RESPONSABILIDADE DE INTERMEDIÁRIOS DENTRO E FORA DA INFRAESTRUTURA DA INTERNET

Julião Braga[1]

Resumo: Este artigo tem como objetivo analisar os intermediários que gravitam em torno da Internet (dentro e fora), identificando sua localização, funções e tipos de interferências onde eventuais danos possam ser causados transmitindo informações equivocadas por falta de compreensão. Localiza os problemas e propõe soluções através do desenvolvimento de um conjunto de regras, pelas múltiplas partes interessadas. O artigo defende a necessidade da criptografia, livremente e por quem interessar, em especial, quando necessário, agregada aos protocolos que garantem as relações entre origem e destino da Internet – padronizada pelo *Internet Engineering Task Force* (IETF) –, evitando a denominada ossificação de protocolos de transporte.

Palavras-chave: Internet; Criptografia; Criptografia Fim-a-fim; Tráfego; Trânsito; *Peering*; Transporte.

[1] Doutorado em Engenharia Elétrica e Computação Universidade Presbiteriana Mackenzie & Universidade de Lisboa (Instituto Superior Técnico). Mestre em Engenharia Elétrica e Computação, na Universidade Presbiteriana Mackenzie (2015), graduação em Logística pela Universidade Anhanguera (2011), MBA em Gestão de Projetos pela Universidade Anhanguera (2013) e mestrado em Teoria da Computação pela Pontifícia Universidade Católica do Rio de Janeiro (1985). Atua em computação desde 1969.

Introdução

Internet é uma rede de redes. Cada uma destas redes possui a característica de ser autônoma e de poder estabelecer suas próprias políticas, principalmente, as políticas de roteamento. Por esta razão ela recebe a denominação de **domínio de roteamento** ou, mais comumente **Sistemas Autônomos** (AS)[2], representados parcialmente na Figura 1.

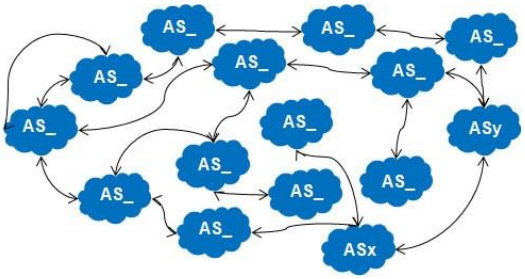

Figura 1 – A Internet e seus ASs. Fonte: (BRAGA, s/d).

Algumas vezes por falta de entendimento técnico mínimo de pessoas ou instituições, a Internet sofre algumas pressões que podem representar uma ameaça ao seu funcionamento, que as partes interessadas mais envolvidas, se esforçam para torná-lo cada vez melhor. o presente artigo segue na direção de propor dois pontos a serem discutidos: a. A proibição do uso da criptografia na Internet; b. A ausência de comportamento ético pelos provedores de mensagens instantâneas e pelos provedores de dados nos moldes de uma proposta para desenvolvedores de algoritmos de Inteligência Artificial[3]. Este ensaio aborda dois conceitos fundamentais, discute suas aplicabilidades, analisa os conceitos equivocados por desconhecimento técnico e propões soluções. O conteúdo deste artigo procura evitar o debate jurídico em torno das questões relacionadas aos intermediários. Tais questões já estão bem encaminhadas e na literatura

[2] HAWKINSON, J. **Guidelines for creation, selection, and registration of an Autonomous System** (AS). [S.l.], March 1996. RFC1930. (DOI: 10.17487/RFC1930).

[3] ARBIX, G. A Transparência no centro da construção de uma IA ética. **Novos estudos CEBRAP**, SciELO Brasil, v. 39, n. 2, p. 395–413, 2020.

tem-se diversos exemplos[4]. Este ensaio tem com base, o artigo Braga e Nobre (2020).

Fundamentos

Dois conceitos são importantes para o entendimento dos objetivos. Eles envolvem noções descritas a seguir, sobre **tráfego** e **criptografia**.

