DOS **QUATRO TÓPICOS** APRESENTADOS, ESCOLHE APENAS **UM** E ESCREVE UM **ENSAIO FILOSÓFICO** SOBRE O MESMO.

INDICAÇÕES:

Tens **três horas** para redigires o teu ensaio, sendo-te concedidos **10 minutos de tolerância para gravação e submissão *online***.
Dos quatro tópicos possíveis, **identifica claramente o tópico escolhido para realizares o teu ensaio**.
Escreve o teu número secreto apenas na primeira página do teu ensaio, **no espaço designado**, e **não escrevas** o teu nome ou qualquer tipo de identificação em nenhum lugar, sob pena de desclassificação.
Vai gravando o teu ensaio, em intervalos regulares, de 30 em 30 minutos.
Não alteres a formatação pré-definida para a realização do ensaio.

Código Secreto
1038

Tópico 3 – Considera que a privacidade está em risco com a web e as redes sociais?

As redes sociais e a Internet têm vindo a crescer, mais e mais com o passar dos anos. Se há pouco mais de 20 anos o telemóvel e o computador eram objetos raros e muito diferentes do que são hoje, no nosso quotidiano, os telemóveis e computadores abundam, nas mais diversas formas, tamanhos, modelos e cores. E com o aumento da diversidade de dispositivos eletrónicos, aumentam também as suas funcionalidades. Passaram-se 24 anos desde o início do novo milénio e os telemóveis funcionam como autênticas câmaras, os computadores como autênticas calculadoras ou enciclopédias automáticas, e estas são apenas três das quase infinitas funções de um computador ou telemóvel. Mas, qual será a função, a característica de um computador ou telemóvel, que os distingue de tudo o resto? Creio ser a capacidade de comunicação instantânea com o outro, além, claro, da enorme capacidade de armazenamento e seleção de informação destes dispositivos. E como é que tudo isto acontece? Através de algo muito singular, especial, inovador e revolucionário – a Internet e as redes sociais.

Efetivamente, as redes sociais e a Internet trouxeram ao mundo uma nova visão, uma nova perspetiva, já que facilitaram um grande leque de trabalhos, mudaram a forma como pesquisamos informação e comunicamos com os outros, além de, obviamente, terem tornado mais acessível a comunicação intercontinental, interestadual, internacional. Hoje, se quisermos combinar um café, enviamos uma mensagem através do WhatsApp para o nosso destinatário, ou então, estabelecemos uma ligação telefónica, ou então, trocamos *direct messages* através

do Instagram. Muitos de nós nem sequer o sabem fazer de outra maneira. Mas, quem nos garante que estamos realmente a conversar com a pessoa que pretendemos e não com alguém que as imita? Como podemos ter a certeza que alguém mal-intencionado não tem acesso às nossas informações e nos tenta assaltar, raptar ou extorquir?

O presente ensaio tem o objetivo de averiguar e apresentar uma tese referente ao problema da segurança no mundo digital. A nossa privacidade e segurança já é um assunto complicado no mundo denominado "real", visto que não estamos nunca 100% seguros, nem livres de nos acontecer algo de mal. Então, no mundo digital, este tópico torna-se ainda mais controverso, complicado e fraturante. Com isto, surge um problema filosófico de extrema relevância – "Será que a nossa privacidade e segurança estão em risco na internet e nas redes sociais?".

Antes de envergar na discussão deste problema filosófico, considero de extrema importância definir e apresentar alguns conceitos essenciais, como redes sociais, Internet, privacidade e segurança. Redes sociais são plataformas de interação entre indivíduos que permitem uma comunicação direta ou indireta entre os mesmos, não estando estes limitados, na sua maioria, pela sua localização, mas apenas pelo acesso à Internet. Internet é um espaço digital, onde se encontram diversas aplicações que pretendem servir diversas funcionalidades, e permite o acesso a todo o tipo de informação e conteúdo a partir de qualquer parte do globo (note-se que a expressão estar online tem o significado de estar ativo, em tempo real, na Internet, ou seja, estar a aceder a algum tipo de plataforma digital através de um motor de busca, ou aplicação de rede social, por exemplo. A expressão mundo digital/virtual é sinónima de Internet). Segurança é um termo que, para os efeitos pretendidos por este ensaio, expressa a característica de um espaço, ou local, em deixar quem nele está situado confortável e sem temer ver a sua privacidade ou integridade, quer física, psicológica, mental ou emocional, atacadas. Privacidade significa, por instância, a capacidade de guardar, de modo secreto, os dados que não tenho a intenção de partilhar. Dando um exemplo concreto:

"O Ivo está de férias em Bali e não pretende que se saiba a sua localização. Contudo, um hacker mal-intencionado entrou no seu telemóvel e divulgou a localização do Ivo a todos os seus amigos (do Ivo)"

Assim, diz-se que a privacidade do Ivo foi invadida.

Esclarecidos os conceitos considerados fundamentais para a redação deste ensaio, é agora crucial apresentar a relevância do problema filosófico em causa.

De facto, este problema tem uma pertinência elevadíssima, já que a resposta a ele pode vir a condicionar o modo como nos comportamos na Internet, no mundo digital. Que fotografias podemos e não podemos partilhar? Que tipos de comentários podemos fazer? Será seguro divulgar a nossa localização a cada minuto de cada hora de cada dia? Devemos ter cuidado com quem nos segue? A nossa segurança é posta em causa várias vezes ao dia, no mundo "real"; será diferente no mundo digital? Com uma incerteza na resposta a este problema filosófico, podemos estar por um lado demasiado expostos ao mundo exterior, ou demasiado inibidos de termos uma presença marcante no mundo digital, o que, para uns, é de extrema importância, e de acedermos a certas informações.

Sendo assim, é deveras necessária uma resposta concreta e fundamentada a este problema, que é o que este ensaio vem propôr.

Este ensaio pretende defender a tese de que a nossa segurança e privacidade estão, sim, comprometidas, na Internet e nas redes sociais. As redes sociais e a Internet têm vindo a crescer exponencialmente, nos últimos anos. E com um crescimento exponencial pouco regulado, pouco restrito, é fácil haver espaço para lacunas de segurança e privacidade, no que toca aos seus utilizadores. Cada vez mais, e desde idades mais tenras, as crianças e jovens têm acesso a este tipo de plataformas e espaços através dos seus dispositivos móveis. Isto causa, portanto, um grave problema: as crianças e jovens vão crescendo com estes tipos de espaços e acessos, e o seu entendimento dos mesmos vai também mudando com o passar dos anos. E porque é isto um problema? Porque, apesar do uso das redes sociais e da Internet ser algo relativamente intuitivo, há páginas a que as crianças não devem aceder, e pessoas com quem não devem conversar. Seria uma falácia da generalização precipitada afirmar que os jovens têm uma tendência para falarem com quem não devem, ou para aceder a páginas cujo conteúdo não é apropriado. Afinal, e felizmente, nem todos os jovens experienciam problemas de segurança online, nem se veem em posições de perigo, o que não quer dizer que estas, por outras circunstâncias, fora do controlo do jovem, não possam surgir. Contudo, isto não quer dizer que não haja muitos casos deste tipo, em que os jovens têm um grande papel para a sua própria colocação em perigo. Muitas vezes, os jovens acabam por cair na espetacular atuação de quem as pretende extorquir, ou raptar, levando ao envio de fotos íntimas e marcação de encontros cara-a-cara, no mundo

real, culminando em extorsões por ameaça de partilha destes conteúdos íntimos, raptos exigindo resgates de valor astronómico, porque o jovem não teve o discernimento para se colocar fora de uma situação de potencial perigo. No primeiro caso, assistimos a uma clara violação da privacidade do jovem, e no segundo, não só a sua segurança estava em causa, mas também a sua vida. Mas, neste caso, a culpa não é só dos jovens, mas também das plataformas, e de quem acompanha estes mesmos jovens. E mais, todos estes tipos de casos não acontecem apenas a jovens, mas também a adultos, idosos, a todos os indivíduos de todas as faixas etárias.

Assim, apresentando uma pequena introdução, exemplificada, ao tema da segurança e privacidade digital, é necessário apresentar argumentos mais concretos que defendam a tese proposta.

