Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

# Gestão da Confiança e da Privacidade em Conteúdos Gerados por Utilizadores em Redes Sociais

Fábio Rúben Teixeira Marques Gomes Pais

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Informática e Gestão

Orientador:

Professor Doutor Carlos Serrão, Professor Auxiliar,

ISCTE - IUL

Setembro, 2015

# Índice

# Índice de Figuras

# Índice de Tabelas

# Índice de Gráficos

# Termos e Abreviaturas

PLUGIN – Programa de computador utilizado para acrescentar funcionalidades a outro programa

CLOUD – Computação em nuvem; uso de memória, capacidades de armazenamento e cálculo de computadores e servidores interligados na Internet

XML – Extensible Markup Language

MPEG – Moving Picture Experts Group

DRM – Digital Rights Management

OPENSDRM – Open and Secure Digital Rights Management

IP – Internet Protocol

GPS – Global Positioning System

API – Application Programming Interface

SMS – Short Message Service

WIDGET – Pequenas aplicações que, por norma, funcionam numa determinada área de trabalho, página ou aplicação

REL – Rights Expression Language

COOKIES – Ficheiros de texto que se alojam no computador do utilizador onde se encontram dados trocados entre o navegador e os servidores das páginas a que este acedeu

BROWSER – Navegador de Internet

SND – Social Network DRM

SND EXTENSION – Extensão para *browser* do sistema SND

QR CODE – Código de Barras bidimensional

BPMN – Business Process Modeling Notation

# Resumo

A utilização de redes sociais encontra-se atualmente massificada e milhões de pessoas utilizam estas plataformas para comunicarem entre si ou partilharem os mais diversos conteúdos e experiências.

Todo o tipo de conteúdos digitais, desde fotografias, vídeos, músicas, documentos, entre outros são alojados e partilhados na *web*, cuja confiança se centra nos prestadores de serviços oferecidos por estas plataformas, que fornecem algum tipo de controlo sobre os mesmos, que pode no entanto não ser o suficiente e originar problemas no que diz respeito à privacidade dos utilizadores. O controlo sobre estes conteúdos pode ficar fora do poder de decisão dos utilizadores a partir do momento em que estes o partilham nestas redes, mesmo com as definições de privacidade que estas oferecem. As políticas de privacidade revelam como estes conteúdos poderão ser utilizados, e em muitos casos, mesmo depois de apagados, eles continuam a existir por um período de tempo indeterminado.

Com vista a criar um diferente paradigma, esta dissertação propõe o desenvolvimento de uma solução que permita oferecer um maior controlo sobre estes conteúdos, bem como uma maior privacidade e segurança na publicação dos mesmos. Para tal, será apresentada uma arquitetura e um protótipo baseados na solução tomada.

Para a sua avaliação e validação, os resultados serão recolhidos e analisados através da realização de dois inquéritos, nomeadamente sobre hábitos de utilização, segurança e privacidade nas redes sociais, e recolha de *feedback* dos testes realizados ao protótipo desenvolvido.

# Abstract

The current mass usage of social networks is done by millions of users in these platforms to communicate with friends and share the various contents and experiences.

All this digital content, from photos to videos, music and documents, are hosted and shared on the web, whose trust focuses on these services provided by these platforms, and provide some kind of control over the content, but this may not be enough, and might cause problems regarding the users' privacy. The content control might be outside the users' decision-making power from the moment they share it on these networks, even with the privacy settings that these networks offer. Privacy policies reveal how this content can be used, and in many cases, even when deleted, they continue to exist for a period of time.

In order to propose a different paradigm, this thesis proposes the development of a solution that provides a greater control over this content, and improves privacy and security settings when publishing and sharing. It will therefore be presented an architecture and a prototype based on this solution.

For their evaluation and validation, the results are collected and analyzed by conducting two surveys, particularly on social networking usage habits for users, security and privacy in social networks, and gathering feedback from the prototype testing.

**Keywords:** Social Networks, Privacy, Digital Rights Management, Content Protection, User-Generated Content, Security

# Introdução

A interação entre as pessoas tem sofrido bastantes alterações ao longo dos tempos. Nos últimos 200 anos, os avanços nas tecnologias de comunicação evoluíram e modificaram-se completamente, sendo que o resultado dos mesmos nas últimas décadas têm levantado algumas preocupações mediante os investigadores desta temática. As plataformas de redes sociais têm ganho uma enorme popularidade pela sua facilidade na comunicação seja para as relações já existentes, ou para novas relações estabelecidas *online* (Dohmen, 2012).

São milhões os utilizadores destas redes, pelo que já é um hábito diário para estas pessoas a utilização destas plataformas. Ao estarem disponíveis para os diversos tipos de públicos com várias necessidades levam à criação de diferentes tipos de ferramentas para a sua utilização, como a conectividade através de dispositivos móveis, serviços de *blogging* e partilha de fotos e vídeos (Boyd & Ellison, 2007).

Torna-se portanto importante a gestão de controlo de privacidade destes conteúdos, mediante o crescimento deste tipo de redes.

## I. Motivação e Problemas

Desde o surgimento das redes sociais que a privacidade nas mesmas tem sido sempre um assunto de debate no que toca aos conteúdos publicados pelos seus utilizadores, bem como a utilização destes e os seus fins. O problema de confidencialidade e privacidade nestas redes não se limita ao simples apagar dos conteúdos, pois estes acabam por na verdade não serem destruídos, ficando muitas das vezes apenas inativos. O promotor da rede social (Facebook, Twitter, Google, entre outras) ficará com acesso total ao conteúdo partilhado pelos utilizadores, mesmo que os mesmos já não tenham conta ativa nessa rede social. Ou seja, o controlo e detenção do conteúdo é realizado pela plataforma de rede social e não pelos seus utilizadores.

Assim, não está apenas em causa a partilha e privacidade dos conteúdos entre os utilizadores das redes sociais - está igualmente em causa o acesso que os fornecedores das plataformas de redes sociais (ou outras parceiras, entidades governamentais, entre outros) fazem dos conteúdos que os utilizadores publicam e partilham.

A configuração incorreta ou pouco informada das definições de privacidade poderá levar à exploração dos conteúdos e provocar diversos efeitos adversos à privacidade dos utilizadores de redes sociais. O acesso não controlado das plataformas em questão aos conteúdos partilhados pelos utilizadores, é igualmente um fator a considerar e a analisar neste trabalho.

De igual forma, um outro fator que motiva este trabalho prende-se no facto de se tentar perceber até que ponto os utilizadores estão dispostos a aceitar e a utilizar soluções que permitam um maior controlo de conteúdos no contexto das redes sociais, e de que forma estas soluções afetam a sua experiência na utilização das mesmas.

Como tal, a realização deste trabalho/dissertação pretende centrar-se nas seguintes duas principais questões de investigação:

- Será possível o desenvolvimento e a aplicação de mecanismos que permitam melhorar a confidencialidade e privacidade de conteúdos gerados pelos utilizadores (fotos, vídeos, e outros) e partilhados nas redes sociais?
- Qual será a aceitação dos mesmos junto dos utilizadores?

## II. Objetivos

As redes sociais fazem parte do dia-a-dia de todos os utilizadores que navegam com regularidade na Internet, quer através de dispositivos móveis, quer através dos seus próprios computadores pessoais. Estes utilizadores, além de partilharem informação que acham relevante ou do seu interesse nestas redes, na maior parte das vezes partilham conteúdos produzidos pelos próprios, sejam opiniões, fotografias ou vídeos pessoais.

Toda a forma como estes conteúdos são geridos, numa perspetiva de privacidade, são não apenas da responsabilidade da rede social, como também do próprio utilizador. No entanto, o controlo desta privacidade, em redes sociais, está muito limitado aos mecanismos de partilha e de privacidade implementados pela própria rede social. Assim, o utilizador que deseje partilhar os seus próprios conteúdos fica limitado a estes mecanismos oferecidos pela plataforma em questão.

Por outro lado, sempre que os utilizadores depositam os seus conteúdos em redes sociais, implicitamente estão a abdicar do controlo e proteção dos mesmos, sendo que mesmo que

abandonem a rede em questão, os seus conteúdos continuam acessíveis, pelo menos, para o promotor da mesma.

Este trabalho/dissertação tem como principal objetivo investigar a forma como os conteúdos depositados em redes sociais são tratados, bem como o planeamento, desenho e implementação de uma plataforma destinada à gestão da partilha e privacidade destes conteúdos, através de uma plataforma específica, assim como o desenvolvimento de um conjunto de extensões apropriadas para *web-browsers* (neste caso, para o Google Chrome) que permitam aos utilizadores interagir com conteúdos protegidos em redes sociais.

De forma a serem atingidos os resultados esperados neste trabalho, foram igualmente definidos os seguintes objetivos:

- Desenvolver uma plataforma para suportar o caso de utilização das redes sociais, criando mecanismos de proteção e de partilha que estendem os da própria rede social;
- Desenvolvimento de um protótipo de uma solução que permita implementar um maior controlo de privacidade e de partilha, centrado no utilizador (*user-centric*), na partilha de conteúdos digitais nas redes sociais;
- Testar e validar a solução junto dos utilizadores de redes sociais;

## III. Contribuição

De uma forma geral, o principal resultado a obter deste trabalho/dissertação passa por oferecer uma forma alternativa de complementar a segurança e privacidade do conteúdo que os utilizadores partilham nas plataformas de redes sociais, bem como dar mais poder aos utilizadores neste campo sobre os seus dados.

O sistema a ser desenvolvido será desenhado de forma a que se consiga integrar com as redes sociais (para este caso de estudo será utilizado a titulo de exemplo o Facebook), bem como quais as implicações que este tipo de desenvolvimento terá sobre o modo de utilização da rede social, quer a nível de utilizador, quer a nível aplicacional.

Pretende-se igualmente avaliar o impacto e aceitação junto dos utilizadores de redes sociais, assim como o impacto no modelo de negócio dos operadores das mesmas.

# IV. Metodologia

De forma a que a orientação deste projeto seja bem delineada, é necessário reunir um conjunto de regras para que o mesmo seja concluído com sucesso.

Tendo este projeto como objetivo a criação de uma solução que possa ser testada por cada pessoa de forma individual, a pesquisa realizada tem de ser baseada em estudos descritivos. Ou seja, como este projeto pretende investigar a forma como os conteúdos depositados em redes sociais são tratados, bem como o planeamento, desenho e implementação de uma plataforma destinada à gestão da partilha e privacidade destes conteúdos, é necessário que a pesquisa realizada revele os benefícios do seu desenvolvimento com clareza e que tal possa ser verificável.

Em termos metodológicos, o que mais se enquadra a este tema é o método quantitativo, pois pretende a procura da relação entre variáveis em estudo e a sua relação causa-efeito.

Para que a avaliação seja feita, é necessário a realização de dois tipos de questionário aos utilizadores de redes sociais. O primeiro questionário aborda os hábitos dos utilizadores, bem como a segurança e privacidade nas redes sociais, onde se pretende identificar os perfis de utilizadores, bem como o seu entendimento de privacidade e das políticas de privacidade nas redes sociais, quais os conteúdos que privilegiam nessas redes, e a sua abertura à utilização de mecanismos de proteção de conteúdo. Este inquérito tem como objetivo a definição de requisitos fundamentais para o desenvolvimento da solução, bem como perceber qual o conhecimento dos utilizadores de redes sociais da privacidade das redes em que estão inscritos, que ferramentas utilizam e qual a sua abertura a uma solução como a proposta nesta dissertação. O segundo inquérito, realizado após o desenvolvimento do protótipo do sistema, tem em vista a obtenção de *feedback* dos utilizadores que testaram a aplicação, e validar a sua viabilidade e receção por parte dos utilizadores. Os questionários são de resposta fechada, salvo casos específicos que se entenda como necessária algumas perguntas de resposta aberta. Os questionários e a sua posterior análise, cujos dados extraídos e análise estatística feita visam tirar conclusões sobre a utilidade da aplicação desenvolvida, bem como as funcionalidades da mesma e aceitação, ou não, pelos utilizadores da solução.

Considera-se portanto, em termos de validação desta dissertação, o *feedback* reunido junto dos utilizadores que testaram o protótipo, de forma a perceber a aceitação da solução desenvolvida perante utilizadores de redes sociais.

# Análise do Estado de Arte

De modo a perceber melhor como se encontram os estudos referentes à privacidade e gestão de direitos nas redes sociais - importante para o presente projeto - segue-se a clarificação de alguns conceitos importantes bem como o estado da segurança e definição de configurações de privacidade nas redes sociais.

## 1. Plataformas de redes sociais

As redes sociais online oferecem diversas formas de comunicação e partilha de informação e interesses pelos seus utilizadores, o que veio mudar o paradigma da comunicação ao progressivamente substituir os meios de comunicação mais tradicionais, como por exemplo o *email* (De Cristofaro et al., 2012). Uma plataforma de rede social define-se como um portal que permite aos utilizadores construir um perfil (público ou semipúblico) dentro de um sistema em que se vai inserir, articulado com uma lista de outros utilizadores com os quais partilha uma ligação (Boyd & Ellison, 2007).

### 1.1. Características e definição de plataformas de redes sociais

O que torna as redes sociais tão únicas não é o facto de permitir aos utilizadores conhecerem "estranhos", mas sim permitir articular e tornar visíveis as suas redes sociais. Isto pode resultar em ligações entre pessoas que de outra forma não seria possível. No entanto, não é esse o objetivo principal destas redes, e estes encontros são frequentemente entre laços latentes (*latent ties*) que partilham alguma "ligação *offline*". Em muitas das grandes redes sociais, os seus utilizadores não estão necessariamente à procura de conhecer novas pessoas - estes utilizadores usam em grande parte estas redes para comunicar com pessoas que já fazem parte do seu grupo social (Boyd & Ellison, 2007).

Muitas destas plataformas permitem portanto a manutenção das próprias redes sociais criadas pelos utilizadores, facilitando assim a sua comunicação interna. Embora nas grandes redes o foco passe por manter estas redes e aumentar a sua comunicação, algumas destas plataformas atraem utilizadores dos mais variados tipos, ou por determinadas crenças ou *hobbies*, gostos, costumes, ou mesmo pela presença ao mesmo país de origem (Francisco, 2012). Estas plataformas têm por norma incorporar novas ferramentas de comunicação e informação,

como a relação de conectividade entre dispositivos móveis, serviços de *blogging* e/ou partilha de vídeos/fotos (Boyd & Ellison, 2007).

Todas as plataformas de redes sociais requerem a criação de um perfil pessoal. O utilizador deve criar o perfil, individual ou de grupo, de forma a interagir e utilizar as funcionalidades e conteúdos da plataforma (Marques & Serrão, 2014).

Embora estas plataformas de redes sociais tenham implementado mais funcionalidades ao longo do tempo, a sua base mantém-se constante, isto é, na visualização de um perfil de utilizador da plataforma que é articulado com a lista de "amigos" que também são utilizadores do sistema. Consideram-se "amigos" os utilizadores do sistema onde estão registados e estabelecem uma relação com o proprietário do perfil (Boyd & Ellison, 2008). O perfil consiste numa página única que pertence ao seu respetivo utilizador e onde são inseridas informações sobre o mesmo, pelo próprio. No ato do registo do utilizador, são colocadas várias questões com vista na obtenção de informação individual. O perfil é então gerado tendo por base esse conteúdo, onde estão tipicamente incluídas informações referentes à idade, localização, interesses culturais, desportos preferidos, descrições de algumas características que o utilizador considere importantes a colocar na secção "Sobre mim", entre outras (Francisco, 2012).

A maioria destas plataformas encoraja os seus utilizadores a fazer o *upload* da sua foto de perfil. Algumas plataformas permitem que os utilizadores enriqueçam os seus perfis ao adicionar conteúdos multimédia ou modificar o aspeto do seu perfil. O Facebook, por exemplo, permite a adição de módulos ("Aplicações") que enriquecem o seu perfil. (Boyd & Ellison, 2007). Entre estas aplicações encontram-se questionários sobre variados temas (cinema, música, desporto, entre outros), jogos, calendários com alertas, eventos, entre outras dos mais variados tipos (Francisco, 2012).

A visibilidade de um perfil de rede social depende de plataforma para plataforma, mediante as configurações definidas pelos seus utilizadores, podendo já estar de igual forma definidas as definições padrão (Boyd & Ellison 2007).

A disponibilização pública das conexões é um componente crucial das plataformas de redes sociais. A lista de amigos contém ligações para o perfil de cada amigo, permitindo aos utilizadores navegar na rede ao clicar sobre estas listas. Na maioria destes portais, a lista de amigos é visível para qualquer utilizador que tenha permissões de visualização do perfil, embora possam existir exceções (Boyd & Ellison, 2007).

Tipicamente existem opções de privacidade da própria rede que permitem omitir as listas de amigos no seu perfil e a maioria das redes sociais providencia um mecanismo que permite aos utilizadores deixarem mensagens nos perfis dos seus amigos - esta funcionalidade envolve geralmente a opção de deixar comentários, embora várias plataformas caracterizem esta funcionalidade com outras designações. Para além disto, estas plataformas também oferecem frequentemente serviços de mensagens privadas similares ao *webmail* (Boyd & Ellison, 2007).

Além dos perfis, amigos, comentários e mensagens privadas, as plataformas de redes sociais diferenciam-se bastante em termos de funcionalidades e base de utilizadores. Algumas providenciam partilha de fotos e/ou vídeos, outras disponibilizam serviços de *blogging* e *instant messaging* embutidos (Boyd & Ellison, 2007).

