Proteção de Dados no e-business: o papel da Inteligência Artificial

Ana Olliveira[1], Célia Talma Gonçalves[2] e Henrique Curado

[1] Instituto Superior de Contabilidade e Administração do Porto

[2] Professora Adjunta – Área Científica de Sistemas de Informação do ISCAP
Investigadora do CEOS.PP e do LIACC (Laboratório de Inteligência Artificial e Ciência de Computadores

Resumo

Esta investigação analisa qual o papel da Inteligência Artificial na proteção de dados no *e-business*, e, para tal, analisa quais os contributos e aplicações destas tecnologias para a segurança dos dados.

Desde a origem do conceito de Negócio Eletrónico e sua utilização, que questões acerca da privacidade e proteção de dados do consumidor têm sido levantadas. O Negócio Eletrónico, ou seja, a compra de produtos ou serviços online, teve início no final do séc. XX, e desde então que a Inteligência Artificial está presente no mesmo. Ainda que na altura fosse uma tecnologia menos conhecida, era possível ver aplicações de Inteligência Artificial no negócio eletrónico desde os seus primórdios. Existem assim diversas tecnologias baseadas em Inteligência Artificial que permitem detetar e impedir estes ataques, sendo esta proteção uma medida da cibersegurança.

No entanto, a proteção começa também na legislação. Para tal, o novo Regulamento Geral da Proteção de Dados apresenta recomendações aplicadas não só a todos os estados-membro da União Europeia, como também a todas as organizações que recolham dados na EU, ainda que não seja a sua localização.

Para esta investigação, foi feita uma revisão da literatura dos conceitos inerentes a comércio eletrónico, proteção de dados e inteligência artificial, bem como a apresentação de algumas tecnologias de Inteligência Artificial disponíveis para prevenir ataques cujo alvo são os dados pessoais.

Palavras-Chave: Negócio Eletrónico; Inteligência Artificial; RGPD; Proteção de Dados; Privacidade; Cibersegurança

Introdução

Para o estudo da presente investigação, a questão inicial centra-se na proteção de dados no e-business, e qual o papel da Inteligência Artificial nesta mesma proteção. Assim, foram primeiramente definidos conceitos chave, acerca de comércio eletrónico, passando então a uma abordagem acerca da Inteligência Artificial, e quais as suas tecnologias e aplicações no negócio eletrónico.

Uma outra área de extrema importância nesta investigação são os dados, a sua proteção e tratamento, pelo que estes conceitos são também definidos para esta investigação. Não seria possível falar da proteção de dados nos tempos atuais sem mencionar o Regulamento Geral de Proteção de Dados (RGPD), que é o regulamento em vigor desde 2018 que abrange não só os estados-membros da União Europeia, como também todas as empresas que efetuem tratamento de dados pessoais na União Europeia.

Por fim, e ainda relativamente aos conceitos estudados, foi feita uma abordagem ao conceito de cibersegurança, quais os ciberataques mais comuns atualmente, e de que forma a Inteligência Artificial atua para prevenir e combater estes ataques, o que se mostra como uma forma de proteção de dados através da Inteligência Artificial.

Posto isto, esta investigação encontra-se estruturada em três secções: a primeira, em que se encontra a introdução e a abordagem metodológica de investigação. Na segunda secção é feita a revisão da literatura, com todos os conceitos mencionados anteriormente e a relação entre os mesmos. Por fim é introduzida a discussão, bem como a conclusão e as referências bibliográficas.

Abordagem Metodológica

Os artigos selecionados para a elaboração do presente artigo tiveram diversas origens. Numa primeira abordagem com a temática, foi fornecido pelos orientadores desta investigação, um conjunto de artigos e dissertações que abordavam as temáticas principais do tema. Relativamente a estes artigos, numa primeira etapa da investigação e de modo a sumarizar a informação contida nos mesmos, foi elaborada uma tabela-resumo. Esta tabela continha apenas duas colunas, em que numa constava o título do artigo, e na outra uma pequena descrição do que continha no artigo. Nesta descrição, foi analisada qual a informação pertinente para o trabalho desenvolvido, bem como as *keywords*, que não só auxiliavam numa melhor perceção do que constava de facto no artigo, como também para uma mais fácil identificação para em que parte do presente trabalho o artigo seria mais útil.

Posto isto, e após esta análise preliminar dos artigos, que foram deveras úteis para começar a compreender os conceitos, a fase seguinte foi a procura de artigos que pudessem auxiliar na complementação da definição dos conceitos e na interligação dos mesmos.

