



# Anonimização e Redes Escuras

José Ramos, Luís Ferreira, and Rafael Silva

University of Minho, Department of Informatics, 4710-057 Braga, Portugal  
e-mail: {a73855, a74264, a76936}@alunos.uminho.pt

**Resumo:** Os métodos de Anonimização e as Redes Escuras são constituintes da secção menos conhecida e mais obscura daquela que é sem sombra de dúvida a plataforma de difusão de informação mais conhecida e utilizada neste nosso mundo, a Internet. Deste modo, este trabalho foca-se em desvendar e desmistificar alguns dos conceitos mais comuns quando abordamos estes temas, procurando elucidar tanto sobre as origens e os termos básicos bem como sobre os métodos e ferramentas a que podemos recorrer para navegarmos nesta secção tendo em atenção a proteção da nossa privacidade e dos nossos dados pessoais. Falaremos ainda dos diversos desafios e dilemas morais que surgem e do impacto dos temas em causa na sociedade atual.

## 1 Introduction

A abordagem de assuntos relacionados com Anonimização de Redes e Redes Escuras tem-se vindo a tornar cada vez mais popular e comum na sociedade e nos diálogos éticos atuais. O poder de divulgação de informação livre, sem condicionamento por parte das autoridades e dos grandes poderes económicos (ex: Média), e o carácter anónimo destas redes que oferecem uma certa privacidade a quem escolhe utilizar estes serviços quer para procura de conhecimento restrito quer para atos ilícitos levou a estes temas se tenham tornado meios muitos procurados pelos internautas da nossa época.



## 2 Desenvolvimento

### 2.1 Anonimização

A anonimização na internet teve o seu crescimento na segunda metade dos anos 2000, com o surgimento do movimento hacker de ativismo social “Anonymous”. Este movimento teve origem com o popular site “image board - 4CHAN”, frequentado por mais de 22 milhões de utilizadores por mês. O 4CHAN fora construído para a simples discussão de “anime” japonês, no entanto, o mesmo transformou-se num fórum de discussão dos mais variados assuntos, incluindo partidas online e ‘raids’ contra sites ou pessoas individuais. É a partir do 4CHAN que surge a sigla “Anonymous”, que deriva da não obrigatoriedade de registo de um utilizador específico, ou seja, todos eram anónimos.



**Figura 1.** Anonymous

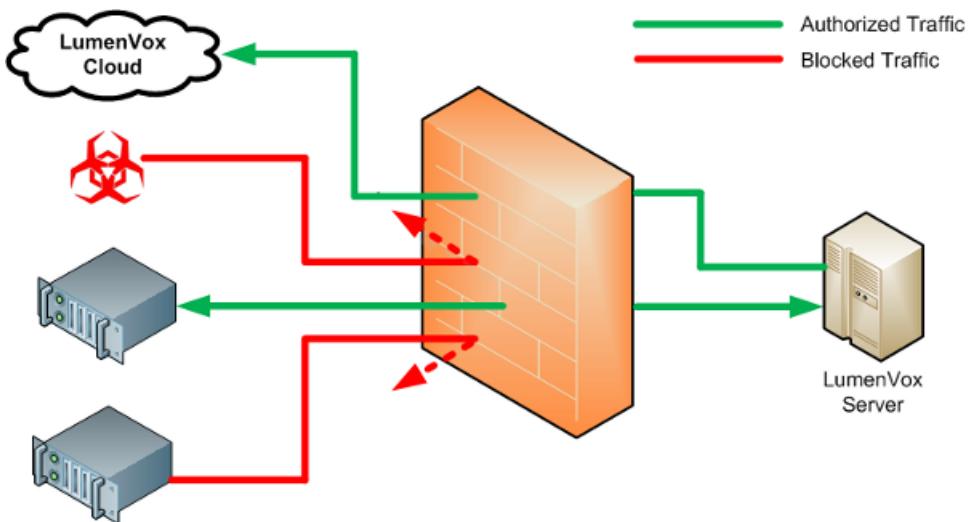
**Fundamentos** A expressão “anonimização” é ela própria vaga, uma vez que abrange uma diversidade de técnicas que podem ser usadas para converter dados pessoais em dados anonimizados. Segundo a definição do Grupo de Trabalho Sobre a Proteção de Dados do Artigo 29.<sup>º</sup> (um órgão consultivo europeu independente, em matéria de proteção de dados e privacidade), “dados anonimizados” são dados relativos a uma pessoa identificada ou identificável que não pode, razoavelmente, voltar a ser identificada ou identificável. O critério da razoabilidade significa que o processo de anonimização deve ser suficientemente robusto, de tal modo que a reversão deste processo seja “razoavelmente impossível”. A anonimização também é definida como “o processo pelo qual a informação pessoal identificável é irreversivelmente alterada, de tal forma que a informação pessoal identificável principal não pode mais ser identificada direta ou indiretamente, quer pelo responsável pelo tratamento, quer em colaboração com terceiros”.