### 1.2. Redes sociais e privacidade

A relação entre privacidade e a rede social de uma pessoa é multifacetada. Por vezes, apenas queremos que certa informação sobre nós apenas seja conhecida por um pequeno grupo de amigos próximos e não por estranhos. Por outro lado, por vezes o inverso pode verificar-se, onde revelamos informação pessoal a estranhos, mas não àqueles que nos conhecem melhor (Gross & Acquisti, 2005).

#### 1.2.1. Redes sociais *online* e redes sociais *offline*

É importante referir as diferenças entre redes sociais *offline* e as plataformas de redes social, nomeadamente as *online*. Em primeiro lugar, as redes sociais *offline* são criadas através de ligações entre as pessoas por via tradicional, que podem ser vagamente categorizadas como fracas ou fortes, mas na realidade são extremamente diversas em termos do quão íntimas ou próximas as relações das pessoas podem ser. Por sua vez, as redes sociais *online* reduzem estas nuances para relações binárias: “Amigo ou não”. Em segundo lugar, o número de relações fortes que uma pessoa pode manter numa plataforma de rede social pode não aumentar significativamente através destas redes. Em terceiro lugar, enquanto uma rede social *offline* pode incluir até uma dúzia de relações íntimas ou relações significativas e entre 1000 a 1700 interações, uma rede social *online* pode listar centenas de “amigos” diretos e incluir

centenas de milhares de amigos adicionais com apenas três graus de separação de uma pessoa (Gross & Acquisti, 2005).

As redes sociais *online* são mais vastas e têm, em média, ligações mais fracas entre as pessoas do que as redes sociais *offline*. Por outras palavras, centenas de utilizadores podem ser classificados como amigos de amigos de um indivíduo e poder ter acesso à sua informação pessoal, enquanto que, ao mesmo tempo, a forma de quantificar um amigo da rede social de um indivíduo é baixa. Isto pode tornar a rede social *online* apenas uma comunidade imaginária. Portanto, a confiança numa rede social *online* pode diferir e ter um significado diferente de uma rede social *offline*. As redes sociais *online* são também mais niveladas, pois a mesma informação pode ser transmitida a um número elevado de amigos interligados à pessoa em causa, em níveis de ligação diferentes. Enquanto que a privacidade pode ser considerada conducente para a intimidade, a confiança pode diminuir dentro de uma rede social online, mas ao mesmo tempo, uma nova forma de intimidade espalha-se, isto é, a partilha de informação pessoal a larga escala e a potenciais números desconhecidos de amigos e estranhos juntos na rede (Gross & Acquisti, 2005).

### 1.2.2. Privacidade nas redes sociais

As plataformas de redes sociais já têm implementadas por predefinição um conjunto de controlos de segurança e privacidade para os conteúdos partilhados, no entanto são limitados. As grandes plataformas oferecem a possibilidade aos utilizadores de partilharem o seu conteúdo sobre regras de privacidade específicas, que são definidas pela própria plataforma e não pelo utilizador. Estas regras são, por norma, extremamente permissivas e diferem de plataforma para plataforma, e 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).

Podem ser definidas duas categorias diferentes de forma a perceber quais os tipos de conteúdo com os quais uma rede social é capaz de lidar: conteúdo direto e conteúdo de atividade. O conteúdo direto inclui toda a informação que está disponível na plataforma diretamente pelo utilizador. O conteúdo de atividade inclui informação que não é colocada diretamente na plataforma devido ao uso de serviços pelos utilizadores. Um exemplo disso é o endereço IP, pois trata-se de uma informação que é fornecida indiretamente (Marques & Serrão, 2014).

Embora a maioria das plataformas de redes sociais forneça mecanismos de proteção de partilha, não está garantido que o conteúdo dos mesmos esteja realmente protegido, mesmo que o utilizador o apague da rede. Redes sociais como o Facebook, Twitter e Google+ fornecem aos utilizadores alguma customização de definições de privacidade. Por outras palavras, os utilizadores podem especificar que utilizadores podem aceder e visualizar o seu conteúdo (Marques & Serrão, 2014).

No entanto, fora de uma rede social, um utilizador não determina a visibilidade de conteúdos pessoais pelo seu formato, mas sim pelo seu contexto, o que tornaria interessante para redes como o Facebook, a implementação de proteções através de contexto previsto, de modo a que cada conteúdo tivesse a sua respetiva proteção por definição ajustada ao seu contexto (Madejski et al., 2011).

Os provedores de redes sociais *online* devem salvaguardar o conteúdo dos seus utilizadores. Caso isso falhe, a sua reputação fica manchada e pode resultar em ações legais. Por exemplo, os termos de uso do Facebook referem que os conteúdos dos utilizadores estão definidos como "públicos" por defeito. Isto levantou várias preocupações em termos de privacidade, como por exemplo, pela US Federal Trade Commission. O conteúdo depositado nas plataformas de redes sociais pode estar sujeito a *break-ins*, ataques por alguém de dentro ou mesmo intimações por questões legais (Marques & Serrão, 2014).

A identificação de utilizadores em diferentes redes sociais também pode ser feita através da comparação de conteúdos, e principalmente através da identificação de caras em fotos. Isto põe em causa principalmente as redes onde são utilizados pseudónimos para manter a anonimidade. Liu e Maes estimam que existe 15% de sobreposição de fotos em duas das maiores redes sociais que estudaram (Liu & Maes, 2005). Como os utilizadores reutilizam com frequência fotos iguais ou similares em redes diferentes, essa identificação é exequível (Gross & Acquisti, 2005).

A informação identificável que é publicada fica portanto, em primeira instância, no portal alojador, que pode usar a informação em diversas formas, normalmente definidas nos termos de utilização e política de privacidade da rede. A informação fica também de igual forma disponível na própria rede, cujo tempo em que está exposta não é de todo conhecido. A facilidade de acesso à rede social e potencial falta de segurança no acesso às redes pode também fazer com que terceiros, desde *hackers* a agências governamentais, acedam à informação sem colaboração direta com a própria rede. (Gross & Acquisti, 2005).

Os riscos de privacidade aumentam pela prática comum de efetuar *caching* de conteúdo e este ser guardado *offline*, mesmo quando os conteúdos foram explicitamente apagados pelo utilizador. A informação de privacidade dos utilizadores pode ser bastante valiosa. Existem dois métodos principais para a utilização de informação recolhida das plataformas de redes sociais: mudança de mãos e uso para o benefício de outro. Quando a informação é valiosa é bastante aliciante a sua venda, principalmente quando gera um grande lucro (Marques & Serrão, 2014).

A informação retirada destas redes e a sua utilização pode portanto variar dependendo do tipo que se trata, e pode ser extensiva e intima. O risco pode ir desde roubo de identidade, perseguição física e/ou *online*, ou até mesmo para questões de chantagem (Gross & Acquisti, 2005).

### 1.3. Legislação existente e diferenças regionais

Existem diversas preocupações em termos da privacidade *online*, que levam a diferentes respostas de diferentes partes do mundo. No que se refere às principais diferenças e abordagens feitas pelos Estados Unidos da América, Europa e Japão, tanto na Europa como no Japão existem regulamentações e documentos que garantem estes direitos, referidos na Constituição Europeia, e como parte do *Japanese Act Concerning Protection of Personal Information*. No entanto, não existe regulamentação universal relativamente aos Estados Unidos, embora a administração de Obama tenha tentado alterar essa abordagem (Kugler, 2015).

Estas diferenças criam desafios de conformidade para empresas internacionais, especialmente para empresas norte-americanas que operem em regiões com restrições de privacidade mais apertadas, como por exemplo, o caso da Google junto dos reguladores europeus, devido às suas práticas de recolha de dados (Kugler, 2015).

Enquanto os Estados Unidos utilizam um modelo autorregulatório, a Europa favorece explicitamente as leis definidas. Um exemplo do modelo autorregulatório é o *Advertising Self-Regulatory Council* (ASRC), que sugere que seja colocado um ícone ao lado de um anúncio publicitário numa página Web, que deverá ter um *link* com a explicação de todo o tipo de informação que é recolhida, mas, no entanto, não existe nenhuma obrigação no seu cumprimento. No entanto, é de notar que enquanto os Estados Unidos têm como maior

preocupação a vigilância governamental, a União Europeia encontra-se mais preocupada com quem reúne os dados pessoais (Kugler, 2015).

Relativamente à União Europeia, o *Charter of Fundamental Rights of the European Union* refere explicitamente as suas provisões relativamente à proteção de dados, no artigo 8: "Todos têm o direito à proteção dos seus dados pessoais. Tais dados devem ser processados de forma justa e para propósitos específicos e com base no consentimento da pessoa envolvida ou noutra base legitima prevista na lei". Os princípios da União Europeia cobrem todos os seus estados membros, mas as suas práticas são feitas país a país (Kugler, 2015).

Por fim, a lei existente no Japão requere que as empresas que gerem as informações pessoais devem especificar a razão e o propósito para o qual estes as estão a reunir, e proíbe que que esta possa ser alterada enquanto ainda exista uma relação substancial para o seu uso, e proíbe ainda que o armazenamento de dados seja feito para além do que é necessário para atingir o seu uso sem o consentimento do utilizador (Kugler, 2015).

Com as fronteiras mundiais de dados a tornarem-se cada vez mais permeáveis, com empresas e governos a reunirem cada vez mais dados, torna-se importante que as diferentes regiões estejam alinhadas sobre estes problemas (Kugler, 2015).

## 2. Definições e controlo de privacidade das redes sociais

As redes providenciam aos seus utilizadores definições de privacidade costumáveis, como por exemplo especificar que grupos podem aceder aos seus conteúdos. A informação deve poder ser classificada por categorias, como texto, foto ou vídeo, e para cada categoria o utilizador pode definir a sua lista de permissões de acesso. No entanto, esta estratégia baseia-se principalmente na confiança dos utilizadores nas redes e na forma como estes tratam os seus dados, pois é neles que estão alojados (De Cristofaro et al., 2012), sejam dados que ainda continuam disponíveis na rede, ou dados que já tenham sido apagados, mas que podem continuar armazenados na rede.

Os prestadores das redes sociais são geralmente incentivados a salvaguardar os conteúdos dos seus utilizadores de forma a não danificar a sua reputação e ações legais. No entanto, existem acordos de utilizador (*user agreements*) que podem incluir cláusulas de permissão do seu acesso a terceiros. Os riscos são ainda maiores quando o conteúdo fica guardado em *cache* ou guardado *offline*, mesmo quando os utilizadores o apagam, tornando-se numa ameaça para a privacidade do utilizador (De Cristofaro et al., 2012).

Os padrões de informação pessoal em termos de privacidade são por norma variáveis nas redes sociais. A presença da identificabilidade do utilizador pode variar de rede para rede, sendo que enquanto algumas possam permitir a utilização de pseudónimos, outras é necessário a identidade real. O tipo de informação revelado nas redes circula em torno dos interesses e gostos dos utilizadores, sendo que o conteúdo pode ser explorado de diferentes formas, resultando em informação semipública, informação privada, e informação *open-ended* (Gross & Acquisti, 2005).

Informação semipública refere-se à situação atual do utilizador de domínio que poderá ser conhecido, como por exemplo escola atual ou escola que já frequentou. Informação privada centra-se em informação mais pessoal do utilizador, como por exemplo hábitos e preferências. Informação *open-ended* refere-se a informação de acesso aberto, como uma publicação feita pelo utilizador num blogue (Gross & Acquisti, 2005).

Por fim, a visibilidade é altamente variável, dependendo das características de privacidade inerentes à rede, podendo estar disponível publicamente, apenas para utilizadores da mesma rede, ou mesmo apenas para o próprio utilizador, se assim o pretender.

## 2.1. Controlo de privacidade

As oportunidades de interação e comunicação nas plataformas de redes sociais são vastas, contudo, o crescimento associado à oferta destas redes levanta novos desafios no que toca à privacidade (Gross & Acquisti, 2005). Portanto, torna-se importante e necessário perceber como as plataformas de redes sociais lidam com a privacidade e como a controlam. Para tal analisou-se as redes que apresentam um maior número de utilizadores.

### 2.1.1. Facebook

Fundado em 2004, o Facebook é uma plataforma de rede social com o intuito de oferecer às pessoas ferramentas de partilha de conteúdos e de conexão entre amigos e família.

O Facebook tem em média cerca de 864 milhões de utilizadores ativos, 703 milhões de utilizadores diários ativos, em média, através de dispositivos móveis, 1.350 milhões de utilizadores mensais ativos, 1.120 milhões de utilizadores mensais ativos através de dispositivos móveis, e aproximadamente 82.2% dos utilizadores ativos diários são de fora dos Estados Unidos da América e Canadá (Facebook Company Info, 2014).

#### 2.1.1.1. Política de privacidade do Facebook

O Facebook armazena diversos tipos de informação, entre os quais:

- Informação de registo, como o nome, *email*, morada, data de nascimento e sexo, sendo que em alguns casos é necessário solicitar mais informação, como por exemplo, o numero de telefone (Facebook Data Use Policy, 2014);
- Informação que o utilizador decide partilhar, como atualizações de estado, fotos ou comentários no perfil de um amigo. Também inclui informação quando o utilizador comunica com a plataforma, tal como quando adiciona um amigo, faz gosto de uma página ou *website*, usa importadores de contactos ou indica que está numa relação (Facebook Data Use Policy, 2014);
- Informação que os outros elementos da rede partilham com o utilizador, como por exemplo quando publicam uma foto em que identificam (*tag*) o utilizador ou numa atualização de estado, de localização, ou quando é adicionado a um grupo. Outras pessoas que utilizam o Facebook podem guardar informação acerca do utilizador,

nomeadamente quando criam e gerem os seus convites e contactos (Facebook Data Use Policy, 2014);

- Outro tipo de informação, como por exemplo, quando um utilizador visita um perfil de outro, envia ou recebe uma mensagem, pesquisa por um amigo ou página, coloca fotos ou vídeos com *metadata* adicional (hora, data, local), informação do computador, telemóvel ou outros dispositivos que tenham aplicações do Facebook instaladas ou acedidas, informações de jogos que utilizam a plataforma do Facebook ou páginas que têm funcionalidades do Facebook (como o *plugin* social) (Facebook Data Use Policy, 2014).

Conforme descrito no Data Use Policy do Facebook, a informação é recolhida de forma a que a rede possa oferecer e sugerir uma variedade de serviços e funcionalidades, como por exemplo sugestões de amigos ou sugerir identificações em fotos. Também pode ser recolhida informações referentes à cidade atual com o GPS, ou outra informação como publicações aos amigos da rede que poderão ser do seu interesse. É garantido pela rede que a localização GPS apenas é mantida até que seja útil para os serviços, como por exemplo manter as ultimas coordenadas GPS para enviar notificações relevantes (Facebook Data Use Policy, 2014).

O Facebook ainda revela informação dos utilizadores aos parceiros de publicidade ou clientes depois de remover o nome dos utilizadores ou qualquer informação que identifique o utilizador em questão, ou tem informação combinada com outros utilizadores, de forma a que não haja qualquer ligação. A rede ainda identifica como "informação pública" aquela que o utilizador decide tornar pública, bem como informação que está sempre definida como tal. Essa informação fica disponível para qualquer pessoa, o que significa que esta pode estar associada ao utilizador em questão mesmo fora do Facebook, surgir no motor de pesquisa da rede ou num motor de pesquisa público, pode estar acessível nos jogos integrados com o Facebook e/ou aplicações/*websites* que o utilizador ou os seus amigos usam, e pode ainda estar acessível a qualquer pessoa que use as APIs da rede. Ainda é referido que por vezes poderá não ser possível alterar as definições do conteúdo, como por exemplo, quando uma publicação ou comentário é feito numa Página, isto porque poderão ser sempre publicações públicas e estão definidas como tal. Por regra, sempre que não é possível ver o ícone de partilha, a informação estará publicamente disponível. Entre a informação que está sempre disponível publicamente encontra-se o nome, foto de perfil e de capa, redes, sexo, *username* e *user ID* (Facebook Data Use Policy, 2014).

O *username* e o *user ID* são a forma do utilizador se identificar na rede social. O *user ID* é composto por um conjunto de números e o *username* é tipicamente uma variação do nome do utilizador. O *username* permite assim a criação de um *link* personalizado do utilizador à rede (exemplo: www.facebook.com/username), facilitando assim a sua partilha. O *username* permite o acesso por terceiros ao perfil do utilizador, podendo recolher a informação definida como pública, e ser utilizada nas APIs da rede. O acesso pode ser restringido pelo utilizador através das definições de privacidade da rede (Facebook Data Use Policy, 2014).

O Facebook disponibiliza também um endereço de *email* aos seus utilizadores através do seu *username*, nomeadamente username@facebook.com, permitindo assim utilizar o serviço de mensagens da rede (Facebook Data Use Policy, 2014).

Ainda é disponibilizada a opção de desativar ou apagar a conta. A desativação da conta implica que esta seja colocada em inatividade, não estando mais acessível aos utilizadores da rede. No entanto, neste estado, a conta não se encontra apagada, podendo ser novamente reativada pelo utilizador e todo o seu conteúdo. A opção de apagar é permanente, pelo que pode demorar até um mês para ser apagada, mas no entanto, certas informações e conteúdos poderão ficar guardadas em cópias de *backup* e *logs* até 90 dias. O Facebook refere ainda que informações como publicações em grupos e envio de mensagens não são apagadas porque não são guardadas na própria conta (Facebook Data Use Policy, 2014).