Como primeiro argumento, encontra-se o facto de não sabendo com quem se conversa, não se poder ter a certeza da intenção por detrás da interação, que não compete ao agente em estudo. Pode um jovem, quando aceita conversar com alguém que desconhece, ter a certeza que a sua segurança e privacidade não serão postas em causa? O argumento que responde a esta pergunta pode ser apresentado sob a seguinte forma:

"Se aceitamos conversar e comunicar, através do mundo digital, com alguém que não conhecemos, então não podemos ter a certeza das suas intenções, o que poderá vir a pôr em causa a nossa segurança e privacidade.

Ora, aceitamos conversar e comunicar, através do mundo digital, com alguém que não conhecemos.

Logo, não podemos ter a certeza das suas intenções, o que poderá vir a pôr em causa a nossa segurança e privacidade."

O argumento mencionado, inferido por *Modus Ponens,* mostra-se como defensor da tese proposta, já que considera que, na eventualidade de um agente aceitar conversar com alguém que desconhece, nunca poderá ter a certeza que realmente está a partilhar e permutar informações, factos e curiosidades (o que constitui uma conversa) sobre si mesmo com alguém de confiança e que tenha boas intenções. O facto de a Internet permitir, através das redes sociais, e não só, a comunicação entre desconhecidos de todos os lugares do mundo pode gerar relações muito frutíferas, mas também criar muitos perigos. Consideremos o exemplo de uma mãe

desempregada, num país subdesenvolvido, e que obteve acesso a uma rede social, através do seu telemóvel, um dos únicos bens que o antigo trabalho lhe deixou. Desesperada, esta mesma mulher entra em contacto com uma empresa através das redes sociais, que lhe promete trabalho, casa, seguro e um ordenado mais do que bom, para poder sustentar a sua família. Mas, na realidade, a mulher entrou em contacto com uma empresa que serve de fachada para uma rede mundial de tráfico de mulheres e crianças. A mulher acabou de entrar numa situação extremamente perigosa, que não só coloca a sua família em perigo, mas também a sua própria vida.

Pensemos noutro exemplo. Um jovem estava a navegar pela sua página de Instagram quando recebe uma mensagem de uma rapariga que tinha visto o seu post mais recente. A rapariga elogia a foto que o jovem postou, e enfatiza o facto de os olhos do rapaz serem de uma cor única. Os dois jovens começam a falar, estabelecendo e fazendo crescer uma relação improvável entre os dois. Passados alguns meses de conversa diária, o rapaz convida essa mesma rapariga para um encontro. Apaixonam-se perdidamente, começam a namorar, e alguns anos depois casam e vivem felizes para sempre.

O primeiro exemplo parece retirado de um filme de drama, com um fim trágico, e o segundo de um apaixonante romance, com um belo final. Qual o ponto em comum? As redes sociais. No primeiro exemplo, e que ocorre hoje em dia, vemos que a mulher foi enganada através das redes sociais e a sua segurança foi posta em causa. No segundo, dois jovens que se conheceram virtualmente, acabaram por construir uma vida a dois. Ambas estas situações poderiam ter tido finais completamente diferentes, mesmo inversos, simétricos. Mas nada garante que numa situação similar com outros agentes, estas não tenham um desfecho totalmente diferente. E, daí, advém o risco associado às redes sociais e à Internet, afinal, tanto esta nos pode trazer muitos benefícios e relações muito felizes, como o desastre, a insegurança e o perigo. De qualquer dos modos, não há garantia da intenção de quem navega no mundo online, e, por isso, há que ter muito cuidado, e navegar com a maior cautela, para evitar situações que comprometam a integridade física, mental, psicológica ou emocional de um indivíduo. Fica então provado que se não conhecermos o interlocutor de uma hipotética conversa e aceitarmos conversar com o mesmo, não podemos ter a certeza das suas intenções.