**Figura 2.** Hacker

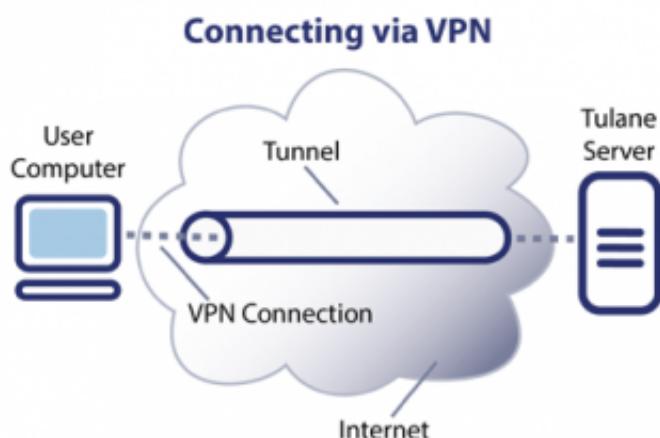
### Defesas contra anonimização:

**1 - FireWall** é um mecanismo para manter o controlo de todo o tráfego que flui dentro e fora da(s) rede(s). A maioria das firewalls que são utilizadas hoje em dia são baseadas no conceito de análise dos pacotes que estão a chegar de toda a rede. Esta análise determina o que deve ser permitido entrar ou sair. O tráfego que é permitido ou bloqueado, pode ser baseado numa variedade de factores ou largamente depende da complexidade da firewall. Por exemplo, pode permitir-se ou não tráfego baseado no protocolo que está a ser utilizado, permitindo tráfego web ou de e-mail, mas bloqueando alguns outros tipos de tráfego. [Higgins, 2008].



**Figura 3.** FireWall

**2 - VPN** A utilização de virtual private networks (VPNs) pode fornecer uma solução para o envio de tráfego sensível através redes inseguras. Uma ligação VPN geralmente é referida como um túnel, e é uma ligação encriptada entre dois pontos.



**Figura 4.** VPN Network

**Ferramentas Segurança de Rede** É possível utilizar-se uma variedade de ferramentas para melhorar a segurança de um utilizador na rede. Muitas dessas ferramentas são as mesmas que são utilizadas pelos atacantes para penetrarem nas redes, e esta é uma das principais razões porque são úteis. Através da utilização de tais ferramentas é possível localizar ameaças de segurança nas redes e assim mitigá-las. Existe um enorme número de ferramentas de segurança que estão no mercado hoje em dia e muitas delas gratuitas. Muitas correm em sistemas operativos Linux, e algumas delas poderão ser um pouco mais difíceis de configurar.



**Figura 5.** Segurança

**Anonimização e Proteção de Dados** A Lei da Proteção de Dados Pessoais portuguesa não clarifica a forma como o processo de anonimização deve ser desenvolvido. Segundo o referido Grupo de Trabalho, um processo de anonimização suficientemente robusto significa que: (1) os custos e o conhecimento exigidos para implementar a reversão da anonimização devam ser consideravelmente elevados; (2) o próprio responsável pelo tratamento de dados não consegue identificar os titulares (se após o processo de anonimização, o responsável pelo tratamento não eliminar o ficheiro original, continuamos a estar perante dados pessoais); (3) Não é mais possível estabelecer relações entre os dados de tal forma que ainda seja possível identificar o seu titular. Recomenda-se que os responsáveis pelo tratamento de dados considerem os riscos residuais de identificação, devendo proceder ao seu controlo, monitorização e reavaliação regular. Assim, a solução ideal sobre o processo de anonimização que apresenta maior robustez deverá ser avaliada caso a caso, ponderando-se as consequências da “re-identificação dos titulares dos dados”. Terminando como começámos, com as palavras de Cory Doctorow, “anonymising data is a very, very difficult business”.

