersegurança e as entrevistas com especialistas, permitiram-me contemplar um espectro vasto de posicionamentos e opiniões sobre cibersegurança e hacktivismo. O foco inicial no grupo *Anonymous* foi-se progressivamente desvanecendo, sobretudo por duas razões: 1) as atividades conotadas com os *Anonymous*, pelo menos em Portugal, desapareceram ou tornaram-se residuais, mesmo quando, a partir de meados de 2018, a contestação social voltou a escalar no país; 2) as atividades que ia monitorizando nas redes sociais e em alguns sites dificilmente poderiam ser classificadas como "hacktivismo". As publicações de notícias em segunda mão ou de tiradas ideológica anti-sistema podem talvez entrar no conceito alargado de ciberativismo, mas, essencialmente, não envolvem práticas de *hacking* nem constituem uma ameaça para a

confidencialidade, integridade, disponibilidade e não-repúdio dos dados ou da informação. Do ponto de vista meramente pessoal, sempre senti alguma dificuldade em perceber a relevância política ou o impacto ideológico de bloquear ou desfigurar temporariamente *sites* do Estado ou de partidos políticos, atividades que motivaram a Operação Caretos, na fase mais ativa do grupo.

Contudo, já nos últimos meses da pesquisa, acabei por tomar conhecimento de duas situações que podem perfeitamente encaixar-se no conceito de hacktivismo, desencadeadas por portugueses. Uma delas surgiu através da plataforma "Revolução dos Bytes"[7] desenvolveu uma extensão, chamada *Ahoy!*, disponível para os *browsersChrome* e *Firefox*, que permite aceder aos *sites* bloqueados em Portugal. Os seus autores apresentam assim a sua tecnologia: "Basta de limites e bloqueios! A internet é de todos e para todos, basta de termos alguém a dizer o que podemos ou não visitar!", o que revela um claro posicionamento ideológico. Apesar de não se poder considerar que esta extensão e a sua utilização constituem algo ilegal ou um fenómeno de *hacking*, já que existem várias formas "legais" de contornar estes bloqueios, nomeadamente pela utilização de VPN's, a verdade é que isso exige conhecimentos técnicos acima da média e não está ao alcance do "utilizador comum" da internet. Assim, a tecnologia oferece aos cibernautas portugueses uma forma simples (basta baixar e instalar a extensão) e gratuita de contornar as leis portuguesas quanto a restrições no acesso a *sites*. Ou seja, partindo-se de conhecimentos técnicos especializados, e assumindo objetivos ideológicos claramente definidos (liberdade na internet), sem objetivos comerciais implícitos, liberaliza-se uma tecnologia que permite a qualquer utilizador usufruir das vantagens desses conhecimentos técnicos, mesmo não os possuindo.

A outra situação a considerar atingiu enormes proporções a nível de mediatismo, pois envolveu uma das atividades mais populares em Portugal, o futebol, e em particular o clube com mais adeptos, o Benfica. Aquilo que acabou por ficar conhecido como "o caso dos *e-mails*", teve um início relativamente discreto, quando órgãos de comunicação ligados aos clubes rivais, assim como alguns blogues na internet, começaram a divulgar *e-mails* de funcionários do Benfica, indiciando algumas práticas ilícitas, eticamente questionáveis, ou mesmo indícios de corrupção. O caso atingiu maior interesse dos *media* portugueses a partir dos finais de 2017, quando a Polícia Judiciária desencadeou várias operações de buscas no Estádio da Luz. Nos meses seguintes, as notícias sobre o *leak* foram-se multiplicando, à medida que também iam sendo revelados novos *e-mails*. Apesar do grande impacto mediático do caso, a autoria dos *leaks* nunca chegou a ser conhecida. Porém, nos últimos meses de 2018, alguma

[7] https://revolucaodosbytes.pt/

comunicação social começou a apontar o nome de Rui Pinto como provável autor desse "roubo de dados", uma vez que se tratava de um *hacker* já conhecido, que esteve alegadamente envolvido num caso anterior de pirataria informática, conhecido como "*football leaks*", em que foram reveladas transferências financeiras suspeitas, envolvendo tanto clubes nacionais como estrangeiros.

Fruto, ou não, da pressão mediática, a verdade é que Rui Pinto acabou por ser detido passadas algumas semanas, na Hungria, onde residia e aguarda julgamento, após uma operação internacional mobilizada pela Polícia Judiciária. Não chegaram a ser especificadas as razões da sua detenção, nem foi confirmada, por parte das autoridades, qualquer relação do detido com o "caso dos *e-mails*". Porém, os *media* portugueses não se inibiram de fazer imediatamente essa associação, passando a foto de Rui Pinto a ter presença frequente nos noticiários televisivos, com o epíteto de "o *hacker* dos *e-mails* do Benfica". O próprio, numa entrevista ao jornal alemão *Der Spiegel*, em janeiro de 2019, revela: "Não li nenhuma declaração das autoridades sobre uma relação entre mim e o escândalo do Benfica. Uma revista publicou a história do Benfica no outono passado. Mudou a minha vida. A minha fotografia estava nas capas dos jornais por todo o país. A minha conta de *Facebook* e o meu *mail* foram inundadas com ameaças de morte"[8]. Na mesma entrevista, Pinto afirma que não se considera um *hacker*, mas "um cidadão que agiu em nome do interesse público", cuja única intenção "era revelar práticas ilícitas que afetam o mundo do futebol".

