INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Por onde andas? - Perceções dos utilizadores sobre o rastreamento online.

Rita Susana da Silva Ganhão

Mestrado em Gestão de Sistemas de Informação,

Orientador:
Doutor Abílio Gaspar de Oliveira, Professor Auxiliar com Agregação,
ISCTE

Novembro, 2021

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias da Informação

Por onde andas? - Perceções dos utilizadores sobre o rastreamento online

Rita Susana da Silva Ganhão

Mestrado em Gestão de Sistemas de Informação,

Orientador:
Doutor Abílio Gaspar de Oliveira, Professor Auxiliar com Agregação,
ISCTE

Novembro, 2021

Agradecimentos

Em primeiro lugar gostaria de agradecer ao Professor Abílio Oliveira, meu orientador, por toda a ajuda, disponibilidade e grandes quantidades de paciência demonstradas ao longo de todo o processo.

A todos os professores de Mestrado que contribuíram para a minha formação, conhecimento e crescimento, em especial ao Professor Bráulio Alturas, por estar sempre presente.

Aos meus colegas de mestrado, Beatriz, Carla, Carolina, Marisa, Bruno e José que, cada um à sua maneira e em momentos cruciais, fizeram com que não baixasse os braços.

Ao meu filho Rodrigo, ao meu marido André, mãe, irmã, cunhado, sobrinho, sogra, sogro e Brigitte, por acreditarem em mim. Obrigada pelo apoio, disponibilidade e paciência.

A todos o meu sincero "Obrigada".

Resumo

O viver na era digital proporcionou aos utilizadores encontrar novas formas de trabalhar, estudar, investigar, entre outras. Mas tal, tanto pode trazer benefícios como desvantagens. A pegada digital, deixada por nós nas diferentes plataformas digitais, quando devidamente trabalhada, permite que as empresas utilizem os dados e informações dessa pegada para atingir os seus objetivos.

Os utilizadores usufruem de serviços totalmente gratuitos, pelo menos aparentemente, pois as empresas em troca desses serviços usam os dados disponibilizados na utilização desses serviços que, com a ajuda de técnicas de interação de uso e algoritmos de rastreamento, proporcionam ao utilizador experiências que sejam benéficas para as próprias empresas.

Com a presente investigação propomo-nos a analisar a perceção dos utilizadores quanto ao rastreamento feito nas diversas plataformas digitais, assim como entender como os utilizadores encaram estas formas de rastreamento relativamente à sua privacidade. Propõe-se também perceber qual a sua predisposição em aceitar esse mesmo rastreamento em troca de eventuais benefícios.

Para chegar aos resultados esperados, a investigação terá duas fases. Numa primeira fase irá ser realizada uma revisão da literatura, que servirá de base para o desenvolvimento de um questionário, tendo em vista a realização de um estudo inferencial, para responder à questão inicial e aos objetivos propostos. Os resultados obtidos permitiram verificar que os utilizadores têm alguma perceção do que é rastreamento online e existem mais desvantagens e perigos associados do que vantagens.

Palavras-Chave: Rastreamento online, Algoritmos, Segurança da Informação, Privacidade online, Controlo de dados.

Abstract

Living in the digital age has enabled users to find new ways to work, study, research, and more. But this can bring both benefits and drawbacks. The digital footprint, left by us on the different digital platforms, when properly handled, allows companies to use the data and information from that footprint to achieve their goals.

Users enjoy totally free services, at least apparently, because companies in exchange for these services use the data made available in the use of these services which, with the help of usage interaction techniques and tracking algorithms, provide the user with experiences that are beneficial for the companies themselves.

With this research we propose to analyse users' perceptions of tracking done on the various digital platforms, as well as understand how users view these forms of tracking in relation to their privacy. It is also proposed to understand their predisposition to accept this same tracking in exchange for possible benefits.

To reach the expected results, the research will have two phases. In the first phase, a literature review will be carried out, which will serve as a basis for the development of a questionnaire, with a view to carrying out an inferential study, to answer the initial question and the proposed objectives. The results obtained showed that users have some perception of what online tracking is, and there are more disadvantages and dangers associated with it than advantages.

Keywords: Online tracking, Algorithms, Information security, Online privacy, Data control.

Índice Geral

Índice de Tabelas

Índice de Figuras

Glossário de Abreviaturas e Siglas

ARPA – Agência de Pesquisa e Projetos Avançados

CFS - Collaborative Filtering Systems

HTML - HyperText Markup Language

HTTP - Hypertext Transfer Protocol

RGPD - Regulamento Geral sobre a Proteção de Dados

SPSS - Statistical Package for the Social Sciences

WEB - World Wide Web

WWW - World Wide Web

Capítulo 1 – Introdução

1.1.Enquadramento do tema

Foi no ano de 1995 que o mundo começou a conhecer novas formas de partilha de informação e de comunicação, essencialmente devido ao aparecimento da Internet. Com a Internet apareceram também as plataformas digitais, que permitiram que os utilizadores tivessem acesso a novas formas de trabalhar, de estudar ou de investigar, entre outras.

A maioria dos serviços que são disponibilizados pelas empresas, e que acabam por ser mais utilizados pelos utilizadores, são serviços que não têm qualquer custo. No entanto, para que isso seja possível, as empresas tiveram de arranjar métodos para que continuassem a ser lucrativas. As grandes empresas, detentoras das maiores e mais conhecidas plataformas digitais, estudam diariamente diferentes formas de atingirem o seu objetivo principal: ter sucesso e gerar lucros.

A disponibilização de publicidade em massa é uma técnica muito utilizada pelas empresas. As empresas perceberam que os seus ganhos aumentavam consideravelmente se os utilizadores se encontrassem ligados por grandes períodos tempo, ao utilizar técnicas de interação de uso mantinham os utilizadores mais tempo online.

De acordo com Eli Pariser, as pesquisas efetuadas por diferentes utilizadores que usam exatamente as mesmas palavras-chave, mesmo que não pertençam à mesma lista de amigos digitais, devolvem diferentes resultados (Pariser, 2011).

A informação que é colocada e partilhada na Internet tornou-se um problema em contínuo crescimento, no entanto, para as grandes empresas, detentoras das plataformas digitais, tornou-se também uma grande oportunidade de negócio. Ao aceder a uma rede social, ao correio eletrónico, a uma notícia, ao fazer um *like* ou comentário numa foto, o utilizador está a criar a sua pegada digital. Pegada esta, que contém informação que fica guardada nas diversas plataformas por onde passa.

Plataformas como o Google e o Facebook, por exemplo, criaram ferramentas que permitem aproveitar o máximo de informação possível deixada por estas pegadas. Os algoritmos têm a capacidade de rastrear todos os movimentos dos utilizadores com base nos seus gostos, necessidades e informações, permitem que as interações dos utilizadores com as plataformas sejam estudadas e mais tarde personalizadas, para lhes retornar exatamente o que preferem e o que desejam.

A personalização de perfis e de partilha de conteúdos personalizados envolve questões quanto ao acesso de informações credíveis e viáveis. Vejamos por exemplo, em caso de divulgação de informação política, a personalização de informação pode levar a situações em que o utilizador nunca vê pontos de vista contraditórios sobre questões políticas ou morais (Bozdag & van den Hoven, 2015).

1.2. Motivação e relevância do tema

A área das tecnologias de informação foi, durante muitos anos, a minha área profissional. Neste momento encontro-me na área de regulação e supervisão de segurança do ciberespaço nacional, nascendo naturalmente o interesse em investigar e saber mais sobre a temática de rastreamento dos utilizadores.

"O Dilema das Redes Sociais", documentário amplamente visionado na Netflix, expõe alguns dos segredos mais bem guardados nas empresas. Ex-funcionários explicam que quando as plataformas foram pensadas, projetadas e por fim disponibilizadas, tinham como objetivo auxiliar as pessoas no seu dia-a-dia. No entanto, esse paradigma mudou e, neste momento, todos estes tipos de plataformas têm, apenas e só, motivações económicas. As atenções estão voltadas para a necessidade de prender o utilizador o mais tempo possível às plataformas, e são criadas estratégias com esse objetivo. Os passos digitais dados pelos utilizadores são registados, guardados e analisados, para tornar a sua experiência a mais adequada à sua realidade e necessidades. A rastreabilidade tornou-se um recurso valioso, todos os *likes*, visualizações de vídeos e fotos, notícias visionadas, amigos aceites, *tags* de fotos feitas ao utilizador ou pelo utilizador, e conteúdo partilhado nas duas direções, são dados importantes para a criação de modelos. Modelos que são importantíssimos para as plataformas, pois estes permitem que seja possível entregar ao utilizador exatamente o que ele quer (ou pode vir a querer) dentro das suas preferências.

Com este trabalho, espera-se verificar o conhecimento que os utilizadores têm deste rastreamento e como lidam com ele. Pretende-se ainda perceber até que ponto o utilizador aceita este tipo de comportamento das plataformas digitais pelo benefício esperado e/ou alcançado. A investigação nesta área poderá alertar utilizadores para esta problemática, prevenir comportamentos de risco ao utilizar as plataformas digitais e ter uma perceção mais alargada sobre esta problemática.

1.3. Questões e objetivos de investigação

Esta dissertação propõe-se a analisar a perceção dos utilizadores quanto ao rastreamento que é feito nas diversas plataformas digitais.

As grandes empresas detentoras das plataformas digitais, estudam diariamente diferentes formas de serem lucrativas. Ao permitirem que os utilizadores usufruam dos seus serviços de forma gratuita, faz com que estas tenham formas de serem lucrativas. Uma das soluções encontradas foi a disponibilização de publicidade em massa. Com o avançar do tempo e após vários estudos realizados sobre o comportamento humano em relação aos seus hábitos na Internet, as grandes empresas perceberam que se utilizassem técnicas de interação de uso para manter os utilizadores online o mais tempo possível, os seus ganhos aumentavam consideravelmente. Usando técnicas de interação de uso, algoritmos de rastreamento e devolvendo ao utilizador o que este deseja ou precisa, as empresas conseguiram atingir o seu objetivo, e em alguns casos de forma muito eficiente.

Assim, é importante estudar a perceção dos utilizadores sobre esta realidade, ou seja:

Quais as perceções dos utilizadores quanto ao rastreamento a que estão sujeitos nas plataformas digitais?

A função de investigação passa por verificar e analisar como é que os utilizadores percecionam o rastreamento que é efetuado por 'terceiros' às pegadas digitais deixadas diariamente nas plataformas digitais. É ainda importante perceber como os utilizadores encaram estas formas de rastreamento relativamente à sua privacidade e qual a sua predisposição em aceitar esse mesmo rastreamento em troca de algum benefício.

Os objetivos da pesquisa são os seguintes:

- Determinar as perceções dos utilizadores sobre o rastreamento online;
- Verificar o que entendem por privacidade online e que importância lhe dão;
- Verificar a importância deste tipo de rastreamento no seu quotidiano;
- Determinar a confiança que têm quanto ao uso das plataformas digitais;
- Verificar as vantagens (ou benefícios práticos) e desvantagens (ou ameaças) que atribuem ao rastreamento online;
- Verificar eventuais ações de prevenção face ao rastreamento online;
- Verificar como se podem relacionar as suas perceções de privacidade, segurança e rastreamento online;

- Analisar as dimensões encontradas em função do género, grupo etário e nível de literacia digital.

1.4. Abordagem metodológica

Esta investigação compreende duas fases.

Numa primeira fase será realizada uma revisão da literatura que servirá de base para a realização de um estudo inferencial, por questionário. O questionário será disponibilizado a utilizadores de diferentes plataformas digitais com idades entre os 18 e os 70 anos.

Dar resposta à questão inicial da investigação assim como aos objetivos da investigação será o objetivo principal deste estudo por questionário.

1.5. Estrutura e organização da dissertação

O presente trabalho está organizado em cinco capítulos que pretendem refletir as diferentes fases até à sua conclusão.

O primeiro capítulo introduz o tema da investigação e objetivos da mesma, bem como uma breve descrição da estrutura do trabalho.

O segundo capítulo reflete o enquadramento teórico, designado por revisão da literatura.

O terceiro capítulo é dedicado à metodologia utilizada no processo de recolha e tratamento de dados bem como os métodos de análise utilizados.

O quarto capítulo apresenta a análise dos resultados obtidos, de acordo com a metodologia que se entendeu apropriada.

No quinto e último capítulo apresentam-se as conclusões da investigação, bem como alguns comentários, dificuldades encontradas e sugestões para trabalhos futuros.

Capítulo 2 – Revisão da Literatura

2.1.Internet e Plataformas online

De todas as definições que se podem encontrar de Internet, Bráulio Alturas no seu livro define-a como um conjunto de centenas de milhares de redes públicas e privadas à escala mundial, com origem nos Estados Unidos da América (Alturas, 2013). Esta permite que os utilizadores troquem mensagens entre si e acedam a uma grande quantidade de informação.

> "A Internet contém uma grande variedade de recursos e serviços, incluindo páginas e documentos interligados por meio de hiperligações da *World Wide Web*, e a infraestrutura para suportar correio eletrónico e serviços, como também a comunicação instantânea e partilha de ficheiros" (Alturas, 2013, p.78).

A sua origem é, no entanto, um pouco imprecisa. Manuel Castells diz-nos que a Internet teve a sua origem nos anos 60 e nasceu de um pequeno programa que surgiu na *Advanced Research Projects Agency* (ARPA – Agência de Pesquisa e Projetos Avançados). Criada em laboratórios militares no Estados Unidos e tinha como objetivo a troca de informações entre computadores pertencentes ao governo (Castells, 2003).

Outros autores defendem que a rede ARPANET foi apenas uma das várias redes, comerciais e não comerciais, desenvolvidas nessa altura, e que a integração destas redes numa Internet era passível de acontecer (Campbell-Kelly et al., 2013).

Alturas (2013) sintetiza assim a história da Internet:

> "1973 – Vinton Cerf cria a Internet a partir de rede de computadores ARPANET, num projeto chefiado por Robert Kahn, conduzido pela *Advanced Research Projects Agency* pertencente ao Departamento de Defesa dos EUA.
>
> 1984 – A tecnologia vira-se para o setor privado e para agências científicas governamentais.
>
> 1985 – Acesso disponível em 180 países (30 milhões de utilizadores).
>
> 2000 – A Internet atinge 100 milhões de utilizadores.
>
> 2010 – A Internet atinge 2000 milhões de utilizadores." (p.79).

Com a Internet apareceram novas formas de comunicação, possibilidades infinitas de transmissão de informação e mais liberdade de expressão. O anonimato que esta

potenciava era o ponto de partida para um novo mundo, a liberdade de expressão poderia ser praticada em pleno. Uma nova era e a possibilidade de interações nunca antes pensadas.

Contudo, a necessidade de esta ser produtiva fez com que fossem desenvolvidas formas de controlo da comunicação (Castells, 2003).

É possível encontrar serviços de todo o tipo na Internet, tais como, o comércio eletrónico (e-Commerce), que permite a compra e venda de serviços; os negócios eletrónios (e-Business), que permitem a gestão, coordenação e comunicação dentro e fora das organizações; o e-Learning, onde é possível a utilização da Internet para o ensino interativo à distância, entre outros (Alturas, 2013).

A utilização da Internet ficou mais facilitada com a chegada de diversos serviços eletrónicos e das ferramentas digitais. As plataformas digitais trouxeram aos utilizadores facilidades de acesso, e neste momento é difícil imaginar um futuro próximo sem elas. As interações sociais, culturais, políticas e económicas tornaram-se muito mais e rápidas e, de certa forma, muito mais facilitadas.

> Empresas como a Google, a Amazon e Meta, foram criadas com objetivos bem diferentes dos que têm atualmente. Inicialmente, estas empresas tinham as suas áreas de atuação bem definidas, a Google para pesquisas, a Amazon para compras, a Meta, com a plataforma Facebook, como rede social. Hoje em dia estas encontram-se a funcionar como infraestruturas vitais (Plantin & Punathambekar, 2019). A Google é mais do que uma plataforma de pesquisa, a Amazon não se dedica apenas à venda e a plataforma do Facebook, como rede social, tornou-se para muitos uma ferramenta de utilização diária e muitos não conseguem passar o dia sem interagir com ela.

Com um papel vital no dia a dia dos utilizadores, as grandes empresas digitais vislumbraram caminhos economicamente mais vantajosos e arranjaram formas eficientes de ganhar dinheiro com serviços que, teoricamente, são gratuitos.

2.1.1 Trabalhar, Pesquisar e Entretenimento

Desde o surgimento da primeira rede de computadores nos Estados Unidos da América, a sua evolução e o seu valor têm tido um crescimento extraordinário. É parte

fundamental do quotidiano social. É utilizada para os mais diversos fins: compras, jogos, operações bancárias, estudos, formação, troca de informações e muitas outras atividades.