Foram assim elaboradas pesquisas nas bases de dados de B-On e RCAAP, bem como no *Google Scholar*. Estas pesquisas foram feitas primeiramente com uma pesquisa simples e o auxílio de keywords, que numa primeira instância em pesquisa foram:

- "*data protection*";
- "*ecommerce*";
- "*artificial inteligence*".

De modo a obter um maior número de resultados, foram feitas pesquisas tanto na língua portuguesa como na língua inglesa, o que pode ser comprovado pela presença dos dois idiomas nas referências bibliográficas. Dada a dificuldade em encontrar informação que conseguisse abranger tanto o tema da proteção de dados como inteligência artificial, uma quarta keyword utilizada na pesquisa foi "*data security*", que apresentava soluções para a segurança dos dados, o que leva à sua proteção. Por sua vez, foi ainda feita uma pesquisa avançada, relativamente ao ano de publicação. Em artigos mais técnicos, é prioridade que a informação esteja o mais atualizada possível, pelo que no Google Scholar foi colocado o filtro para apenas apresentar resultados publicados desde 2017 até agora.

Relativamente a critérios de inclusão e exclusão, foi dada maior relevância a artigos técnicos, que fornecessem informação fidedigna acerca do conceito, e não uma opinião do tema. Apesar de também serem importantes, não era o objetivo principal desta investigação, mas sim a definição e interligação dos conceitos acerca da temática. Como tal, e para comprovar a qualidade de um artigo, um critério de exclusão poderia ser o número de citações, mas tal não foi o caso, pois esse critério só será válido se o artigo não for recente. Não é possível comparar o número de citações de uma publicação com dez anos, com uma publicação de apenas dois anos, por exemplo. Assim, algo que também foi levado em conta para a escolha dos artigos foi a relevância do autor na área.

Posto isto, primeiramente foram obtidos 37 artigos que poderiam ser relevantes para esta investigação. Após leitura dos mesmos e a aplicação destes critérios, foram escolhidos para a elaboração desta investigação onze publicações.

Revisão da Literatura

Comércio Eletrónico

Segundo Laudon & Trevor (2013), comércio eletrónico pode ser definido como a utilização da Internet para efetuar transações comerciais. Ou seja, todas as transações comerciais online entre organizações ou indivíduos, desde que envolvam a troca de valor monetário em troca de produtos ou serviços, são consideradas comércio eletrónico.

Para Kalakota e Robinson (2001), o negócio eletrónico são todas as atividades, internas e externas sustentadas pelo meio eletrónico, pelo que o comércio eletrónico está englobado no mesmo.

Este tipo de negócio veio trazer diversas alterações à visão do consumidor do que é uma transação comercial e de que forma esta pode ser executada, dado que é possível fazer uma compra online desde que se tenha acesso à Internet.

A Inteligência Artificial e o *E-Business*

Um outro conceito de extrema importância para esta pesquisa é o conceito de Inteligência Artificial (IA). Para Turban et al.(2018), Inteligência Artificial possui várias definições, mas esta explicação pode ser simplificada se forem realçados os dois aspetos básicos da Inteligência Artificial: o primeiro, que a IA é baseada no estudo do processo do pensamento humano, de modo a perceber a inteligência, e o segundo que IA representa e duplica esses processos de pensamento em máquinas (tecnologia).

A Inteligência Artificial é uma área muito vasta, dado que as suas aplicações e tecnologias podem ser encontradas nos mais variados âmbitos. Deste modo, existem diversas aplicações da Inteligência Artificial no *e-business*, que visam melhorar e proteger o processo de compra. Apesar de a utilização de tecnologias de inteligência artificial no *e-business* ser algo desejado desde o aparecimento do mesmo, nos finais do séc.XX, foi apenas em 2014 que estas tecnologias começaram a ser usadas neste âmbito, graças à grande melhoria das capacidades da IA. (Turban et al., 2018)

Ainda assim, aquando do aparecimento do *e-business*, estas tecnologias serviam maioritariamente para sustentar atividades como a procura de produtos, obtenção de recomendações, aumentar e melhorar a segurança digital, facilitar pagamentos, entre outros (Turban et al., 2018). Ou seja, estava presente nas mais variadas atividades relacionadas com a compra de um produto online, apresentando vantagens tanto para o fornecedor como para o consumidor, ainda que, nos primeiros anos do seu desenvolvimento, auxiliasse de forma mais simples. Assim, os maiores benefícios passavam pelo aumento da velocidade, redução de custos e melhorias no apoio ao cliente.