### 2.1.2. Twitter

O Twitter é uma plataforma de rede social de *microblogging*, cujas partilhas (*tweets*) não podem conter mais que 140 caracteres. A rede permite ainda a partilha de imagens, e de vídeos de 6 segundos através da plataforma Vine. O Twitter tem ainda 284 milhões de utilizadores mensais ativos, cerca de 500 milhões de *tweets* enviados por dia, acessos de 80% dos seus utilizadores ativos através de dispositivos mobile e 77% de contas de utilizadores fora dos Estados Unidos da América (About Twitter, 2014).

#### 2.1.2.1. Política de privacidade do Twitter

A política de privacidade do Twitter descreve como e quando a rede social reúne, usa e partilha a informação dos seus utilizadores nos seus serviços. Essa informação pode ser recolhida através de websites, SMS, APIs, notificações de *email*, aplicações, botões, *widgets*,

publicidade e serviços de comércio, parceiros e terceiros. Um exemplo dado pela rede é o envio ou receção de publicações via SMS ou o acesso à rede através de aplicações para esse efeito (Twitter Privacy Policy, 2014).

Mais detalhadamente, a informação recolhida passa por:

- Informação básica da conta: Entre estes dados está incluído o nome, *username*, *password* e endereço de email. Em alguns casos poderá ser solicitado o número de telefone, como por exemplo, para usar o Twitter via SMS ou para prevenir *spam* e/ou ações de fraude e/ou abuso. O nome e *username* são listados publicamente nos serviços, incluindo a página de perfil e resultados de pesquisa, sendo que alguns serviços, como a pesquisa e os perfis públicos não necessitam de registo na rede (Twitter Privacy Policy, 2014);
- Informação adicional: O utilizador pode fornecer informação adicional à rede de forma a torná-la pública, como uma curta biografia, localização, *website* ou uma imagem. A informação pode ser utilizada pela rede para o envio de informação sobre serviços do Twitter. Estas notificações podem ser desabilitadas nas definições da conta. Podem ser criadas restrições ao acesso a esta informação através das configurações de controlo de privacidade. O utilizador pode ainda importar a sua lista de contactos para o Twitter de forma a identificar quais dos seus contactos estão registados na rede. Informação adicional poderá também ser enviada no acesso a um serviço com ligação à conta do Twitter. A rede assegura que quando é feita a desconexão, esta é apagada algumas horas depois (Twitter Privacy Policy, 2014);
- Tweets, Seguir, Listas e outra informação pública: Entre esta informação encontram-se as publicações feitas na rede (*tweets*), bem como listas de seguidores e toda a sua *metadata* associada, como favoritos, *retweets*, e outra informação que pode resultar de utilização de serviços da rede. Os serviços da rede disseminam instantaneamente a informação pública a um elevado alcance de utilizadores, clientes e serviços. Por predefinição, esta informação está definida como pública, podendo ser alterada para privada nas definições (Twitter Privacy Policy, 2014);
- Informação de localização: Ao conteúdo publicado pode ser enviada igualmente a sua localização. Outros dados podem ser utilizados para determinar a localização como, por exemplo, informação de redes *wireless* ou o endereço de IP. Esta informação pode ser ainda utilizada para os serviços da rede, bem como para revelar informação mais

relevante como publicidade, tendências locais (*local trends*), histórias, e sugestões de pessoas para seguir (Twitter Privacy Policy, 2014);

- Ligações *(Links)*: O Twitter pode guardar as interações com os links partilhados nos serviços da rede, incluindo notificações de *email*, serviços de terceiros e aplicações, através de redireccionamento de cliques ou outros meios (Twitter Privacy Policy, 2014);
- *Cookies*: A rede pode utilizar *cookies* de sessão e *cookies* persistentes para monitorizar o tráfico para os serviços e as atividades na rede dos utilizadores e para melhorar os seus serviços. As alterações em termos de *cookies*, relativamente à sua disponibilização, devem ser feitas ao nível do browser (Twitter Privacy Policy, 2014);
- Log Data: Informação como o endereço de IP, tipo de *browser*, sistema operativo, página web referente, páginas visitadas, localização, rede móvel, informação do dispositivo, termos de pesquisa e informações de pesquisa podem ser recebidos pelo Twitter, ao que se chama de Log Data. O uso desta informação pode ser utilizada, por exemplo, para interagir com os serviços da rede. Pode ser ainda utilizada para fornecer, perceber e melhorar os serviços. Esta informação pode ser apagada num espaço de 18 meses (Twitter Privacy Policy, 2014);
- *Widget Data*: Informação referente aos *widgets* da rede, nomeadamente *websites* de terceiros que integrem botões ou *widgets* do Twitter, pode ser recebida pela rede e incluir a página web visitada e o cookie que identifica o *browser*. O processo de eliminação destes dados é feito num prazo máximo de 10 dias (Twitter Privacy Policy, 2014);
- Serviços de comércio: Guardam informação relativamente a transações e compras feitas no Twitter. Entre a informação fornecida está o cartão de crédito/débito, data de expiração do cartão, código CVV, morada de pagamento e morada de entrega. As definições de privacidade destes dados podem ser alteradas através das definições da conta, bem como a sua remoção (Twitter Privacy Policy, 2014);
- Terceiros e parceiros: O Twitter utiliza uma variedade de serviços de terceiros para melhorar os seus serviços, como o alojamento dos *blogs* e *wikis*, e melhorias do uso dos serviços, como o Google Analytics. Os prestadores de serviços de terceiros podem recolher informação fornecido pelo *browser*, como cookies ou o endereço de IP. Os parceiros de publicidade podem partilhar informação como o URL de páginas visitadas, ID do dispositivo móvel utilizado de forma a melhorar os anúncios a

mostrar. Os utilizadores podem desligar os anúncios (*tailor ads*) através das definições de privacidade, de forma a que a sua informação não seja enviada para os parceiros de publicidade (Twitter Privacy Policy, 2014).

A política de privacidade do Twitter descreve ainda de que forma a informação dos seus utilizadores pode ser partilhada. Esse conteúdo é partilhado mediante o consentimento do utilizador, quando este autoriza, por exemplo, em aplicações de terceiros; prestadores de serviços, como a monitorização de pagamentos em serviços; mediante a lei, regulação e por requisito legal; afiliações e transações de negócios, nas situações de falência, aquisição, fusão, reorganização ou venda de bens do Twitter; e por fim, informação não-privada e não-pessoal, com por exemplo o perfil público de utilizador ou *tweets* públicos (Twitter Privacy Policy, 2014).

### 2.1.3. Google+

O Google+ é a plataforma de rede social da Google, com funcionalidades semelhantes ao serviço prestado pelo Facebook, e incorpora todos os serviços disponíveis na plataforma Google.

#### 2.1.3.1. Política de privacidade do Google+

O Google+ explica na sua política de privacidade que, por ser criada uma conta Google e esta estar associada aos vários serviços da empresa, a informação partilhada na rede dá a possibilidade de os melhorar, apresentar anúncios e resultados de pesquisa mais relevantes, ajudar no contacto com as pessoas e ainda a possibilidade de uma partilha de informação mais rápida e fácil (Política de Privacidade Google, 2014).

Entre a informação recolhida, o Google referencia:

- Informações que o utilizador fornece, como a informação fornecida na inscrição de uma conta Google, como os dados pessoais (nome, endereço de email, numero de telefone, cartão de crédito), bem como a criação de um Perfil do Google, que será publicamente visível (Política de Privacidade Google, 2014);
- Informações recolhidas da utilização dos serviços Google, como a visualização de um vídeo no YouTube ou interação com os anúncios. Entre a informação recolhida

encontram-se detalhes de como são utilizados os serviços, informações de registo telefónico, endereço IP, informações de eventos do dispositivo (falhas, atividades de sistema, entre outros), e *cookies* (Política de Privacidade Google, 2014);

- Informações de localização, através do endereço de IP, GPS, ou outros sensores;
- Números de aplicações exclusivos, para atualizações automáticas das aplicações nos dispositivos (Política de Privacidade Google, 2014);
- Armazenamento local, como armazenamento web do *browser* e cache de dados de aplicações (Política de Privacidade Google, 2014);
- *Cookies* e identificadores anónimos (Política de Privacidade Google, 2014).

A informação é utilizada para disponibilizar, manter, proteger e melhorar os serviços Google e desenvolver novos serviços, podendo ser utilizada para questões de identificação nos serviços, ações da própria rede, como marcações com +1, críticas escritas e comentários publicados. É também mantido o registo de comunicações feitas com a Google, referindo que o endereço de *email* pode ser utilizado para enviar informações acerca dos serviços (Política de Privacidade Google, 2014).

A Google refere ainda a transparência e escolha, dado a opção do utilizador tomar decisões relativamente à forma como as suas informações são utilizadas, podendo este:

- Consultar e controlar determinados tipos de informações associadas à conta Google através do painel de controlo;
- Ver e editar as suas preferências relativamente aos anúncios que vê na rede e em toda a internet;
- Utilizar o editor da Google para ver e ajustar o seu perfil;
- Controlar com quem partilha as suas informações:
- Retirar informações dos serviços que pretende;
- Escolher se pretende que o nome e fotografia do perfil apareçam em recomendações partilhadas apresentadas em anúncios.

É referindo ainda que conteúdos relacionados com *cookies* podem ser bloqueados através do *browser* do utilizador, sendo este alertado que alguns serviços poderão não funcionar corretamente se estes estiverem desativados (Política de Privacidade Google, 2014).

No acesso às informações dos utilizadores e respetiva atualização pode ser solicitado a confirmação da sua identidade, de forma a manter a informação coerente. A Google reserva-

se ao direito de recusar pedidos demasiado repetitivos e que prejudiquem a privacidade de terceiros (Política de Privacidade Google, 2014).

Entre as informações partilhadas, estas podem ser feitas com conhecimento do utilizador, com administradores de domínio, para processamento externo, e por motivos legais (Política de Privacidade Google, 2014).

Em termos de segurança, a informação publicada é encriptada pelos serviços da Google utilizando SSL, confirmação em dois passos para o acesso à conta Google, revisão das práticas de recolha, processamento e armazenamento de informações, e restrição do acesso a informações pessoais a funcionários (Política de Privacidade Google, 2014).

### 2.1.4. Instagram

O Instagram é uma plataforma de partilha de conteúdo multimédia, nomeadamente fotografias e vídeos curtos (15 segundos). A rede é composta por mais de 300 milhões de utilizadores mensais ativos e tem mais de 70 milhões de partilhas diárias de fotografias e vídeos (Instagram Press Page, 2014).

#### 2.1.4.1. Política de privacidade do Instagram

Na sua política de privacidade, o Instagram refere que esta explica a forma como a rede e os seus parceiros reúnem, usam, partilham e protegem a informação relativa aos seus serviços móveis, *website*, e qualquer software ou conexão feita aos serviços do Instagram. O utilizador ao utilizar o serviço concorda que a rede permite ao utilizador publicar conteúdo, incluindo fotos, comentários e outro tipo de materiais, descrito como "conteúdo do utilizador (*user content*)" e o partilha publicamente, bem como o fato da política de privacidade ser transversal a todos os visitantes, utilizadores, e outros que usem o serviço. (Instagram Privacy Policy, 2013)

Entre a informação recolhida pelo Instagram encontra-se:

- Informação fornecida diretamente à rede, como o *username*, *password* e endereço de email no ato do registo, perfil de utilizador (primeiro e último nome, fotografia, número de telefone), conteúdo de utilizador (nomeadamente fotos, comentários, entre

outros publicados na rede), e comunicações entre o utilizador e o Instagram, como por exemplo, verificação de conta, mudanças e atualizações do serviço;

- Encontrar amigos no Instagram através da lista de contactos, aplicações de terceiros ou pesquisa por nomes e *usernames* na rede;
- Informação analítica, através de ferramentas de terceiros de forma a que a rede possa medir o tráfego e tendências de uso do serviço. A informação recolhida é enviada do dispositivo ou do serviço, incluindo páginas visitadas, *add-ons*, ou outra informação que permita a melhoria do serviço;
- *Cookies* e tecnologias similares;
- Identificadores de dispositivos;
- *Metadata*, incluíndo *hashtags*, *geotags*, comentários ou outros dados.

A informação é utilizada pelo Instagram essencialmente para melhorar a própria rede, desenvolver e testar novos produtos e fornecer conteúdos personalizados e informação para o utilizador e outros, que pode incluir anúncios *online* e outras formas de marketing (Instagram Privacy Policy, 2013).

A informação armazenada e publicada na rede pode ser partilhada a afiliados do Instagram e negócios que fazem parte da rede da empresa. A informação partilhada pode ser usada para fornecer, perceber e melhorar o próprio serviço e dos afiliados. A informação pode ser ainda fornecida através de *cookies*, ficheiros de *log*, identificadores de dispositivos e dados de localização, com a ajuda de organizações terceiras que ajudam na prestação do serviço (Instagram Privacy Policy, 2013).

Certa informação pode também ser enviada para parceiros de publicidade de forma a fornecer anúncios que vão ao interesse do utilizador em questão. Podem ser de igual forma removidos certos dados que possam identificar o utilizador, sendo que esta informação é tornada anónima e partilhada com outros parceiros, sendo esta combinada com outra informação não relacionada com o utilizador de forma a garantir o anonimato (Instagram Privacy Policy, 2013).

Em caso de venda ou transferência do Instagram para outra entidade, os conteúdos dos utilizadores poderão estar entre os bens a transferir, no entanto, o conteúdo continua a pertencer ao utilizador e a nova entidade deverá comprometer-se à política de privacidade (Instagram Privacy Policy, 2013).

A informação guardada no Instagram dos utilizadores pode estar guardada e processada nos Estados Unidos da América ou outro país onde o Instagram, Afiliados ou prestadores de serviços tenham instalações, pelo que a informação dos utilizadores pode ser deslocada para outro país caso seja necessário perante a lei do país em específico (Instagram Privacy Policy, 2013).

A rede ainda proporciona definições de privacidade, que permitem a atualização da conta de utilizador, retirar subscrição de comunicações *email* do Instagram, exceto comunicações relacionadas com o serviço. Os conteúdos podem ser mantidos mesmo depois de serem apagados por questões de *backup*, arquivo ou auditorias (Instagram Privacy Policy, 2013).

### 2.2. Comparação entre as diferentes políticas de privacidade

As plataformas de redes sociais analisadas apresentam-se bastante similares em diversos aspetos, tendo estas como principal intuito o estabelecimento de comunicação entre pessoas através de uma comunidade.

Apesar de terem alguns propósitos distintos, são semelhantes no que toca ao seu público-alvo, criação de perfis de utilizador e partilha de conteúdo digital.

Enquanto o Facebook e o Google+ apresentam características mais semelhantes, o Twitter diferencia-se por ser uma plataforma de *microblogging*, e o Instagram por estar mais direcionado para fotografia e vídeo.

De modo a comparar o conteúdo que é guardado pelas plataformas de redes sociais, consideremos o Conteúdo Direto e o Conteúdo de Atividade. Definimos como Conteúdo Direto toda a informação que é disponibilizada na plataforma de forma direta e consciente por parte do utilizador da mesma, como por exemplo, quando efetua o registo e é necessário colocar a respetiva informação por parte do utilizador. Considera-se Conteúdo de Atividade todo aquele que não é entregue à plataforma de forma direta, mas em consequência da utilização de serviços nas plataformas, como por exemplo, um serviço que necessite do endereço de IP, em que este é fornecido de forma indireta (Francisco, 2012).

A Tabela 1 que se segue faz o cruzamento da informação anteriormente referida.

| | | Critérios | |
|---|---|---|---|
| | | Conteúdo Direto | Conteúdo de Atividade |
| Plataformas de Redes Sociais | Facebook | Informação de registo, conteúdo partilhado, informação de outros utilizadores | Informação de dispositivos, informação de localização, tipo de *browser*, páginas visitadas, mensagens, pesquisas, anúncios, informação proveniente de APIs |
| | Twitter | Informação de registo, informação adicional, informação pública (*tweets*). Informações de transações | Informação de localização, ligações, *cookies*, serviços externos (proveniente de aplicações de terceiros, *widgets*, botões) |
| | Google+ | Informação de registo, informação adicional, conteúdo partilhado | Informação de dispositivos, informação de localização, *cookies*, identificadores anónimos, informações de serviços Google, armazenamento local |
| | Instagram | Informação de registo, conteúdo de utilizador, comunicações entre o utilizador e a rede | Informação analítica, *cookies*, identificadores de dispositivos, *metadata* |

Tabela 1 - Comparação entre os conteúdos armazenados nas plataformas de redes sociais

Relativamente ao Conteúdo Direto, as quatro plataformas são bastante semelhantes. Muita da informação reunida através do registo é de preenchimento obrigatório, e varia de plataforma para plataforma. A informação adicional é, por norma, informação de preenchimento não-obrigatório, pelo que apenas é preenchido se o utilizador pretender tornar público.

O conteúdo partilhado refere-se aos diferentes formatos que os utilizadores partilham nestas redes, sejam atualizações de estado, fotografias, vídeos ou ligações a outros meios, como por exemplo, páginas Web, ligações de amigos, notícias, entre outros. Por predefinição, esta informação é considerada pública, conforme especificado nas políticas de privacidade das próprias redes, permitindo que sejam posteriormente alterado para um público específico nas definições da rede. A abordagem do Facebook e Google+ mediante este conteúdo baseia-se numa configuração geral, isto é, aplicável a todos estes conteúdos, podendo o utilizador no ato da publicação alterar para o perfil de publicação que prefere, nomeadamente público, apenas para amigos, amigos de amigos, pessoas específicas, apenas ao próprio utilizador. Já o Twitter e Instagram são mais restritivos, pelo que os seus conteúdos são públicos, ou restringidos apenas aos seus seguidores.