Como segundo argumento, apresenta-se a questão de aquando de uma navegação na Internet, não sabermos exatamente quais os dados que o sítio que

estamos a utilizar guarda para si, divulga com terceiros, e por quanto tempo o faz, após a nossa primeira entrada no site. Este armazenamento de dados denomina-se, na maioria das instâncias, *cookies.* Deste modo, os *cookies* são algo que pode comprometer a nossa identidade digital, e aquilo que permitimos que seja divulgado. Mas há que mencionar que a maioria dos espaços digitais, aplicações e sítios (*websites*) da internet apresentam ao utilizador uma proposta de consentimento para estes mesmos *cookies*. Mas, nesse caso, porque está a nossa segurança em causa? Por três razões principais – nem todos os sites permitem o acesso total dos utilizadores a menos que estes consintam a utilização de *cookies*, este consentimento é extremamente longo, minucioso e pouco percetível, na grande maioria dos websites (existem estudos que referem que o tempo que perderíamos a ler todos os *cookies* de todos os sítios que acessamos anualmente consumiria dias, o que simplesmente não é viável para a grande maioria das pessoas) e porque nem todos os websites têm uma política de *cookies* aberta e que não comprometa o utilizador.

Assim, e tendo todos estes fatores em consideração, é possível formular o seguinte argumento:

"Se não é percetível o que um sítio da Internet partilha em relação a um dado utilizador, e o funcionamento desse mesmo sítio requer o consentimento de partilha e armazenamento de dados (na maioria dos sítios) então nem a nossa segurança nem a nossa privacidade estão garantidas.

Ora, não é percetível o que um sítio da Internet partilha em relação a um dado utilizador, e o funcionamento desse mesmo sítio requer o consentimento de partilha e armazenamento de dados (na maioria dos sítios).

Logo, nem a nossa segurança nem a nossa privacidade estão garantidas."

Esta inferência (mais uma vez) por *Modus Ponens* permite defender a tese proposta inicialmente de que a nossa segurança e privacidade estão em risco, quando navegamos na Internet. Pelo facto de os relatórios de consentimento de *cookies* serem altamente específicos, minuciosos e longos, os utilizadores, na sua grande maioria, não prestam a devida atenção a estes e acabam por ceder à partilha e armazenamento de certos dados, cujos fins são, por vezes, incertos, o que pode comprometer a segurança e privacidade dos mesmos. Ao, por exemplo, entrarem num site cuja política de cookies envolva a cedência de dados a diversas organizações, os utilizadores arriscam-se a verem os seus dados transmitidos a

entidades e armazenados pelas mesmas por tempo definido não pelo próprio utilizador, mas pelas entidades terceiras detentoras, agora, dos dados. Esses dados ficam disponíveis, e podem constituir base para estudos falsos, manipulação de algoritmos e interferências com a vida pessoal do indivíduo. Além disso, muitos sítios não permitem o acesso de utilizadores, sem que estes forneçam uma grande quantidade de dados através de *cookies*. Isto faz com que os utilizadores, querendo aceder a algumas informações, ou a alguns conteúdos, se vejam obrigados a consentir uma partilha de dados através dos *cookies*. Em adição, como é possível garantir que estes dados são utilizados da melhor maneira por quem os detém após o consentimento do utilizador? Infelizmente, não é. O mundo digital, sendo um "mundo livre", quase semelhante a um estado por natureza, quase totalmente desregulado, sem uma entidade oficial reguladora que controle todos os acessos e garanta a segurança total dos utilizadores, pode pôr em causa a segurança e privacidade dos mesmos. Se num estado por natureza, as guerras e complicações a nível social surgiriam com muita facilidade, também no mundo digital as complicações podem emergir com facilidade. O utilizador fica desprotegido se cede os seus dados a terceiros, por vezes difíceis de identificar, o que constitui um claro atentado à segurança e privacidade do utilizador, para não mencionar as possíveis consequências da cedência destes dados, como furtos de identidade, furto financeiro, entre outros, pelo acesso a dados vitais do utilizador.

Sendo assim, ficam apresentados dois argumentos que permitem defender a tese de que a segurança de um indivíduo é, sim, posta em causa nas redes sociais e na Internet.

Mas, e se um indivíduo tiver tempo para ler e verificar todos os dados que cede e todos os terceiros a que os cede, e se apenas contactar com quem conhece? Esta objeção apresenta-se-nos como uma proposta que vem refutar a tese defendida neste ensaio. Esta mesma crítica pode formalizar-se através da seguinte inferência:

"Se um indivíduo tiver tempo para ler e verificar todos os dados que cede e todos os terceiros a que os cede, e se apenas contactar com quem conhece, então estará seguro.