Relativamente a casos reais de aplicação da Inteligência Artificial no *e-business*, os mesmos autores mencionam no seu livro "*Electronic Commerce 2018: A Managerial and Social Networks Perspective*" (Turban et al., 2018) diversas empresas que possuem aplicações de IA no seu negócio, tais como o Facebook e a Amazon. Começando pelo Facebook, o *CEO Mark Zuckerberg* sempre se mostrou recetivo a implementar tecnologias de IA na sua rede social, pelo estão a ser desenvolvidos diversos projetos nas áreas de publicidade e apoio ao cliente, que envolvam esta inteligência artificial na resolução de problemas. Como mencionado, a IA foi aplicada no *e-business* logo desde os primórdios da sua existência, nos finais do séc.XX, e a Amazon foi empresa pioneira nessa altura, no que toca à introdução da IA no seu negócio, com o desenvolvimento de um mecanismo de sugestão de livros ao consumidor, tendo em conta as suas preferências. Atualmente, uma das aplicações mais conhecidas de IA na Amazon são os seus armazéns robotizados, que, entre várias funções, desenvolvem o trabalho humano no âmbito de gerir as encomendas, desde a sua receção à sua expedição do armazém. Estas tecnologias de Inteligência Artificial permitem assim que as empresas tenham capacidade de melhor se posicionarem no mercado, já que alguns dos benefícios diretos de tecnologias de IA como a usada no armazém da Amazon permite a diminuição de custos e aumento de produção e produtividade.

Dados Pessoais e o seu tratamento

Segundo Azmi (2002), o conceito de dados pessoais define-se como qualquer informação registada num documento que possa ser processada informaticamente ou que esteja direta ou indiretamente relacionada com um indivíduo que possa ser identificado a partir dessa informação. Ou seja, qualquer informação que possa identificar alguém, tal como nome ou morada, é considerada como informação pessoal. No entanto, esta definição não só se aplica aos exemplos mencionados de dados pessoais, mas também a opiniões. Assim, o autor defende também que as opiniões pessoais são um tipo de dados pessoais, desde que identifique um indivíduo. (Azmi, 2002).

Para uma melhor definição do que é efetivamente um dado pessoal, o Regulamento Geral de Proteção da Dados tem presente, no número 1 do artigo 4º, a informação de que dados pessoais definem-se como "(…) toda a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)" (Saldanha, 2018) e, de modo a esclarecer o que é uma pessoa identificável, acrescenta ainda que:

> "(…) é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificador por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica,

> genética, mental, económica, cultural ou social dessa pessoa singular" (Saldanha, 2018, p.31)

Segundo o RGPD, tratamento de dados define-se como "uma operação ou conjunto de operações efetuadas sobre os dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados" (Saldanha, 2018). Assim o tratamento de dados são todas as ações que serão efetuadas com os dados possuídos, podendo estas ações ser a: recolha, registo, organização, estruturação, conservação, alteração, recuperação, consulta, divulgação ou destruição dos dados, entre diversas outras ações (Saldanha, 2018).

No entanto, nem todos os dados são passíveis de ser tratados. Na sua composição, este regulamento faz a distinção de um conjunto de dados pessoais, que anteriormente eram denominados de dados sensíveis: a categoria de dados especiais (Saldanha, 2018). Este conjunto de dados têm caraterísticas sensíveis relativamente a direitos e liberdades fundamentais, pelo que o tratamento dos mesmos poderia trazer grandes riscos de violação desses mesmos direitos. Assim, são considerados dados sensíveis, e por sua vez proibidos de tratamento, os dados que revelem origem racial ou étnica, opiniões políticas, religião, convicções filosóficas ou filiação sindical; dados acerca de tratamentos de dados genéticos ou biométricos que identifiquem inequivocamente um indivíduo; e dados relativos, à saúde, vida sexual ou orientação sexual. (Saldanha, 2018) Anteriormente, este conjunto de dados sensíveis apenas abrangia dados acerca da origem racial ou étnica, opiniões políticas, religiosas ou dados acerca da saúde e vida sexual, pelo que esta nova designação visa à maior proteção dos indivíduos, dos seus dados e do tratamento dos mesmos.