Tudo o que se movimenta nos meios físicos de transmissão de dados, através dos protocolos. Tudo! Tráfego é bit! Seja lá o que os bits representem é denominado de **tráfego**[2]. Para atender ao que será dito neste artigo identifica-se três tipos de tráfego, a saber: a. **Trânsito:** é o tráfego trocado entre os ASs. Isto é, o tráfego de pacotes que seguem na direção da Internet; b. **Transporte**: é o tráfego que não segue na direção da Internet e geralmente é o tráfego trocado entre dois pontos de conexão quaisquer; c. ***Peering***: é o tráfego trocado em um ambiente, sem custo. De um modo geral é o tráfego trocado entre um AS e um Ponto de Troca de Tráfego ou IX. Para ilustrar estas três noções de tráfego vamos supor que o ASz seja um provedor de conteúdo, por exemplo, filmes. E que o ASx seja um provedor de acesso à Internet com, digamos, aproximadamente 30.000 usuários interessados no conteúdo do ASz. Inicialmente, no momento t0, o acesso ao conteúdo do ASz é feito pela Internet. Esta alternativa de acesso, pelo tráfego de trânsito é a mais cara e paga pelo ASx que, na realidade cobra de seus usuários. Os usuários de ASx, por outro lado, pagam ao ASz pelo acesso aos filmes. O ASx, incomodado com os custos de trânsito para atender a demanda de acesso ao ASz solicita uma reunião para discutirem esta questão e chegam à conclusão de que podem resolver este problema de duas maneiras: via tráfego de transporte dedicado ou ASz instalaria uma cópia de seus servidores de conteúdo, dentro das instalações do ASx. Resolvem começar com o transporte e assim que o ASz estiver preparado, encaminharão a segunda solução. A primeira solução reduziu drasticamente o custo operacional e a segunda solução reduziram os custos do ASx para zero! Embora o custo zero seja a melhor alternativa, a disponibilidade de intermediários ofertando conteúdos para os usuários da Internet tem aumentado e algumas vezes para implementar soluções locais de espelhamento exigem

[4] SANTOS, B. M. dos. **Uma avaliação do Modelo de Responsabilidade de Intermediários do Marco Civil para o desenvolvimento da Internet no Brasil**. 2020. Disponível em: https://isoc.org.br/files/1_51635601273656445 11.pdf. Acessado em fevereiro de 2021.

investimentos iniciais elevados e a manutenção do conteúdo pode exigir tráfego de trânsito. No caso específico do Brasil, são muitos os ISPs que demandam os provedores de conteúdo e um grande número não possui o número de usuários mínimos que justifiquem instalação local. Considerando a demanda e tais ponderações fizeram com que os responsáveis pela governança da Internet em âmbito nacional propusessem a criação de um ambiente apropriado para troca de **tráfego de *peering*** a partir de conexões via **tráfego de transporte**. Tais ambientes foram denominados Pontos de Troca de Tráfego (IX ou PTT). Esta ideia foi um sucesso. Kurose e Ross[5] propões quatro propriedades desejáveis para uma comunicação segura: (A)

Confidencialidade: somente a origem e o destino devem estar habilitados ao acesso à mensagem; (B) **Integridade da mensagem**: A origem e o destino esperam que o conteúdo da mensagem não será alterado, por má fé ou por acidente; (C) **Autenticação de ponto final**: Cada um dos participantes da comunicação, origem e destino devem estar habilitadas a confirmar a cada um, que a outra parte é realmente quem afirma ser; (D) **Segurança operacional**: Para garantir esta propriedade, intermediários são usados extensivamente, como por exemplo firewalls e *Intrusion Detection Systems* (IDS). As três primeiras propriedades (A, B e C), são diretamente dependentes de **criptografia**. A última propriedade (D) é garantida por **intermediários** e será visto na seção relacionada. Criptografia passa a ser importante e alguns textos são recomendados. Uma abordagem acadêmica e atual é o livro de Stallings[6]. Um texto precioso e suficientemente didático para ser compreendido é **O Livro dos Códigos**, do Simon Singh em Singh[7]. Para um entendimento rápido, completo e, também, didático é a **Cartilha de Segurança para a Internet**, do CERT.br. Entretanto a recomendação que cumpre as exigências deste artigo é o Capítulo 8 de Kurose e Ross[8]. Há duas técnicas de criptografia que serão vistas a seguir: i. **Criptografia simétrica** é a técnica de criptografar usando uma única chave. A chave usada para criptografar é a mesma usada para decriptografar; ii.

---

[5] KUROSE, J. F.; ROSS, K. W. **Computer networking: a top-down approach**. 7. ed. [S.l.]: Pearson Education Limited, 2017.

[6] STALLINGS, W. **Criptografia e Segurança de Redes**: Princípios e Práticas. 6. ed. São Paulo, Brasil: Pearson Education do Brasil, 2015.