Em termos de Conteúdo de atividade, existem ligeiras variações no que toca aos conteúdos armazenados. A forma de acesso às redes bem como os endereços IP são registados para análise, bem como informações de localização, *cookies*, dados agregados, entre outros. Esta informação também é por norma utilizada para a melhoria dos serviços das próprias redes, gestão de marketing e informações para parceiros.

Em suma, seja diretamente ou indiretamente, as plataformas de redes sociais armazenam imensa informação, seja ela de cariz direto ou indireto, pelo que os utilizadores devem ter alguma precaução sobre as suas publicações. Conforme referido pelas políticas de privacidade, uma vez publicado, após mesmo a sua remoção, os dados mantém-se guardados nas próprias redes.

# 3. Gestão de Direitos Digitais

A informação partilhada em plataformas de redes sociais está sujeita a políticas de privacidade, conforme anteriormente referido. No futuro, é esperado que os utilizadores destas redes possam escolher as suas preferências de privacidade com maior riqueza em termos de definições, e talvez com técnicas derivadas de princípios de Gestão de Direitos Digitais (Digital Rights Management – DRM). Estas técnicas podem inclusive melhorar as políticas atuais, que atualmente são imperfeitamente executadas (Rodríguez et al., 2009). Procede-se primeiro à definição do que são conteúdos digitais.

## 3.1. Conteúdos digitais

Conteúdo digital define-se por qualquer informação que esteja disponível digitalmente e que seja processada e acondicionada de forma a que esta seja percetível (Francisco, 2012). Entre exemplos de conteúdos encontram-se o áudio, vídeo, gráficos, animações, imagens, texto, ou qualquer combinação dos conteúdos referidos.

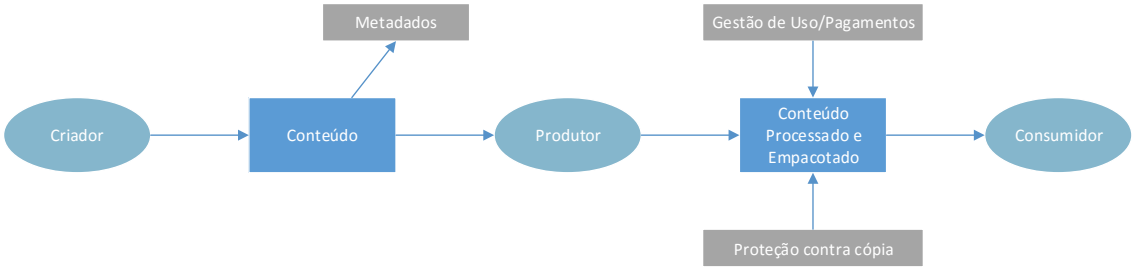



Figura 1 - Fluxo de um controlador desde o criador até ao consumidor

A distribuição destes conteúdos pode ser dividida em duas categorias: *offline* e *online*. A sua distribuição *offline* consiste, por norma, na sua disponibilização em suportes físicos e limitados no volume de dados, como por exemplo, um CD ou DVD. A distribuição *online*, por sua vez, pode consistir no envio de conteúdos por meios online, isto é, por envio de correio eletrónico para os consumidores ou inserção dos mesmos conteúdos num servidor para o efeito. A forma como o servidor de conteúdos distribui a informação nele contido pode ser realizada de duas formas: via *download* (descarregamento) ou via *streaming* (transmissão). Por via de *download*, o conteúdo é adquirido pelo dispositivo juntamente com os seus direitos de utilização ou de forma separada. O conteúdo é, por sua vez, guardado

localmente e só será processado mediante o direito de utilização no dispositivo em causa. No *streaming* não existe um armazenamento integral do conteúdo, portanto, o conteúdo é protegido através de um mecanismo de encriptação da transmissão antes da sua difusão. Esta transmissão é descodificada e processada posteriormente no dispositivo em que será utilizado (Subramanya & Yi, 2006).

A distribuição de conteúdos pode estar, no entanto, na origem de alguns problemas sérios, nomeadamente a pirataria de conteúdos (Torres et al., 2008).

### 3.2. Conceito de Gestão de Direitos Digitais

O termo de Gestão de Direitos Digitais refere-se ao conjunto de políticas, técnicas e ferramentas que servem de orientação para um uso adequado dos conteúdos digitais (Subramanya & Yi, 2006). Portanto, de forma a contornar alguns problemas originados pelo uso e distribuição não autorizada de conteúdos, foram criadas algumas medidas tecnológicas de forma a contornar a situação, entre as quais a encriptação, o *scrambling* e a marca de água (*watermark*) de conteúdos (Francisco, 2012). A Gestão de Direitos Digitais é uma medida mais complexa que inclui regras de uso e de negócio dos conteúdos (Torres et al., 2008).

### 3.3. Sistemas de Gestão de Direitos Digitais

Os Sistemas de Gestão de Direitos Digitais podem gerir bens digitais de uma forma controlada, e de acordo com os termos impostos pelos seus criadores. As plataformas de redes sociais conseguem fazer a gestão do conteúdo, nomeadamente o conteúdo gerado pelo utilizador, mas não conseguem obter todos os objetivos que são alcançados pelos sistemas DRM. Estes sistemas permitem a criação, adaptação, distribuição e consumo de conteúdos multimédia de acordo com as permissões impostas pelos seus criadores (Rodríguez et al., 2009).

Estes sistemas têm como principais funcionalidades a facilidade no empacotamento de conteúdos puros num formato apropriado para uma fácil divulgação e distribuição. A proteção dos conteúdos é feita de forma a não poder ser falsificada na sua transmissão, a proteção de conteúdos de uma utilização não autorizada e a especificação de direitos que determinem a forma como o conteúdo pode ser utilizado (Francisco, 2012).

Estes sistemas devem ainda facilitar a personalização dos conteúdos, sendo possível a sua adaptação de acordo com a preferência dos seus consumidores, ser interoperáveis, permitir diferentes formatos de conteúdos de um modo claro e transparente, e devem igualmente permitir a manipulação de diferentes níveis de granularidade de acesso de conteúdo, isto é, uma unidade de tamanho de um conteúdo que pode ser selecionada, distribuída e consumida de forma independente (Subramanya & Yi, 2006).

Entre as características que um Sistema de Gestão de Direitos Digitais deve ter é a facilidade da sua utilização por parte dos criadores, produtores e consumidores; robustez na evasão de regras de utilização; politicas justas de uso de conteúdos; transparência no uso dos conteúdos para os diferentes fornecedores e serviços; justiça na atribuição de tarifas para os vários tipos de consumo de conteúdos; e por fim, a inovação nas formas de fixação de preços e pagamentos (Subramanya & Yi, 2006).

### 3.3.1. Elementos de Sistemas de Gestão de Direitos Digitais, comparados com as suas contrapartidas nas plataformas de redes sociais

A Gestão de Direitos Digitais aborda diversos conteúdos, pelo que deve ser feita a sua abordagem às suas contrapartidas nas plataformas de redes sociais (Rodríguez et al., 2009). Entre os elementos encontram-se:

- Objetos Digitais: O processo de criação de objetos digitais envolve a combinação de bens digitais protegidos com a sua *metadata* associada de forma a criar objetos digitais que incluam regras de utilização, informação relativa às ferramentas de proteção ou outros dados, como o criador do bem. Os dados gerados pelos utilizadores numa plataforma de rede social não diferem da propriedade intelectual protegida trocada nas plataformas de Gestão de Direitos Digitais, mas as ferramentas para criar e para incluir regras de utilização não são normalmente fornecidas (Rodríguez et al., 2009).
- Expressões de direitos: estas expressões governam os bens digitais através de uma cadeia de valor digital completa nos sistemas de Gestão de Direitos Digitais. Estes são apresentados aos vários atores da cadeia de valor através de ficheiros XML, usualmente chamados de licenças, que são expressas de acordo com uma coma Linguagem de Expressão de Direitos específica e rica (*Rights Expression Language* – REL). As licenças podem proteger informação, como as chaves necessárias para decifrar o conteúdo digital e possuem normalmente assinatura digital para garantir a

sua integridade e autenticidade do seu conteúdo, e os seus dados sensíveis estão usualmente encriptados. Nas plataformas de redes sociais, os utilizadores podem, no melhor caso, especificar qual é o público-alvo (nenhum, todos, amigos, amigos de amigos, entre outros), mas não podem restringir com condições, conforme é possível através do REL (Rodríguez et al., 2009).

- Obrigatoriedade de direitos: Os sistemas DRM têm de garantir que os termos de licença dos bens digitais são respeitados pelos utilizadores da cadeira de valor digital, e para tal, ferramentas de autorização são elementos importantes deste tipo de sistemas. Este tipo de licenças é responsável por verificar se o utilizador tem a licença que lhe garante o direito de efetuar a operação pretendida caso cumpra as condições para tal. Nas plataformas de redes sociais, tudo se baseia na confiança que o utilizador tem no fornecedor da plataforma, pelo que a satisfação desta obrigatoriedade apenas está vagamente garantida por auditorias externas (Rodríguez et al., 2009).
- Ferramentas de Proteção de Propriedade Intelectual: Os sistemas de DRM possuem diferentes técnicas de proteção, como técnicas de encriptação e de *scrambling*, ou outras como o *watermark* e o *fingerprinting* para questões de verificação. As redes sociais normalmente não fornecem este tipo de proteção pois, em grande parte dos casos, assumem que não são necessárias (Rodríguez et al., 2009).
- Notificação de Eventos: Alguns participantes da cadeia de distribuição, como os criadores de conteúdos ou distribuidores, podem querer monitorizar o uso do seu material protegido com direitos de autor. Para tal, são necessários alguns mecanismos que permitam ao sistema partilhar informação sobre eventos relacionados com conteúdo multimédia e quem interage com o mesmo. As redes sociais fornecem apenas informação residual de eventos, ou seja, nem sempre é possível saber quem viu determinada imagem, mas em algumas situações é possível saber quantos utilizadores a viram (Rodríguez et al., 2009).
- Leitores de DRM: Este tipo de leitores podem consumir objetos digitais de acordo com os termos e condições especificados nas respetivas licenças. O uso da licença é feito mediante a ferramenta de autorização que decide se os utilizadores estão autorizados a aceder aos conteúdos. Os leitores de DRM têm tipicamente um repositório seguro para o armazenamento de licenças, informação de proteção, relatórios de operações *offline* e outros dados críticos. Normalmente, a única forma de aceder ao conteúdo gerado pelos utilizadores em plataformas de redes sociais é através

da navegação no próprio portal. No entanto, as APIs destes portais podem fornecer e dar permissões para construir leitores de conteúdos que funcionam independentemente dos *websites* das redes sociais, através de leitores embebidos ou *software* criado através das APIs disponíveis (Rodríguez et al., 2009).

### 3.4. Arquiteturas de Gestão de Direitos Digitais

Existem diferentes tipos de modelos e arquiteturas de Gestão de Direitos Digitais com diversas formas de implementação e formas de organizar o conteúdo que é gerido, ou seja, de especificar as regras de uso do conteúdo. No entanto, a base destes sistemas é a mesma e encontra-se dividido em quatro partes: O fornecedor de conteúdo (*Content Provider*), o distribuidor de conteúdo (*Distributor*), a *Clearinghouse* e o consumidor (*Consumer*) (Francisco, 2012).

O fornecedor de conteúdo detém os direitos sobre os conteúdos para os quais quer garantir o seu cumprimento. Exemplos de fornecedores são uma produtora de música ou um estúdio de cinema. O distribuidor fornece os canais pelos quais os conteúdos são distribuídos, como por exemplo, uma loja *online*. Este cria um catálogo Web onde apresenta o seu conteúdo e os metadados dos direitos para a promoção do conteúdo. Os consumidores são quem usa o sistema para aceder aos conteúdos por meio de um canal de distribuição, podendo fazer *download* ou *streaming* do conteúdo pretendido após a aquisição da respetiva licença. A aplicação usada pelo utilizador é responsável por efetuar o pedido de licença à *Clearinghouse* e de fazer cumprir os direitos de uso do conteúdo. A *Clearinghouse* é responsável pela emissão da licença digital ao consumidor e pelo pagamento das taxas de direitos (*royalties*) ao fornecedor de conteúdos e das taxas de distribuição ao distribuidor de conteúdos (Francisco, 2012).

O Sistema de Gestão de Direitos Digitais é, geralmente, integrado com um sistema de comércio económico (*e-commerce*) que lida com as transações financeiras e aciona a *Clearinghouse*, conforme demonstrado tipicamente pelas componentes ilustradas na Figura 2 (Liu et al., 2003).

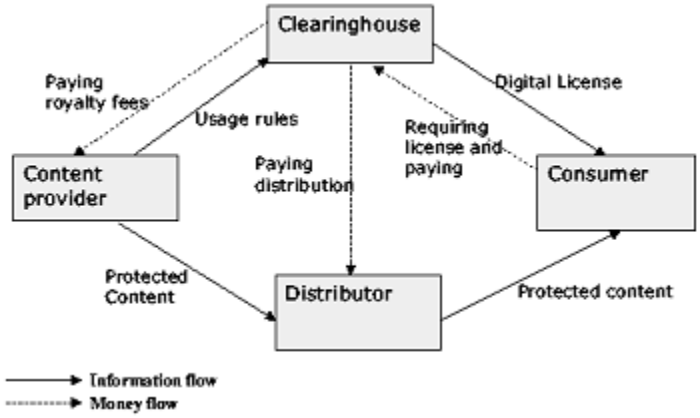



Figura 2 - Componentes típicos de um Sistema de DRM integrado no comércio eletrónico (Liu et al., 2003)

No caso de distribuição de conteúdo sem controlo de pagamento, a arquitetura de alto nível utilizada encontra-se representada pela Figura 3.

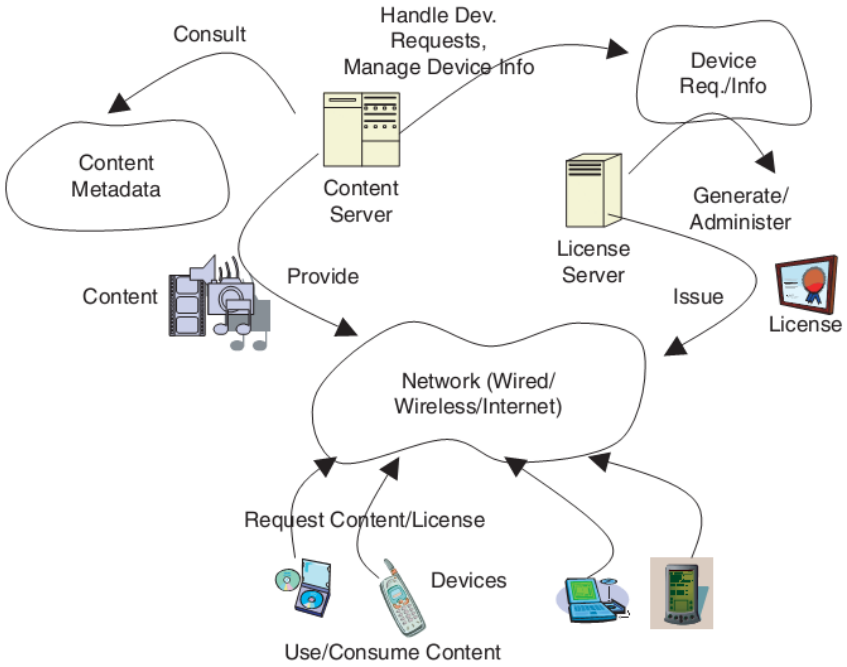



Figura 3 - Arquitetura de alto nível de um Sistema de DRM sem controlo de pagamento (Subramanya & Yi, 2006)

Os dispositivos de interpretação utilizados pelos utilizadores nesta arquitetura comunicam com o servidor de conteúdos e com o servidor de licenças através de uma rede. O servidor de conteúdos é quem detém o conteúdo que se encontra num formato apropriado para reprodução pelos consumidores. O servidor de licenças gera e monitoriza as licenças de direitos de

utilização, sendo este responsável por indicar quais os direitos associados ao conteúdo e aos utilizadores (Subramanya & Yi, 2006).

Uma das arquiteturas de Gestão de Direitos Digitais propostas é baseada na *framework* de gestão de direitos chamada Open and Secure Digital Rights Management (OpenSDRM). Este sistema é baseado na arquitetura DRM adaptada e pode ser configurada para uso em diferentes modelos de negócio e tipos de conteúdo. Este modelo aplica a solução tradicional de Gestão de Direitos Digitais para conteúdos protegidos e pode ser aplicado para a publicação e troca de conteúdos multimédia digitais, conforme ilustrado na Figura 4 (Marques & Serrão, 2014).