O facto de o maior e mais mediático *leak* acontecido em Portugal, envolvendo um escândalo de corrupção, estar relacionado com o futebol, acaba por ser nefasto para uma reflexão racional sobre o papel dos *whistleblowers*. É sabido que o futebol gera mais paixões do que argumentações racionais, e isso parece afetar, em larga medida, os próprios órgãos de comunicação social. Mesmo sem qualquer prova de que Rui Pinto está relacionado com o caso dos *e-mails*, o seu julgamento público foi feito, enquanto criminoso. Na verdade, os *media* deram muito maior destaque aos alegados crimes cometidos pelo suposto *hacker* do que aos crimes que estavam implícitos naquilo que foi revelado, tanto no caso dos *e-mails* como no do *football leaks*. Aliás, o próprio conceito de "denunciante" ou "*whistleblower*" raramente foi veiculado pela comunicação social portuguesa, que quase sempre optou pelo negativamente conotado "*hacker*". Uma das poucas vozes públicas que levantou esta questão foi a da eurodeputada Ana Gomes, que na sua conta de *Twitter* escreveu: "Pirata ou "whistleblower"? Expôs corrupção

8 https://tribunaexpresso.pt/football-leaks/2019-02-02-A-entrevista-a-Rui-Pinto-na-integra-Tenho-medo-de-entrar-numa-prisao-portuguesa-principalmente-em-Lisboa-e-nao-sair-de-la-vivo

bem entrincheirada. A seguir com atenção"[9]. Tais declarações provocaram imensas reações negativas, na própria rede social, o que é revelador do quão sensíveis se tornam estas questões, quando o futebol está envolvido. Porém, para quem pretende entender o hacktivismo, aquilo que Rui Pinto assume ter feito, relativamente ao caso do *football leaks*, que se prende com a denúncia de práticas ilícitas, terá de ser considerado exatamente como *whistleblowing*, e servir para uma reflexão cuidada sobre os seus efeitos.

8 Conclusão: em busca de uma teoria da prática

O processo reflexivo e analítico que se expõe neste artigo pretende contribuir para uma melhor definição dos conceitos de *hacking*, hacktivismo e *whistlebowing*, assim como das práticas que lhes estão associadas. Com base no trabalho empírico realizado, aqui exposto parcialmente, que procurou abranger uma grande diversidade de pontos de vista sobre estes fenómenos, espera-se ajudar reduzir as ambiguidades inerentes a tais conceitos, ao mesmo tempo que se propõem definições capazes de resistir às diferenças ao nível dos posicionamentos ideológicos. Para isso, será importante tentar retirar qualquer valor moral, positivo ou negativo, a todos estes conceitos, começando desde logo pelo de *hacker*. Acima de tudo, um *hacker* é um indivíduo dotado de recursos técnicos que lhe permitem entrar em zonas restritas e efetuar operações que, por desenho técnico ou imposição legal, lhe estão à partida negadas. Isto não significa que um *hacker* tenha obrigatoriamente que cometer ilegalidades. Como foi revelado ao longo do artigo, hoje em dia existem várias formas legais de praticar estas aptidões, nomeadamente competições internacionais que visam colocar à prova estas capacidades. Em suma, um *hacker* é um técnico de segurança informática, que testa sistemas. E, como em muitas outras áreas de atividade, alguém pode fazê-lo dentro ou fora da legalidade. Talvez seja útil esvaziar de sentido outros conceitos, esses sim de caráter moral, como *black* ou *white hat*: a lei europeia de cibersegurança, da qual deriva a portuguesa, é muito clara na definição do que constitui ou não um crime, o que se prende com a existência de uma autorização prévia para realizar esses testes.