A proteção de dados no *e-business*

Apesar de a questão da proteção de dados online ser uma questão que perdura há bastante tempo, são poucas as leis e políticas desenvolvidas por países relacionadas com a problemática. Um exemplo de tentativa de legislar a atividade comercial online é o Regulamento Geral de Proteção de Dados (RGPD). Este regulamento, aprovado pelo Parlamento Europeu e pelo Conselho Europeu, foi aplicado a 25 de maio de 2018 em todos os países membros da União Europeia e "considera a proteção das pessoas singulares, relativamente ao tratamento dos seus dados pessoais (…) independentemente da nacionalidade ou local de residência (…)" (Saldanha, 2018).

Para Vaz (2018), "O RGPD assume como fim basilar a supressão das falhas e da insegurança jurídica causadas pela e pela sua heterogénea aplicação nos vários Estados-Membros.", ou seja, este regulamento foi criado dada a necessidade de legislar a proteção de dados na União Europeia. Havia esta

necessidade pois, segundo Saldanha (2018) cada estado-membro, a partir da Diretiva 95/46/CE acabou por fazer as suas próprias leis no assunto, o que acabou por ter consequências na diversidade de informação existente. Para pôr fim a tais problemas, foi então desenvolvido um regulamento que pudesse ser aplicado a cada estado-membro, sem espaço para interpretações diferentes, com regras e indicações claras.

É essencial que sejam desenvolvidos métodos para proteger os dados pessoais dos consumidores de *e-business*. Esta proteção terá também um impacto na predisposição do consumidor a comprar, pois esta segurança durante as transações trará mais conforto para compras futuras.

Segundo Barkatullah (2018) os consumidores não têm cuidados quanto à sua segurança quando compram online, pois não estão conscientes dos riscos de fornecer as suas informações privadas, tais como dados bancários. São diversas as burlas que podem ocorrer nestes casos, tais como roubo de identidade, de informações bancárias, ou uso indevido de informação pessoal, o que leva a problemas de violação de privacidade (Barkatullah, 2018).

Posto isto, de modo a tentar solucionar estes problemas, os países têm vindo a desenvolver métodos de proteção que, segundo o mesmo autor, passam por criar um modelo *standarizado* que impõe regras de como é que os vendedores podem recolher, manter, usar e divulgar informação privada dos seus clientes. No entanto, também cabe ao vendedor a criação de princípios de privacidade de dados, desenvolvendo assim um código de práticas para websites. Para tal, podem ser utilizadas soluções tais como protocolos de encriptação para oferecer mais segurança aos consumidores, quando colocam as suas informações pessoais durante as transações (Barkatullah, 2018, as cited in Ivascanu, 2010). O autor afirma ainda que estas medidas de segurança passam também pelo uso de criptografia ou assinaturas digitais.

A Inteligência Artificial e a proteção de dados no e-business

Posto isto, e indo de acordo com a temática desta investigação, de que forma é que a Inteligência Artificial atua na proteção de dados no *e-business*?

As tecnologias estão a desenvolver-se a uma grande velocidade. Com esta melhoria constante de tecnologias e criação de novas, também os casos de ataques informáticos têm vindo a aumentar (Xin et al., 2018). Num negócio online, há sempre o grande risco da perda de dados, fruto destes ataques e, para tal, é necessário desenvolver mecanismos que possam prevenir estes ataques. Como tal, as aplicações da Inteligência Artificial poderão ter um grande impacto nesta prevenção, protegendo assim os dados tanto de consumidores como de fornecedores.

Para perceber de que forma é que a inteligência artificial pode atuar na proteção de dados, é necessário entender quais as ameaças existentes. Sendo baseado no acesso à Internet, existem diversas vulnerabilidades às quais o *e-business* está exposto, tais como acesso não-autorizado, fraude e roubo (González et. al, 2016). Segundo o autor, acesso não-autorizado é o acesso ilegal aos sistemas ou dados. Estes acessos mostram-se como uma grande ameaça pois permitem eu o indivíduo possa modificar ou eliminar os dados, o que se demonstra uma grande quebra na proteção de dados. Por sua vez, a fraude e roubo pode ser uma consequência direta da vulnerabilidade apresentada anteriormente, o acesso não autorizado à informação. Exemplos destes ataques são emails fraudulentos, em que são enviados emails de modo a parecerem os originais, que por norma contêm um link que redireciona o utilizador para algum tipo de *malware*, ou o ataque denominado de "*Man in the middle*", em que o hacker se coloca na comunicação entre consumidor e cliente, e consegue alterar ou roubar dados. (González et. al, 2016)

A tecnologia que permite combater estas ameaças é a cibersegurança. Segundo Xin et al.,(as cited in Aftergood, 2017) a cibersegurança define-se com um conjunto de tecnologias e processos desenvolvidos para proteger as máquinas, redes e dados dos ataques como os mencionados anteriormente. Estas tecnologias são constituídas por sistemas, que por sua vez possuem sistemas de segurança, as *firewalls,* softwares antivírus e sistemas de deteção de intrusos, que permitem descobrir e identificar comportamentos não autorizados no sistema.