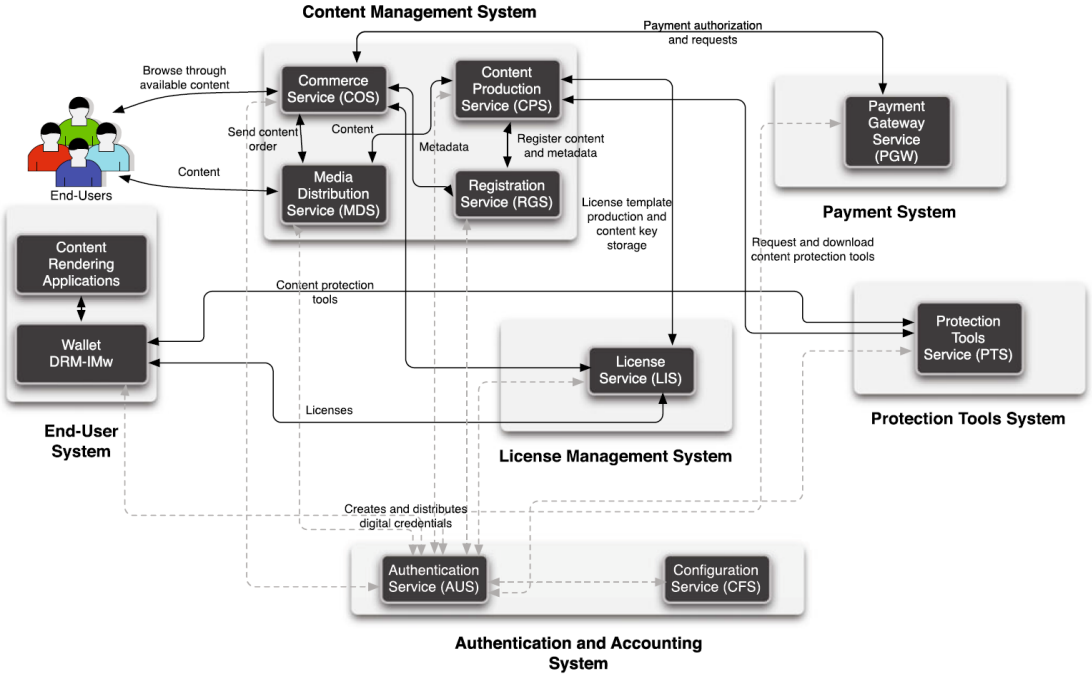



Figura 4 - Arquitetura da *framework* OpenSDRM (Marques & Serrão, 2014)

A aplicação do OpenSDRM tem também aplicações à partilha de conteúdos em plataformas de redes sociais. A principal diferença entre a partilha através das funcionalidades de uma rede social normal e via OpenSDRM é que a segunda dá total controlo do conteúdo partilhado ao utilizador (Marques & Serrão, 2014).

### 3.5. Geração de Licenças

As licenças existentes na Gestão de Direitos Digitais contêm os direitos e onde se encontram os termos e condições relacionadas com a reprodução e utilização deste tipo de conteúdos.

Estas licenças incluem as chaves que são necessárias para o desbloqueio do conteúdo, caso este esteja protegido. Para tal, é utilizada uma chave-semente (*key seed*), que se trata de uma chave apenas conhecida pelo produtor do conteúdo (*producer*) e pelo fornecedor de licenças (*manager*), e um identificador de chave (*KEY ID*). Com isto, a chave é produzida através de um processo de geração de chaves. A chave será utilizada pelo proprietário do conteúdo ou produtor para encriptar o conteúdo quando necessário. A chave é igualmente compactada juntamente com os direitos do conteúdo para gerar uma licença. Este processo é descrito através da Figura 5 (Subramanya & Yi, 2006).

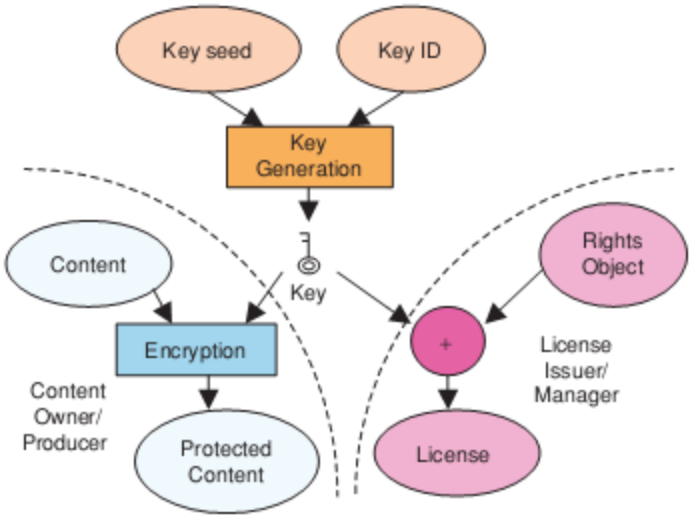



Figura 5 - Diagrama de geração de chaves e licenças (Subramanya & Yi, 2006)

Apenas após o cumprimento dos termos e condições indicadas na licença de utilização de um conteúdo é que é validada a sua utilização. A licença pode ser incorporada juntamente com o conteúdo ou pode ser enviada em separado. A presença da licença pode ser implícita, isto é, quando um utilizador não tem conhecimento do processo de entrega da licença, ou explícita, no caso em que o utilizador participa ativamente através, por exemplo, de formulários e fornecendo informações relevantes para a obtenção da licença. Entre outras características de licenciamento está a sua não transferibilidade, não podendo ser transferida de um utilizador para outro sem que exista informação que o permita, ou a possibilidade de revogação quando os termos e condições de utilização são violados. (Subramanya & Yi, 2006).

# 4. Plataformas semelhantes

Existem atualmente no mercado algumas plataformas que apresentam a aplicação de Gestão de Direitos Digitais no conteúdo individual. Como objeto de análise, foi escolhido a Phantom, um em caso particular a imagens partilhadas, e a SmartRM, que é aplicada à partilha de conteúdo no Twitter, mas que no entanto foi descontinuada.

## 4.1. Phantom

A aplicação Phantom, disponível para iOS e Android nas respetivas lojas de aplicações, permite a partilha de imagens com possibilidade de adicionar à mesma uma mensagem, se assim o for pretendido, em que o controlo de quantas pessoas podem ver, bem como o tempo que está disponível e tempo de visualização está do lado do utilizador. Apenas quem tem acesso ao *link* disponibilizado para a visualização do conteúdo, a aplicação instalada, e um leitor de *QR Code* é que o poderá aceder.

### 4.1.1. Funcionamento da aplicação Phantom

O utilizador pode tirar uma fotografia ou escolher uma foto que já esteja na sua galeria, que pretenda partilhar. Após a fotografia estar selecionada, procede-se às definições da própria fotografia, como efeitos, texto adicional, e também as suas restrições, como o tempo de visualização, número de pessoas que podem visualizar, e tempo disponível até expirar, sendo que, uma vez expirada, a fotografia é eliminada permanentemente. Após estas configurações estarem definidas, a imagem é pixelizada e desfocada de forma a que, sem o acesso devido esta esteja inacessível. O utilizador pode então posteriormente escolher onde deseja partilhar a sua imagem, como no Twitter, Facebook, Google+, Wordpress, Blogger, entre outros.

Para este caso, conforme ilustrado na figura 6, as definições escolhidas foram 9 segundos para visualização, limite de 5 pessoas, e disponível por 5 minutos.

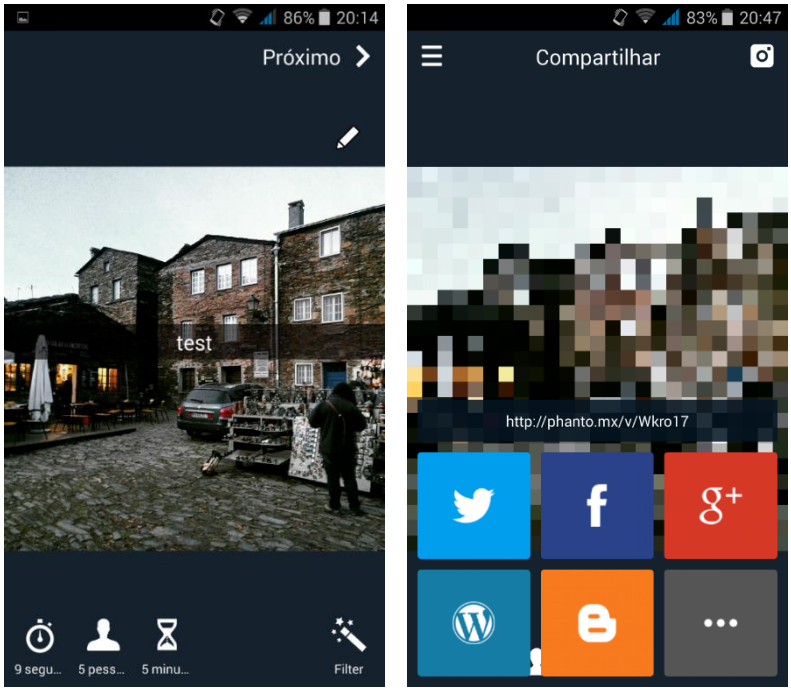



Figura 6 - Definições de publicação de imagens no Phantom

A título de exemplo, selecionou-se a partilha pelo Facebook, conforme ilustrado na Figura 7.

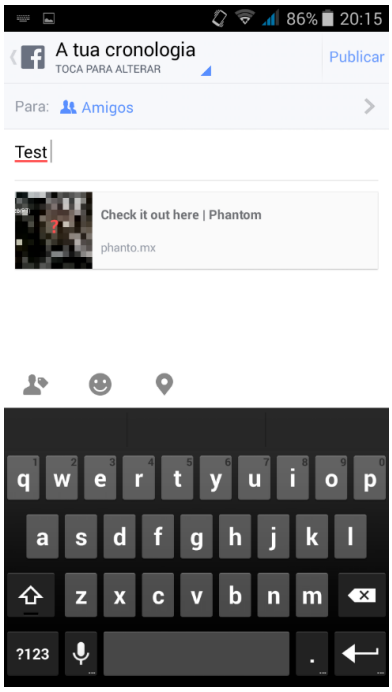



Figura 7 - Exemplo de partilha de imagem publicada no Phantom no Facebook

Após partilhada, quem aceder ao *link* irá encontrar a seguinte página, conforme ilustrado na Figura 8.

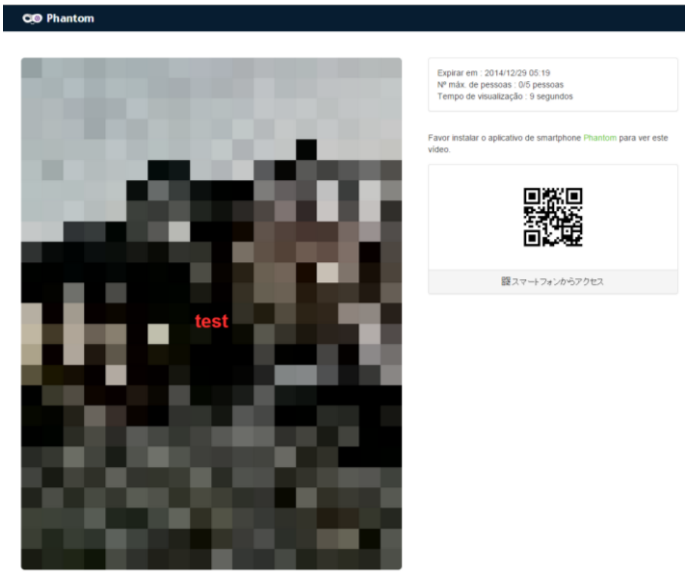



Figura 8 - Página da imagem publicada no Phantom

Na página, o utilizador encontra a imagem ainda codificada, pelo que terá de ler um leitor de *QR Code* e a aplicação instalada no seu dispositivo por forma a ver o seu conteúdo. Quando este acede ao conteúdo, pode visualizar ao premir sobre a aplicação, em que, após o seu tempo de visualização, esta expira, conforme ilustrado na Figura 9.


Figura 9 - Imagem após a sua visualização e acesso

O conteúdo apenas fica alojado no servidor da aplicação enquanto este não estiver expirado, garantindo assim a proteção dos conteúdos dos utilizadores.

No entanto, esta plataforma não revela de que forma é protegido o conteúdo, se é reversivel, e que segurança é utilizada. A política de privacidade da aplicação apenas refere que unicamente a informação pessoal, como nome, email, data de nascimento, número de telefone, entre outros, poderá ser reunída de forma moderada, e que estes conteúdos não serão revelados exceto em situações como a sua divulgação com o consentimento do utilizador e/ou obrigatoriedade pela lei (Phantom Privacy Policy, 2014).

### 4.2. SmartRM

A plataforma SmartRM é uma extensão para o *browser* Mozilla Firefox que permite a proteção de conteúdo através de definições definidas por cada utilizador, e que utiliza o Twitter para a sua partilha. (Francisco, 2012). Entre as principais funcionalidades destacavam-se:

- Proteção de conteúdo digital individual;
- Envio de conteúdo protegido por *email* a amigos;
- Envio de conteúdo seguro a amigos utilizadores do Twitter;
- Reprodução de ficheiros no formato MPEG-21.

No entanto, a plataforma já não se encontra disponível, pelo que os seus endereços estão inacessíveis e desatualizados, mas não deixa de ser uma solução semelhante à plataforma proposta.

#### 4.2.1. Funcionamento da plataforma SmartRM

Para a utilização da plataforma SmartRM é necessário que o utilizador se registe de forma a que possa ser identificado e realizar a gestão dos seus conteúdos. Para tal, é ainda necessário que o mesmo associe à sua conta do SmartRM o seu utilizador do Twitter, de forma a poder importar os seus contatos e partilhar nesta rede (Francisco, 2012).

A ação de partilha de conteúdo encontra-se ilustrada na Figura 10.

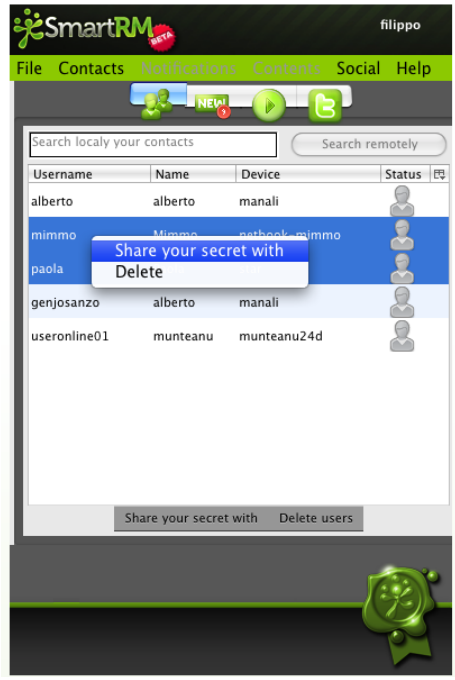



Figura 10 - Ecrã de contactos do SmartRM (Francisco, 2012)

Para proceder à partilha, é necessário indicar qual a directoria do mesmo, conforme descrito na Figura 11.

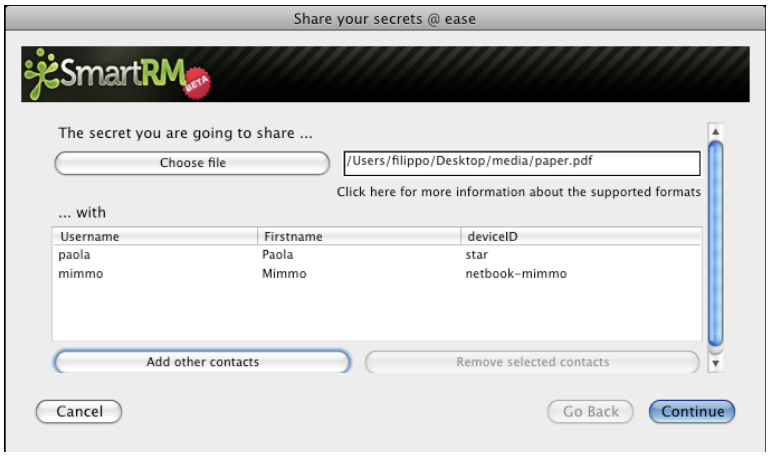



Figura 11 - Ecrã de escolha de conteúdo do SmartRM (Francisco, 2012)

O utilizador terá de indicar qual o nome a atribuir ao ficheiro e a sua descrição. Após essas definições, o utilizador pode proceder à limitação do acesso ao seu conteúdo, entre tipo de utilização (leitura, edição, ou leitura e edição), opção de uso *online* e *offline*, data de início de

uso, data de fim de uso, duração permitida de uso, e número de vezes que o mesmo pode ser utilizado (Francisco, 2012). Este processo encontra-se ilustrado na Figura 12.

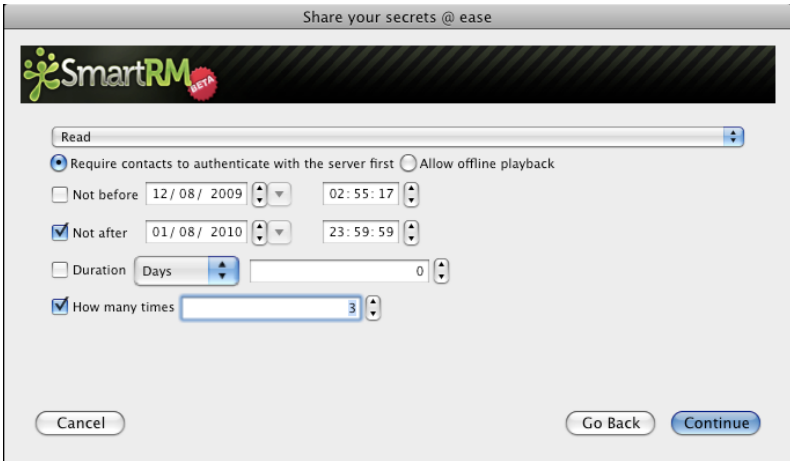



Figura 12 - Ecrã de limites de acesso ao conteúdo do SmartRM (Francisco, 2012)

Após este processo, o conteúdo pode ser partilhado no Twitter, como anexo a uma mensagem de email, ou através de qualquer suporte físico, como por exemplo um dispositivo de memória ligado através de USB. (Francisco, 2012).