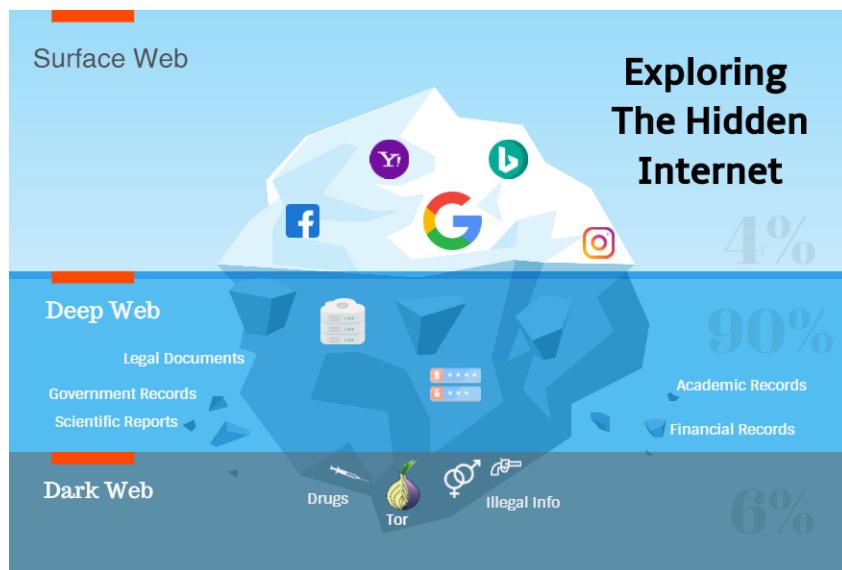


**Figura 6.** Proteção de Dados

**“If you think you’ve anonymized a data set, you’re probably wrong”** (1)

## 2.2 Redes Escuras

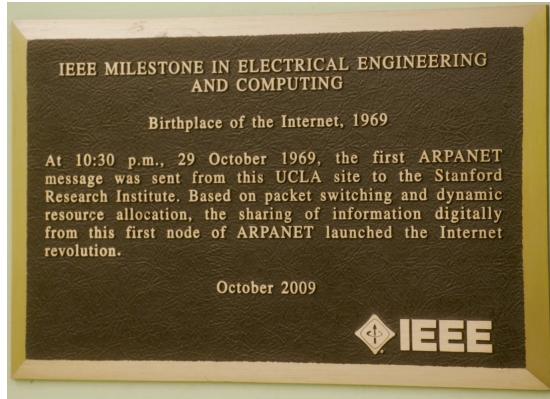
As Redes Escuras são redes de computadores com acesso restrito e não indexado que são usadas primariamente para conexões e partilhas de informação peer to peer de caráter privado.



**Figura 7.** Estratificação da Internet

## Historia

A história das redes escuras inicia-se no começo dos anos 70 logo com o aparecimento da APARNET, que seria um dos esqueletos iniciais da internet dos Estados Unidos, onde já existiam redes obscuras para a partilha de informação secretas aparecendo assim asdenominadas "darknets". Estas conexões secretas, onde circulavam informações sigilosas, eram dotadas de endereços que não apareciam nos índices oficiais de laboratórios, bases militares e universidades ou qualquer outro método de acesso a redes informáticas que fosse possível naquela época uma vez que estas recebiam dados da ARPANET, mas não se encontravam abertas nem enviavam informações para fora.