[7] SINGH, S. **O Livro dos Códigos**. 5. ed. São Paulo: Editora Record, 2005.

[8] KUROSE, J. F.; ROSS, K. W. **Computer networking: a top-down approach**. 7. ed. [S.l.]: Pearson Education Limited, 2017.

Criptografia assimétrica é a técnica de criptografar usando duas chaves: **pública** e **privada**. Se Alice tem de enviar uma mensagem para Bob, Alice precisa de descobrir qual a chave pública de Bob para usá-la no processo de criptografar. Seguem duas aplicações da Criptografia Assimétrica: a. **PGP** *Pretty Good Privacy* (PGP) foi escrito por Philip Zimmermann em 1997 e padronizado pelo IETF em2007 como OpenPGP[9]. As etapas do PGP, para manipular o processo de criptografia são executadas automaticamente pelo software cliente de e-mail usado por Alice. Ele descobre a chave pública de Bob, armazenada em algum servidor especializado ou localmente, quando esta não for a primeira mensagem. NO destino da mensagem, o software de Bob confirma se a mensagem veio de Alice e se foi criptografada usando a chave pública de Bob; b. *Transport Layer Security* (TLS) é uma técnica de criptografia fim-a-fim e sucessor da famosa técnica *Secure Sockets Layer* (SSL) em sua versão 3[10]. Padronizada pelo IETF[11]. A TLS, em sua versão 1.3 reduziu significativamente o tempo para estabelecer a criptografia fim-a-fim, e as etapas de preparo que antecedem o pedido de transferência de uma página de Web através do protocolo *HTTPS* pelo cliente. O processo de preparação, denominado *handshake*. O detalhamento das etapas do *handshake* foge do escopo do presente artigo, mas, seu comportamento pode ser compreendido no detalhamento da RFC8446 Rescorla[12]. Complementarmente, há uma interpretação daquela RFC, no *The Cloudflare Blog*.

A Internet e os intermediários

Alguns intermediários são AS (Sistemas Autônomos), outros fazem parte da rede de um Sistema Autônomo. Dividiu-se os intermediários em dois tipos: **intermediários externos** e **intermediários internos** representados na Figura

---

[9] CALLAS, J. et al. **OpenPGP Message Format**. [S.l.], November 2007..

[10] RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3**. [S.l.], August 2018.

[11] DIERKS, T.; RESCORLA, E. The Transport Layer Security (TLS) Protocol Version 1.1. [S.l.], April 2006. DOI: 10.17487/RFC4346; RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3**. [S.l.], August 2018.

[12] RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3**. [S.l.], August 2018.

2. Os **intermediários externos** são os fornecedores de serviços que em sua grande maioria são ASs. Embora sua oferta de serviços é feita via **tráfego de trânsito**, eles procuram estar presente nos **IXs**, o que torna o custo de acesso a seus serviços, consideravelmente mais baixo. Esta independência faz com que sua representação esteja em nuvem, na figura acima. Os **intermediários internos** estão presentes internamente na rede de um AS. Eles são apresentados em dois tipos: as **caixas intermediárias** ou *middle boxes* e os **servidores de infraestruturas**. Os **servidores de infraestruturas** estão representados para mostrar que são intermediários que não representam perigo para a Internet. Pelo contrário são intermediários fundamentais para o funcionamento da Infraestrutura da Internet de um país. Dois deles estão representados: os servidores de DNS (autoritativos ou recursivos) e os servidores roots. O primeiro é um dos mais importantes intermediários da Internet e está bem desenvolvido sob o ponto de vista da segurança de suas funções. Uma técnica de criptografia assimétrica garante a **integridade** das informações que ele passa aos clientes de DNS. Os servidores de root representam a peça de suporte aos servidores de DNS e com um grande número de espelhamento espalhados pelo mundo garante a **segurança operacional** da resolução de nomes tornando inviável o ataque de terceiros interessados em ofender o bom funcionamento da Internet. Adicionalmente, a presença de servidores root em maior ou menor número em outros países não representam agressão à soberania distribuída da Internet. As **caixas intermediárias** podem representar, com frequência, um perigo para a Internet e somente podem ser impedidos através do uso da criptografia, em sua maioria, a **criptografia fim-a-fim**. Estes intermediários são discutidos na sequência.