# 5. Conclusões

O conteúdo publicado nas plataformas de redes sociais tem portanto uma gestão não só da parte dos prestadores destes serviços, mas também dos que nelas estão inscritos, sendo a sua utilização escrutinada nas politicas de privacidade de cada rede, e podendo estar vulnerável a utilização de terceiros, mesmo após estes sejam apagados.

As plataformas existentes acabam por ter os seus prós e contras quando cruzadas em termos de privacidade, mas intersectam-se em grande parte dos casos. Utilizam maioritáriamente os dados fornecidos para melhorias dos seus próprios serviços, bem como para parceiros como promotores de *marketing*.

O surgimento de sistemas e ferramentas de proteção de conteúdos digitais tornam-se importantes para este tipo de plataformas, pelo que o seu desenvolvimento e aplicação poderá dar aos utilizadores uma maior gestão e proteção dos seus conteúdos. Os Sistemas de Gestão de Direitos Digitais são amplamente utilizados em vários conteúdos multimédia, pelo que é importante a sua aplicação em conteúdos de utilizadores nas redes sociais. No entanto, terá que existir sempre a confiança destes, não só nas plataformas de redes sociais, como também nestes sistemas de gestão de direitos.

# Solução de gestão dos direitos digitais de conteúdos gerados por utilizadores partilhados em redes sociais

## 1. Introdução

A solução apresentada neste documento, que visa a gestão de conteúdos e direitos digitais dos utilizadores em redes sociais, tem como objetivo incrementar a privacidade dos utilizadores destas redes, garantindo um maior controlo do seu conteúdo, bem como integridade e segurança do mesmo.

Para tal, e após do estudo de toda a envolvente nesta temática, desenvolvida no âmbito do estado de arte, é necessário definir quais os tópicos que serão abordados, componentes utilizados, requisitos e arquitectura da solução:

- Levantamento e análise de requisitos: levantamento e definição dos requisitos que devem ser satisfeitos pela solução;
- Arquitectura conceptual da solução (alto nível): apresentação de forma superficial e generalizada do conceito;Arquitectura da solução de gestão de conteúdos e direitos digitais: elaboração da arquitectura da solução tendo em conta os requisitos levantados da solução.

Os tópicos referidos são fundamentais para o desenvolvimento da solução proposta e para que esta se possa realizar com sucesso.

# 2. Arquitetura da Solução

O seguinte tópico refere-se à arquitectura da solução desenvolvida no âmbito desta dissertação.

## 2.1. Levantamento e análise de requisitos

Para uma melhor compreenção de quais as características e funcionalidades a desenvolver para a aplicação, segue-se um conjunto de requisitos que deverão ser tidos em conta para o desenvolvimento da solução.

É necessário, primeiramente, definir quais são os principais *stakeholders* da solução a implementar, seguindo-se as categorias dos requisitos, bem como o seu levantamento e descrição, para a sua melhor compreensão.

### 2.1.1. Stakeholders

Para a solução a implementar, identificaram-se dois stakeholders relevantes, isto é, que se consideram fundamentais para o sistema. Primeiramente, o utilizador de redes sociais, pois é este que faz uso do sistema e é o principal benificiário da aplicação, pois os conteúdos a proteger pelo sistema pertencem ao mesmo. Seguidamente, destaca-se o gestor do sistema, que é o responsável pela monitorização, controlo, e manutenção do sistema, que é quem deve garantir a integridade da plataforma, servindo de moderador do sistema, de forma a prevenir violações de direitos e potenciais excessos por parte dos utilizadores.

Considere o seguinte diagrama de use-cases, ilustrado na Figura 13, que reflete as ações destes stakeholders:

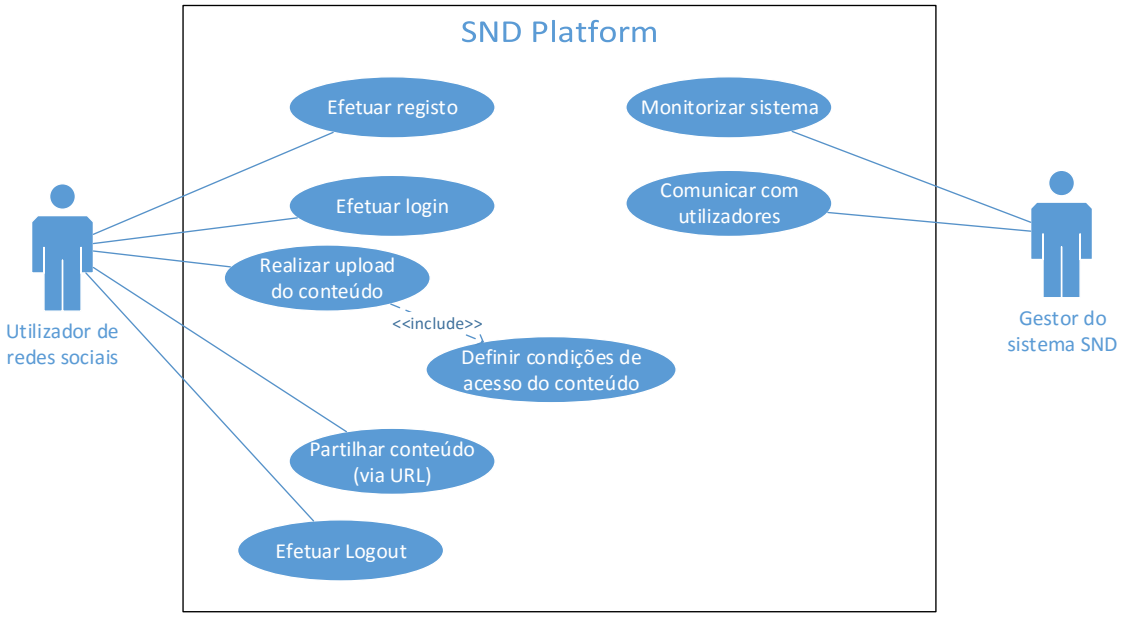



Figura 13 - Diagrama de use-cases da plataforma SND

Atendendo ao diagrama de use-cases, é necessário esclarecer alguns pontos relativamente às acções dos stakeholders.

Considerando o utilizador de redes sociais:

- Os use-cases representam a interacção do utilizador com o sistema, isto é, as opções que este tem ao seu dispor na aplicação, conforme representado no diagrama;
- O use-case "Realizar upload do conteúdo" inclui ainda o "Definir condições de acesso do conteúdo", pois, no momento de realizar a ação do upload do conteúdo, é necessário definir quais as suas condições de acesso para os utilizadores que poderão ter acesso ao mesmo.

Considerando o gestor do sistema SND:

- O use-case "Monitorizar sistema" refere-se ao controlo deste, como por exemplo, a exclusão de utilizadores, validação de conteúdo ou a verificação de disponibilidade do sistema;
- O use-case "Comunicar com utilizadores" refere-se ao possivel contato com os utilizadores da plataforma, seja para divulgar informação pertinente da própria plataforma, ou resposta a potenciais mensagens enviadas para o sistema.

### 2.1.2. Requisitos da solução

Os requisitos de um produto são tipicamente classificados por duas categorias, nomeadamente requisitos funcionais (RF) e requisitos não-funcionais (RNF) (Sommerville, 2007).

Os requisitos funcionais são serviços que devem ser fornecidos pelo sistema, indicar como o sistema deve reagir perante determinados *inputs*, e como este deve se comportar perante determinadas situações. Estes podem separar-se em requisitos de utilizador e requisitos de sistema (Sommerville, 2007).

Os requisitos não funcionais são condições de serviço ou fnucionalidades oferecidas pelo sistema, que podem incluir condições temporais, condições de desenvolvimento e condições impostas por *standards*. Este tipo de requisitos aplicam-se frequentemente a um sistema como um todo e não a funcionalidades ou serviços individuais do sistema (Sommerville, 2007).

Considerando então estas definições, definiu-se na Tabela 2 os requisitos a ter em conta para o desenvolvimento da solução. Estes estão identificados através da sua categoria, identificador, e respectiva descrição.

| Stakeholder | Categoria | Requisitos | |
|---|---|---|---|
| | | ID | Descrição |
| Utilizador de redes sociais | RF | 1 | O utilizador deve ter acesso à internet para aceder à plataforma. |
| Utilizador de redes sociais | RF | 2 | O utilizador deve aceder à plataforma através de uma extensão de um navegador *web*. |
| Utilizador de redes sociais | RF | 3 | O sistema deve permitir o registo e criação de uma conta de utilizador. |
| Utilizador de redes sociais | RF | 4 | O sistema deve permitir ao utilizador autenticar-se através de uma rede social. |
| Utilizador de redes sociais | RF | 5 | O sistema deve permitir ao utilizador efetuar o login e o *logout* da sua conta. |
| Utilizador de redes sociais | RF | 6 | O sistema deve permitir o *upload* de conteúdos pelo utilizador. |
| Utilizador de redes sociais | RF | 7 | O sistema deve permitir a configuração de condições de utilização do conteúdo ao utilizador. |
| Utilizador de redes sociais | RF | 8 | O sistema deve gerar um URL do conteúdo que permita a partilha do mesmo pelo utilizador |
| Utilizador de redes sociais | RF | 9 | O sistema deve permitir a eliminação de conteúdo por parte do utilizador. |
| Utilizador de redes sociais | RF | 10 | O utilizador deve poder remover a sua conta do sistema. |
| Gestor do sistema | RF | 11 | O sistema deve permitir a sanção de utilizadores que tenham uma conduta imprópria na plataforma. |
| Gestor do sistema | RF | 12 | O sistema deve permitir o envio de notificações ao utilizador. |
| Utilizador de redes sociais | RNF | 13 | O utilizador deve ser utilizador de redes sociais para poder utilizar a plataforma. |
| Gestor do sistema | RNF | 14 | O sistema deve garantir que os dados estão protegidos de acessos não autorizados. |

Tabela 2 - Requisitos funcionais e não funcionais do sistema SND

É necessário que todos os requisitos referidos sejam cumpridos de modo a que o sistema possa funcionar corretamente e dentro do seu âmbito. A tabela completa dos requisitos encontra-se no Anexo A.

## 2.2. Arquitetura de alto nível conceptual da solução proposta

Para uma melhor compreensão da arquitetura pretendida, bem como o seu funcionamento, apresenta-se na figura seguinte (Figura 14) a interacção entre os diversos elementos.

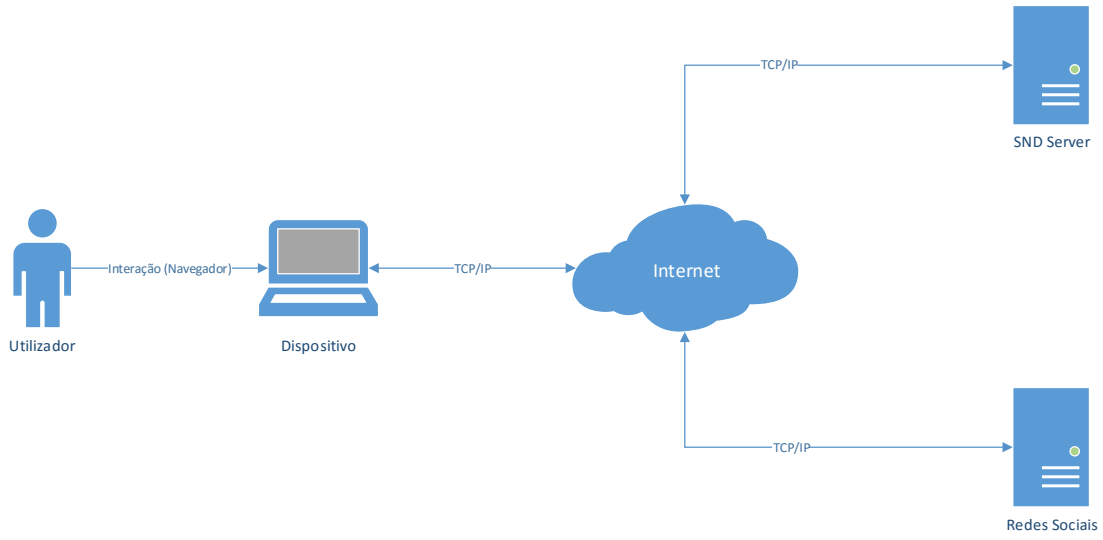



Figura 14 - Arquitetura conceptual da solução (alto-nível)

A arquitetura representada (Figura 14) apresenta a interacção de alto-nível entre os diversos envolvidos. Consideram-se os elementos principais os utilizadores de redes sociais, os dispositivos de comunicação, o sistema de gestão de conteúdos e direitos digitais de redes sociais (SND Server), e as redes sociais.

Os utilizadores de redes sociais irão comunicar com a solução proposta por via dos seus dispositivos de comunicação que disponham de um navegador e acesso à internet. A interação entre o utilizador e a plataforma SND é efectuada através da publicação do conteúdo a partilhar posteriormente nas redes sociais, sendo, desta forma, a solução interpretada como um intermediário para o alojamento e gestão dos conteúdos. Considerando como redes sociais as plataformas que o utilizador utiliza para partilhar o seu conteúdo, esta solução visa disponibilizar elementos que tem como objetivo a partilha desses mesmos conteúdos, mas com a sua devida proteção, gerida através da plataforma SND, que será responsável pela gestão do mesmo. A plataforma servirá como via de proteção dos seus conteúdos, onde, após se conectarem, poderão criar uma publicação, que será gerida pelo sistema SND.

Por via a compreender melhor a interação entre o utilizador e a solução apresentada, considere o diagrama ilustrado na Figura 15.

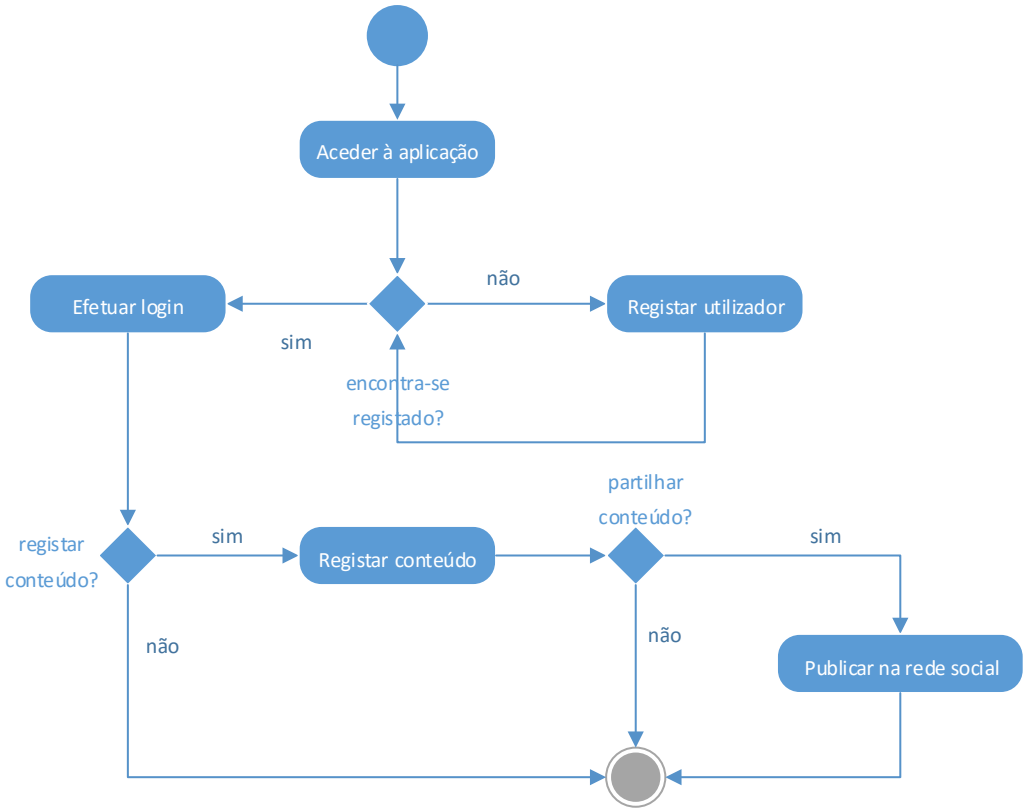



Figura 15 - Diagrama de Atividades UML do funcionamento da aplicação (alto nível)

O utilizador regista-se no sistema, de forma a poder autenticar-se no mesmo. Posto isto, este poderá partilhar o seu conteúdo em que terá a possibilidade de, por exemplo, restringir a pessoas em específico, número de visualizações e/ou data de validade. O sistema SND irá efectuar o armazenamento e proteção do conteúdo, devolvendo um link ao utilizador. Esse *link* poderá ser partilhado para os contactos do utilizador, sendo que o mesmo poderá ter restrições, como ficar restringido a determinadas pessoas, ou expirar. Após o conteúdo expirar, este é eliminado do sistema, deixando de estar acessível de qualquer forma.

Para perceber melhor o processo de autenticação e registo de utilizadores considere o diagrama ilustrado na Figura 16.