**Figura 8.** Birthplace of APARNET

Na década de 80, o método para escapar as conexões tradicionais mudou. Nasceu a ideia de se usarem servidores em países distantes com o intuito de facilitar a partilha de todo o tipo de conteudos até mesmo de ambito ilegal como paraisos fiscais com informações e serviços obscuros que não se quer que o publico geral ou mesmo as autoridades tenham conhecimento. Países como as Caraibas eram muito utilizados como hosts deste tipo de conteúdo, que podia abranger os temas mais diversos como por exemplo apostas e pornografia. Esta estratégia de abrigar servidores em terras com leis mais flexíveis e favoraveis a este tipo de atividades e serviços existe até hoje, com, entre outros, sites de pirataria que se encontram sediados em países com leis que permitem tais métodos de modo a evadirem as leis das nações que protegem os direitos intelectuais dos ficheiros que disponibilizam.



**Figura 9.** Exemplo de um site de pirataria banido pelas autoridades

Quando chegamos a década de 1990, o desenvolvimento das tecnologias de rede e informação alcança a um ponto em que começa a aumentar o uso comercial da Internet multiplicando-se aos poucos em todos os pontos do planeta com a facilidade de acesso dos consumidores comuns nascendo assim uma rede centralizada nasce. Esta rede é vista como algo prejudicial para as pessoas que procuravam reaizar atos obscuros e às escondidas tal que novas estrategias começaram a ser desenvolvidas com o intuito de permitir privacidade a quem a procurasse. Uma destas estratégias era proteger sites com passwords só para utilizadores autorizados. Para além dos métodos desenvolvidos o governo dos Estados Unidos, nomeadamente os seus órgãos militares , 'United States Naval Research Laboratory',financiou e criou o projeto TOR (The Onion Router) de onde nasceu o atual "navegador dos confins da internet"usado muitas vezes, nos dias de hoje, para a pratica de crimes. Contudo, a ideia inicial do projeto, dos cientistas Paul Syverson, Michael G. Reed e David Goldschlag, procurava um método para encobrir a identidade online dos agentes americanos em missões de campo ou até informantes infiltrados.

Com o tempo as redes escuras foram sendo cada vez mais procuradas sendo popularizadas na indústria nos anos de 2001 e 2002, quando vários artigos académicos ,de quatro cientistas da Universidade de Stanford, foram divulgados abrindo um novo mundo a muita gente que procurava um meio de transmitir informação livre das correntes metafóricas criadas pelos grandes poderes economicos e governos de certos países que procuram controlar as massas através de propagação de informação falaciosa e condicionada, como se pode verificar ainda hoje em certos ambientes políticos, como por exemplo na Coreia do Norte.

### 2.3 Deep Web

A deep web é um subconjunto da Internet simplesmente demasiado grande e / ou obscuro para ser indexado devido às limitações do software de indexação e rastreamento,isto é, limitações dos principais mecanismos de pesquisa (como Google / Bing);

Isto significa que de modo a termos acesso a estes sites que não se encontram indexados nem podem ser rastreados através dos motores de pesquisa a que temos acesso precisamos de algo que nos permita aceder aos sites diretamente em vez de os pesquisar uma vez que não há instruções para os encontrar. Não deixando de existir e podendo ser acedidos apenas se tivermos o endereço correto e em certos casos é também necessária uma senha de permissão de leitura.



**Figura 10.** Deep Web

## 2.4 Dark Web

A Dark Web pode ser situada metaforicamente em cima de sub-redes adicionais, como Tor, I2P e Freenet e pode ser considerada um subconjunto da DeepWeb.

A Dark Web é utilizada maioritariamente para assuntos como a distribuição de média, com ênfase em interesses especializados e particulares, e trocas ou vendas de produtos ou serviços ilegais. Devido ao caráter dúbio do tipo transações e interações que ocorrem nestes sites, eles procura vincular os seus clientes/utilizadores através de vários requesitos, e requesitos estes que procuram criar um laço de cupa mutua recorrendo a confirmações de pagamento, monetário ou intelectual, prévio ao serviço e mesmo a recolha de dados pessoais tal que esteja garantida cumplicidade de modo garantir que os utilizadores não avisem ou denunciem o site em questão às autoridades competentes. Esta denúncia depois porcederia de um processo na lei sobre estes sites que os procuraria bannir ou apagar uma vez que estão frequentemente associados a atividades criminosas de vários graus, incluindo compra e venda de drogas, pornografia, jogos de azar, etc.