Segundo Lincoln (2019), os algoritmos de *machine learning* baseados em Inteligência Artificial são desenvolvidos de modo a conseguirem detetar algum comportamento suspeito no sistema e posteriormente informar o utilizador. Sendo então baseados em Inteligência Artificial, estes algoritmos adquirem conhecimento com a sua utilização, o que leva a que este despiste se torne cada vez mais minucioso e certo, pois o seu desempenho é potencializado a cada momento, e estas aprendizagens tornam-se permanentes na tecnologia.

Assim, de modo a identificar e prevenir os ataques mencionados anteriormente, a Inteligência Artificial possuiu as seguintes tecnologias:

- *Login* biométrico;
- Processamento de Linguagem Natural (NLP);
- Cybersecurity Ratings, que avalia o grau de vulnerabilidades;
- Deteção e prevenção de invasão de rede.

Assim, segundo Lincoln (2019) existem diversos benefícios na implementação de tecnologias de Inteligência Artificial no *e-business*, tais como:

- **Identificação e Prevenção de ataques**: Como mencionado, grande parte dos ataques têm como objetivo a modificação, eliminação ou roubo de dados pessoais, o que é um enorme problema para qualquer plataforma de *e-business*. Os fornecedores têm que estar preparados com a tecnologia necessária para proteger os seus dados pessoais e os dos seus consumidores. Quando um hacker tenta entrar no seu sistema, o algoritmo de IA deteta esse ataque e com a informação que regista, aumenta a sua capacidade de prevenir um ataque futuro.
- **Necessidade mínima de intervenção humana**: Como mencionado, as tecnologias de Inteligência Artificial diferenciam-se pelo facto de recolherem informação acerca do pensamento humano, e reproduzem-no. Como tal, estes algoritmos são treinados por humanos para detetar qualquer anomalia na segurança do sistema, conseguindo assim combater esta anomalia sem necessidade de intervenção humana. Estas tecnologias são de tal forma avançadas que já começam a fazer análises preditivas, o que leva a que estes consigam fazer uma intervenção mais rápida que a intervenção humana. Além disso, um outro nível de segurança presente nestes sistemas é a autenticação multifator, que permite que o sistema recolha as credenciais mais relevantes de acesso, e posteriormente faça uma análise do comportamento do utilizador.
- **Proteção de plataformas de grande escala:** As tecnologias de Inteligência Artificial conseguem analisar o comportamento de vários níveis, especialmente em *logins* e áreas protegidas por *logins* biométricos. Diversos sistemas têm proteção a partir de impressões digitais analisadas a partir da IA ou análise de retina, o que permite um *login* bastante seguro através de dados biométricos. Após recolha automática destes dados, os mesmos serão utilizados com a tecnologia de Processamento de Linguagem Natural, de modo a detetar ameaças. (Lincoln, 2019)

Discussão

Existem assim diversas tecnologias desenvolvidas a partir de tecnologias de Inteligência Artificial que visam à proteção dos ciberataques. Estas tecnologias fazem parte da área da cibersegurança, que permite a prevenção e identificação destes ataques, comunicando o sucedido ao sistema e combatendo-o. Algumas dessas tecnologias são, como já mencionado:

- *Login* biométrico, que faz uma leitura a partir dos dados biométricos do utilizador;
- Processamento de Linguagem Natural (NLP);
- *Cybersecurity Ratings*, que avalia o grau de vulnerabilidades;
- Deteção e prevenção de invasão de rede.

No entanto, existem de facto limitações à utilização da Inteligência Artificial na cibersegurança, como é o facto de uma tecnologia tão sensível e cada vez mais poderosa, pode ser utilizada para causar danos, e não combatê-los. Esta é uma área imensa e que ainda não está toda explorada, e esta quebra na sua exploração pode apresentar graves consequências.