Inicialmente o computador não era mais do que uma mera ferramenta que servia para facilitar as tarefas do dia a dia. Atualmente, as pessoas não passam sem as tecnologias de informação e comunicação, dependendo delas para quase todas as tarefas do seu quotidiano.

Internet, em conjunto com as plataformas digitais, possibilita formas mais simples de trabalhar, de pesquisar e de entreter. Existem uma infinidade de plataformas e aplicações disponíveis e estas podem ficar disponíveis e ser acedidas de acordo com as preferências, intenções e necessidades dos utilizadores.

Olhando para alguns estudos realizados, é possível verificar que houve uma alteração nos hábitos e nas relações sociais. É ainda possível verificar que a utilização da Internet, de aplicações e de plataformas digitais sofreu um crescimento colossal nos últimos anos.

Um estudo realizado por Marc Prensky diz que, em média, os estudantes universitários passam menos de 5.000 horas da sua vida a ler e mais de 10.000 horas a jogar videojogos. "Os jogos de computador, o correio eletrónico, a Internet, os telemóveis e as mensagens instantâneas são partes integrantes das suas vidas" (Prensky, 2001, p.1).

De acordo com o relatório *"Digital 2021 Global Overview Report",* presentemente, devido aos diversos confinamentos impostos em virtude da pandemia, as aplicações mais utilizadas pelas pessoas são as que permitem a realização de aulas à distância e o teletrabalho.(OLD, 2021)

Frases como, "Estão a ouvir?", "Conseguem ver o meu ecrã?", "Estás mute", ecoam pelas casas de milhares de pessoas, e continuarão a ecoar por algum tempo, pois até o paradigma do trabalho se alterou.

Todavia, para além do crescimento das plataformas de teletrabalho e de estudo, também a utilização de plataformas de comunicação e de videoconferência para fins lúdicos e para momentos em família teve um crescimento monstruoso.

De acordo com o *"Digital 2021 Global Overview Report",* no início de 2021 cerca de 4,66 milhões de pessoas em todo o mundo utilizavam a Internet, ou seja, cerca de 60 por cento da população mundial total, grande parte dos utilizadores de Internet utiliza dispositivos móveis (92,6%) para se ligarem e em média encontram-se ligados cerca de

6H e 54M. Como curiosidade, em janeiro de 2021 verificou-se um crescimento de 7,3% de utilização da Internet em Portugal em relação a janeiro de 2020 (OLD, 2021) .

De acordo com o mesmo relatório podemos verificar que a plataforma preferida pelos utilizadores em termos de comunicação laboral continua a ser o email com 93% de preferência, seguindo-se as plataformas de colaboração e videoconferências com 73%, e por fim as Videochamadas com 71%.

2.1.2 Privacidade, Segurança e Comunicação online

Por predefinição, as plataformas digitais já têm implementado um conjunto de controlos de segurança e privacidade para conteúdos partilhados, no entanto, estes são limitados e muitas vezes não garantem a segurança e privacidade que os utilizadores pretendem ou precisam.

Em certas plataformas é oferecido aos utilizadores a possibilidade de partilha de conteúdos, mas as regras de privacidade são definidas pelas próprias plataformas e o utilizador não tem a possibilidade de as criar ou definir, tendo como única possibilidade, a aceitação e partilha dos seus conteúdos ou rejeitar e ficar sem acesso ao serviço. Por norma, estas regras são extremamente permissivas e diferem de plataforma para plataforma. O seu conteúdo pode muitas das vezes ser partilhado de uma forma não-protegida, tornando mais fácil o seu uso e partilha não autorizada (Marques & Serrão, 2014).

A tecnologia faz parte do dia a dia de qualquer ser humano, até a pessoa com uma literacia digital mais limitada tem acesso às inúmeras possibilidades e a uma serie de plataformas e faculdades que a Internet possui. Quantas pessoas partilham nas redes sociais fotos ou documentos pessoais sem ter essa intenção? Quantas pessoas partilham dados ou aceitam que os seus dados sejam recolhidos sem ter a perceção de ter dado tal consentimento?

Só se pode considerar que a recolha de dados identificáveis por parte das plataformas online é justa quando o utilizador tem o controlo da sua informação, quando este é informado de forma simples e clara sobre quais são as intenções de uso da informação por parte das plataformas (Rodrigues, 2018).

Os denominados *digital natives*, geração que nasceu com Internet e rodeada de tecnologia e *gadgets*, são mais vulneráveis à ingenuidade e ao erro. Esta ingenuidade está ligada à falsa ilusão de privacidade e segurança que muitos jovens assumem que a Internet

tem por padrão. Muitas vezes expõem as suas vidas e utilizam as plataformas digitais, por exemplo os blogs e redes sociais, como se fossem os seus diários pessoais. Estes testemunhos fazem com que se verifique um crescimento acentuado de situações de humilhações, danos reputacionais e sentimentos magoados devido a divulgação pública de informação pessoal (Rodrigues, 2018).

Os utilizadores, mesmo sabendo e manifestando muita preocupação com os riscos que a publicação de grandes quantidades de informação e dados pessoais sensíveis podem acarretar, fazem-no espontânea e voluntariamente (Hallam & Zanella, 2017).

Não é só a partilha de informação em redes sociais e blogs que faz com que os utilizadores ofereçam ao mundo a sua privacidade. A crescente massificação dos serviços baseados na *cloud*[1] faz com que os utilizadores troquem cada vez mais a sua privacidade por serviços (Bergström, 2015).

Empresas como a Meta, a Google, a Microsoft, ou a Amazon controlam a *cloud,* assim, é assumido desde logo, que os utilizadores que beneficiem e utilizam este tipo de serviço correm o sério risco de perder o controlo da sua privacidade e da sua informação (Rodrigues, 2018).

A preocupação com a privacidade dificilmente afeta a divulgação ou a partilha de informação pessoal. Se existe uma mais valia com a partilha e ou divulgação essa vontade prevalece.

A comunicação e transferência de informação é bastante imediata nos dias de hoje, com apenas um toque no ecrã a informação fica acessível no momento. Os utilizadores com menos literacia digital não têm noção da quantidade de informação que é transmitida em apenas alguns segundos. Hoje, os mais novos, tem à sua disposição, toda a informação que necessitam em meros segundos, as idas às bibliotecas para pesquisas têm os seus dias contados. É dado como certo e adquirido que toda a informação que necessitamos se encontra algures na Internet. No entanto, a tolerância provocada por este acesso quase automático à informação em conjunto com o acesso a *chat rooms*, fóruns, blogs, e redes sociais pode provar-se bastante perigosa (Rosenblum, 2007).

[1] A nuvem é uma metáfora para a Internet. É uma reformulação da Internet", diz Reuven Cohen, cofundador do Cloud Camp (Regalado, 2011)

Um dos reais perigos da frequência diária na Internet, como já foi dito, é o registo digital que é deixado por todos os utilizadores. Tudo o que é colocado na Internet não sai mais da Internet. Pode parecer um cliché, mas as pessoas devem ter essa consciência. A colocação de imagens e observações menos próprias ou até comprometedoras, podem ser pesquisadas mais tarde por terceiros que podem estar a avaliar o perfil de um candidato a uma posição de emprego.

Tal como diz Rosenblum, a Internet é uma paisagem virtual de comunicação persistente que pode ser prejudicial para carreiras e oportunidades académicas, se vistas fora do contexto social original (Rosenblum, 2007).

A segurança dos dados pessoais e da informação é um tema com alguma relevância no meio digital. Nos últimos tempos foram conhecidos alguns abusos por parte de algumas organizações, tal como é indicado mais abaixo.

As organizações utilizam a plataformas digitais como meios publicitários, dispõem de um público cativo, um indicador de preferências de compra, e um tipo de registo abreviado de tendências demográficas (Rosenblum, 2007).

A coleta e posterior partilha de dados pessoais e de informação pessoal dos utilizadores podem ser questionáveis. No entanto, existem organizações que o fazem de forma dissimulada e sem que os proprietários dos dados o saibam.

Veja-se o caso da plataforma Facebook em 2016, após as eleições presidenciais dos EUA e da ligação à Cambridge Analytica, tornou-se o símbolo obscuro das redes sociais. Este caso foi amplamente difundido e acabou mesmo por ser feito o documentário 'Nada É Privado: O Escândalo da Cambridge Analytica', onde se explica como foi utilizada a informação de dados para moldar a opinião dos eleitores indecisos de forma a votarem num candidato específico.

Esta empresa ficou conhecida por usar os dados dos utilizadores, sem o seu consentimento e conhecimento, para fins de marketing de campanhas políticas (Calheiros, 2019).

Mas não é só nas redes sociais que os acessos a dados dos utilizadores são feitos, há relatórios que detalham a existência de *smartphones* iPhone e Android que enviam localização dos seus utilizadores para a Apple e Google (Kshetri, 2014).

A previsão comportamental é uma técnica amplamente utilizada, sobretudo no marketing. Com esta técnica é possível prever atributos altamente sensíveis da personalidade de uma pessoa, tais como: orientação sexual, etnia, visão religiosa e política, traços de personalidade, inteligência, felicidade, uso de substâncias aditivas, estado civil dos seus pais, idade e sexo, e para isso é só necessário utilizar registos públicos de comportamento, como por exemplo os *likes* no Facebook (Kosinski et al., 2013).

Existe uma outra questão que se coloca quando se fala em privacidade e segurança dos dados dos utilizadores. A manipulação de conteúdos consoante as preferências dos utilizadores é um facto. Os passos digitais dados pelos utilizadores são registados, guardados e analisados para tornar a sua experiência a mais adequada à sua realidade. Todos os gostos, visualizações de vídeos e fotos, notícias visionadas, amigos aceites, *tags* de fotos que são feitas ao utilizador ou pelo utilizador, e conteúdo partilhado nas duas direções, são dados importantes para a criação de modelos. Estes modelos são essenciais para que as plataformas consigam dar exatamente o que utilizador prefere, mesmo que essa não seja a sua intenção inicial.

Existem estudos que indicam que a fonte noticiosa comum se foi alterando nos últimos anos. No Relatório "A Internet e o consumo de notícias online em Portugal" de julho 2015, podemos verificar que para além da alteração do hábito de fonte noticiosa também nos diz que é de "realçar que as redes sociais, como fontes noticiosas, tendem já a ser mais consideradas do que fontes mais tradicionais, como é o caso da versão impressa de um jornal"(Obercom, 2015).

O mesmo relatório dá conta das diferenças e das preferências, no que respeita a conteúdos noticiosos, entre o género masculino e o género feminino. Tais algoritmos utilizam os rastos online deixados pelos utilizadores para mapear os interesses dos mesmos e para decidir o que deve ou não ser apresentado e assim direcionar e reforçar a importância de determinado assunto.

Com o aumento da personalização de conteúdos disponibilizados, alguns investigadores sentiram necessidade de verificar junto dos utilizadores quais as suas perceções relativamente a esta questão (Thurman et al., 2019).

Thurman et al. em 2019 consideraram uma vasta literatura e verificaram as seguintes questões quanto ao ponto de vista dos utilizadores e académicos:

Relativamente a preocupações relacionadas com a privacidade, os autores verificaram que embora os utilizadores gostassem que os *websites* mostrassem notícias adaptadas aos seus interesses, se essa adaptação se baseasse no seu comportamento de navegação na web então os utilizadores preferiam que não existisse.

Em termos de preocupações relacionadas com a falta de informação importante, tendo como princípio de que os utilizadores podem recear perder informações importantes ao utilizar serviços noticiosos personalizados, não existe consenso na literatura quanto a este receio.

Quanto a preocupações relacionadas com a falta de pontos de vista diferentes, os académicos têm sérias dúvidas sobre a seleção algorítmica. Dizem que este tipo de seleção pode levar uma redução na exposição a pontos de vista diferentes, uma vez que a personalização pode favorecer as notícias que correspondem às preferências do utilizador. Alguns dos académicos ainda sugeriram que haverá uma redução na diversidade ideológica (Thurman et al., 2019).

Um dos maiores receios dos utilizadores é, como foi indicado em cima, a falta de pontos de vista diferentes, mas também o receio da perda de informações importantes.

Esta problemática poderá trazer aos utilizadores tanto informação como desinformação, correndo o risco de que estes não consigam diferenciar.

2.2 Rastreamento online

2.2.1 Rastreamento de utilizadores

Todos os passos digitais dos utilizadores são registados, guardados e analisados para tornar a sua experiência a mais adequada à sua realidade. A rastreabilidade tornou-se um recurso valioso para as grandes empresas.

Este tipo de técnica permite que sejam guardados todos os gostos, visualizações de vídeos e fotos, as notícias visionadas, os amigos aceites, *tags* de fotos que são feitas ao utilizador ou pelo utilizador, e conteúdo partilhado nas duas direções.

De acordo com Pariser, as pesquisas efetuadas por diferentes utilizadores, mesmo fazendo parte de uma qualquer lista de amigos digitais e utilizando exatamente as mesmas palavras-chave, devolvem resultados diferentes. Resultados ajustados à realidade do utilizador (Pariser, 2011).

Atualmente, todas as grandes plataformas digitais web registam informações sobre os seus visitantes. A recolha de dados varia quanto ao tipo de informação que as próprias empresas necessitam.

Embora o rastreamento seja de grande interesse para os investigadores, os primeiros estudos sérios sobre a questão apenas surgiram em 2005, contudo, foi em 2009 que a investigação mais avançou, após o lançamento do documento técnico das normas de cookies HTTP (Lerner et al., 2016). O documento técnico das normas de cookies HTTP encontra-se em constante evolução e a sua última atualização é de abril de 2011 (Barth, 2014).

Bujlow apresenta métodos de estudo utilizados para rastreamento de utilizadores: Rastreamento por mecanismo de armazenamento, rastreamento por mecanismo de cache, rastreamento por mecanismos de impressões digitais, entre outros (Bujlow et al., 2017).

Rodolfo Avelino (2019) apresenta as seguintes descrições sobre os tipos de rastreamentos estudados por Bujlow et al.:

- "Rastreamento por mecanismo de armazenamento: depende do armazenamento explícito dos dados no computador do usuário. São mais avançados que os métodos "sem estado", e são capazes de reconhecer características do computador.
- Rastreamento por mecanismo de cache: Funciona de maneira semelhante às técnicas de rastreamento por mecanismo de armazenamento, entretanto o identificador não é armazenado no computador do usuário. Neste tipo de rastreamento um usuário pode ser identificado pela disponibilidade de arquivos em cache ou por informações armazenadas em metadados de arquivos.
- Rastreamento por mecanismos de impressões digitais (*fingerprinting*): Este mecanismo abrange todas as técnicas que tendem a reconhecer um usuário. A identificação do usuário é realizada por intermédio de informações geradas ou entregues pelo próprio dispositivo do usuário. Várias técnicas de rastreamento e identificação são combinadas para garantir que exista entropia suficiente."(pp. 5-6).

2.2.2 Tipos e métodos de rastreamento

Os avanços em *cookies*, *Flash* cookies, e *Web beacons*, juntamente com novas iniciativas de rastreio de empresas, resultaram em bases de dados cada vez mais extensas de perfis de consumidores (Angwin e McGinty 2010).

Os métodos e tipos de rastreamento são inúmeros, sendo o mais conhecido pelos utilizadores, o uso de *cookies*. Para além de ser o método mais conhecido é também o método mais utilizado.

Os *cookies* foram inventados no ano de 1994 e tinham como objetivo permitir que um estado fosse mantido entre os servidores e os utilizadores. O *cookie* é um bloco de texto, mais ou menos complexo, que é colocado no navegador de Internet quando se acede a um determinado servidor – é devolvida no cabeçalho ao servidor sempre que exista uma solicitação do utilizador ao mesmo (Cahn et al., 2016).

Para que haja uma melhor compreensão de definição de *cookies* e dos seus objetivos será necessário que se compreenda de como a *World Wide Web* (WWW ou "Web") funciona (Kristol, 2001).

No artigo "*HTTP Cookies: Standards, Privacy, and Politics*", Kristol (2001), descreve o funcionamento dos *cookies* da seguinte forma:

> "*Web-based applications often use cookies to maintain state in the otherwise stateless HTTP protocol. As part of its response, a server may send arbitrary information, the "cookie," in a Set-Cookie response header. This arbitrary information could be anything: a user identifier, a database key, whatever the server needs so it can continue where it left off. Under normal circumstances (and simplifying greatly), a cooperating client returns the cookie information verbatim in a Cookie header, one of its request headers, each time it makes a new request to the same server. The server may choose to include a new cookie with its responses, which would supersede the old one. Thus there is an implied "contract" between a server and client: the server relies on the client to save the server's state and to return it on the next visit*."((p. 153).

