

2.1.2 • A comunicação mundializada • A galáxia internet

Internet e censura do Estado

PORTUGAL NÃO É propriamente um dos casos críticos em matéria de censura, filtragem, ou bloqueio de *websites*.

Em 2015, após a assinatura do Memorando de Entendimento, que foi promovido pela secretaria de Estado da Cultura e associou operadores de telecomunicações, indústria audiovisual e ONG de combate à pirataria, o número de *sites* bloqueados era noventa.

No *Boletim Estatístico das Actividades Culturais* referente a 2015 (2016:11) diz-se “No âmbito do memorando de entendimento, a IGAC pediu o bloqueio de 196 *websites*; com o bloqueio dos *sites* e analisando o respetivo conteúdo foi possível evitar a disponibilização ilegítima de 74.815.711 obras e/ou conteúdos”

No entanto, em Janeiro de 2016 surgia um alerta, com origem no Bloco de Esquerda, onde se argumentava, seguindo de certa maneira as posições do Movimento Partido Pirata Português (MPPP), que a filtragem começava nas questões de pirataria, mas rapidamente poderia passar a um qualquer ato de censura. Tendo-se tratado de um erro de identificação do Serviço de Regulação e Inspeção de Jogos (SRJ), a que correspondeu o bloqueio do *site Carbon Games*, os bloquistas aproveitaram para pedir ao ministro da Cultura a anulação dos dois “mecanismos de censura indiscriminada e sem qualquer controlo judicial”, isto é, o Memorando de Entendimento e o Decreto-Lei nº 66/2015, que basicamente protegem os direitos de autor e permitem o bloqueio de *sites* piratas.

Protecção de direitos de autor ou violação de direitos humanos?

A questão é que em muitas outras situações não são os direitos de autor que estão em causa, mas sim os direitos humanos, a liberdade de expressão e de informação, e aqui estamos já claramente no domínio da censura de Estado. No plano global, este é um problema incontornável, que procuraremos caracterizar neste enquadramento inicial.

Os casos conhecidos são múltiplos, sendo que o sistema mais elaborado no plano internacional é conhecido como a Grande *Firewall* da China, a maior fronteira digital do mundo, sendo claro que a rede na China se chama mesmo *Chinanet*. Desde há uns anos a esta parte que o acesso à internet chinesa está inclusive controlado através das vias alternativas, como o VPN (Virtual Proxy Network), por decisão do governo, no caso do Ministério da Indústria e Tecnologia de Informação (MIIT), e os serviços VPN mais utilizados pelos chineses, como o TunnelBear, Strong VPN e Astrill, começaram a dar problemas de conexão.

Há muito que as grandes plataformas ocidentais estão bloqueadas na China: Facebook e Twitter, por exemplo, foram bloqueados em Julho de 2009, depois dos violentos conflitos étnicos no Xinjiang, os quais, como dá conta o artigo *‘Grande Firewall da China’ reforça controlo sobre a Internet*, segundo o regime haviam sido ‘instigados’ através da rede por “separatistas e extremistas religiosos radicados no estrangeiro”.

Ao longo dos últimos anos a *Chinanet* foi assim redefinindo e clonando as grandes plataformas digitais universais, e apesar do Weibo, nomeadamente, ser uma ferramenta muito usada pelos mais de trezentos milhões de *microbloggers* chineses, o certo é que toda a palavra usada que esteja indexada no rol do que não é permitido, será rastreada e bloqueada e, muito provavelmente, de acordo com os princípios locais, severamente reprimido aquele que a digitou, sendo contínuas as situações que envolvem prisão e perseguição de utilizadores por críticas ao sistema chinês.