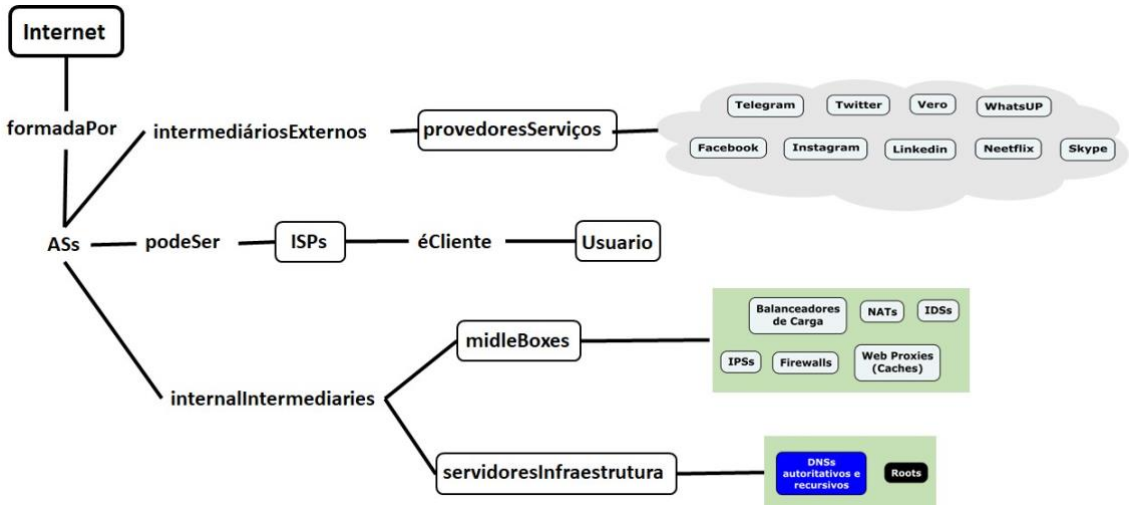

Figura 2 – Os intermediários e a Internet

Middle Boxes

A definição de **caixas intermediárias** é: Um *middlebox* é definido como qualquer dispositivo intermediário que executa funções diferentes das funções normais e padrões de um roteador IP no caminho do pacote entre um dispositivo de origem e um dispositivo de destino[13]. As caixas intermediárias interferem no pacote TCP/IP durante sua passagem pelo ambiente de um AS. Algumas destas caixas são bem conhecidas e os padrões do Internet *Engineering Task Force* (IETF) regulam seu comportamento através de RFCs. Outras, não são reguladas e são ofertadas pelo mercado de desenvolvedores, sem que se saiba exatamente os detalhes de seus algoritmos mas com promessas de eficiência e controle adicional, de interesse dos administradores de ASs. Quando uma **caixa intermediária** faz uma mudança no pacote do TCP/IP, contrariando os padrões estabelecidos pelo IETF o projeto do protocolo envolvido perde sua flexibilidade e causa uma disfunção na Internet conhecida como **ossificação do protocolo**, o qual se discute na subseção seguinte. Em sua maioria os protocolos afetados estão na camada de transporte. Estes protocolos são responsáveis pela **confiabilidade** e **integridade** além de especificarem qual o destino (aplicação) o conjunto de pacotes deverá ser dirigido. **Ossificação** de protocolo é uma redução progressiva na flexibilidade do projeto do protocolo de rede causada pela presença de *middleboxes* na rede, que não podem ser facilmente removidos ou atualizados para permitir alterações de protocolo. Mudanças no TCP também sofrem de ossificação: algumas caixas entre um cliente e o servidor remoto irão detectar novas opções de TCP desconhecidas e bloquear tais conexões, já que eles não sabem quais são as opções. Se puderem detectar detalhes do protocolo, os sistemas aprenderão como os protocolos normalmente se comportam e, com o tempo, torna-se impossível alterá-los. A única maneira verdadeiramente eficaz de "combater" a ossificação é criptografar o máximo possível o tráfego de trânsito evitando que as caixas intermediárias interfiram. Uma metodologia relatada por Edeline[14] procurando por caixas intermediárias

[13] SRISURESH, P. et al. **Middlebox communication architecture and framework.** [S.l.], August 2002. DOI: 10.17487/RFC3303; CARPENTER, B.; BRIM, S. **Middleboxes**: Taxonomy and Issues. [S.l.], February 2002. DOI: 10.17487/RFC3234.