Uma definição mais simples de como este método funciona é dada por Avelino e Amadeu: cada vez que um utilizador acede a um *site*, o *browser* envia de volta o *cookie* de *web* correspondente da página com o propósito de controlar a experiência que cada utilizador tem no *site*. O principal intento é identificar o utilizador e preparar páginas

personalizadas ou guardar informações do *site* para futuras utilizações (Avelino & Amadeu, 2016).

Existem dois tipos de *cookies*, os *cookies* de sessão, que são criados e guardados durante a duração da sessão em determinado *site* e após o término da sessão são apagados do dispositivo do utilizador, e os *cookies* persistentes que ficam guardados no dispositivo um tempo específico, tempo esse que se encontra definido no servidor (Avelino, 2019).

Dando exemplos concretos, os cookies de sessão são normalmente utilizados nas aplicações de *ecommerce* e permitem que os artigos, escolhidos pelo utilizador numa sessão anterior, sejam mantidos no carro de compras até nova visita. Os *cookies* persistentes, permitem que os dados sejam armazenados por um período de tempo, que pode ir de apenas uns minutos como a vários anos, consentindo que estes sejam acedidos e tratados durante esse período de tempo. São normalmente aplicados por empresas *Data Brokes* [2](Corretores da Dados), tais como *Axiom, Datalogix* e *Epsilon,* anunciantes online e aplicações de rastreamento como o *Google Analytics* (Cahn et al., 2016).

Uma outra tecnologia utilizada para rastreamento são os *flash cookies*, que são mais resistentes que os outros cookies. São mais difíceis de detetar, de limpar ou apagar pelos utilizadores. Estes tipos de cookies não podem ser eliminados com os comandos existentes nos *browsers*, limpar histórico e eliminar *cookies*.

Os *flash cookies*, são dados armazenados e normalmente são utilizados pelo Adobe Flash Player para armazenar configurações relacionadas a este programa. Os *flash cookies* guardam, por exemplo, informações sobre vídeos em *flash* que um utilizador assistiu em determinado site.

É necessário saber como funcionam os *flash cookies*, como estas são guardados e como o sistema à volta delas atua para entender o seu funcionamento.

Os dados do *fash* são guardados em pasta diferentes, consoante o sistema operativo que nos encontramos a utilizar. Por exemplo num computador com sistema operativo Mac, os objetos partilhados do Flash (rotulados .sol) são armazenados em*: / users / [nome do utilizador] / Library / Preferences / Macromedia / Flash Player /*. Num computador

[2] Empresas que coletam informações pessoais de consumidores e as revendem ou compartilham

com sistema operativo Windows, são guardados em*: \ Documents and Settings \ [nome do utilizador] \ Application Data \ Macromedia \ Flash Player* (Soltani et al., 2009).

Por defeito os *flash cookies* podem ser guardados ou recuperados sempre que um utilizador acede a uma página que contenha uma aplicação *flash*. E estes encontram-se definidos para não pedir consentimento ao utilizador para guardar os seus dados. A maioria dos utilizadores nem sequer têm conhecimento deste tipo de cookies e nem sabe como as apagar (Sipior et al., 2011). Assim, é possível que um utilizador conviva durante anos com um cookie de rastreamento sem que se aperceba.

Para além dos últimos dois exemplos de rastreamento também é possível encontrar os *beacons*, também conhecidos como *Web beacons*, *Web bugs*, *pixel tags*, ou *clear gifs*.

São *tags* de imagem, *GIF - graphics interchange format* aplicados em documentos *HTML – hypertext markup language,* e colocados em páginas *Web* ou numa mensagem de email com o objetivo de monitorizar o comportamento do utilizador (Sipior et al., 2011).

2.3 Algoritmos

O crescimento exponencial dos dados disponíveis tornou impraticável o tratamento dos mesmos em tempo útil. A necessidade de encontrar/selecionar informação útil, fez com que fosse urgente encontrar formas mais práticas e rápidas de contornar este problema. Uma das soluções foi a utilização de algoritmos.

Embora exista um número incontável de definições para algoritmos, podemos descrevê-los como uma série finita de regras ou processos descritos com precisão para resolver um problema. *"It is a sequence of stages that transforms input through specified computational procedures (throughput) into output"* (Cormen et al., 2001)**.**

Os algoritmos e a automatização tornaram-se omnipresentes, se não mesmo um componente da vida contemporânea.

Rodrigo Zamith enfatiza a questão da tendência para a personalização algorítmica que se encontra a criar fluxos coagidos. Acrescenta, que esta tendência pode resultar numa mudança acentuada do enfoque tradicional do jornalismo (Zamith, 2019).

As personalizações algorítmicas têm vários objetivos, sendo a base tecnológica e parte integrante das caraterísticas funcionais de vários serviços de Internet populares e bem-

sucedidos mundialmente, como por exemplo o Google, a Meta, a Amazon, a Netflix ou o Spotify (Latzer et al., 2014).

Estes vieram moldar a vida quotidiana e as realidades de todos. Conseguem mudar a perceção do mundo e afetam o comportamento humano, influenciando todas as escolhas.

Este fenómeno em rápido crescimento dá pelo nome de algoritmo de seleção (Latzer et al., 2014). No entanto podemos encontrar na literatura diversos tipos de algoritmos com os mais variadíssimos objetivos.

Em meados de 1990 surgiram os algoritmos colaborativos para sistemas de recomendação. Os algoritmos colaborativos são utilizados por uma quantidade considerável de empresas com o intuito de gerar recomendações aos utilizadores. Com as recomendações sugeridas os utilizadores têm ao seu alcance uma coletânea de produtos, um subconjunto de menor dimensão de produtos que se adequa mais ao seu perfil, e assim, não perder tempo a visualizar um conjunto mais abrangente de produtos.

Estes sistemas consistem em metodologias que permitem gerar recomendações de diferentes produtos através da informação agregada da interação entre o utilizador e o sistema. A Amazon e Netflix são duas empresas que aplicam este tipo de sistema de recomendação personalizada com sucesso.

Os *collaborative filtering systems* (CFS) utilizam dados de atividades passadas do utilizador, como por exemplo o histórico de transações ou satisfação do utilizador expressa em classificações. O CFS é bastante utlizado e sugerido como a mais viável (Takács et al., 2009).

Os algoritmos de CFS conseguem identificar as relações entre os utilizadores e os itens consultados e fazem associações utilizando esta informação para prever as preferências dos utilizadores (Takács et al., 2009).

Outro tipo de algoritmo utilizado pelas plataformas é o já mencionado algoritmo de seleção. Para além de sugerirem amigos, notícias, canções, estes conseguem também produzir artigos de notícias e mensagens de forma automática.

Ao recolher este tipo de informação são construídas novas realidades que guiam as ações dos utilizadores para o acesso de produtos ou serviços importantes para as empresas (Latzer et al., 2014).

Gizmodo[3] publicou vários artigos que continham entrevistas a empregados do Facebook, onde eram revelados uma série de segredos. Num primeiro artigo, funcionários da plataforma davam conta da existência de equipas no Facebook, responsáveis por gerir e verificar os tópicos e os resumos das notícias, que encaminhavam os utilizadores para as notícias mais fiáveis e para outras notícias que poderiam sair mais tarde, sobre o mesmo assunto (Duguay, 2018).

O segundo artigo acabou por gerar controvérsia porque nas entrevistas realizadas aos empregados da Meta estes indicaram que seguiram diretivas para suprimir as notícias conservadoras (Duguay, 2018).

Na sequência das notícias avançadas pelo *Gizmodo*, a Meta acabou por desmantelar a equipa responsável pelos tópicos de tendência. Passou então a ser apresentado o título da notícia e o número de pessoas que se encontram a falar sobre ele, algo mais fabricado por algoritmos.

Uma preocupação crescente que se tem sentido em torno desta temática, é a dependência que os meios de comunicação social têm das plataformas e dos seus algoritmos para a divulgação das notícias (Meese & Hurcombe, 2020).

Meese & Hurcombe referem ainda, que existem estudiosos que argumentam que a lógica dos algoritmos tem como propósito uma adotação das prioridades e valores das plataformas (Meese & Hurcombe, 2020).

2.4 Trabalhos e Estudos anteriores

Na tabela seguinte é apresentada uma lista de trabalhos de investigação que têm como objeto de estudo temas relacionados com a privacidade, a segurança, os tipos de rastreamento e o rastreamento propriamente dito.

Tabela 1- Estudos e trabalhos de investigação anetriores relacionados com privacidade e segurança

Autore(s)	Titulo	Objectivo do estudo
Sipior et al. (2011)	*Cookies, and Web Beacons*	O artigo tinha como objetivo examinar as questões de privacidade dos utilizadores associadas aos *Cookies* e *Web Beacons*.

[3] Gizmodo - blog publicado originalmente nos Estados Unidos e propriedade de Gawker Media - https://gizmodo.com/ (*Gizmodo | We Come from the Future*, n.d.)

Kshetri (2014)	*Big data's impact on privacy, security and consumer welfare*	Investigação sobre como as várias características inerentes aos *Big data* estão relacionadas com a privacidade, segurança e bem-estar do consumidor. A relação entre as características do *Big data* e as questões de privacidade, segurança e bem-estar dos consumidores é examinada do ponto de vista da recolha, armazenamento, partilha e acessibilidade dos dados.
Lerner et al (2016)	*Internet jones and the raiders of the lost trackers: an archaeological study of web tracking from 1996 to 2016*	Apresentação de medições de comportamentos de rastreamento na *web*, por terceiros, entre os anos 1996 e 2016. Descoberta que a localização de terceiros na *web* aumentou em prevalência e complexidade desde o primeiro rastreador de terceiros observado em 1996.
Avelino & Amadeu, (2016)	A dependência do rastreamento comportamental online para a economia globalizada	Investigação da tecnologia de rastreamento baseada em web cookies inseridos na navegação dos dez sites de notícias mais acedido por utilizadores de Internet brasileiros em abril de 2015 e maio de 2016.
Bujlow et al.(2017)	*A Survey on Web Tracking: Mechanisms, Implications, and Defenses*	Análise da literatura existente sobre os métodos utilizados pelos serviços *web* para localizar os utilizadores online, bem como os seus objetivos, implicações e possíveis defesas dos utilizadores.
Nelson Rodrigues (2018)	Está por aí alguém? Perceções da exposição e da privacidade nas redes sociais, entre estudantes universitários	Compreender como é que os estudantes universitários percecionam o modo como se expõem *online* e a importância que isso tem na sua privacidade e na segurança da informação partilhada nas redes sociais.
Thurman et al. (2019)	*My Friends, Editors, Algorithms, and I*	Estudo que explora o que o público pensa sobre os mecanismos de seleção de notícias e porquê. É referido até que ponto o público acredita que a seleção de histórias por editores e a seleção de histórias por algoritmos uma boa opção de obter notícias online.
Avelino (2019)	A evolução dos mecanismos de rastreamento e vigilância intrusivos em clientes web.	Um breve levantamento histórico sobre o surgimento e a evolução dos mecanismos de rastreamento e de vigilância intrusivos em navegadores, propõe-se ainda a analisar as características dos principais mecanismos de rastreamento de comportamento online intrusivos.

Capítulo 3 – Investigação

3.1 Abordagem metodológica

Na revisão da literatura verificou-se existirem várias técnicas de rastreamento e muitas delas conseguem ser praticamente impercetíveis aos utilizadores. A presença constante dos dispositivos ligados à Internet favorece as práticas de rastreamento dos utilizadores por parte das grandes empresas tecnológicas. Propusemo-nos a realizar um estudo inferencial, onde foi construído um questionário com base no levantamento teórico-conceptual. Num primeiro momento disponibilizámos o questionário com um grupo restrito de pessoas de ambos os sexos e das faixas etárias existentes para validação do mesmo, posteriormente, foi disponibilizado em plataformas digitais, como o Facebook, o Linkedin, o Gmail e o WhatsApp.

Os dados recolhidos no questionário foram alvo de validação e normalização. Foram identificadas algumas repostas não válidas que foram removidas da amostra (p.e. respostas dadas por pessoas com menos de 18 anos). Das 162 respostas iniciais, foram validadas 148 (N = 148). Por fim, os dados obtidos foram alvo de tratamento estatístico descritivo, fatorial e correlacional.

3.2 Questão de investigação e objetivos

Recordamos a questão de investigação: **Quais as perceções dos utilizadores quanto ao rastreamento a que estão sujeitos nas plataformas digitais?**. Para conseguir dar resposta a esta questão, foram traçados os seguintes objetivos:

- Determinar as perceções dos utilizadores sobre o rastreamento online;
- Verificar o que entendem por privacidade online e que importância lhe dão;
- Verificar a importância deste tipo de rastreamento no seu quotidiano;
- Determinar a confiança que têm quanto ao uso das plataformas digitais;
- Verificar as vantagens (ou benefícios práticos) e desvantagens (ou ameaças) que atribuem ao rastreamento online;
- Verificar eventuais ações de prevenção face ao rastreamento online;
- Verificar como se podem relacionar as suas perceções de privacidade, segurança e rastreamento online;
- Analisar as dimensões encontradas em função do género, grupo etário e nível de literacia digital.

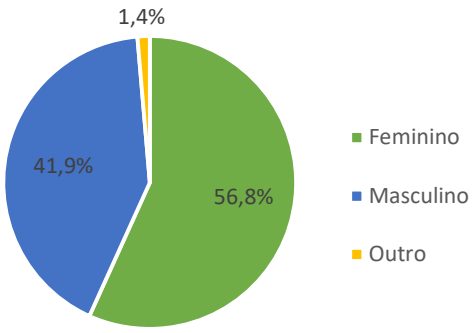
3.3 Estudo inferencial

3.3.1 Amostra

A amostra resulta da recolha de dados por intermédio de um questionário em formato digital, distribuído a vários participantes, recorrendo a plataformas digitais para sua distribuição. A amostra foi aleatória e obedeceu aos seguintes critérios: a) participação voluntária e anónima; b) idades compreendidas entre os 18 e 70 anos.

Das respostas obtidas (N = 148), de participantes de ambos os sexos e idades compreendidas entre os 18 e 68 anos, relativamente ao género, 56,8% eram do sexo feminino (N[4] = 84), 41,9% do sexo masculino (N = 62) e 1,4% outro (N = 2), conforme se encontra representado na figura 1.

Figura 1- Gráfico relativo ao género

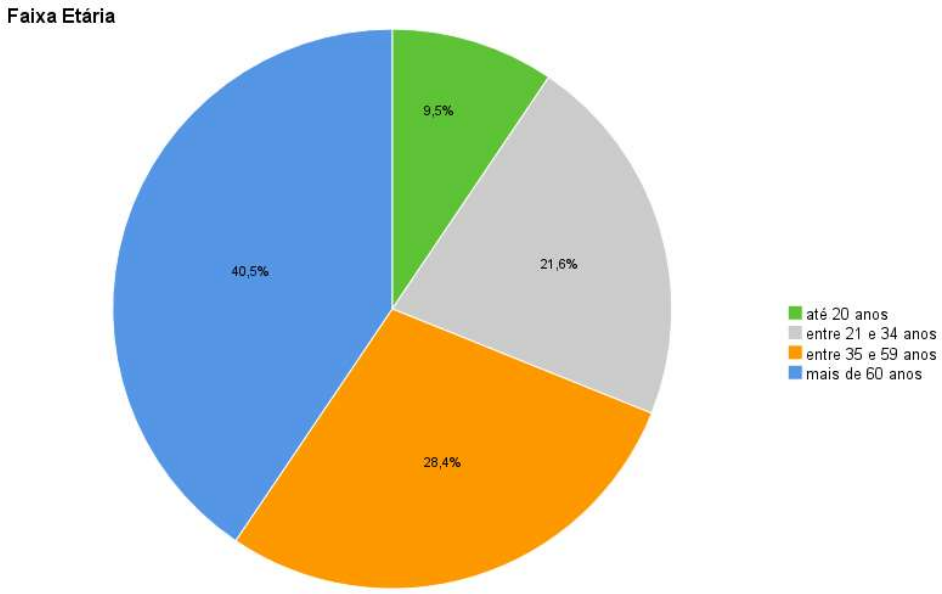


A idade foi recodificada em quatro grupos. O primeiro grupo até aos 20 anos, que agrupa os utilizadores dos 18 aos 20 anos e identifica os inquiridos jovens (N = 14) 9,5%, entre os 21 e os 34 anos, jovens adultos (N = 32) 21,6%, dos 35 aos 59 anos a representar a população adulta (N = 42) 28,4 % e mais de 60 anos a representa a população sénior (N = 60) a representar 40,5% dos inquiridos.