**Figura 11.** Dark Web

Internet/DeepWeb/DarkWeb	Indexed	Non indexed
Restricted	—	DarkWeb
Accessible	Internet	DeepWeb

**Figura 12.** Tabela de camadas da Internet

## 2.5 Rede TOR

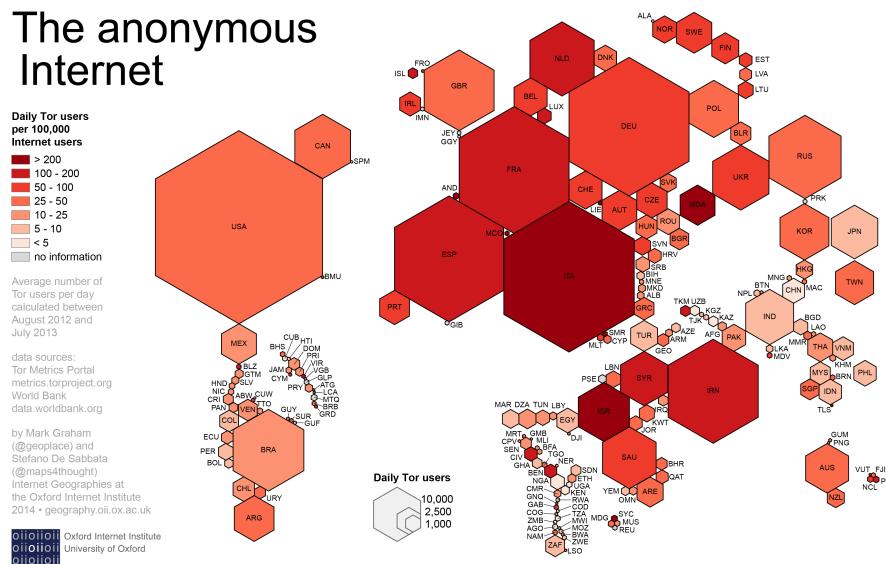
TOR (The Onion Router) é um sistema que permite a anonimização dos seus utilizadores através de saltos entre routers da rede. O caminho que o tráfego toma tem no mínimo três saltos, e as informações do encaminhamento são criadas e mantidas por servidores da própria rede.

A informação que passa na rede está encriptada, e cada router só tem conhecimento do nodo de onde provem o tráfego e qual o próximo router para que deve encaminhar o mesmo. Assim, torna-se impossível um único router conseguir determinar a origem e o destino, simultaneamente, de um certo pedido.

No entanto, os routers de entrada têm conhecimento da origem, e os routers de saída tem conhecimento da fonte. Isto constitui uma vulnerabilidade, dado que uma entidade que controle nodos de entrada e de saída ao mesmo tempo pode inferir sobre quem está a utilizar a rede e a que informação está a aceder. Este é um dos poucos pontos fracos conhecidos deste sistema, apesar de não comprometer gravemente a anonimidade do utilizador, pois é muito difícil de se reunir as condições para que tal situação aconteça.

## 2.6 Exemplos de Uso

Este serviço é usado um pouco por todo o mundo, no entanto é registada uma maior atividade nos países da Europa Central e nos Estados Unidos da América.



**Figura 13.** Distribuição geográfica dos utilizadores do TOR

Esta distribuição deve-se ao facto de estes países operarem grande parte dos serviços ocultos que existem no TOR. A atividade proveniente dos países do médio oriente associa-se ao facto de nesta região existir um maior controlo da atividade online dos utilizadores por parte dos governos, sendo esta rede uma boa forma de fugir a essas limitações.