“ Há assim um conjunto de *sites* de tracking que perseguem o nosso rasto digital: os *websites* em que nós podemos estar a navegar, ou mesmo os que não visitámos sequer. ”

Se o Weibo foi mantendo sempre a sua popularidade entre os utilizadores como uma das preferidas redes sociais na China, a verdade é que o RenRen, em parte devido às dinâmicas censórias do regime, estava decadente já no final de 2015. Emergia entretanto o WeChat (Weixin), idêntico ao WhatsApp, particularmente desenhado para *smartphone*, que tinha no início de 2016 mais de 500 milhões de contas, apostando nas mensagens instantâneas nos círculos de amigos e nos pagamentos *online*.

Francisco Rui Cádima

Simultaneamente, o Weibo, que na China também estava limitado a 140 caracteres – o que, aliás, significava a possibilidade de colocar bastante mais informação do que sucedia no ocidente com o alfabeto romano, dada a característica ideogramática do alfabeto chinês – anunciava a abertura da plataforma a um número de caracteres ilimitado, sem que, no entanto, tal possa ser entendido como um atenuar do modelo de rastreio implantado.

O uso de *astroturfing*

Complementarmente ao rastreio da Internet, os regimes autocráticos colocam em prática modelos informacionais de *astroturfing*, isto é, sistemas automatizados de propaganda, através de *robots* informáticos, de produção de informação e de comentários *online* politicamente favoráveis aos regimes no poder, ou que se enquadram como respostas ou comentários *online*, em diferentes plataformas, rebatendo massivamente as opiniões desfavoráveis aos governantes, quer de forma regular, quer com acções mais direccionadas para períodos eleitorais, como sucedeu, por exemplo, na Rússia de Putin, ou na Sérvia.

Neste último caso, e de acordo com Tatiana Vehovec, há diversas situações reportadas, a diferentes níveis, quer no domínio do ciber-assédio, quer nos fóruns de discussão *online*, ou na criação de informações falsas, rumores que se põem a correr nas redes sociais, etc., com envolvimento de grupos de pressão até partidos políticos, ou mesmo de governos, devidamente intermediados por sistemas automatizados e *bots* que, em boa parte dos casos, respondem, ou por via de *tweets* difamatórios, fazendo uma espécie de *ciber-linchamento*, ou através de modelos de *online stalking*, isto é, denegrindo os opositores independentemente do conteúdo da mensagem original. Foi também reportada a ligação entre práticas de ciber-assédio *online* e extensões do fenómeno aos jornais tablóides, de forma a amplificar a perseguição a determinados políticos ou mesmo jornalistas.

Nº de websites que disponibilizavam todo o tipo de obras protegidas de representados dos titulares de direitos, em streaming ou por download	90
Nº de websites que disponibilizavam filmes/obras cinematográficas	72
Nº de websites que disponibilizavam obras musicais	19
Nº de websites que disponibilizavam por streaming (conteúdos multimédia, música, filmes, Tv, jogos...) de direitos, em streaming ou por download	9
Nº de websites que disponibilizavam videojogos	4
Nº de websites que disponibilizavam Jornais e ou Revistas	2
Total	196

Ações repressivas em ambiente digital por parte da IGAC: bloqueio de sites

Fonte: Inspeção-Geral das Actividades Culturais (2016). *Boletim Estatístico das Actividades Culturais 2015*, p. 70, original disponível em <https://www.igac.pt/documents/20178/48338/BE+2015/825b26a7-5081-4d19-998e-242ec0c71ea>.

No caso da Rússia, temos o envolvimento do próprio serviço de segurança federal russo a FSB, agência russa de Serviços de Informação que sucedeu ao KGB, na altura dirigida por Putin, nas próprias estratégias de disseminação massiva de *bots*, sendo que a difusão de comentários adversos podem ser, por exemplo, dirigidos por provedores ou empresas contratadas especificamente para o efeito.

Propaganda digital

São sistemas complexos presentes na rede que garantem desde o bloqueio de simples caixas de comentários ao controlo e a produção de conteúdos falsos ou maléficis, com objectivos políticos determinados.