De acordo com a figura 2, verificamos que a maior percentagem de respostas foi dada por pessoas que se encontram entre a população sénior, ou seja, na faixa etária com mais de 60 anos.

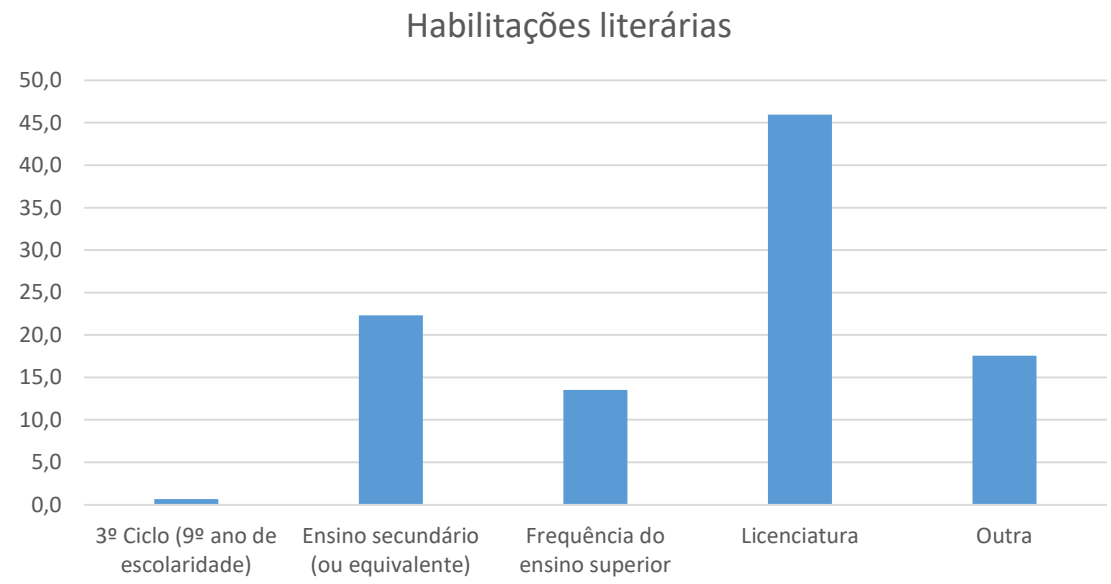
[4] N = Frequência

Figura 2- Gráfico faixa etária



Relativamente às habilitações literárias, e como se pode comprovar pelo gráfico representado na figura 3, verificou-se que apenas 0,7 % (N = 1) detinha o 3º Ciclo (9º ano de escolaridade). Relativamente ao ensino secundário (ou equivalente) encontrámos 22,3% (N = 33). Quanto à frequência no ensino superior encontramos 13,5 % (N = 20), sendo a licenciatura o nível com maior percentagem, 45,9% (N = 68).

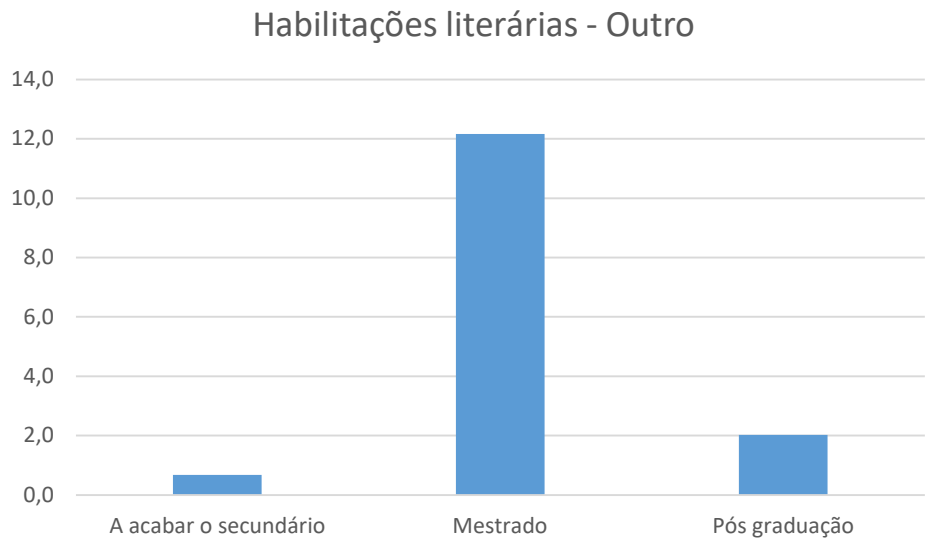
Figura 3- Gráfico relativo às habilitações literárias



Em termos da categoria "Outra" encontrámos uma percentagem de 17,6% (N = 26), que por ter uma representação ainda significativa faz todo o sentido verificar o seu universo.

Temos ainda um inquirido a acabar o secundário, o que dá uma percentagem de 0,7% (N = 1). Já com o mestrado encontrámos um universo de 12,2% (N = 18) e pós-graduação 2,0% (N = 3) (Figura 4).

Figura 4- Gráfico relativo à categoria Outro das habilitações literárias



3.3.2 Questionário

Partindo da questão e dos objetivos da investigação e da revisão da literatura, foi elaborado um questionário (cf. Apêndice A). Apesar da possibilidade de uma baixa obtenção de respostas e/ou respostas não válidas.[5]

De modo a validar o questionário o mesmo foi partilhado com um grupo restrito de pessoas de ambos os sexos e nas diferentes faixas etárias.

Na página de apresentação do questionário encontrava-se descrito o objetivo do estudo, questões de ética, tais como a participação no mesmo ser voluntária e a confidencialidade dos dados. Ainda indicava a quem este se encontrava direcionado:

[5] A escolha desta técnica também se deveu a um fator essencial: a possibilidade de obtenção rápida de respostas, fator importante, devido à janela temporal deste trabalho.

pessoas adultas, maiores de 18 anos. Os participantes tinham sempre a possibilidade de desistirem do preenchimento do mesmo se assim o desejassem.

O questionário encontra-se dividido em duas partes. A primeira parte refere-se à caracterização sociodemográfica da população inquirida onde se tenta traçar o perfil do participante recolhendo dados como a da idade, género, e habilitações literárias. Na segunda parte existem perguntas associadas a escalas do tipo *Likert,* entre 1 e 5, onde o valor inferior pode corresponder, por exemplo, a 1 (Nada importante) e o valor superior a 5 (Muito importante).

A primeira pergunta, tem como objetivo perceber o nível de entendimento de rastreamento online de cada utilizador. Para que o participante pudesse continuar com o questionário, mesmo não sabendo à partida do que se tratava rastreamento online, foi disponibilizada a definição após a resposta à primeira pergunta.

Com a questão dois e três pretende-se verificar até que ponto os utilizadores têm noção da utilização do rastreamento por parte das plataformas. Na questão dois, o utilizador tem à sua disposição uma lista de plataformas e deverá responder para cada uma delas qual o nível de conhecimento que tem sobre as técnicas de rastreamento utilizadas pelas mesmas. A questão três pretende verificar, de acordo com uma listagem de diferentes finalidades disponibilizada por nós, para que são utilizadas as técnicas de rastreamento.

Na pergunta quatro é pedido que os utilizadores digam, para cada uma das plataformas indicadas, qual o seu nível de confiança nas mesmas.

Nas questões 6, 7, 8 e 9, os utilizadores são confrontados com uma listagem de várias afirmações. Para cada uma delas devem responder, de acordo com a escala de *Likert* disponível, o que mais se encontra de acordo com as suas opiniões.

A questão 6 pretende recolher dados sobre possíveis ações de prevenção que os utilizadores têm quando utilizam as plataformas. Têm ao seu dispor uma escala de resposta onde podem escolher responder entre “1 – nunca”, até “5 - muito frequentemente”.

As questões 7 e 8 são utilizadas para conseguirmos ter noção de qual a é importância dada pelos utilizadores para questões como a privacidade e a segurança. Aqui encontra-se disponível uma escala entre 1 e 5, onde 1 corresponde a nada importante e 5 a muito importante.

A questão 9 tem como finalidade verificar a preocupação dos utilizadores, relativamente aos dados recolhidos pelas plataformas no rastreamento que é feito. Para isso é disponibilizada uma listagem de afirmações onde têm que responder de acordo com a escala disponibilizada, na qual podem escolher entre 1 nada preocupante e 5 muito preocupante.

As perguntas 11 e 12 são questões de resposta livre e pedem que os utilizadores digam quais as vantagens (ou benefícios práticos) e quais são para si, as desvantagens (ou ameaças) de utilizar plataformas digitas, sabendo que estas têm técnicas de rastreamento online.

A questão 5, pretendia verificar com que fins eram utilizadas as plataformas listadas ao longo do questionário.

O questionário foi produzido na plataforma Qualtrics e distribuído apor diversas plataformas digitais, tais como o Facebook, Linkedin e WhatsApp.

3.4 Técnicas de Análise de Dados

Uma vez recolhidos os dados, foi realizado o devido tratamento, recorrendo à ferramenta IBM SPSS Statistics v.27. Numa primeira fase, recorremos à estatística descritiva para a caracterização da amostra e de todas as questões do questionário. De seguida, realizaram-se 2 análises de componentes principais, para ser possível alcançar as dimensões relacionadas com previsão comportamental, influência de comportamentos, privacidade, prudência, segurança, prevenção e preocupação.

3.5 Resultados

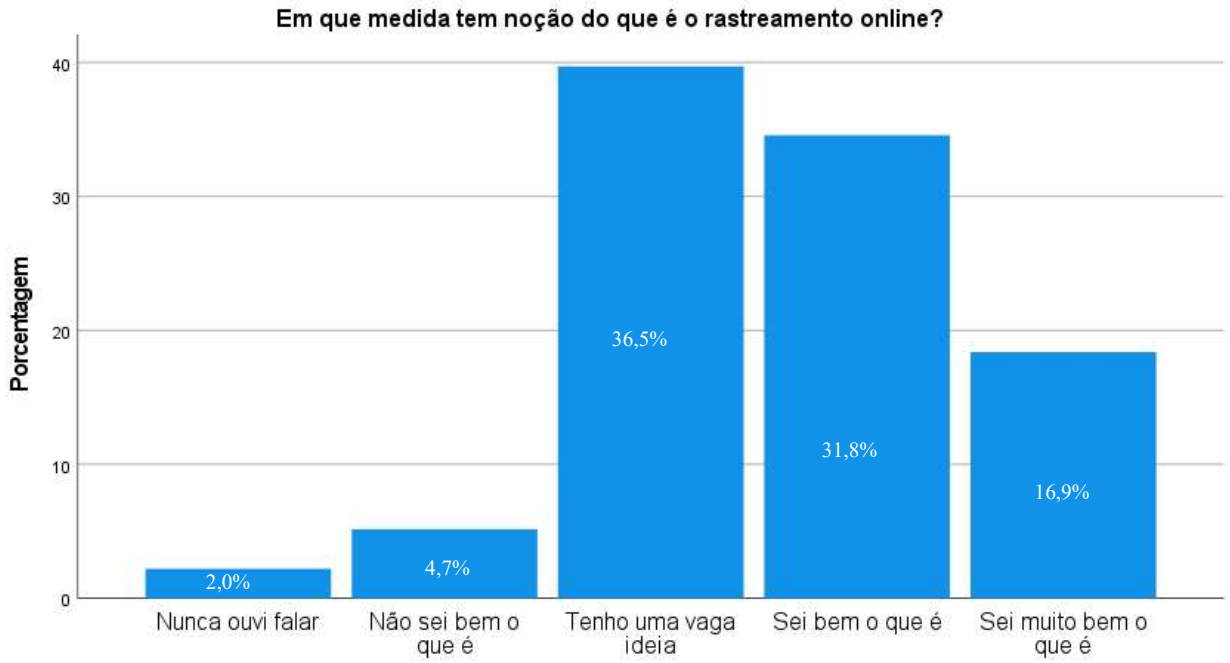
Em seguida são apresentados os resultados, para cada um dos objetivos propostos.

3.5.1 Determinar as perceções dos utilizadores sobre o rastreamento online;

De modo a determinar as perceções dos utilizadores sobre o rastreamento online, o questionário tinha ao dispor dos inquiridos duas questões.

A questão do questionário (cf. Apêndice A) era solicitado aos utilizadores que respondessem a noção que tinham sobre rastreamento online.

Figura 5- Gráfico - Noção dos utilizadores sobre Rastreamento Online



De acordo com a figura 5, grande parte dos inquiridos tem uma vaga ideia do que é o rastreamento online, com uma percentagem de 36,5%. O grupo de inquiridos que sabe o

que é, tem uma percentagem de 31,8% e apenas 16,9% dos inquiridos sabe bem o que é. De realçar que as percentagens dos inquiridos que nunca ouviram falar e dos inquiridos que não sabem muito bem o que é são apenas de 2,0% e 4,7% respetivamente.

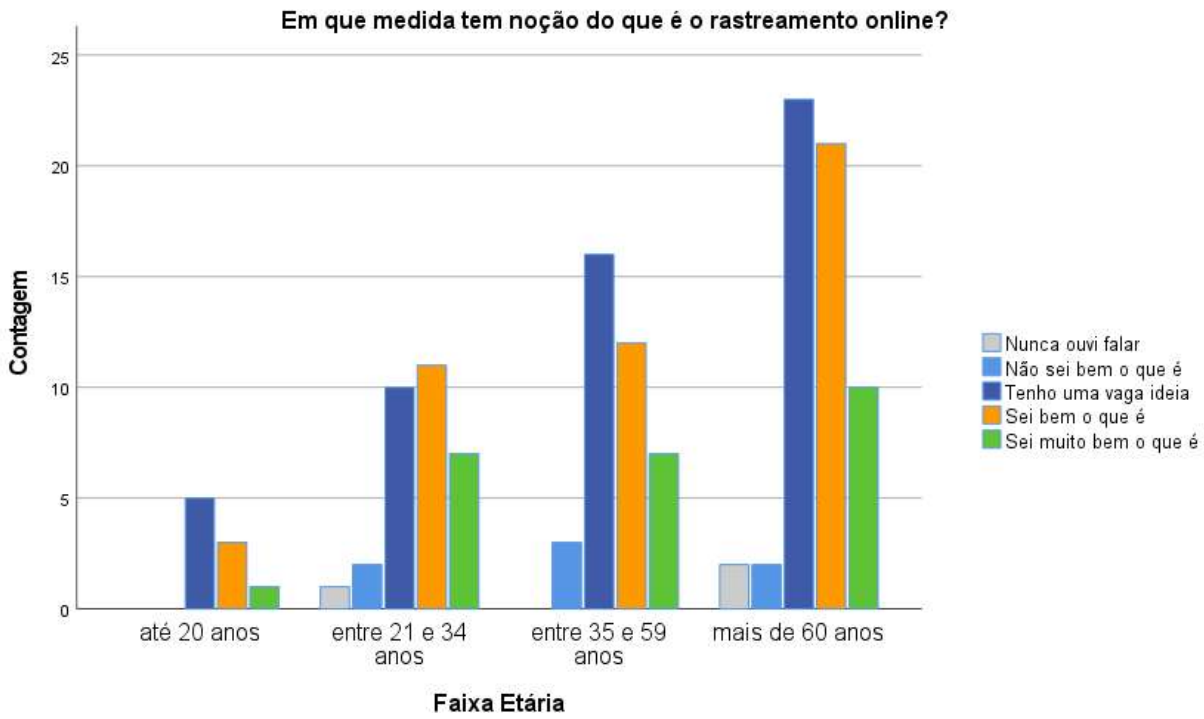
Na tabela dois é possível verificar a frequência das respostas dos utilizadores para cada opção.

Tabela 2- Tabela de frequências da noção dos utilizadores sobre Rastreamento Online

Em que medida tem noção do que é o rastreamento online?					
		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Nunca ouvi falar	3	2,0	2,2	2,2
	Não sei bem o que é	7	4,7	5,1	7,4
	Tenho uma vaga ideia	54	36,5	39,7	47,1
	Sei bem o que é	47	31,8	34,6	81,6
	Sei muito bem o que é	25	16,9	18,4	100,0
	Total	136	91,9	100,0	
Omisso	Sistema	12	8,1		
Total		148	100,0		

Na figura 6 podemos verificar que é na faixa etária entre os 21 e os 34 anos que os utilizadores sabem bem o que é o rastreamento online. Verifica-se também que a maior percentagem de resposta “Tenho uma vaga ideia” se encontra entre a faixa etária sénior, ou seja, mais de 60 anos.