Protocol	Connections	Bytes	Destinations
HTTP	12,160,437 (92.45%)	411 GB (57.97%)	173,701 (46.01%)
SSL	534,666 (4.06%)	11 GB (1.55%)	7,247 (1.91%)
BitTorrent	438,395 (3.33%)	285 GB (40.20%)	194,675 (51.58%)
Instant Messaging	10,506 (0.08%)	735 MB (0.10%)	880 (0.23%)
E-Mail	7,611 (0.06%)	291 MB (0.04%)	389 (0.10%)
FTP	1,338 (0.01%)	792 MB (0.11%)	395 (0.10%)
Telnet	1,045 (0.01%)	110 MB (0.02%)	162 (0.04%)
Total	13,154,115	709 GB	377,449

**Figura 14.** Tráfego de saída da rede TOR

Quanto ao tipo de tráfego que passa na rede, é observado que a vasta maioria das conexões devem-se a tráfego interactivo (HTTP). No entanto, existe uma grande desproporcionalidade entre a banda larga usada por protocolos como BitTorrent e o número de conexões que estes acarretam.

## 2.7 Impacto

### Na sociedade

A anonimização confere uma segurança aos utilizadores que lhes permite usar a web de uma forma menos ortodoxa (do ponto de vista dos governos). As pessoas devem ter o direito de se poderem expressar livremente, e por vezes estas ferramentas são a única maneira de o conseguirem. Em sociedades onde a liberdade de expressão está bastante limitada, ferramentas como o TOR têm um impacto enorme pois permitem uma livre discussão de assuntos por vezes censurados na surface web.

### Na Economia

A omissão de identidade permite a livre existência de mercados paralelos nestas redes. Estes mercados têm uma dimensão razoável e permitem a compra e venda de muitos produtos e serviços que não se encontram disponíveis nos mercados convencionais. O impacto na economia global não é significativo, mas representa uma ameaça na facilidade com que alberga os 'mercados negros'.

## 2.8 Problemas Éticos

A anonimização online gera problemas éticos, visto que, em princípio, seria um direito fundamental dos utilizadores poderem manter a confidencialidade da sua atividade digital. No entanto, a anonimização conferida por ferramentas como o TOR facilita a realização de atividades ilegais online, que se tornam praticamente impossíveis de controlar por parte das autoridades.

Algumas entidades de proteção nacional como a NSA têm vindo a contrariar esta tendência, através do controlo de certos nodos de entrada e de saída, que lhes permitem usar métodos sofisticados para rastrearem a origem de atividades ilegais. Mais uma vez, gera-se um problema ético, pois todo o tráfego que circule em nodos controlados por essas entidades está sujeito a escrutínio por parte dos mesmos.

Este continua a ser um assunto sensível e difícil de abordar, para o qual ainda não se encontrou uma solução ideal. Existe uma linha ténue entre a segurança e a liberdade individual, que torna difícil encontrar uma solução que satisfaça ambos os lados.

### **3 Conclusions**

A Anonimização e Redes Escuras são duas existências que não podem mais ser negadas nem esquecidas como parte do nosso mundo e sociedades atuais.

Com os grandes acontecimentos políticos que tem vindo a ocorrer desde já há alguns anos como por exemplo: Caso Snowden, ou os conflitos na Coreia do Norte com as suas políticas da ditadura prevalente nesse país, que condiciona de forma muito agressiva a transmissão e divulgação da informação para os habitantes dessa nação em que essas pessoas apenas podem ter acesso a notícias do mundo exterior recorrendo a redes escuras e a ferramentas como o TOR, podemos ver que tem um impacto na sociedade.

Contudo diversos pontos de vista realçam-se e para cada um deles o impacto destas tecnologias vê-se de forma diferente, negativo como é o caso de quem defende a proteção do povo, de conhecimento que não é benéfico nem necessário que podeira causar destabilizações numa sociedade. Ou positivo como no ponto de vista que defende-mos, a liberdade da informação na qual qualquer ser humano comum teria acesso à informação existente no mundo e, dotando-se de pensamento crítico, agir comfor-me os seus ideais e lições tomadas dessa informação.

### **Referências**

1. <https://www.plmj.com/xms/files/ArtigosOpiniao/2016/ITChannel.pdf>
2. <https://repositorio.ucp.pt/bitstream/10400.14/15325/1/DissertaçãoDiogoMendes.pdf>
3. Michael Bergmann, O Valor escondido da Deep Web e A Darknet e o futuro da distribuição de conteúdo
4. McCoy, Damon, et al. "Shining light in dark places: Understanding the Tor network." International Symposium on Privacy Enhancing Technologies Symposium. Springer, Berlin, Heidelberg, 2008.