Este tipo de moderação automatizada de conteúdo está na base não somente de uma intervenção organizada para viciar a interacção nas plataformas digitais, mas está também na origem de um novo tipo de censura e de controlo das opiniões dissidentes. Esta nova estratégia de contra-informação ou de propaganda na era digital assenta em múltiplos dispositivos intermediários de controlo da rede, fundamentalmente com o objectivo de inverter o sentido do discurso sempre que este se torna inconveniente para o campo do poder político ou governamental. As ferramentas analíticas de moderação de conteúdo são portanto geridas por *robots* que criam tópicos ou gerem *hashtags* nas redes sociais, redistribuindo mensagens de forma massiva, inflacionando acessos aos *rending topics* do Twitter, por exemplo, ou mesmo criando perfis falsos para despistar qualquer identificação da origem da manipulação.

Na Rússia, em particular, o Kremlin terá iniciado um processo massivo de resposta propagandística aos protestos que se seguiram às contestadas eleições legislativas de Dezembro de 2011. O Twitter foi rapidamente inundado de contas

	Na China
Google	Baidu
Twitter	Weibo
Facebook	Renren
YouTube	Youku e Tudou
WhatsApp	WeChat (Weixin)

A internet na China, um processo de clonagem

Conteúdo website	Nº de obras/suportes
Obras cinematográficas	38 244 581
Música	13 886 537
Séries televisivas	8 966 797
Programas informáticos/ software – obras/conteúdos	8 867 643
Obras literárias	3 681 972
Videojogos	1 017 935
Jornais e revistas	38 244 581

Ações repressivas em ambiente digital por parte da IGAC: conteúdos dos websites bloqueados

Fonte: Inspeção-Geral das Atividades Culturais (2016). *Boletim Estatístico das Atividades Culturais 2015*, p. 71, original disponível em <https://www.igac.pt/documents/20178/48338/BE+2015/825b26a7-5081-4d19-998e-242ec0c071ea>.

falsas cujo objectivo era atacar os *hashtags* mais populares introduzindo informações falsas ou irrelevantes de forma a torpedear o sentido da comunicação.

Dados referidos por Morozov (2012) apontam para quase cinquenta mil contas no Twitter envolvidas na discussão sobre as eleições russas, sendo que mais de metade eram criadas a partir de *bots*, que terão postado cerca de 440 mil *tweets* sobre os temas em debate.

Para além disso, havia uma política do governo que exigia aos ISPs da Rússia a instalação de um dispositivo que ligaria directamente o provedor de internet à agência de segurança interna (FSB). Essa tecnologia permitiria desde logo interceptar o tráfego de internet, chamadas móveis, voz sobre IP, correios electrónicos, sendo mais tarde abrangidos todos os tipos de comunicações.

Tráfego bot

Dados que vão sendo conhecidos apontam para números verdadeiramente avassaladores de tráfego *bot* na net. Em 2013, por exemplo, todo este tipo de tráfego representava 61,5% da totalidade do tráfego *web*. Segundo os mesmos dados, a maioria do tráfego *website* (51%) era gerada por entidades não-humanas, 60% dos quais eram *bots* claramente maliciosos.

Os mesmos dados relativos a 2015 são algo mais tranquilizadores, segundo o *Imperva Incapsula's Annual Bot Traffic Report*, na medida em que os *bad bots* representam 'apenas' 29% do tráfego, enquanto os *good bots* correspondem a 19,5%, sendo o tráfego humano correspondente a 51,5%.

No fundo, o reforço dos mecanismos de controlo do virtual é uma das tendências mais relevantes da nova era digital, pelo que as potenciais lógicas de autonomização da *web*, face às múltiplas intermediações propagandísticas, aos *bots* e à contra-informação dos Estados, sobretudo daqueles que não lidam bem com a liberdade de expressão e os direitos humanos, é uma pura mistificação.