Figura 6 - Noção dos utilizadores sobre Rastreamento Online por faixa etária



A segunda questão apresenta uma lista de plataformas onde, para cada uma delas, os utilizadores tinham a possibilidade de responder perante a seguinte escala: 1 (Não tenho conhecimento) a 5 (Rastreamento Exagerado) se o rastreamento online é utilizado.

Da análise realizada sobre os dados recolhidos na pergunta 2, verificamos que se destacam três plataformas que os utilizadores asseguraram que utilizam mais técnicas de rastreamento online, o Facebook (M[6] = 4,47), o Google (M = 4,46) e o Instagram (M = 4,23) (Figura 7). As plataformas Amazon (M = 3,63), WhatsApp (M = 3,47), Netflix (M = 3,10), Firefox (M = 2,96), Zoom (M = 2,67), HBO (M = 2,64), Teams (M = 2,39) apresentam valores mais baixos, mas os utilizadores consideram que todas elas utilizam técnicas de rastreamento (Tabela 3).

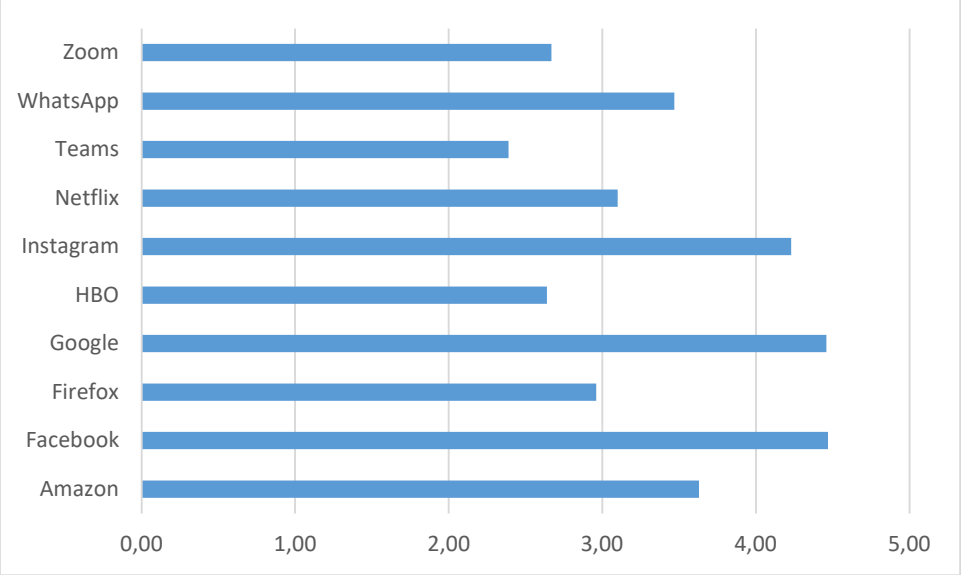
Tabela 3 - Tabela de frequências de utilização de técnicas de Rastreamento Online

	N		Média	Desvio Padrão
	Válido	Omisso		
Facebook	135	13	4,47	1,006
Google	135	13	4,46	1,020
Instagram	134	14	4,23	1,268
Amazon	136	12	3,63	1,460
WhatsApp	135	13	3,47	1,397
Netflix	134	14	3,10	1,440

[6] M = Média

Firefox	134	14	2,96	1,524
Zoom	135	13	2,67	1,607
HBO	134	14	2,64	1,499
Teams	134	14	2,39	1,450

Figura 7 - Utilização de Técnicas de Rastreamento por plataforma



3.5.2 Verificar o que entendem por privacidade online e que importância lhe dão;

Para o segundo objetivo, verificar o que entendem por privacidade online e que importância lhe dão, os dados utilizados foram os recolhidos na questão número 7 do questionário (cf. Apêndice A). Nessa questão, os utilizadores classificam em função da sua importância, com uma escala de 1 (nada importante) a 5 (muito importante), um leque de afirmações relativas à privacidade das plataformas. Com exceção da questão relacionada com a afirmação "Ser apresentado nas diversas plataformas digitais publicidade direcionada (publicidade relevante apenas para si)" (M = 3,51) a maioria dos utilizadores acham muito importante as restantes afirmações, destacando-se afirmações como: a possibilidade de gerir a que informação e/ou dados as organizações podem aceder (M = 4,72), a possibilidade de remover a permissão de acesso à localização das plataformas digitais (M = 4,71), as plataformas digitais informarem quais dados são recolhidos (M =4,7) e as plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. câmara do telemóvel, localização) (M = 4,69)(Tabela 4).

Tabela 4 - Tabela de frequências relativas à privacidade

	N	Média	

	Válido	Omisso		Desvio Padrão
A possibilidade de gerir a que informação e/ou dados as organizações podem aceder	112	36	4,72	,674
A possibilidade de remover a permissão de acesso à localização das plataformas digitais	115	33	4,71	,659
As plataformas digitais informarem quais dados são recolhidos	115	33	4,70	,678
As plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. camara do telemóvel, localização)	115	33	4,69	,776
Ter a possibilidade de verificar que informação/dados são vendidos ou cedidos a outras organizações.	114	34	4,68	,756
Não ser possível a verificação e divulgação da localização do utilizador através do envio de mensagens, fotos e ou vídeos tiradas/feitos no dispositivo do utilizador	114	34	4,61	,827
As plataformas digitais informarem de que forma irão ser tratados os dados recolhidos	116	32	4,59	,855
A implementação do RGPD a nível europeu (Regulamento Geral sobre a Proteção de Dados)	115	33	4,57	,928
As plataformas digitais apresentarem políticas de privacidade claras e simples	115	33	4,46	,949
Ser apresentado nas diversas plataformas digitais publicidade direcionada (publicidade relevante apenas para si)	115	33	3,51	1,347

3.5.3 Verificar a importância deste tipo de rastreamento no seu quotidiano;

Para verificar a importância deste tipo de rastreamento no seu quotidiano, foram utilizados os dados recolhidos na questão 9 (cf. Apêndice A), onde os utilizadores eram

convidados demonstrar a sua opinião através de várias afirmações relacionadas com a utilização dos seus dados.

Apurando os dados recolhidos, verificou-se que os utilizadores demonstram uma grande preocupação na utilização dos seus dados. Houve um maior destaque para a venda de dados a terceiros (M = 4,72), para a partilha de notícias falsas (M = 4,68) e para influenciar a tendência de voto (M = 4,64). Ao que os inquiridos dão menor importância é à utilização dos seus dados para o desenvolvimento de novos produtos (M = 3.09).

Com o objetivo de averiguar a importância que os utilizadores dão ao rastreamento, fez-se a análise fatorial dos componentes principais (ACP), dos itens na questão 9, que nos permitiu identificar as suas dimensões centrais (Tabela 5).

O primeiro fator (50,40% de variância explicada com alfa de *Cronbach* α= ,717) agrupa itens referentes previsão de comportamentos dos utilizadores.

O segundo fator (21,88% de variância explicada com alfa de *Cronbach* α= ,860) agrupa itens referentes a influenciar de comportamentos de utilizadores.

Tabela 5 - ACP –Importância do rastreamento

Matriz de componente rotativa		
	Componente	
	Prever comportamentos	Influenciar comportamentos
Partilha de publicidade direcionada	,843	,119
Desenvolvimento de novos produtos	,834	-,184
Previsão do comportamento dos utilizadores	,607	,521
Venda de dados a terceiros	,069	,926
Influenciar a tendência de voto	,049	,909
Partilha de notícias falsas (fake news) sobre temas de interesse	,041	,907
Influenciar os utilizadores nas suas compras	,517	,571
Partilha de propaganda sobre assuntos de interesse do utilizador	,531	,546
Valores próprios	4,03	1,75
Variância Explicada (%)	50,40	21,88
Alpha de Cronbach	,717	,860

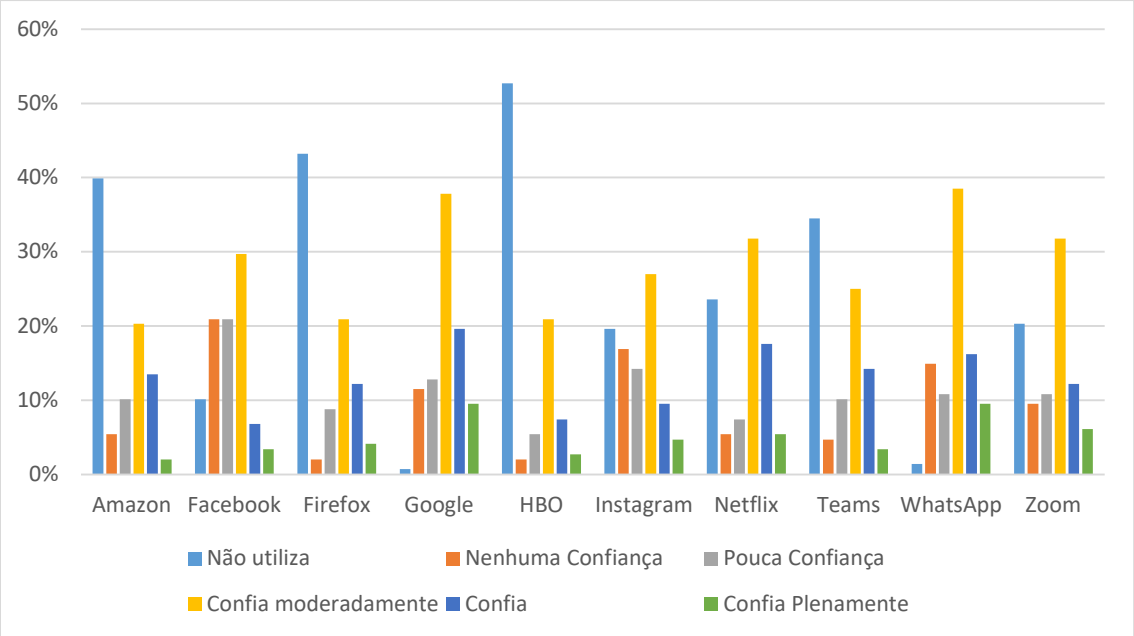
Nota: Resultado da ACP: matriz após rotação Varimax, com normalização Kaiser, convergente em 3 iterações. Medida KMO= ,838; Teste de Bartlett = 505,604; Significância = ,000

3.5.4 Determinar a confiança que têm quanto ao uso das plataformas digitais;

Para determinar a confiança dos utilizadores nas plataformas digitais, foi apresentada uma lista de plataformas e para cada uma delas os utilizadores tinham à sua disposição a escala de 1 (não confio) a 5 (confia plenamente). Na pergunta 4 foi ainda dada a hipótese de os utilizadores responderem que não utilizavam a plataforma listada.

De acordo com a figura 8 verifica-se que a plataforma em que os utilizadores menos confiam é o Facebook, com uma percentagem de 20,90%. No geral, os utilizadores confiam moderadamente em todas as plataformas sendo o WhatsApp (38,50%) e o Google (37,80%) as que recebem maior percentagem de respostas.

Figura 8- Nível de confiança nas plataformas



3.5.5 Verificar as vantagens (ou benefícios práticos) e desvantagens (ou ameaças) que atribuem ao rastreamento online;

O quinto objetivo visa verificar as vantagens e/ou desvantagens do rastreamento online. Desta forma, foram disponibilizadas duas questões de resposta aberta.

Para a questão 10: "Quais são, para si, as vantagens (ou benefícios práticos) de utilizar plataformas digitas, sabendo que estas têm técnicas de rastreamento online?", a generalidade das respostas aponta que a obtenção de conhecimento e de informação é feita de uma forma mais fácil e prática. As palavras informação, conhecimento e

facilidade foram as mais usadas. No entanto, a expressão "não há vantagem" é também ela bastante mencionada, particularmente nas faixas etárias mais elevadas, onde podemos encontrar respostas como "Não vejo vantagens, pois ainda sou do tempo da Internet sem este "rastreamento".

As respostas à questão 11: "Quais são para si, as desvantagens (ou ameaças) de utilizar plataformas digitas, sabendo que estas têm técnicas de rastreamento online?", evidenciaram uma grande preocupação relativamente à perda de privacidade e o constante sentimento de controlo, por parte das plataformas. A divulgação dos dados pessoais a terceiros é também uma forte preocupação dos utilizadores. Outras duas desvantagens aprontadas pelos inquiridos são a manipulação do conteúdo a ser apresentado, tendo em conta as preferências de cada, e a influência que essa manipulação poderá ter nos mesmos.

3.5.6 Verificar eventuais ações de prevenção face ao rastreamento online;

Para o sexto objetivo da presente investigação, verificar eventuais ações de prevenção face ao rastreamento online, foram utilizados os dados recolhidos na questão 6 do questionário (cf. Apêndice A), onde indicaram a frequência com que costumam ter uma série de ações respeitantes a métodos de prevenção.

De acordo com as respostas dadas, podemos verificar que os utilizadores ainda têm poucas ações de prevenção. Ainda assim, os utilizadores raramente aceitam as políticas de privacidade sem as ler (M = 3,97). A verificação e seleção de cookies a ser utilizadas é uma das ações mais praticadas (M = 3,14) seguida pela verificação a que dados as aplicações pretendem aceder (M = 2,93). De todas as afirmações disponibilizadas, deram menos importância ao facto de as plataformas terem sistemas automáticos para apagar ficheiros de retenção de dados (M = 1,91) (Tabela 6).

Tabela 6- Tabela de frequências de prevenção

	N		Média	Desvio Padrão
	Válido	Omisso		
Aceitar as políticas de privacidade sem as ler	116	32	3,97	1,099
Verificar as cookies e selecionar as que permito serem utilizadas	116	32	3,14	1,338
Verificar a que dados as aplicações pretendem aceder	116	32	2,93	1,297

Apagar as cookies (armazenadas após utilização) dos browsers	116	32	2,67	1,277
Usar aplicações que ajudam a proteger, ou previnem, a gravação de cookies	116	32	2,17	1,218
Ter sistemas automáticos para apagar ficheiros de retenção de dados	116	32	1,91	1,176

3.5.7 Verificar como se podem relacionar as suas perceções de privacidade, segurança e rastreamento online;

Para responder ao objetivo 7 do presente trabalho, analisámos numa primeira fase as respostas dadas à questão 8 do questionário (cf. Apêndice A), onde foi solicitado que os participantes indicassem a importância dada a uma lista de afirmações relativas a segurança. De uma forma geral os utilizadores acham muito importante as afirmações apresentadas destacando opções relacionadas com os dados dos próprios, como ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si (M = 4,85) e saber se a sua informação/dados se encontram seguros (M = 4,82%). Podemos também verificar que a afirmação que os utilizadores dão menos importância é a existência de uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si) (M = 4,60%). Verifica-se que todas as médias são bastante elevadas (Tabela 7).

Tabela 7 - Tabela de frequência da importância sobre rastreamento

	N		Média	Desvio Padrão
	Válido	Omisso		
Ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si	116	32	4,85	,462
Saber se a sua informação/dados se encontram seguros	116	32	4,82	,486
Existir a possibilidade de bloquear o acesso à sua localização pelas aplicações e plataformas	116	32	4,81	,474

Existir uma opção de "não rastreamento" do seu tráfego de navegação	116	32	4,75	,558
Ser possível autorizar de forma simples quais as organizações que podem aceder aos seus dados	116	32	4,73	,651
Poder definir para cada uma das organizações, a que dados podem aceder	113	35	4,70	,611
Existir uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si)	116	32	4,60	,733

O último objetivo pretende verificar como se podem relacionar as suas perceções de privacidade, segurança e rastreamento online. Para isso, foram utilizadas as questões número 7, 8 e 9 do questionário (cf. Apêndice A).

A estas questões os utilizadores tinha ao seu dispor, na questão 7 e 8, uma escala de 1 (nada importante) a 5 (muito importante) onde deveriam escolher de acordo com as hipóteses apresentadas sobre a frequência com que costumam ter uma série de ações respeitantes a privacidade e segurança. A questão 9 tinha uma série de afirmações sobre a importância do rastreamento do quotidiano dos utilizadores, onde, utilizando a escala de 1 (nada preocupante) a 5 (muito preocupante) podiam dar a sua opinião.

Para verificar como se relacionam estas três dimensões fez-se uma análise fatorial dos componentes principais – que permitiu identificar as suas dimensões centrais (Tabela 8).

O primeiro fator (33,19% de variância explicada com alfa de Cronbach α= ,935) agrupa itens referentes à privacidade.

O segundo fator (11,81% de variância explicada com alfa de Cronbach α= ,867) agrupa itens referentes à preocupação dos utilizadores.

O terceiro fator (10,17% de variância explicada com alfa de Cronbach α= ,852) agrupa itens referentes à segurança.

O quarto fator (7,48% de variância explicada com alfa de Cronbach α= ,758) agrupa itens referentes à previsão de comportamentos dos utilizadores.