Posto isto, e para fazer esta investigação, uma das grandes dificuldades foi encontrar informação que relacionasse as tecnologias de inteligência artificial diretamente à proteção de dados no *e-business*. É uma área ainda não muito estudada, ou pelo menos os resultados ainda não estão acessíveis ao público, o que teria sido bastante útil para melhores resultados nesta investigação.

É importante um estudo real do comportamento do utilizador quando em contacto com o *e-business*, de que forma este protege os seus dados. Com estes resultados, e após uma investigação de todo o potencial da Inteligência Artificial, apresentar quais as potencialidades e tecnologias que a Inteligência Artificial possuiu para proteger estes dados, quer pela visão do consumidor, quer pela visão do fornecedor. A falta deste estudo mostra-se como uma lacuna na área, pois é informação que não foi encontrada após a exaustiva procura de informação para este tema.

Conclusão

Em suma, existem efetivamente diversas tecnologias de Inteligência Artificial que permitem a prevenção de ataque, o que leva à proteção de dados. Estas ações tornam-se imperativas em qualquer negócio eletrónico, pois a necessidade de proteger os dados tanto do fornecedor como do consumidor é enorme.

No entanto, sem a ajuda de legislação que apoie estas tecnologias de proteção de dados, esta proteção não seria tão eficaz. Para tal é imperativo incluir as recomendações de proteção de dados nas técnicas de proteção das organizações, e é aí que se torna importante implementar o RGPD em todas as situações de tratamento de dados pessoais. A perda destes dados traz grandes problemas às organizações, mas também aos seus clientes, pois das burlas mais comuns são, por exemplo, o roubo de dados bancários dos clientes, sendo que estes dados devem ser protegidos ao máximo.

Posto isto, o desenvolvimento destas tecnologias de proteção deve sempre acompanhar o avanço da tecnologia, pois os hackers tendem a atacar onde observam falhas. Um sistema desatualizado é o primeiro passo para a possibilidade de um ataque a dados do sistema. A Inteligência Artificial tem a capacidade de uma constante atualização face às tecnologias atuais, pelo que as plataformas de e-*business* devem optar por trabalhar com estas tecnologias, de modo a apresentarem um ambiente seguro, tanto para seus consumidores como para os próprios fornecedores.

Referências Bibliográficas

Azmi, I. M. (2002). E-commerce and privacy issues: an analysis of the personal data protection bill. *International Review of Law, Computers & Technology*, *16*(3), 317-330. https://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=0&sid=55e736f1-6d47-471d-8352-b9cbe8f27fda%40sdc-v-sessmgr01

Barkatullah, A. H. (2018). Does self-regulation provide legal protection and security to e-commerce consumers?. *Electronic Commerce Research and Applications*, *30*, 94-101. https://www.sciencedirect.com/science/article/pii/S1567422318300565?via%3Dihub

González Briones, A., Chamoso Santos, P., & López Barriuso, A. (2016). Review of the main security problems with multi-agent systems used in e-commerce applications. https://gredos.usal.es/bitstream/handle/10366/132092/Review_of_the_Main_Security_Problems_wit.pdf?sequence=1&isAllowed=y

Kalakota, R., e Robinson, M. (2001). e-business 2.0:Roadmap for sucess. http://dinus.ac.id/repository/docs/ajar/e-business_roadmap_for_success_full.pdf

Laudon, K. C., & Traver, C. G. (2013). E-commerce. Pearson Educación. http://courseware.deadcodersociety.org/csis3241-e_commerce/ch1.pdf

Lincoln, S. (2019, June 13). The Role of Artificial Intelligence in Cyber Security. AboutSSL. https://aboutssl.org/role-of-artificial-intelligence-in-cyber-security/

Macmillan, R. (2019). Big Data, Machine Learning, Consumer Protection and Privacy. *Machine Learning, Consumer Protection and Privacy (July 26, 2019)*.

Saldanha, N. (2018). Novo Regulamento Geral da Proteção de Dados. (1ºedição). FCA.

Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2018). *Electronic commerce 2018: a managerial and social networks perspective*. Springer. http://ce.sharif.ir/~abtahi/EC/EC2018.pdf

Vaz, A. R. F. (2018). *O Regulamento Geral de Proteção de Dados: Desafios e Impactos* (Doctoral dissertation, Universidade de Coimbra). https://eg.uc.pt/handle/10316/85758

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *6*, 35365-35381. https://ieeexplore.ieee.org/abstract/document/8359287