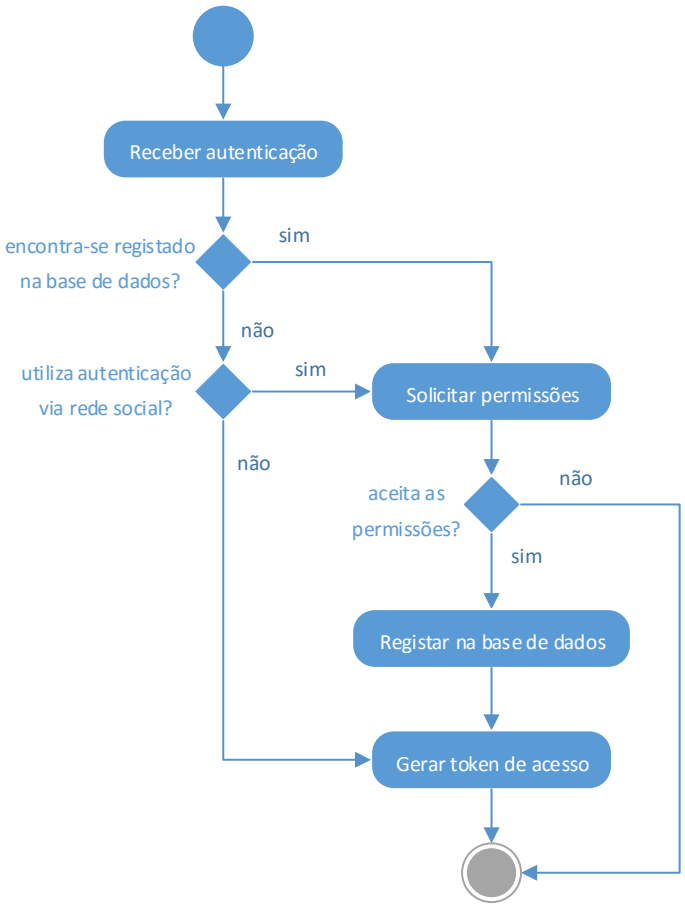



Figura 16 - Diagrama de Atividades UML do registo e autenticação de utilizadores (alto nível)

Ao aceder à aplicação, o utilizador irá submeter a sua autenticação ao sistema e este irá verificar se o mesmo se encontra registado. Caso não se encontre registado, o utilizador poder-se-á registar via rede social, ou via registo nativo na aplicação. O registo via rede social permite a facilidade no acesso às permissões necessárias, como o nome, email ou lista de amigos, sendo estes registados caso o utilizador assim o permita. O registo nativo irá necessitar do preenchimento de um formulário a solicitar a referida informação. Após o registo, o utilizador é autenticado, sendo gerado um token de acesso de forma a permitir o acesso à aplicação e a aceder às suas funcionalidades.

O processo de registo de conteúdo passa pelo seu armazenamento, a geração da sua licença, com base nas definições inseridas pelo utilizador, e a geração de um link de acesso ao conteúdo, que estará pronto a ser partilhado. O processo, da perspectiva *server-side*, encontra-se ilustrado na Figura 17.

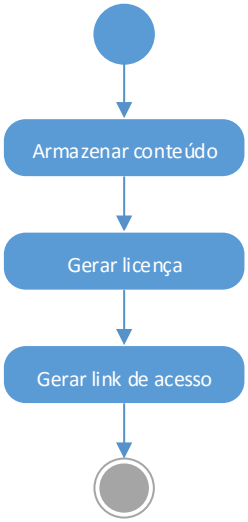



Figura 17 – Diagrama de Atividades UML do processo de registo de conteúdo (alto nível)

Uma vez publicado, o conteúdo será gerido através da sua licença. É esta que irá determinar o seu acesso, bem como possível expiração, como por exemplo, quando excede o número de visualizações ou passa a data de validade. Para este último caso, considere o diagrama ilustrado na Figura 18.

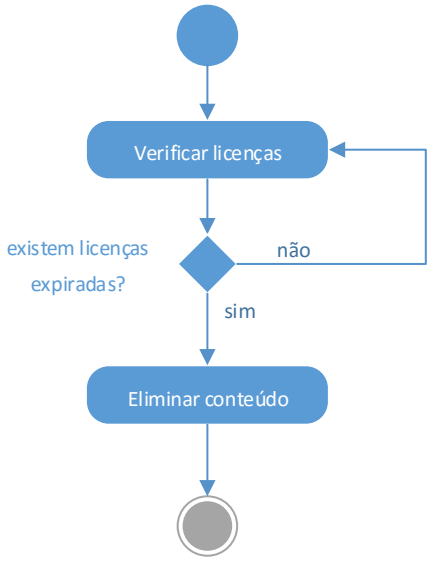



Figura 18 - Diagrama de Atividades UML de verificação de licenças

As licenças são verificadas periódicamente através de um agendamento (*job schedule*) no servidor, que verifica a existência de licenças expiradas. Caso estas tenham expirado, o seu

respectivo conteúdo será eliminado do sistema, deixando de estar acessível de qualquer forma.

É importante referir que o acesso ao conteúdo está dependente da licença e das permissões que esta permite. Caso o utilizador cumpra com as permissões da licença, este não terá acesso ao conteúdo, sendo-lhe então negado pela plataforma o acesso aos conteúdos.

Para compreender melhor o processo de gestão de licenças e conteúdo, é necessário perceber a arquitectura OpenSDRM, uma arquitectura DRM adaptável que se pode adaptar a diversos tipos de conteúdo e modelos de negócio, para a publicação, partilha e proteção de conteúdos digitais multimédia (Marques & Serrão, 2014).

### 2.3. OpenSDRM e a gestão de conteúdo e licenças

A plataforma OpenSDRM, desenvolvida no âmbito do projeto MOSES (Balestri et al., 2002) apresenta diversos elementos que acompanham a cadeia de valor de distribuição de conteúdo, como a produção, registo, preparação, distribuição, negociação e aquisição de conteúdo e ainda autenticação de utilizadores e visualização/*playback* condicional (Marques & Serrão, 2014).

Conforme ilustrado na Figura 4, incluída no estado de arte, o OpenSDRM dispõe de diversos elementos para a gestão de conteúdo, nomeadamente o Sistema de Gestão de Conteúdo, Módulo de Entrada de Pagamento, Sistema de Gestão de Licenças, Sistema de Ferramentas de Proteção de Conteúdo, e o Sistema de Conta e Autenticação, estando cada um destes subdividido em sub-módulos, que farão a gestão do conteúdo (Torres et al., 2008).

Para a interação com esse mesmo conteúdo, é necessário compreender quais os papéis representados pelas diversas entidades na cadeia de valor (Torres et al., 2008), nomeadamente:

- Sociedades gestoras de direitos de autor, que são responsáveis pela defesa dos direitos de propriedade e conteúdo;
- Fornecedores de conteúdo, que representam os autores de conteúdos produzidos e distribuídos digitalmente;
- Produtores de dispositivos;

- Fornecedores de ferramentas de segurança, através de meios tecnológicos nos dispositivos de processamento de conteúdo;
- Utilizadores finais, isto é, os utilizadores que irão fazer uso de um determinado conteúdo.

No âmbito da arquitetura, é considerado como fundamental para adaptação a esta realidade o Serviço de Licenças (LIS), uma versão mais simplificada e atualizada do Sistema de Gestão de Conteúdo e do Sistema de Conta e Autenticação, nomeadamente com o *Content Management Server* e o *Authentication Server*, conforme descrito no tópico que se segue, referente à arquitetura da solução. Esta simplificação surge de forma a adapta-la melhor à realidade das redes sociais, visto que o OpenSDRM é adaptável a várias plataformas, e ao estarmos perante uma situação mais específica, a sua simplificação torna a sua perceção mais fácil, bem como eventuais alterações, mais centradas nas redes sociais. No entanto, a ideia modular mantém-se de forma a manter o sistema ágil e organizado.

### 2.4. Arquitectura da solução de gestão de conteúdos e direitos digitais

Após a concepção e análise realizada nos pontos anteriores, pretende-se apresentar a solução proposta para a gestão de conteúdos e direitos digitais, com vista a melhorar a privacidade associada à gestão destes direitos numa rede social. A solução, em termos de arquitectura, encontra-se ilustrada na Figura 19.

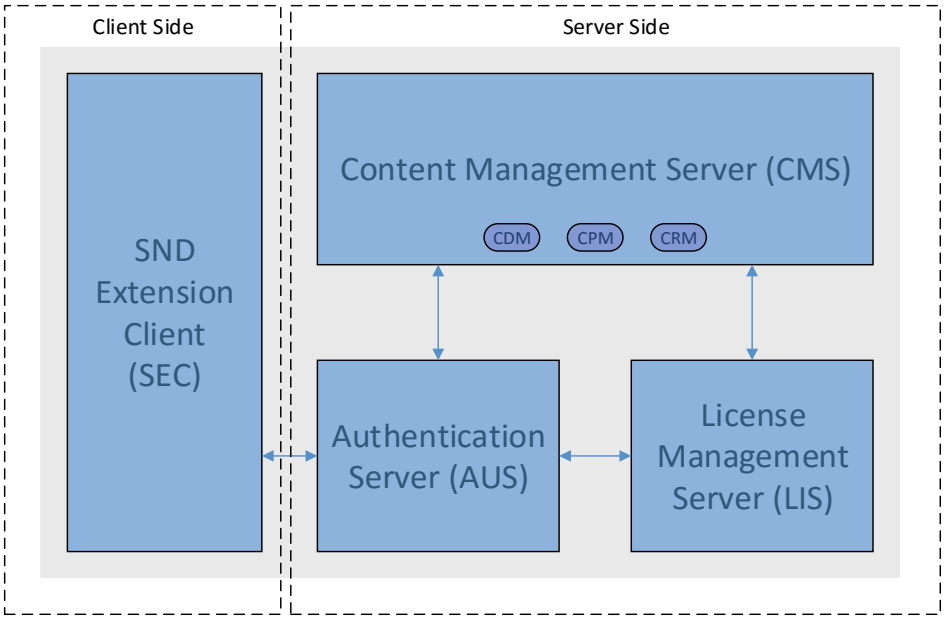



Figura 19 - Arquitetura proposta para o sistema SND

Conforme foi refereido anteriormente, a solução apresenta módulos provenientes do sistema OpenSDRM, adaptados perante a realidade aqui apresentada, e de forma mais simplificada. A solução é composta pelos seguintes sistemas e módulos:

- *SND Extension Client*: É uma aplicação desenvolvida como uma extensão para um *browser* Web, que irá realizar a interação entre o utilizador e o sistema SND;
- *Content Management Server* (CMS): É o sistema responsável pela gestão de todo o processo envolvente no conteúdo que é colocado no sistema. É dividido em três módulos:
    - *Content Definition Module* (CDM): É responsável pela agregação da informação do conteúdo, preparado devidamente para ser registado.
    - *Content Protection Module* (CPM): É responsável pela proteção e encriptação do conteúdo, garantindo assim a sua integridade.
    - *Content Registration Module* (CRM): É responsável pelo registo do conteúdo anteriormente definido, geração da sua licença e respectivo URL para a sua partilha.
- *Authentication Server* (AUS): É o sistema responsável pela gestão do registo e autenticação dos utilizadores no sistema. Este deverá garantir a integridade dos dados dos utilizadores e respectiva proteção.
- *License Manager Server* (LIS): É o sistema responsável pela geração de licenças dos conteúdos carregados no sistema.

O OpenSDRM, é, no entanto, uma arquitectura adaptável à gestão de direitos digitais, e que pode ser configurada para uma utilização que implique diversos modelos de negócios e diferentes tipos de conteúdo, sendo assim bastante abrangente, permitindo ser aplicada ainda na divulgação e comercialização de conteúdo digital multimédia (Francisco, 2012).

A sua arquitetura é baseada em extensões do MPEG-4 IPMP (King & Kudumakis, 2002) e componentes de identificação de itens digitais MPEG-21 DII (Burnett, 2006), sendo constituída por diversos elementos opcionais que cobrem todas as fases da cadeia de valor, desde a produção de conteúdo até ao seu uso, distribuição, comercialização e produção do mesmo (Francisco, 2012).

A modularidade presente no OpenSDRM permite que este seja adaptável para outros cenários, por ser composto por componentes independentes e que são implementados numa abordagem orientada a serviços (Francisco, 2012).

Portanto, esta simplificação proposta vem eliminar a redundância de alguns módulos e sistemas do OpenSDRM, que do ponto de vista de partilha de conteúdo em redes sociais, não trariam muita utilidade, e assim, é possivel simplificar-se a plataforma perante o que é pretendido.

Poderemos assim considerar que o Sistema SND encontra-se preparado para contribuir para o aumento da privacidade dos utilizadores de redes sociais, aumentando a proteção e o controlo destes para com o seu conteúdo.

O sistema proposto apresenta ainda uma solução *client-side*, nomeadamente uma extensão para *browser*, que permitirá ao utilizador, após a respectiva autenticação, definir as regras de controlo de acesso do conteúdo a publicar, realizar o seu upload para a plataforma, de forma a proceder à sua partilha nas suas redes sociais, e monitorizar o respectivo acesso ao conteúdo.

Torna-se, portanto, importante para esta solução assumir os seguintes pressupostos:

- Todos os compoentes desta plataforma são confiáveis, isto é, não foram modificados e o seu comportamento é exactamente o que é esperado. A simplificação realizada aos componentes do OpenSDRM consiste apenas na utilização dos módulos relevantes para a concepção desta solução;
- A comunicação na plataforma entre os diversos sistemas e módulos é realizada através de um canal seguro e autenticado;
- Todo o conteúdo que tenha uma licença expirada será sempre removido na sua totalidade do sistema, garantindo assim a sua indisponibilidade e maior proteção contra possíveis intrusões no sistema;

Posto isto, segue-se a explicação detalhada das funcionalidades e comportamentos da solução apresentada.

### 2.4.1. Registo e acesso do utilizador

O registo do utilizador na plataforma, e o respectivo acesso, segue o seguinte procedimento:

- O utilizador acede à aplicação, seleccionando a extensão no seu *browser*, e poderá registar-se via sistema próprio, ou via rede social, ou então, caso já esteja registado, realizar o seu *login*;
- Registo via sistema próprio:

  - O utilizador preenche um formulário com os dados solicitados, incluindo o seu *username* e *password*;
  - À *password* é aplicado um hash, de modo a que esta seja codificada aquando da sua submissão ao sistema AUS. Aquando da submissão, o AUS armazenará a *password* codificada de forma segura, sendo que apenas o utilizador a conhecerá como ela é originalmente, isto é, sem codificação;
  - Antes de ser registado, o AUS confirma a informação do utilizador e o seu respectivo endereço de correio electrónico, que em caso afirmativo, gera um ID próprio;
  - Após confirmação, o AUS confirma o registo do utilizador e todas as suas credenciais, que permitirão assim o acesso à plataforma.
- Registo via rede social:
  - O utilizador seleciona qual a rede social que pretende utilizar como *login*;
  - A comunicação é realizada entre a o *client* da aplicação (extensão), a API da rede social e o sistema AUS, por via de um formulário de autenticação gerado pela rede social;
  - É comunicado ao utilizador as configurações que serão necessárias para o registo no sistema;
  - Após ser aceite, o AUS irá confirmar a informação do utilizador, permitindo assim o seu acesso por esta via de autenticação, não sendo assim necessário o armazenamento das suas credênciais. Será gerado um ID no sistema, ao qual será associado o ID do utilizador na rede social.
- Acesso de um utilizador via sistema próprio:
  - Após a inserção das credenciais, o AUS irá validar, de forma a autorizar o seu acesso;
  - Quando validado, é apresentado ao utilizador a sua lista de opções na plataforma. Caso contrário, é-lhe negado o acesso.
- Acesso de um utilizador via rede social:
  - O AUS verifica se o utilizador se encontra ligado via rede social;
  - Em caso afirmativo, é tipicamente gerado um *access token* pela plataforma da rede social, que permitirá então o acesso à aplicação;
  - Em caso negativo, o utilizador terá de se autenticar de novo na rede social;
  - Caso o *access token* tenha expirado, por *time out*, este terá de ser novamente gerado pelo utilizador, através de uma nova autenticação.

O registo na plataforma encontra-se ilustrado através de um diagrama de sequência nas Figuras 20 e 21, por via de sistema próprio e autenticação por rede social respetivamente.