O quinto fator (5,09% de variância explicada com alfa de Cronbach α= ,793) agrupa itens referentes à prevenção por parte dos utilizadores.

O sexto fator (4,31% de variância explicada) apresenta apenas um item referente à preocupação demonstrada pelos utilizadores.

Tabela 8- Matriz de componente rotativa perceções de privacidade, segurança e rastreamento online

Matriz de componente rotativa					
	Componente				
	Privacidade	Prudência	Segurança	Previsão comportamentais	Prevenção
As plataformas digitais informarem de que forma irão ser tratados os dados recolhidos	,823	-,019	,076	,012	,367
A implementação do RGPD a nível europeu (Regulamento Geral sobre a Proteção de Dados)	,807	,156	,045	,111	,147
As plataformas digitais informarem quais dados são recolhidos	,805	,183	,107	,045	,207
As plataformas digitais apresentarem políticas de privacidade claras e simples	,772	,017	-,004	,048	,423
A possibilidade de gerir a que informação e/ou dados as organizações podem aceder	,755	,263	,179	,108	-,002
As plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. camara do telemóvel, localização)	,735	,169	,129	-,122	-,021
Não ser possível a verificação e divulgação da localização do utilizador através do envio de mensagens, fotos e ou vídeos tiradas/feitos no dispositivo do utilizador	,677	,122	,278	,141	-,205
A possibilidade de remover a permissão de acesso à	,675	,256	,311	,162	,011

localização das plataformas digitais					
Ter a possibilidade de verificar que informação/dados são vendidos ou cedidos a outras organizações.	,593	,247	,321	,056	-,084
Partilha de notícias falsas (fake news) sobre temas de interesse	,137	,879	-,035	,001	,002
Venda de dados a terceiros	,210	,869	,148	,025	,071
Influenciar a tendência de voto	,232	,853	,095	-,002	,070
Influenciar os utilizadores nas suas compras	,154	,599	,040	,476	,183
Existir a possibilidade de bloquear o acesso à sua localização pelas aplicações e plataformas	,108	,041	,873	,116	,086
Ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si	,042	,059	,840	,004	,134
Saber se a sua informação/dados se encontram seguros	,143	-,004	,823	,025	,198
Existir uma opção de "não rastreamento" do seu tráfego de navegação	,306	,310	,718	,005	-,020
Existir uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si)	,236	-,120	,532	,237	,118
Desenvolvimento de novos produtos	-,064	-,138	,064	,828	,047
Partilha de publicidade direcionada	,110	,126	,153	,825	-,064
Previsão do comportamento dos utilizadores	,127	,509	,106	,586	,118
Partilha de propaganda sobre assuntos de interesse do utilizador	,122	,521	-,038	,524	-,053
Ser possível autorizar de forma simples quais as	,239	,164	,282	,010	,767

organizações que podem aceder aos seus dados					
Poder definir para cada uma das organizações, a que dados podem aceder	,201	,076	,410	,041	,657
Valores próprios	8,298	2,953	2,542	1,871	1,271
Variância Explicada (%)	33,19	11,81	10,17	7,48	5,09
Alpha de Cronbach	,935	,867	,852	,758	,793

Nota: Resultado da ACP: matriz após rotação Varimax, com normalização Kaiser, convergente em 11 iterações. Medida KMO= ,809; Teste de Bartlett = 1664,080 ; Significância = ,000

Capítulo 4 – Discussão dos Resultados

Esta investigação visa compreender como os utilizadores percecionam o rastreamento feito pelas plataformas digitais, qual o entendimento destes sobre privacidade, que confiança têm nestas, que medidas de prevenção tomam e quais as vantagens e/ou desvantagens que encontram nesta prática. Todos os objetivos delineados foram verificados. Para facilitar a discussão dos resultados, é indicado no início de cada parágrafo o objetivo que se está a abordar e os respetivos resultados obtidos.

- *Determinar as perceções dos utilizadores sobre o rastreamento* online

O rastreamento é considerado uma ameaça séria à privacidade, utilizando técnicas de rastreamento as plataformas online podem recolher e acumular enormes quantidades de informação pessoal das atividades de navegação através de plataformas diferentes. A recolha e análise de dados e de informações pessoais em grande escala é, para muitas empresas com serviços online, a principal atividade (Bujlow et al., 2017).

Os rastreadores de terceiros são considerados como uma séria ameaça à privacidade, uma vez que podem recolher e acumular enormes quantidades de informação pessoal da nossa atividade de navegação através de muitos websites diferentes

Foi possível verificar que grande parte dos utilizadores tem uma vaga ideia do que é o rastreamento online, sobretudo os que se encontram na faixa etária entre os 41 e 50 anos. Na faixa etária entre os 21 e os 30 anos encontramos uma percentagem maior de respostas na opção “sei bem o que é”, concluindo-se que as pessoas entre estas idades estão mais informadas sobre este processo. A percentagem de pessoas que nunca ouviu falar é mínima, o que significa que os utilizadores estão interessados nas questões de privacidade e segurança online. Na questão onde era solicitado que nos indicassem quais as plataformas que utilizavam mais técnicas de rastreamento, foi apontada a rede social Facebook, o Google e o Instagram. Porém, os utilizadores consideram que todas as plataformas utilizam técnicas de rastreamento. Podemos concluir que os utilizadores têm perceções bastante expressivas do que é o rastreamento online.

- *Verificar o que entendem por privacidade* online *e que importância lhe dão*

No inicio da Internet a privacidade era protegida pelo anonimato e era quase impossível identificar a origens e o conteúdo das mensagens (Castells, 2003).

No que respeita à privacidade online os utilizadores destacam como mais importante a possibilidade de gerir a que informação e/ou dados que as organizações podem aceder, a possibilidade de remover a permissão de acesso à localização das plataformas digitais, as plataformas digitais informarem quais dados são recolhidos e as plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (p.e., câmara do telemóvel, localização). Ao que os utilizadores deram menor importância foi ao facto de os dados obtidos pelo rastreamento possibilitarem a apresentação de publicidade direcionada (publicidade relevante apenas para si). Assim, podemos concluir que os utilizadores dão grande importância à sua privacidade e para eles é pertinente saber para quê, como e quando os seus dados são utilizados.

- *Verificar a importância deste tipo de rastreamento no seu quotidiano*

A importância do rastreamento no quotidiano dos utilizadores está relacionada com prever comportamentos e influenciar comportamentos. Ou seja, os utilizadores demonstram preocupação relativamente à recolha de informação e dos seus dados para questões que se relacionam com a previsão dos seus comportamentos e com questões de serem influenciados pelas plataformas que utilizam.

- *Determinar a confiança que têm quanto ao uso das plataformas digitais*

Os utilizadores têm uma confiança moderada nas plataformas digitais. É de destacar que a Google é a plataforma em que os utilizadores mais confiam, seguida pelo WhatsApp. O Facebook é a plataforma em que os utilizadores menos confiam, seguida pelo Instagram. Em suma, os utilizadores não confiam a 100% nas plataformas que utilizam, no entanto algumas das mais utilizadas para estudar, trabalhar e pesquisar, como é o caso da plataforma Google, merece uma confiança moderada, enquanto plataformas de redes socias, como o Facebook e o Instagram, que são utilizadas para entretenimento, são as que merecem menos confiança por parte dos utilizadores.

Giddens (1991), definiu a confiança e segurança em sistemas como:

> "…a condição do distanciamento tempo-espaço e das grandes áreas de segurança na vida quotidiana que as instituições modernas oferecem em comparação com o mundo tradicional (p.102).

- *Verificar as vantagens (ou benefícios práticos) e desvantagens (ou ameaças) que atribuem ao rastreamento* online

Relativamente às vantagens e desvantagens atribuídas ao rastreamento online, os utilizadores identificam a existência de ambas. Como vantagens foram identificadas a obtenção de conhecimento e de informação. A generalidade das pessoas diz que esta obtenção é feita de uma forma mais fácil e prática. Na faixa etária mais elevada encontrou-se várias referências de que não existia nenhuma vantagem.

Como desvantagens foram salientadas a perda de privacidade, o constante sentimento de controlo por parte das plataformas, a divulgação dos dados pessoais a terceiros, a manipulação do conteúdo a ser apresentado, tendo em conta as preferências de cada, e a influência que essa manipulação poderá ter nos utilizadores.

Podemos concluir que os utilizadores encontram mais desvantagens do que vantagens, e estas apontam todas para o perigo de perda de privacidade. No entanto, no meio do perigo e medo também conseguem encontrar algumas vantagens associadas.

- *Verificar eventuais ações de prevenção face ao rastreamento* online

Os utilizadores negligenciam muito as ações de prevenção face ao rastreamento. Ainda assim, preocupam-se com o aceitar políticas de privacidade sem ler, verificar e selecionar que cookies podem ser utilizadas, e verificar a que dados as aplicações pretendem aceder.

Sintetizando, os utilizadores são mais propensos a ter ações de prevenção quando elas são mais diretas, ou seja, são oferecidas diretamente pelas plataformas em forma de pergunta ou informação. Ações que necessitem de uma ação mais proactiva por parte do utilizador, como por exemplo, apagar as cookies ou ter sistemas automáticos para apagar ficheiros de retenção de dados, não são tidas como práticas importantes.

- *Verificar como se podem relacionar as suas perceções de privacidade, segurança e rastreamento* online

Ao relacionar as perceções de privacidade, segurança e rastreamento online verificou-se que estas se encontram relacionadas com os itens privacidade, prudência, segurança, previsão de comportamentos, prevenção e por fim preocupação. Em suma, a privacidade e segurança, que se encontram implicitamente figuradas em todos os itens apresentados, são preocupações constantes entre os utilizadores.

Capítulo 5 – Conclusões

5.1 – Principais conclusões

As redes registam tudo o que fazemos *online*. Tudo. Sabem o que vemos, quando vemos, onde e durante quanto tempo. Sabem quando as pessoas veem fotos dos seus ex-namorados, se procuram namorado numa aplicação de encontros, se encomendam comida para um ou para seis, se preferem *sushi* ou hambúrgueres, a que horas vão para o trabalho, o que fazem à noite, se têm insónias. Sabem tudo isso e muito mais. Todos esses dados são arquivados, cruzados e usados para fazer previsões cada vez mais acertadas sobre os nossos comportamentos (Caetano, 2020).

Para que isto aconteça são utilizadas técnicas de rastreabilidade, que se tornaram um recurso valioso. Os dados que são arquivados, cruzados e usados, são utilizados para a criação de modelos vitais para as plataformas. Estes modelos permitem que seja possível entregar ao utilizador exatamente o que ele quer, enquadrado nas suas preferências.

No período de confinamento a tendência de estar sempre online aumentou. As pessoas, que se encontravam impedidas de fazer a sua vida normal no exterior, passaram muito mais tempo em frente a qualquer dispositivo ligado à Internet, quando comparado com o periodo anterior ao confinamento. Estar em casa fez com que a grande maioria das pessoas ficasse online para trabalhar, para estudar, para fazer compras, para socializar, entre muitas outras coisas.

Neste trabalho foi possível verificar e justificar os objetivos propostos, e responder à questão de investigação, verificando que os utilizadores têm perceções sobre o rastreamento online bastante expressivas, destacando fatores como a previsão comportamental, a influência de comportamentos, a privacidade e a segurança, como possíveis perigos relacionados com esta técnica.

De uma forma global, os utilizadores têm uma vaga ideia do que é o rastreamento online. À medida que se progride na faixa etária, a perceção sobre isso vai-se esbatendo. Utilizadores entre os 21 e os 34 anos estão mais familiarizados com este tipo de técnica, e por isso mais alertados para o que deve ser feito para a evitar.

Para questões como a privacidade, a segurança e a prevenção, os utilizadores demonstram preocupação com a sua privacidade e, ao mesmo tempo, a constante ameaça de a perder, com a informação pessoal recolhida pelas plataformas digitais.

Em questões de privacidade verificou-se que os utilizadores negligenciam a tomada de ações, no entanto, as que são de fácil acesso são adotadas. Estas ações são geralmente disponibilizadas automaticamente pelas plataformas, como por exemplo, as políticas de privacidade, ou de verificar as cookies que irão ser utilizadas. Em termos de confiança foi possível determinar que os utilizadores confiam mais nas plataformas que utilizam para trabalhar e estudar, enquanto que as plataformas usadas para entretenimento, mais precisamente as de redes sociais, são as que merecem menos confiança.

Por fim, os utilizadores encontram muito mais desvantagens e perigos associados ao rastreamento do que vantagens. A grande desvantagem é a perda de privacidade que este tipo de técnica traz.

Este trabalho contribui para aprofundar a temática do rastreamento online e a sua prática pelas diversas plataformas. Espera-se também, que contribua para aumentar o nível de alerta dos utilizadores para esta problemática. Por fim seria interessante que servisse para a promoção de investigações mais vastas com o objetivo da criação de regulamentação que diligencie a proteção dos interesses dos utilizadores.

5.2 – Limitações e dificuldades

Sem dúvida que a grande dificuldade encontrada para a realização deste trabalho foi os confinamentos constantes, e a obrigatoriedade de distanciamento social, que dificultou a interação cara a cara com professores e colegas, bem como o acesso a bibliotecas e materiais de investigação em papel. Uma outra dificuldade foi a recolha de dados. Com a recolha a ser feita apenas virtualmente, sem possibilidade de a fazer pessoalmente, acabou por resultar numa maior dificuldade de obtenção de respostas e pelo mesmo motivo tornando-as impessoais.

5.3 – Propostas para o futuro

Como propostas para futuros trabalhos seria interessante estudar que influência poderão ter as técnicas de rastreamento no comportamento das pessoas. Um bom exemplo seria perceber a influência que as plataformas podem ter, utilizando os dados recolhidos com esta técnica, nas preferências, atitudes, intenção de voto e antipatias dos utilizadores.

Um outro estudo possível seria tentar perceber, junto da geração que nasceu com a Internet, rodeada de tecnologia e *gadgets*, se estes (jovens) são mais vulneráveis à ingenuidade e ao erro.

Por fim, seria interessante conseguir uma amostra mais significativa, onde se poderiam relacionar todas as dimensões encontradas com a idade e com o género, e assim averiguar uma eventual influência da idade ou do género na perceção de rastreamento.

Referências Bibliográficas

Alturas, B. (2013). *Sistemas de Informação Organizacionais* (Silabo (Ed.); 1st ed.).

Avelino, R., & Amadeu, S. (2016). *A DEPENDÊNCIA DO RASTREAMENTO COMPORTAMENTAL ONLINE PARA A ECONOMIA GLOBALIZADA La dependência del rastreamiento comportamental online para la economia globalizada INTRODUÇÃO Em sua primeira fase comercial , em meados de 1995 , a Internet era constituída* (Issue May).

Avelino, Rodolfo. (2019). *A evolução dos mecanismos de rastreamento e vigilância intrusivos em clientes web The evolution of the intrusive tracking and surveillance mechanisms on web clients La evolución de los mecanismos de rastreo y vigilancia intrusivos en los clientes web*.

Barth, A. (2014). *RFC: HTTP State Management Mechanism*. 1–74. https://tools.ietf.org/html/rfc6265

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, *53*, 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Bozdag, E., & van den Hoven, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology*, *17*(4), 249–265. https://doi.org/10.1007/s10676-015-9380-y

Bujlow, T., Carela-Espanol, V., Lee, B. R., & Barlet-Ros, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, *105*(8), 1476–1510. https://doi.org/10.1109/JPROC.2016.2637878

Caetano, M. (2020). "O Dilema das Redes Sociais". Será possível escapar-lhes? *Diário de Notícias*. https://www.dn.pt/edicao-do-dia/19-set-2020/o-dilema-das-redes-sociais-sera-possivel-escapar-lhes-12738287.html

Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016). An empirical study of web cookies. *25th International World Wide Web Conference, WWW 2016*, 891–901. https://doi.org/10.1145/2872427.2882991

Calheiros, S. (2019). O poder dos dados no documentário 'Nada É Privado: O Escândalo da Cambridge Analytica', na Netflix. *Visão*.

Campbell-Kelly, M., Garcia-Swartz, D. D., & Campbell-Kelly, M. (2013). The history of the internet: the missing narratives. *Journal of Information Technology*, *28*, 18–33. https://doi.org/10.1057/jit.2013.4

Castells, M. (2003). *(PDF) The Internet Galaxy: Reflections on the Internet, Business, and Society. By Manuel Castells*. https://www.researchgate.net/publication/249471554_The_Internet_Galaxy_Reflections_on_the_Internet_Business_and_Society_By_Manuel_Castells

Cormen, T. H., Leiserson, C. E., & Rivest, R. L. (2001). *Introduction to Algorithms , Second Edition* (Vol. 7).