Ora, um indivíduo tem tempo para ler e verificar todos os dados que cede e todos os terceiros a que os cede, e apenas contacta com quem conhece.

Logo, estará seguro."

Primeiramente, é de notar que este cenário é algo utópico, pelos factos apresentados acima, e porque todo este minucioso processo é dispendioso, em termos de tempo, e pode privar o indivíduo de certos tipos de informação. Quanto ao contacto com apenas conhecidos, essa atitude trata-se de uma escolha, que não é de todo utópica, e apenas requer alguma força de vontade e consciência. Apesar da conjunção destes dois cenários ser pouco realista, vamos assumi-la como um caso real, apenas para efeitos de estudo, não tendo esta suposição qualquer contribuição para o valor de verdade desta premissa. Começando por uma analogia algo banal, podemos ser muito cuidadosos quando saímos à rua, apenas atravessar a passadeira com o sinal verde e andar com 8 guarda-costas a rodearem-nos, a cada passo, mesmo assim, um raio atingir-nos na cabeça e ficarmos gravemente feridos, ou até morrermos. O que se pretende referir com esta analogia é que mesmo com todos os cuidados, indivíduos com maus propósitos, como hackers cujo objetivo seja furtar ou prejudicar um indivíduo, tentarão sempre levar o seu propósito avante, e, por vezes, sucederão. Até as organizações mais conceituadas e protegidas a níveis digitais sofreram perdas de informação, ataques cibernéticos, divulgação de dados, entre outros crimes. Se organizações, entidades e sistemas muito protegidos, como governos de países, empresas de telecomunicações, polícias nacionais, organizações de serviços secretos e sistemas eleitorais foram atacados, o que garante que uma pessoa cuidadosa não possa também ser? Há apenas que ter cuidado, instalar as versões mais recentes de antivírus, não clicar em links suspeitos, e não partilhar informações sensíveis, mas, mesmo assim, nada nos garante que um dia não possamos ser nós a ser atacados. A nossa proteção, segurança e privacidade são matérias de absoluta, extrema e crítica relevância, pelo que devemos navegar digitalmente com a maior das cautelas. Estamos 100% seguros? Não. Tal como no "mundo real".

Assim, refuta-se a primeira premissa de que o indivíduo estará seguro se não aceder a sítios suspeitos, nem ceder dados que não pretenda através de *cookies*, nem falar com ninguém que desconheça, já que a insegurança pode ter origem noutras situações como ataques cibernéticos não previstos. Refuta-se também a segunda premissa, pelo facto de ser utópica uma conjunção entre a total leitura e entendimento de um relatório de *cookies* e a inexistência de contacto com desconhecidos através do mundo digital, já que uma leitura integral de todos os relatórios de cookies de todos os sítios que acedemos por ano é algo inviável em

termos de tempo, mas também porque o acesso à grande maioria dos sítios requer uma parcial cedência de dados para funcionamento dos mesmos sítios. Por fim, e também para não colocar em causa a estrutura lógica desta objeção, a conclusão é falsa, porque os indivíduos, podendo contactar com este tipo de situações, não estarão seguros, pelo que é falacioso e incorreto afirmar o contrário.

E claro, nunca é demais reforçar a célebre frase, uma vez na Internet, para sempre na Internet. Os nossos posts em redes sociais, sobretudo em contas públicas ficam disponíveis para todo o globo. Todo o globo, literalmente. Por isso, não podemos apenas reduzirmo-nos a um pensamento esperançoso e demasiado otimista que nada de mal acontecerá.

Em suma, este ensaio menciona uma perspetiva de defesa da tese que a nossa segurança e privacidade estão, sim, postas em causa no mundo digital, apresentando dois argumentos defensores deste mesmo ponto de vista, o facto da segurança não estar garantida quando comunicamos com um desconhecido, e o facto dos dados cedidos e armazenados pelos websites poderem comprometer o utilizador dos mesmos. Foi também apresentada uma objeção relevante e refutada, o que enfatiza a perspetiva defendida por este ensaio e a prova ainda mais válida.

Termina então este ensaio, tendo o seu propósito de defender uma tese, que responde ao problema filosófico referido, sido servido.