Rasto digital

Quanto ao *tracking*, a questão que a certo momento se coloca não é apenas a do acesso à rede e a sua democratização, ou a questão da neutralidade da rede, mas bem mais do que isso, saber de que Internet estamos a falar... Eric Schmidt (2013) no seu livro sobre a nova era digital, alerta para aquilo que ele chama a "balcanização da Internet". Isto é, de acordo com as múltiplas intervenções dos Estados rastreadores, quaisquer que sejam, a *World Wide Web* acaba por ver-se fragmentada e/ou bloqueada em diferentes áreas, originando, para determinados públicos, línguas, etc., redes significativamente diferentes umas das outras. Assim é se compararmos, por exemplo, a WWW propriamente dita com a Chinanet, ou com a *deep web*.

O rastreamento, sendo uma prática muito comum, utilizado globalmente por múltiplas entidades – das políticas e policiais às comerciais

– também é corrente nos países em que predomina a liberdade de expressão. É algo transversal a toda a Internet.

Numa conferência TED (Tecnologia, Entretenimento, Design) especificamente sobre o tema do *tracking*, Gary Kovacs (2012) chamava a atenção para o problema do "rastreamento comportamental" (*behavioral tracking*) dos utilizadores, não autorizado por estes, afirmando que "há todo um sector económico que se dedica a seguir os nossos passos pelas florestas digitais e a construir o perfil de cada um de nós. E quando possuem toda essa informação podem fazer praticamente tudo o que quiserem com ela".

Há assim um conjunto de *sites de tracking* que perseguem o nosso rasto digital: os *websites* em que nós podemos estar a navegar, ou mesmo os que não visitámos sequer, mas que têm interesse na nossa 'pegada digital' e ainda os que não fazemos ideia quem são...

A questão é que este negócio representa, para as empresas que denominam este tipo de dados, dezenas de milhares de milhões de dólares de receita, num mercado totalmente desregulado, deixando a privacidade do internauta totalmente desprotegida e a gestão dos seus dados pessoais entregue a múltiplas entidades que, em regra, não têm autorização para tal. ■

Referências

- Bloco de Esquerda diz que mecanismos de bloqueio de sites em Portugal são 'censura indiscriminada'* (2016) Tek SAPO. Disponível em http://tek.sapo.pt/noticias/internet/artigo/bloco_de_esquerda_diz_que_bloqueio_de_sites_em_portugal_e_censura_indiscriminada-45882noo.html.
- Bot Traffic Report* (2015), Imperva Incapsula, disponível em <https://www.incapsula.com/blog/bot-traffic-report-2015.html>.
- Elder, M. (2012). Emails give insight into Kremlin youth group's priorities, means and concerns. *The Guardian* (7 Feb), disponível em <http://www.theguardian.com/world/2012/feb/07/nashi-emails-insight-kremlin-groups-priorities>.
- 'Grande Firewall da China' reforça controlo sobre a Internet (2015), *Diário de Notícias* (Madeira), (26 Jan.), disponível em <http://www.dnoticias.pt/actualidade/mundo/494736-grande-firewall-da-china-reforca-controlo-sobre-a-internet>.
- Inspeção-Geral das Atividades Culturais (2016). *Boletim Estatístico das Atividades Culturais 2015*, disponível em <https://www.igac.pt/documents/20178/48338/BE+2015/825b26a7-5081-4d19-998e-242ec0c071ea>.
- Kovacs, G. (2012). Tracking our online trackers. *TED Conference*, disponível em https://www.ted.com/talks/gary_kovacs_tracking_the_trackers.
- Morozov, E. (2012). Na vida digital, cada vez mais intermediários". *Folha de S. Paulo*, (29 Out), disponível em <http://www1.folha.uol.com.br/colunas/evgenymorozov/1175587-na-vida-digital-cada-vez-mais-intermediarios.shtml>.
- Schmidt, E. & Cohen, J. (2013). *A nova era digital*. Lisboa, D. Quixote.
- Soldatov, A. & Borogan, I. (2015). Inside the Red Web: Russia's back door onto the internet *The Guardian*, (8 Sept.), disponível em <http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet>.