Duguay, S. (2018). Social media's breaking news: the logic of automation in Facebook Trending Topics and Twitter Moments. *Media International Australia*, *166*(1), 20–33. https://doi.org/10.1177/1329878X17737407

Gizmodo | We come from the future. (n.d.). Retrieved December 28, 2021, from https://gizmodo.com/

Guiddens, A. (1991) *As consequências da modernidade(* tradução de Raul Fiker, UNESP, 5th ed.).

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox

explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/J.CHB.2016.11.033

Hill, M., & Hill, A. (2009). *Investigação por Questionário* (Silabo (Ed.); 2nd ed.).

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kristol, D. M. (2001). HTTP Cookies: Standards, Privacy, and Politics. *ACM Transactions on Internet Technology*, *1*(2), 151–198. https://doi.org/10.1145/502152.502153

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. https://doi.org/10.1016/J.TELPOL.2014.10.002

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2014). The Economics of Regulating Privacy on the Internet. *Handbook on the Economics of the Internet*, *36*(22), 968–973.

Lerner, A., Simpson, A. K., Kohno, T., & Roesner, F. (2016). Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016. *Proceedings of the 25th USENIX Security Symposium*, 997–1013.

Meese, J., & Hurcombe, E. (2020). Facebook, news media and platform dependency: The institutional impacts of news distribution on social platforms. *New Media and Society*. https://doi.org/10.1177/1461444820926472

Obercom. (2015). *A Internet e o consumo de notícias online em Portugal*. https://obercom.pt/wp-content/uploads/2016/06/A-Internet-e-o-consumo-de-notícias-online-em-Portugal-2015.pdf

OLD. (2021). Digital 2021: Global Overview Report — DataReportal – Global Digital Insights. In *Kepios Pte. Ltd., We Are Social Ltd. and Hootsuite Inc.* https://datareportal.com/reports/digital-2021-global-overview-report

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

Plantin, J.-C., & Punathambekar, A. (2019). Digital media infrastructures: pipes, platforms, and politics. *Media, Culture & Society*, *41*(2), 163–174. https://doi.org/10.1177/0163443718818376

Prensky, M. (2001). Digital Natives, Digital Immigrants. In *From Digital Natives to Digital Wisdom: Hopeful Essays for 21st Century Learning* (Vol. 9, Issue 5, pp. 67–85). MCB University Press. https://doi.org/10.4135/9781483387765.n6

Regalado, A. (2011). *Who Coined "Cloud Computing"? | MIT Technology Review*. MIT Technology Review. https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/

Rodrigues, N. (2018). *Está por aí alguém ? Perceções da exposição e da privacidade nas redes sociais , entre estudantes universitários*.

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy*, *5*(3), 40–49. https://doi.org/10.1109/MSP.2007.75

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce*, *10*(1), 1–16. https://doi.org/10.1080/15332861.2011.558454

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). *Flash Cookies and Privacy School of Information*. 158–163.

Takács, G., Németh, B., Frasconi, P., Kersting, K., Toivonen, H., & Tsuda, K. (2009). Scalable Collaborative Filtering Approaches for Large Recommender Systems István Pilászy * Domonkos Tikk *. In *Journal of Machine Learning Research* (Vol. 10). https://doi.org/10.5555/1577069.1577091

Thurman, N., Moeller, J., Helberger, N., & Trilling, D. (2019). My Friends, Editors, Algorithms, and I: Examining audience attitudes to news selection. *Digital Journalism*, *7*(4), 447–469. https://doi.org/10.1080/21670811.2018.1493936

Zamith, R. (2019). Algorithms and Journalism. In *Oxford Research Encyclopedia of Communication*. https://doi.org/10.1093/acrefore/9780190228613.013.779

Apêndices e Anexos

Apêndice A – Questionário

O presente questionário destina-se a recolher dados para uma dissertação de mestrado cujo principal objetivo é compreender como é que as pessoas adultas percecionam a possibilidade de serem rastreadas online (ou seguidas, p.e., por empresas), em termos da sua privacidade e de eventuais contrapartidas ou benefícios encontrados.
A sua participação é extremamente valorizada e consiste no preenchimento de um questionário com uma duração estimada de 10 minutos.
Neste questionário não existem respostas certas nem respostas erradas, a sua participação é voluntária e poderá interromper a sua participação em qualquer momento. Esperamos que responda da forma mais espontânea e sincera possível. Todos os dados serão tratados de forma totalmente anónima e estritamente confidencial, sendo os resultados exclusivamente usados para fins científicos.

Agradecemos, desde já, a sua disponibilidade!

Se existir alguma questão relativamente ao trabalho, ou se pretender feedback deste projeto, poderá contactar via correio eletrónico para o endereço rita_susana_ganhao@iscte-iul.pt.

Li a informação descrita e presto desta forma o meu consentimento voluntário para participar na investigação.

- ○ Sim
- ○ Não

Idade: (maiores de 18 anos)

Género:

- ○ Feminino
- ○ Masculino
- ○ Outro

Habilitações literárias:

- ○ 1º Ciclo ou ensino primário
- ○ 2º Ciclo ou ensino preparatório
- ○ 3º Ciclo (9º ano de escolaridade)
- ○ Ensino secundário (ou equivalente)
- ○ Frequência do ensino superior
- ○ Licenciatura
- ○ Outra

Em que medida tem noção do que é o rastreamento online?

- Nunca ouvi falar
- Não sei bem o que é
- Tenho uma vaga ideia
- Sei bem o que é
- Sei muito bem o que é

Rastreamento online é o processo que é feito pelas plataformas digitais e que tem como objetivo analisar todos os passos digitais dados pelos utilizadores com a intenção de recolher dados que possam beneficiar de alguma forma as plataformas digitais.

2. Em que medida pensa que as plataformas online seguintes utilizam técnicas de rastreamento? (Escala: 1. Não tenho conhecimento 2. Não utilizam 3. Tem rastreamento básico 4. Rastreamento moderado 5. Rastreamento exagerado)

	Não tenho conhecimento	Não utilizam	Rastreamento básico	Rastreamento moderado	Rastreamento exagerado
1. Amazon					
2. Facebook					
3. Firefox					
4. Google					
5. HBO					
6. Instagram					
7. Netflix					
8. Teams					
9. WhatsApp					
10. Zoom					

3. Indique até que ponto considera que as plataformas digitais utilizam técnicas de rastreamento para as diferentes finalidades: (Escala: 1. Improvável 2. Pouco Provável 3. Nem improvável, nem provável 4. Provável 5. Muito Provável)

	Improvável	Pouco provável	Nem improvável, nem provável	Provável	Muito provável
A partilha de publicidade direcionada					

	Improvável	Pouco provável	Nem improvável, nem provável	Provável	Muito provável
Estudar					
Pesquisar					
Entretenimento					

4. De 1 a 5, diga-nos por favor, qual o seu nível de confiança nas plataformas digitais que utiliza: (Escala:1. Nenhuma confiança 2. Pouca confiança 3. Confia moderadamente 4. Confia 5. Confia plenamente)

	Não utiliza	1	2	3	4	5
Amazon						
Facebook						
Firefox						
Google						
HBO						
Instagram						
Netflix						
Teams						
WhatsApp						
Zoom						

5. Em termos de utilização diga-nos para que fim utiliza as seguintes plataformas: (é possível escolher mais de que uma opção)

	Não utiliza	Trabalhar	Estudar	Pesquisar	Entretenimento
Amazon					
Facebook					
Firefox					
Google					
HBO					
Instagram					
Netflix					
Teams					
WhatsApp					
Zoom					

6. Ao utilizar plataformas digitais, diga p.f. com que frequência costuma: (Escala: 1. Nunca 2. Raramente 3. Por vezes 4. Frequentemente 5. Muito Frequentemente)

	Nunca	Raramente	Por vezes	Frequentemente	Muito Frequentemente
Aceitar as políticas de privacidade sem as ler					
Verificar as cookies e selecionar as que permito serem utilizadas					
Apagar as cookies (armazenadas após utilização) dos browsers					
Ter sistemas automáticos para apagar ficheiros de retenção de dados					
Verificar a que dados as aplicações pretendem aceder					
Usar aplicações que ajudam a proteger, ou previnem, a gravação de cookies					

7. Em termos de privacidade até que ponto considera importante as seguintes opções: (Escala: 1. Nada importante 2. Pouco importante 3. Moderadamente importante 4. Importante 5. Muito importante)

	1	2	3	4	5
As plataformas digitais apresentarem políticas de privacidade claras e simples					
As plataformas digitais informarem de que forma irão ser tratados os dados recolhidos					

	1	2	3	4	5
A implementação do RGPD a nível europeu (Regulamento Geral sobre a Proteção de Dados)					
As plataformas digitais informarem quais dados são recolhidos					
As plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. camara do telemóvel, localização)					
Não ser possível a verificação e divulgação da localização do utilizador através do envio de mensagens, fotos e ou vídeos tiradas/feitos no dispositivo do utilizador					
A possibilidade de remover a permissão de acesso à localização das plataformas digitais					
A possibilidade de gerir a que informação e/ou dados as organizações podem aceder					
Ser apresentado nas diversas plataformas digitais publicidade direcionada (publicidade relevante apenas para si)					
Ter a possibilidade de verificar que					

	1	2	3	4	5
informação/dados são vendidos ou cedidos a outras organizações.					

8. Em termos de segurança até que ponto considera importante as seguintes opções: (Escala: 1. Nada importante 2. Pouco importante 3. Moderadamente importante 4. Importante 5. Muito importante)

	1	2	3	4	5
Ser possível autorizar de forma simples quais as organizações que podem aceder aos seus dados					
Poder definir para cada uma das organizações, a que dados podem aceder					
Saber se a sua informação/dados se encontram seguros					
Ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si					
Existir uma opção de "não rastreamento" do seu tráfego de navegação					
Existir uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si)					
Existir a possibilidade de bloquear o acesso à sua localização pelas aplicações e plataformas					

9. Pensando no modo como podem ser utilizados os dados recolhidos pelas plataformas digitais, diga-nos, p.f., até que ponto o preocupa que estes sejam usados

para: (Escala: 1. Nada preocupante 2. Pouco preocupante 3. Moderadamente preocupante 4. preocupante 5. Muito preocupante)

	1	2	3	4	5
Desenvolvimento de novos produtos					
Partilha de publicidade direcionada					
Previsão do comportamento dos utilizadores					
Influenciar os utilizadores nas suas compras					
Venda de dados a terceiros					
Influenciar a tendência de voto					
Partilha de notícias falsas (fake news) sobre temas de interesse					
Partilha de propaganda sobre assuntos de interesse do utilizador					

10. Quais são para si, as vantagens (ou benefícios práticos) de utilizar plataformas digitas, sabendo que estas têm técnicas de rastreamento online?

11. Quais são para si, as desvantagens (ou ameaças) de utilizar plataformas digitas, sabendo que estas têm técnicas de rastreamento online?

Apêndice B – Estatísticas descritivas (Frequência, médias e desvio-padrão)

1. Em que medida tem noção do que é o rastreamento online?

Tabela 9- Tabela de frequência de perceção dos utilizadores sobre rastreamento online

		N	%
Válido	Nunca ouvi falar	3	2,0%
	Não sei bem o que é	7	4,7%
	Tenho uma vaga ideia	54	36,5%
	Sei bem o que é	47	31,8%
	Sei muito bem o que é	25	16,9%
	Total	136	91,9%
Omisso	Sistema	12	8,1%
Total		148	100,0%

Tabela 10- Tabela de média e desvio-padrão de perceção dos utilizadores sobre rastreamento online

N	Média	Desvio Padrão
136	3,62	,919

2. Em que medida pensa que as plataformas online seguintes utilizam técnicas de rastreamento?

Tabela 11- Tabela de frequência de perceção de utilização de técnicas de rastreamento nas diversas plataformas digitais

	Não tenho conhecimento		Não utilizam		Rastreamento básico		Rastreamento moderado		Rastreamento exagerado	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Amazon	26	17,6%	3	2,0%	14	9,5%	46	31,1%	47	31,8
Facebook	7	4,7%	1	0,7%	6	4,1%	28	18,9%	93	62,8%
Firefox	44	29,7%	3	2,0%	23	15,5%	42	28,4%	22	14,9%
Google	7	4,7%	1	0,7%	8	5,4%	26	17,6%	93	62,8%
HBO	55	37,2%	4	2,7%	22	14,9%	40	27,0%	13	8,8%
Instagram	14	9,5%	2	1,4%	5	3,4%	31	20,9%	82	55,4%
Netflix	36	24,3%	6	4,1%	19	12,8%	55	37,2%	18	12,2%
Teams	63	42,6%	7	4,7%	23	15,5%	31	20,9%	10	6,8%
WhatsApp	20	13,5%	12	8,1%	29	19,6%	32	21,6%	42	28,4%
Zoom	57	38,5%	7	4,7%	20	13,5%	26	17,6%	25	16,9%

Tabela 12 - Tabela de média e desvio padrão de perceção de utilização de técnicas de rastreamento nas diversas plataformas digitais

	N	Média	Desvio Padrão
Amazon	136	3,63	1,460
Facebook	135	4,47	1,006
Firefox	134	2,96	1,524
Google	135	4,46	1,020
HBO	134	2,64	1,499
Instagram	134	4,23	1,268
Netflix	134	3,10	1,440
Teams	134	2,39	1,450
WhatsApp	135	3,47	1,397
Zoom	135	2,67	1,607

3. Indique até que ponto considera que as plataformas digitais utilizam técnicas de rastreamento para as diferentes finalidades: (Escala: 1. Improvável 2. Pouco Provável 3. Nem improvável, nem provável 4. Provável 5. Muito Provável)

Tabela 13 - Tabela de frequência de perceção de utilização de técnicas de rastreamento para diferentes finalidades

	Improvável		Pouco Provável		Nem improvável, nem provável		Provável		Muito Provável	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
A partilha de publicidade direcionada			1	0,7%	4	2,7%	26	17,6%	104	70,3%
Estudar	1	0,7%	12	8,1%	24	16,2%	57	38,5%	42	28,4%
Pesquisar	1	0,7%	3	2,0%	8	5,4%	59	39,9%	65	43,9%
Entretenimento	2	1,4%	5	3,4%	10	6,8%	51	34,5%	68	45,9%

Tabela 14- Tabela de média e desvio padrão de perceção de utilização de técnicas de rastreamento para diferentes finalidades

	N	Média	Desvio Padrão
A partilha de publicidade direcionada	135	4,73	,552
Estudar	136	3,93	,952
Pesquisar	136	4,35	,756
Entretenimento	136	4,31	,874

4. De 1 a 5, diga-nos por favor, qual o seu nível de confiança nas plataformas digitais que utiliza: (Escala:1. Nenhuma confiança 2. Pouca confiança 3. Confia moderadamente 4. Confia 5. Confia plenamente)

Tabela 15- Tabela de frequência de perceção de utilização de técnicas de rastreamento para diferentes finalidades

	Não utiliza		1		2		3		4		5	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Amazon	59	39,9%	8	5,4%	15	10,1%	30	20,3%	20	13,5%	3	2,0%
Facebook	15	10,1%	31	20,9%	31	20,9%	44	29,7%	10	6,8%	5	3,4%
Firefox	64	43,2%	3	2,0%	13	8,8%	31	20,9%	18	12,2%	6	4,1%
Google	1	0,7%	17	11,5%	19	12,8%	56	37,8%	29	19,6%	14	9,5%
HBO	78	52,7%	3	2,0%	8	5,4%	31	20,9%	11	7,4%	4	2,7%
Instagram	29	19,6%	25	16,9%	21	14,2%	40	27,0%	14	9,5%	7	4,7%
Netflix	35	23,6%	8	5,4%	11	7,4%	47	31,8%	26	17,6%	8	5,4%
Teams	51	34,5%	7	4,7%	15	10,1%	37	25,0%	21	14,2%	5	3,4%
WhatsApp	2	1,4%	22	14,9%	16	10,8%	57	38,5%	24	16,2%	14	9,5%
Zoom	30	20,3%	14	9,5%	16	10,8%	47	31,8%	18	12,2%	9	6,1%

Tabela 16- Tabela de média e desvio padrão de perceção de utilização de técnicas de rastreamento para diferentes finalidades

	N	Média	Desvio Padrão
Amazon	135	2,65	1,650
Facebook	136	3,13	1,270
Firefox	135	2,66	1,728
Google	136	4,01	1,158
HBO	135	2,30	1,640
Instagram	136	3,04	1,490

Netflix	135	3,33	1,630
Teams	136	2,89	1,667
WhatsApp	135	3,90	1,223
Zoom	134	3,27	1,562