Por outro lado, o conceito de hacktivismo está em estreita relação com o de *hacking* mas, por natureza, terá uma maior tendência para se situar fora das margens da legalidade. Isto porque, partindo de uma definição mais simplista, o hacktivismo constitui um tipo de "*politically motivated hacking*" (Jordan, 2002), o que influencia o seu tipo de intervenção. Outra definição, mais recente, propõe o seguinte: "O

9 https://www.jn.pt/justica/interior/hacker-expoes-corrupcao-bem-entrincheirada-diz-eurodeputada-ana-gomes-10453747.html

hacktivismo é uma forma de ativismo político em que as habilidades de *hacking* são fortemente empregadas contra poderosas instituições comerciais e governos, entre outros alvos"[10] (Sorell, 2015: 391 tradução do autor). Esta definição aproxima-se bastante daquela que é assumida neste artigo, embora sejam necessários alguns ajustes. Porém, realce-se a importância atribuída às "*hacking skills*" para a compreensão do conceito. São estas que separam o hacktivismo de outras formas de ciberativismo, igualmente empenhadas politicamente, mas que não dependem das capacidades técnicas que caracterizam o *hacking*. A maior dificuldade, ou ambiguidade, será definir com maior precisão o que pode ser definido como "ativismo político".

Em "*Everyday Forms of Resistance",* James Scott (1989) salienta que as principais estratégias de resistência quotidiana de pessoas submetidas a várias formas de poder coercivo passam sobretudo pelo anonimato e pela discrição. Táticas como a caça furtiva, a fuga aos impostos ou a deserção são utilizadas, em sigilo, por quem tem de sobreviver dentro de um sistema opressivo. Por norma, são táticas privadas, anónimas e silenciosas, ao contrário da resistência política geralmente reconhecida como tal: a dos movimentos sociais, partidários ou sindicais, que fazem da força do coletivo e do protesto público a sua forma de luta. Contudo, não devemos desprezar as primeiras enquanto formas de resistência e de ação política, já que estas podem efetivamente vir a ter um efeito avassalador sobre o sistema de controlo, a longo prazo. A resistência "invisível" pode corroer paulatinamente os mecanismos de controlo a partir de dentro, tornando o sistema disfuncional e improdutivo, obrigando a reformas e alterações no modelo de produção e de controlo. Assim, é muito difícil definir *a priori* o que é uma atitude política ou não política, ativista ou não ativista, já que esta não passa necessariamente por uma ação coletiva, em nome de um grupo. Há muitas formas de resistência aos comportamentos autoritários, repressivos e hegemónicos que podem manifestar-se na vida pessoal e privada de cada indivíduo.

A definição de hacktivismo que aqui se propõe é: uma forma de ação, individual ou coletiva, dependente da utilização de capacidades de *hacking*, que têm o propósito político-ideológico de enfraquecer, limitar ou destruir o poder coercivo de instituições ou Estados. Neste sentido, algumas destas ações podem transcender os limites da legalidade, uma vez que as leis tendem a proteger as entidades que detêm maior poder económico, político e legislativo. O *whistleblowing*, constituindo essencialmente uma prática de denúncia de situações de abuso ou uso indevido do poder, pode classificar-se como um subtipo de hacktivismo,

10 "Hacktivism is a form of political activism in which computer hacking skills are heavily employed against powerful commercial institutions and governments, among other targets" (texto original).

pois depende também da aplicação de *skills* técnicas que permitam o acesso a dados confidenciais. Apesar de muitas destas práticas serem passíveis de constituir crime informático, ameaçando a confidencialidade, integridade, disponibilidade e não-repúdio dos dados ou da informação, será pertinente questionar se, não só do ponto de vista ético e moral, mas também no âmbito da justiça social, deverá ser considerado criminoso quem assim revela a prática de crimes profundamente mais lesivos para o bem-estar social. Esta questão dependerá sempre de valores morais e de posicionamentos ideológicos. Ainda assim, de forma a alimentar a reflexão, gostaria de terminar este artigo com uma afirmação de Julian Assange (2012: 284): "a justiça, quando devidamente defendida, é uma forma de verificação do poder e a única maneira de tomarmos conta do povo é assegurando-nos de que a política nunca controla inteiramente a informação".

Referências

ASSANGE, Julian. *A Autobiografia Não Autorizada*. Carnaxide: Objectiva, 2012.

COLEMAN, Gabriella *As Muitas Faces dos Anonymous*. Lisboa: Relógio de Água, 2016.

GLASER, Barney; STRAUSS, Anselm. *The Discovery of Grounded Theory:* strategies for qualitative research. Chicago: Aldine Publishing Company, 1967.

HILDENBRAND, Bruno. Mediating Structure and Interaction in Grounded Theory *In:* BRYANT, A.; CHARMAZ, K. (Ed.) *The SAGE handbook of grounded theory*. London: Sage, 539-565, 2007.

JORDAN, Tim. *Activism! Direct Action, Hactivism and the Future of Society.* London: Reaktion Books, 2002.

KOZINETS, Robert. *Netnography:* doing ethnographic research online. London: SAGE Publications, 2010.

SCOTT, James. Everyday Forms of Resistance. *Copenhagen Papers*, Copenhagen, n. 4, p. 33-62, 1989.

SORELL, Tom. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. *Journal of Human Rights Practice*, v. 7, n. 3, p. 391-410, 2015.