[14] EDELINE, K. **TCP path brokenness and transport layer evolution**. November 2020. APNIC. Disponível em: https://blog.apnic.net/2020/11/03/tcp-path-brokenness-and-transport-layer-evolution/. Acessado em fevereiro de 2021.

em cerca de 52,8 milhões de caminhos, descobriu-se que 20,5 milhões (38,9%) de caminhos estão cruzando pelo menos uma caixa intermediária. A metodologia foi definida por Detal et al.[15]. Os resultados foram: a. 32,4% incluem uma caixa intermediária benigna; b. 6,5% são potencialmente prejudicados; c. 0,1% envolvem uma caixa intermediária que bloqueia o tráfego; d. 0,8% estão interrompidos por apresentarem deficiências múltiplas; e. 5,6% são afetados por caixas intermediárias de interrupção de tráfego.

Os paradoxos que rondam as sociedades abertas

A tolerância ilimitada leva ao desaparecimento da tolerância. Este é o paradoxo[16] estabelecido em 1945 pelo grande filósofo contemporâneo Karl Popper[17]. Popper esclarece: "se estendermos a tolerância ilimitada mesmo aos intolerantes, e se não estivermos preparados para defender a sociedade tolerante do assalto da intolerância, então, os tolerantes serão destruídos e a tolerância com eles". Os intermediários, com sua poderosa presença na Internet tendem a imporem seus interesses, de forma intolerante e sem respeito sobre os que lhe dão o poder.

Em 1971, o filósofo Paul Rawls concluiu em sua obra *Theory of Justice*, que uma sociedade justa deve tolerar o intolerante, caso contrário, a sociedade seria então ela própria intolerante, e, portanto, injusta[18]. Rawls também insiste, como Popper, que a sociedade tem um direito razoável de autopreservação que supera o princípio da tolerância: "ao passo que uma seita intolerante não possui pretexto para reclamar de intolerância, a sua liberdade deve ser restringida em relação aos tolerantes somente quando estes últimos creem que a sua própria segurança e as instituições que preservam a liberdade estão em perigo".

---

[15] DETAL, G. et al. Revealing middlebox interference with tracebox. In: **Proceedings of the 2013 conference on Internet measurement conference**. [S.l.: s.n.], 2013. p. 1–8.

[16] BUNCH, B. **Mathematical fallacies and paradoxes**. [S.l.]: Courier Corporation, 2012. CALLAS, J. et al. OpenPGP Message Format. [S.l.], November 2007.

[17] POPPER, K. R. **The open society and its enemies:** Hegel and Marx. [S.l.]: Princeton University Press, 2020. v. 119.

[18] RAWLS, J. **A theory of justice**. [S.l.]: Harvard University Press, 2009.

Conclusões

Do exposto e em exemplos como, o protocolo **QUIC** no qual se usou criptografia para evitar as **caixas intermediárias**, a solução indica a **criptografia**, que além de evitar a ossificação garante a presença das quatro propriedades (A, B, C, D), de Kurose. A proposta é diminuir o crescimento das vozes e esforços para eliminar a criptografia da Internet. Tal preocupação deve ser global. Os produtores de **caixas intermediárias** devem se ater às especificações das propostas produzidas pelas organizações que cuidam do desenvolvimento de padrões, como o IETF. Até porque, as caixas intermediárias poderão frustrar seus objetivos com as implementações cada vez mais apropriadas e eficazes das técnicas de **criptografia fim-a-fim**. Imprescindível esclarecer a importância de se manter a confidencialidade de mensagens trocadas entre humanos. Como consequência deve ficar claro que o mensageiro não deve ser punido, mas ele deve se juntar ao esforço da proposta do parágrafo anterior. Arbix[19] lembra que a **Declaração de Toronto** proposta em 2018 em defesa dos sistemas de aprendizagem de máquinas. Tal proposta pode ser adaptada às questões que envolvem intermediários. As múltiplas partes interessadas, produtores de caixas intermediárias, prestadores de serviços intermediários e os próprios usuários da Internet e intermediários, incluindo instituições e organizações, também interessados em garantir que a Internet funcione cada vez melhor, precisam estabelecer em conjunto, **propostas de regras associadas com o intermediário** – regras éticas, por exemplo. Tais propostas devem possuir indicações e interpretações das leis mais gerais, como a Constituição e leis específicas, além das recomendações de comportamentos que o intermediário e os produtores de caixas intermediárias devem aceitar e se comprometer a adotar quando desenvolver algoritmos, técnicas ou aplicações no país que ele desejar se estabelecer. A criação de, por exemplo, fundamentos éticos a serem respeitados por aqueles que adotam a intolerância no estabelecimento de regras unilaterais é uma oportunidade de seguir a proposta de um salto na ciência, com a criação de paradigmas, recomendado pelo não menos brilhante filósofo contemporâneo, Thomas Kuhn[20].