5. Em termos de utilização diga-nos para que fim utiliza as seguintes plataformas: (é possível escolher mais de que uma opção)

Tabela 17- Tabela de frequência para que fim se utilizam as plataformas

	Não utiliza		Trabalhar		Estudar		Pesquisar		Entretenimento	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Amazon	60	40,5%	5	3,4%	3	2,0%	32	21,6%	36	24,3%
Facebook	17	11,5%	4	2,7%	1	0,7%	18	12,2%	92	62,2%
Firefox	63	42,6%	31	20,9%	18	12,2%	39	26,4%	16	10,8%
Google	1	0,7%	68	45,9%	55	37,2%	107	72,3%	51	34,5%
HBO	72	48,6%	5	3,4%	1	0,7%	5	3,4%	36	24,3%
Instagram	27	18,2%	6	4,%	1	0,7%	13	8,8%	85	57,4%
Netflix	35	23,6%					2	1,4%	79	53,4%
Teams	45	30,4%	64	43,2%	11	7,4%			2	1,4%
WhatsApp	1	0,7	37	25,0%	10	6,8%	4	2,7%	106	71,6%
Zoom	33	22,3%	73	49,3%	27	18,2%	1	0,7%	16	10,8%

6. Ao utilizar plataformas digitais, diga p.f. com que frequência costuma:

Tabela 18- Tabela de frequência de hábitos de utilização das plataformas

	Nunca		Raramente		Por vezes		Frequentemente		Muito Frequentemente	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Aceitar as políticas de privacidade sem as ler	4	2,7%	9	6,1%	20	13,5%	36	24,3%	47	31,8%
Verificar as cookies e selecionar as que permito serem utilizadas	15	10,1%	27	18,2%	25	16,9%	25	16,9%	24	16,2%
Apagar as cookies (armazenadas após utilização) dos browsers	28	18,9%	24	16,2%	33	23,3%	20	13,5%	11	7,4%
Ter sistemas automáticos para apagar ficheiros de	58	39,2%	31	20,9%	12	8,1%	9	6,1%	6	4,1%

retenção de dados										
Verificar a que dados as aplicações pretendem aceder	20	13,5%	24	16,2%	33	22,3%	22	14,9%	17	11,5%
Usar aplicações que ajudam a proteger, ou previnem, a gravação de cookies	48	32,4%	25	16,9%	22	14,9%	17	11,5%	4	2,7

Tabela 19- Tabela de média e desvio padrão de hábitos de utilização das plataformas

	N	Média	Desvio Padrão
Aceitar as políticas de privacidade sem as ler	116	3,97	1,099
Verificar as cookies e selecionar as que permito serem utilizadas	116	3,14	1,338
Apagar as cookies (armazenadas após utilização) dos browsers	116	2,67	1,277
Ter sistemas automáticos para apagar ficheiros de retenção de dados	116	1,91	1,176
Verificar a que dados as aplicações pretendem aceder	116	2,93	1,297
Usar aplicações que ajudam a proteger, ou previnem, a gravação de cookies	116	2,17	1,218

7. Em termos de privacidade até que ponto considera importante as seguintes opções:

Tabela 20 - Tabela de frequência de importância de opções de privacidade

	1 – Nada importante		2 – Pouco importante		3 - Moderadamente importante		4 - Importante		5 – Muito importante	
	N	**%**	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**

As plataformas digitais apresentarem políticas de privacidade claras e simples	2	1,4%	4	2,7%	13	8,8%	16	10,8%	80	54,1%
As plataformas digitais informarem de que forma irão ser tratados os dados recolhidos	2	1,4%	3	2,0%	7	4,7%	17	11,5%	87	58,8%
A implementação do RGPD a nível europeu (Regulamento Geral sobre a Proteção de Dados)	4	2,7%	3	2,0%	2	1,4%	20	13,5%	86	58,1%
As plataformas digitais informarem quais dados são recolhidos	1	0,7%	1	0,7%	5	3,4%	18	12,2%	90	60,8%
As plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. camara do telemóvel, localização)	1	0,7%	5	3,4%	1	0,7%	15	10,1%	93	62,8%
Não ser possível a verificação e divulgação da localização do utilizador através do envio de mensagens, fotos e ou vídeos tiradas/feitos no dispositivo do utilizador	2	1,4%	1	0,7%	10	6,8%	14	9,5%	87	58,8%
A possibilidade de remover a permissão de acesso à localização das plataformas digitais			3	2,0%	4	2,7%	16	10,8%	92	62,3%
A possibilidade de gerir a que informação e/ou dados as organizações podem aceder	1	0,7%	1	0,7%	5	3,4%	14	9,5%	91	61,5%
Ser apresentado nas diversas plataformas digitais publicidade direcionada (publicidade relevante apenas para si)	13	8,8%	13	8,8%	28	18,9%	24	16,2%	37	25,0%
Ter a possibilidade de verificar que informação/dados são vendidos ou cedidos a outras organizações.	1	0,7%	3	2,0%	5	3,4%	13	8,8%	92	62,2%

Tabela 21- Tabela de média e desvio padrão de importância de opções de privacidade

	N	Média	Desvio Padrão
As plataformas digitais apresentarem políticas de privacidade claras e simples	115	4,46	,949
As plataformas digitais informarem de que forma irão ser tratados os dados recolhidos	116	4,59	,855
A implementação do RGPD a nível europeu (Regulamento Geral sobre a Proteção de Dados)	115	4,57	,928
As plataformas digitais informarem quais dados são recolhidos	115	4,70	,678
As plataformas digitais informarem as funcionalidades do dispositivo que vão aceder (ex. camara do telemóvel, localização)	115	4,69	,776
Não ser possível a verificação e divulgação da localização do utilizador através do envio de mensagens, fotos e ou vídeos tiradas/feitos no dispositivo do utilizador	114	4,61	,827
A possibilidade de remover a permissão de acesso à localização das plataformas digitais	115	4,71	,659
A possibilidade de gerir a que informação e/ou dados as organizações podem aceder	112	4,72	,674

Ser apresentado nas diversas plataformas digitais publicidade direcionada (publicidade relevante apenas para si)	115	3,51	1,347
Ter a possibilidade de verificar que informação/dados são vendidos ou cedidos a outras organizações.	114	4,68	,756

8. Em termos de segurança até que ponto considera importante as seguintes opções:

Tabela 22- Tabela de frequência de importância de opções de segurança

	1 – Nada importante		2 – Pouco importante		3 - Moderadamente importante		4 - Importante		5 – Muito importante	
	N	%	N	%	N	%	N	%	N	%
Ser possível autorizar de forma simples quais as organizações que podem aceder aos seus dados	1	0,7%			7	4,7%	13	8,8%	96	64,2%
Poder definir para cada uma das organizações, a que dados podem aceder			1	0,7%	6	4,1%	19	12,8%	87	58,8%
Saber se a sua informação/dados se encontram seguros					5	3,4%	11	7,4%	100	67,6%
Ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si					5	3,4%	7	4,7%	104	70,3%
Existir uma opção de "não rastreamento" do seu tráfego de navegação					7	4,7%	15	10,1%	94	63,5%
Existir uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si)	1	0,7%			11	7,4%	20	13,5%	84	56,8%
Existir a possibilidade de bloquear o acesso à sua localização pelas aplicações e plataformas					4	2,7%	14	9,5%	98	66,2%

Tabela 23- Tabela de média e desvio padrão de importância de opções de segurança

	N	Média	Desvio Padrão
Ser possível autorizar de forma simples quais as organizações que podem aceder aos seus dados	116	4,73	,651
Poder definir para cada uma das organizações, a que dados podem aceder	113	4,70	,611
Saber se a sua informação/dados se encontram seguros	116	4,82	,486
Ter a garantia de que os seus dados só são acedidos por pessoas/organizações autorizadas por si	116	4,85	,462
Existir uma opção de "não rastreamento" do seu tráfego de navegação	116	4,75	,558
Existir uma opção que possibilite o bloqueio da partilha de publicidade direcionada (publicidade relevante apenas para si)	116	4,60	,733
Existir a possibilidade de bloquear o acesso à sua localização pelas aplicações e plataformas	116	4,81	,474

9. Pensando no modo como podem ser utilizados os dados recolhidos pelas plataformas digitais, diga-nos, p.f., até que ponto o preocupa que estes sejam usados para:

Tabela 24- Tabela de frequência de importância dada à utilização de dados

	1 – Nada preocupante		2 – Pouco preocupante		3 - Moderadamente preocupante		4 - Preocupante		5 – Muito preocupante	
	N	%	N	%	N	%	N	%	N	%
Desenvolvimento de novos produtos	12	8,1%	25	16,9%	41	27,7%	15	10,1%	22	14,9%

Partilha de publicidade direcionada	2	1,4%	15	10,1%	35	23,6%	31	20,9%	33	22,3%
Previsão do comportamento dos utilizadores	3	2,0%	5	3,4%	24	16,2%	29	19,6%	55	37,2%
Influenciar os utilizadores nas suas compras	3	2,0%	2	1,4%	21	14,2%	26	17,6%	64	43,2%
Venda de dados a terceiros	3	2,0%			4	2,7%	12	8,1%	97	65,5%
Influenciar a tendência de voto	3	2,0%			8	5,4%	14	9,5%	91	61,5%
Partilha de notícias falsas (fake news) sobre temas de interesse	3	2,0%	1	0,7%	7	4,7%	7	4,7%	96	64,9%
Partilha de propaganda sobre assuntos de interesse do utilizador	3	3,0%	8	5,4%	24	16,2%	31	20,9%	50	33,8%

Tabela 25- Tabela de média e desvio padrão de importância dada à utilização de dados

	N	Média	Desvio Padrão
Desenvolvimento de novos produtos	115	3,09	1,239
Partilha de publicidade direcionada	116	3,67	1,078
Previsão do comportamento dos utilizadores	116	4,10	1,042
Influenciar os utilizadores nas suas compras	116	4,26	,988
Venda de dados a terceiros	116	4,72	,764
Influenciar a tendência de voto	116	4,64	,828
Partilha de notícias falsas (fake news) sobre temas de interesse	114	4,68	,845
Partilha de propaganda sobre assuntos de interesse do utilizador	116	4,01	1,075

Apêndice C – Análise de Componentes Principais

Objetivo 3 – Análise de Componentes Principais – Questão 9

Tabela 26- KMO e Teste de Bartlett's da ACP da importância do rastreamento

Teste de KMO e Bartlett		
Kaiser-Meyer-Olkin (KMO)		,838
Teste de Bartlett	Qui-quadrado aproximado	505,604
	Grau de liberdade	28
	Sig.	,000

Tabela 27- Variância total explicada da ACP da importância do rastreamento

Variância total explicada						
Componente	Auto valores iniciais			Somas de extração de carregamentos ao quadrado		
	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa
1	4,031	50,390	50,390	4,031	50,390	50,390
2	1,751	21,886	72,277	1,751	21,886	72,277
3	,668	8,355	80,632			
4	,468	5,854	86,486			
5	,387	4,838	91,324			
6	,320	4,003	95,327			
7	,206	2,578	97,905			
8	,168	2,095	100,000			
Método de Extração: análise de Componente Principal.						

Tabela 28- Matriz de transformação de componentes da ACP da importância do rastreamento

Matriz de transformação de componente		
Componente	1	2
1	,863	,506
2	-,506	,863
Método de Extração: análise de Componente Principal. Método de Rotação: Varimax com Normalização de Kaiser.		

Objetivo 7 – Análise de Componentes Principais – Questão 7, 8 e9

Tabela 29- KMO e Teste de Bartlett's da ACP das perceções de privacidade, segurança e rastreamento online

Teste de KMO e Bartlett		
Kaiser-Meyer-Olkin (KMO)		,809
Teste de Bartlett	Qui-quadrado aproximado	1664,080
	Grau de liberdade	300
	Sig.	,000

Tabela 30 - Variância total explicada da ACP das perceções de privacidade, segurança e rastreamento online

Variância total explicada

Componente	Autovalores iniciais			Somas de extração de carregamentos ao quadrado			Somas de rotação de carregamentos ao quadrado		
	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa	Total	% de variância	% cumulativa
1	8,298	33,191	33,191	8,298	33,191	33,191	5,424	21,695	21,695
2	2,953	11,813	45,004	2,953	11,813	45,004	3,637	14,547	36,241
3	2,542	10,169	55,173	2,542	10,169	55,173	3,617	14,467	50,709
4	1,871	7,483	62,655	1,871	7,483	62,655	2,385	9,540	60,249
5	1,271	5,086	67,741	1,271	5,086	67,741	1,608	6,432	66,681
6	1,078	4,314	72,055	1,078	4,314	72,055	1,344	5,374	72,055
7	,905	3,620	75,675						
8	,755	3,020	78,695						
9	,661	2,642	81,337						
10	,636	2,546	83,883						
11	,597	2,389	86,272						
12	,461	1,843	88,115						
13	,418	1,674	89,789						
14	,414	1,654	91,443						
15	,353	1,413	92,856						
16	,278	1,112	93,967						

17	,269	1,076	95,044						
18	,237	,948	95,991						
19	,219	,875	96,867						
20	,184	,735	97,602						
21	,168	,673	98,275						
22	,150	,601	98,875						
23	,114	,455	99,330						
24	,088	,351	99,681						
25	,080	,319	100,000						
Método de Extração: análise de Componente Principal.									

Tabela 31 - Matriz de transformação de componentes da ACP das perceções de privacidade, segurança e rastreamento online

Matriz de transformação de componente						
Componente	1	2	3	4	5	6
1	,720	,432	,436	,219	,218	,097
2	-,164	,744	-,505	,329	-,194	-,135
3	-,601	,115	,655	,441	,022	-,041
4	,163	-,437	-,265	,765	-,068	,349
5	-,020	-,128	-,190	,197	,757	-,580
6	-,258	,198	-,141	-,156	,580	,716
Método de Extração: análise de Componente Principal. Método de Rotação: Varimax com Normalização de Kaiser.						

Apêndice D – Correlações

Tabela 32- Correlação da importância do rastreamento

Correlações

		Desenvolvimento de novos produtos	Partilha de publicidade direcionada	Previsão do comportamento dos utilizadores	Influenciar os utilizadores nas suas compras	Venda de dados a terceiros	Influenciar a tendência de voto	Partilha de notícias falsas (fake news) sobre temas de interesse	Partilha de propaganda sobre assuntos de interesse do utilizador
Desenvolvimento de novos produtos	Correlação de Pearson	1	,562**	,360**	,239**	-,067	-,037	-,052	,303**
	Sig. (2 extremidades)		,000	,000	,010	,480	,694	,582	,001
	N	115	115	115	115	115	115	113	115
Partilha de publicidade direcionada	Correlação de Pearson	,562**	1	,464**	,440**	,185*	,188*	,160	,513**
	Sig. (2 extremidades)	,000		,000	,000	,047	,044	,089	,000
	N	115	116	116	116	116	116	114	116
Previsão do comportamento dos utilizadores	Correlação de Pearson	,360**	,464**	1	,658**	,484**	,457**	,433**	,481**
	Sig. (2 extremidades)	,000	,000		,000	,000	,000	,000	,000
	N	115	116	116	116	116	116	114	116
Influenciar os utilizadores nas suas compras	Correlação de Pearson	,239**	,440**	,658**	1	,510**	,477**	,453**	,456**
	Sig. (2 extremidades)	,010	,000	,000		,000	,000	,000	,000
	N	115	116	116	116	116	116	114	116
	Correlação de Pearson	-,067	,185*	,484**	,510**	1	,817**	,808**	,479**

Venda de dados a terceiros	Sig. (2 extremidades)	,480	,047	,000	,000		,000	,000	,000
	N	115	116	116	116	116	116	114	116
Influenciar a tendência de voto	Correlação de Pearson	-,037	,188*	,457**	,477**	,817**	1	,788**	,482**
	Sig. (2 extremidades)	,694	,044	,000	,000	,000		,000	,000
	N	115	116	116	116	116	116	114	116
Partilha de notícias falsas (fake news) sobre temas de interesse	Correlação de Pearson	-,052	,160	,433**	,453**	,808**	,788**	1	,522**
	Sig. (2 extremidades)	,582	,089	,000	,000	,000	,000		,000
	N	113	114	114	114	114	114	114	114
Partilha de propaganda sobre assuntos de interesse do utilizador	Correlação de Pearson	,303**	,513**	,481**	,456**	,479**	,482**	,522**	1
	Sig. (2 extremidades)	,001	,000	,000	,000	,000	,000	,000	
	N	115	116	116	116	116	116	114	116
**. A correlação é significativa no nível 0,01 (2 extremidades).									
*. A correlação é significativa no nível 0,05 (2 extremidades).									