---

[19] ARBIX, G. A Transparência no centro da construção de uma IA ética. **Novos estudos CEBRAP**, SciELO Brasil, v. 39, n. 2, p. 395–413, 2020.

[20] KUHN, T. S. **A Estrutura das Revoluções Científicas**. 1. ed. São Paulo: Perspectiva, 1996.

Se o mensageiro não respeitar as regras assim estabelecida, então ele deve ser punido. Observa-se que no início do ano de 2021, diversos intermediários, à revelia, puniram um outro intermediário, o **Parler** com argumentos de ausência de uma ética criada por um estreitíssimo ambiente de partes interessadas.

Trabalhos futuros

As atividades que podem garantir o avanço sobre as ideias aqui propostas envolvem, principalmente, recomendações às instituições que se preocupam, diretamente, com a governança da Internet e, em particular, com direitos humanos digital. Adicionalmente seria oportuno o desenvolvimento de um esboço técnico preliminar com tópicos justificados, como forma de alavancagem de debates.

Referências bibliográficas

ARBIX, G. A Transparência no centro da construção de uma IA ética. **Novos estudos CEBRAP**, SciELO Brasil, v. 39, n. 2, p. 395–413, 2020.

BRAGA, J. **Ambiente para Aquisição de Conhecimento por Agentes em Domínios Restritos na Infraestrutura da Internet**. Tese (Doutorado) — Instituto Superior Técnico & Universidade Presbiteriana Mackenzie. Portuguese version: https://thesiscommons.org/nzmtf/ and English version: https://thesiscommons.org/83ztf/. Acessado em fevereiro de 2021.

BRAGA, J.; NOBRE, J. C. **Responsabilidade de intermediários dentro e fora da infraestrutura da Internet: uma abordagem não jurídica**. OSF Preprints, Dec 2020. Disponível em: <osf.io/r4pfa>. Acessado em fevereiro de 2021.

BUNCH, B. **Mathematical fallacies and paradoxes**. [S.l.]: Courier Corporation, 2012.

CALLAS, J. et al. **OpenPGP Message Format**. [S.l.], November 2007. DOI: 10.17487/RFC4880.

CARPENTER, B.; BRIM, S. **Middleboxes: Taxonomy and Issues**. [S.l.], February 2002.

DETAL, G. et al. Revealing middlebox interference with tracebox. In: **Proceedings of the 2013 conference on Internet measurement conference**. [S.l.: s.n.], 2013. p. 1–8.

DIERKS, T.; RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.1**. [S.l.], April 2006.

EDELINE, K. **TCP path brokenness and transport layer evolution. November 2020. APNIC**. Disponível em: https://blog.apnic.net/2020/11/03/ tcp-path-brokenness-and-transport-layer-evolution/. Acessado em fevereiro de 2021.

HAWKINSON, J. **Guidelines for creation, selection, and registration of an Autonomous System (AS**). [S.l.], March 1996. RFC1930. (DOI: 10.17487/RFC1930).

KUHN, T. S. **A Estrutura das Revoluções Científicas**. 1. ed. São Paulo: Perspectiva, 1996.

KUROSE, J. F.; ROSS, K. W. **Computer networking: a top-down approach**. 7. ed. [S.l.]: Pearson Education Limited, 2017.

POPPER, K. R. **The open society and its enemies: Hegel and Marx**. [S.l.]: Princeton University Press, 2020. v. 119.

RAWLS, J. **A theory of justice**. [S.l.]: Harvard university press, 2009.

RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3.** [S.l.], August 2018. DOI: 10.17487/RFC8446.

SANTOS, B. M. dos. **Uma avaliação do Modelo de Responsabilidade de Intermediários do Marco Civil para o desenvolvimento da Internet no Brasil**. 2020. Disponível em: https://isoc.org.br/files/1_5163560127365644511.pdf. Acessado em fevereiro de 2021.

SINGH, S. **O Livro dos Códigos**. 5. ed. São Paulo: Editora Record, 2005.

SRISURESH, P. et al. **Middlebox communication architecture and framework. [S.l.],** August 2002.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6. ed. São Paulo, Brasil: Pearson Education do Brasil, 2015.