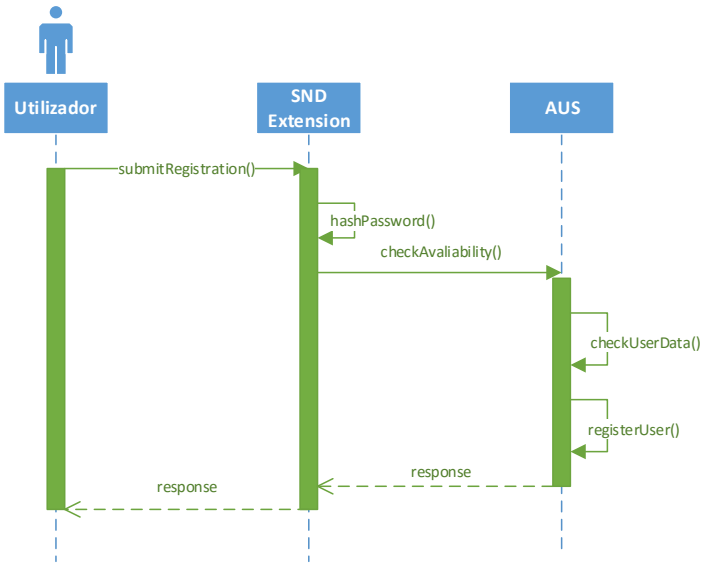



Figura 20 - Registo na plataforma SND por sistema próprio

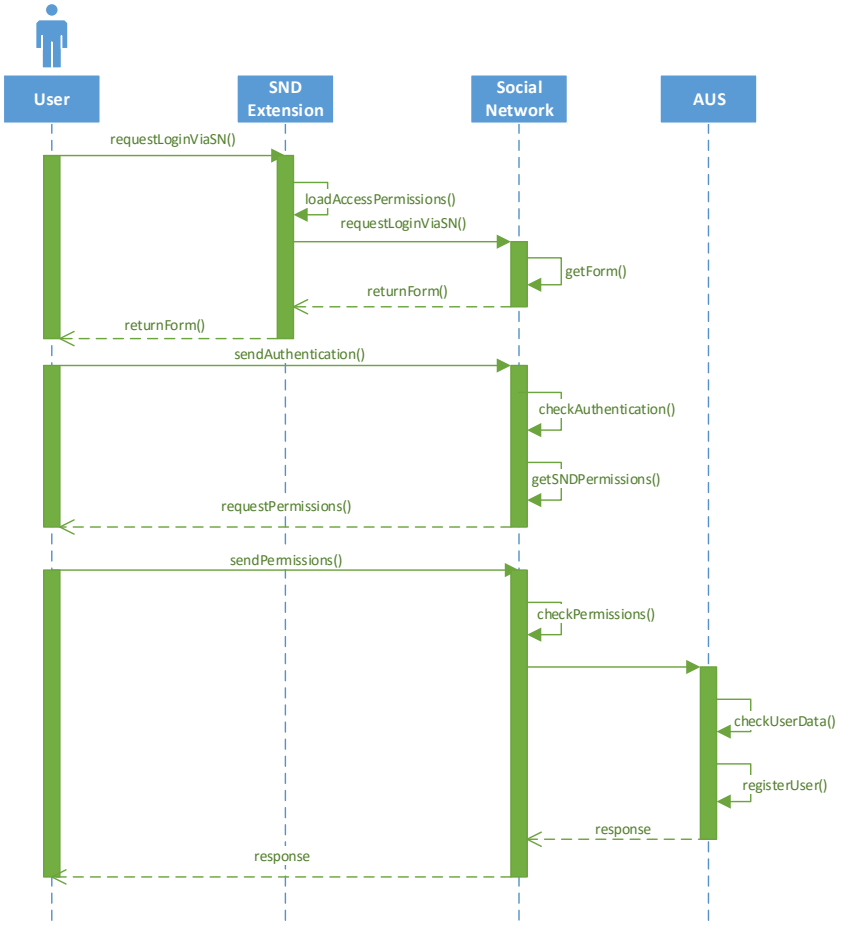



Figura 21 - Registo na plataforma SND por autenticação na rede social

### 2.4.2. Publicação e definição de regras de partilha de conteúdo

A publicação de conteúdo na plataforma segue o seguinte procedimento:

- O utilizador acede à plataforma por via da extensão para o browser. Se o utilizador não tiver a sua sessão iniciada, ou caso esta tenha expirado, terá de realizar de novo o seu *login*;
- O sistema irá validar a autenticação através da componente AUS, podendo, em caso afirmativo, proceder na aplicação;
- O utilizador introduz as configurações de acesso para o seu conteúdo, e a respectiva selecção do mesmo, de forma a proceder ao seu carregamento, através do preenchimento de um formulário. Este formulário irá gerar metadata, que descreve o conteúdo carregado, e o seu respectivo *hash*, definido no sistema CMS através do módulo CDM, responsável por definir o conteúdo;
- O conteúdo é então carregado para o sistema através do CMS, acionando o módulo CRM e realizando assim o seu registo. Após o seu carregamento, é gerada uma página HTML, para a qual será associado o conteúdo a visualizar;
- A encriptação da localização do conteúdo é realizada através do módulo CPM. Para simplificar, assumimos que o conteúdo é encriptado, devido à existência de várias técnicas e métodos de proteção;
- O CRM irá contactar o serviço LIS de forma a proceder à criação e associação de uma licença do conteúdo. A licença é gerada através dos metadados gerados, sendo gerado um identificador-chave que identificará a licença e o associará ao conteúdo, sendo efectuado um registo na base de dados;
- O CRM irá, posteriormente, gerar um URL especial para o conteúdo, nomeadamente a página HTML gerada, e devolvê-lo ao utilizador, de forma a que este possa partilhar o seu conteúdo. O URL é um atalho global que permite o acesso ao conteúdo localizado na plataforma.

A Figura 22 ilustra o comportamento dos diversos sistemas e módulos da plataforma. Uma versão de maior resolução pode ser consultada no Anexo B.

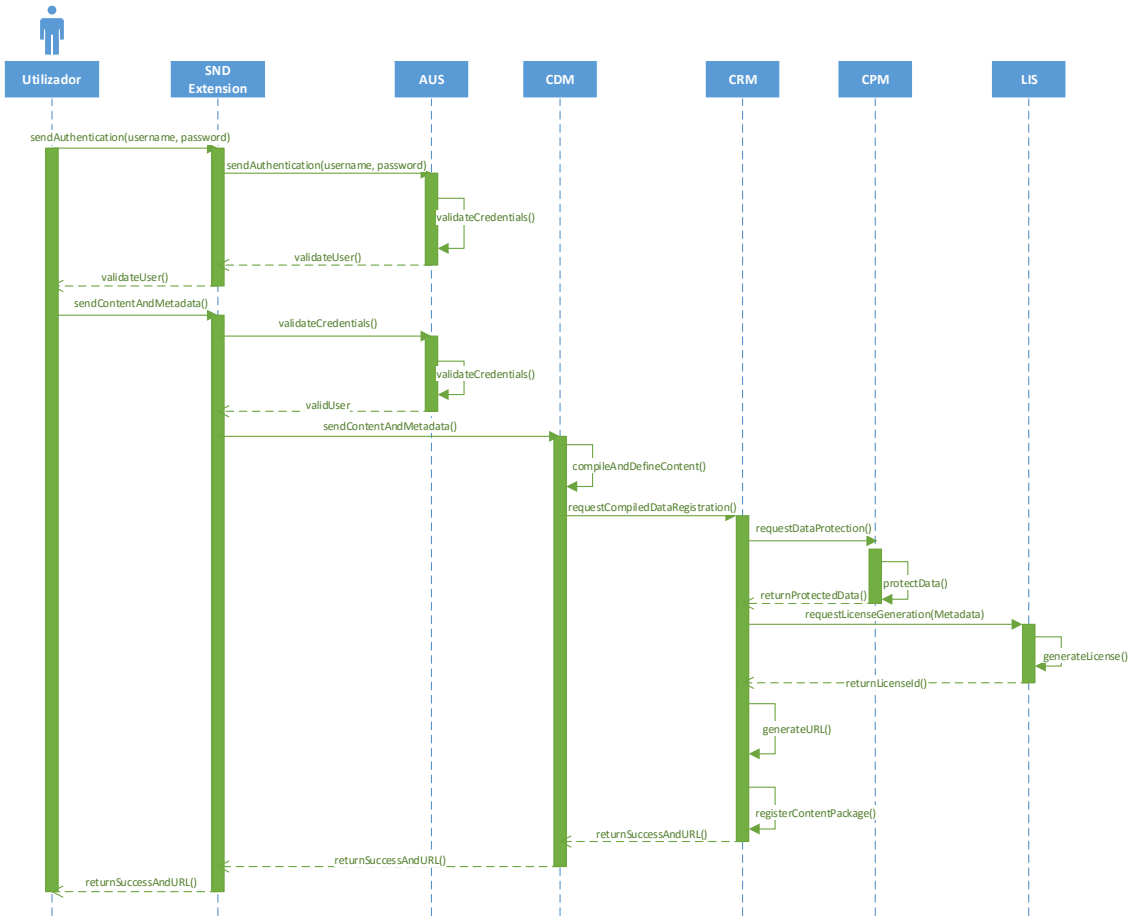



Figura 22 - Diagrama de estados da partilha de conteúdo na plataforma SND

As regras de acesso ao conteúdo na plataforma, conteúdo esse a ser partilhado, seguem o seguinte procedimento:

- Aquando do registo do conteúdo por parte do utilizador, este tem à sua disposição diversas ferramentas de configuração da sua licença, entre as quais:
    - Número de visualizações: o conteúdo fica disponível até este atingir o número de visualizações que o utilizador configurar;
    - Data e hora: o conteúdo fica disponível até à data e hora que o utilizador definir;
    - Contactos: o conteúdo fica apenas disponível aos contactos que o utilizador definir. Estes poderão ser importados através da rede social pela qual o utilizador está autenticado.

- Após a submissão do conteúdo, e aquando do registo dentro do CMS, o CRM irá contactar o LIS, que irá gerar a licença com base nos metadados fornecidos, e nos gerados pelo próprio LIS, nomeadamente:
    - ID do owner do conteúdo;
    - ID único do conteúdo;
    - Número de visualizações;
    - Data e hora de validade;
    - Chave de encriptação de conteúdo: elemento que irá proteger o conteúdo.
- Criada a licença, esta é registada na base de dados do sistema;
- Uma licença é considerada como expirada assim que um dos seus elementos deixar de ser válido.

### 2.4.3. Partilha e acesso do conteúdo

A partilha de conteúdo na plataforma e o seu respetivo acesso segue o seguinte procedimento:

- Após ter sido gerado o URL na plataforma, o utilizador poderá partilhá-lo nas redes sociais que pretender;
- Sempre que o *link* é acedido, é executado primeiramente um acesso à licença. É realizado um pedido ao CMS, nomeadamente ao módulo CPM, que irá efectuar o pedido de acesso ao LIS para o acesso ao conteúdo. Caso o acesso seja concedido quem acede ao *link* tem permissões de acesso ao conteúdo e este é visualizado.
- Para o caso específico da restrição por número de visualizações, este será sempre atualizado na sua licença, de forma a mate-la sempre atualizada, aquando da sua expiração por esta via;
- O CPM engloba um agendamento (*job schedule*) que irá verificar a existência de conteúdo expirado. Caso encontre, este será totalmente removido do sistema, deixando de existir qualquer tipo de acesso ao mesmo.

A Figura 23 ilustra o processo de pedido de acesso ao conteúdo.

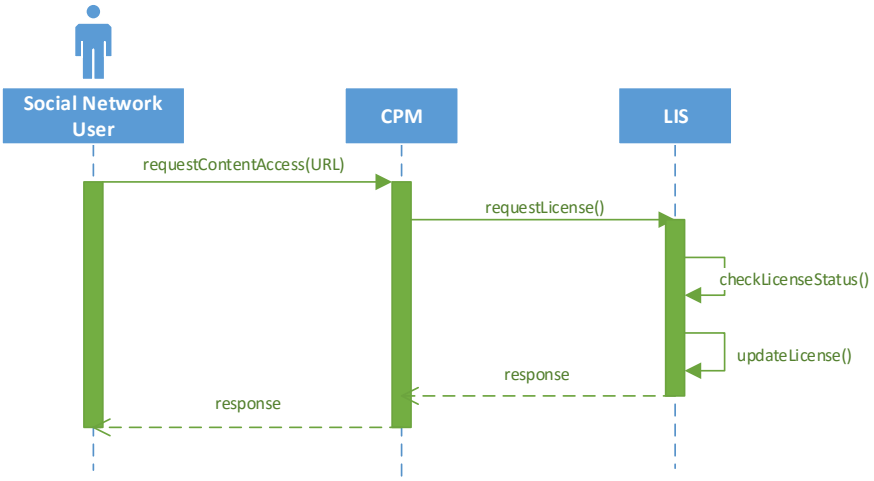



Figura 23 - Pedido de acesso ao conteúdo

### 2.4.4. Remoção de conteúdo expirado

A remoção de conteúdo expirado segue o seguinte procedimento:

- O CPM engloba um agendamento que é executado periódicamente em curtos de tempo (inferiores a um minuto), e quando um conteúdo atinge o limite máximo de visualizações, realiza um request ao LIS de forma a proceder à verificação de licenças expiradas;
- Caso existam licenças expiradas, o LIS irá realizar a remoção de todas as licenças expiradas e o levantamento do ID do conteúdo expirado a enviar ao CPM, procedendo assim à remoção de todo o conteúdo associado a este ID;
- O CPM comunica com o CRM, identificando o conteúdo expirado e procedendo com a sua remoção;
- O conteúdo deixa de estar acessível, sendo totalmente removido do sistema.

A Figura 24 ilustra todo esse processo por cada iteração.

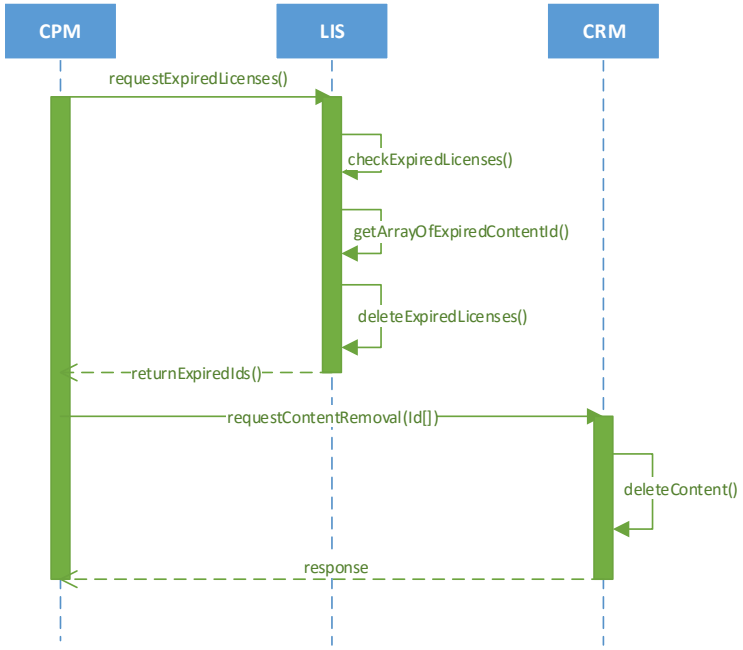



Figura 24 - Processo de remoção de conteúdo expirado

## 2.5. Protótipo

De forma a perceber a viabilidade da criação de um sistema de gestão de conteúdo e direitos digitais aplicado às redes sociais, que tem por base a investigação levada ao longo desta dissertação, desenvolveu-se um protótipo de um sistema nesta área, centrado no utilizador, de forma a que pudesse ser testado pelo mesmo.

Para este protótipo foram desenvolvidas algumas das funcionalidades pretendidas para um sistema deste tipo, que cumprem os objetivos propostos, e que permitem aos *testers* (utilizadores que testaram o sistema) perceber o sistema com vista à sua utilização e viabilidade. Posto isto, o seu desenvolvimento teve como base os seguintes propósitos:

- Tornar real a possibilidade dos utilizadores de redes sociais utilizarem um sistema com funcionalidades de proteção de conteúdos partilhados nas redes sociais;
- Demonstrar essa proteção com a explicação de todo o processo por detrás do sistema;
- Recolher uma avaliação real do trabalho desenvolvido no âmbito deste projecto, através de um questionário de avaliação por parte dos *testers*.

A implementação segue uma abordagem baseada na prototipagem, possibilitando, conforme referido, a criação de algumas funcionalidades-chave da aplicação e demonstrar as suas

potencialidades de um sistema de gestão de direitos digitais em conteúdos partilhados pelos utilizadores de redes sociais. As funcionalidades desenvolvidas e presentes neste protótipo são as seguintes:

- Acesso ao sistema através de uma extenção desenvolvida para o *browser* Google Chrome;
- Registo do utilizador no sistema através de uma rede social:
    - Utilizou-se, por questões de teste e simplificação, a autenticação via Facebook.
- Definição de condições de acesso ao conteúdo:
    - Número de visualizações permitidas;
    - Data e hora que o conteúdo expira.
- Registo de conteúdo:
    - Utilizou-se, para questões de teste e simplificação, o upload de imagens como conteúdo a ser registado na plataforma.
- Criação de um URL único por cada conteúdo gerado no sistema, a ser partilhado pelo utilizador;
- Validação do acesso ao conteúdo;
- Eliminação de conteúdo cujas licenças estão expiradas.

O protótipo desesenvolvido é baseado nas linguagens PHP, HTML5, JavaScript e CSS, no formato JSON e na base de dados MySQL, tendo sido utilizado para o seu desenvolvimento o PHPStorm como IDE (JetBrains, 2015), MySQL Workbench para gestão da base de dados (Oracle Corporation, 2015), WAMP Server para gestão do servidor e tecnologias utilizadas (Bourdon, 2015), e phpJobScheduler como gestor de agendamentos (Walker, 2014). Foram utilizados ainda as APIs para as extensões do Google Chrome (Google Chrome APIs, 2015) e do Facebook (Facebook Developers, 2015) para a integração da plataforma desenvolvida com estes sistemas.

### 2.5.1. Exemplo de utilização

De forma a compreender melhor o funcionamento do protótipo desenvolvido, vamos considerar o seguinte exemplo de utilização.

A extensão para o Google Chrome, apelidada de SND Extension (Social Network Digital Rights Management Extension), apresenta no seu primeiro contacto entre o utilizador e o sistema através de uma janela que solicita a autenticação deste, que deverá ser feita através do Facebook, através do botão *Login with Facebook*.

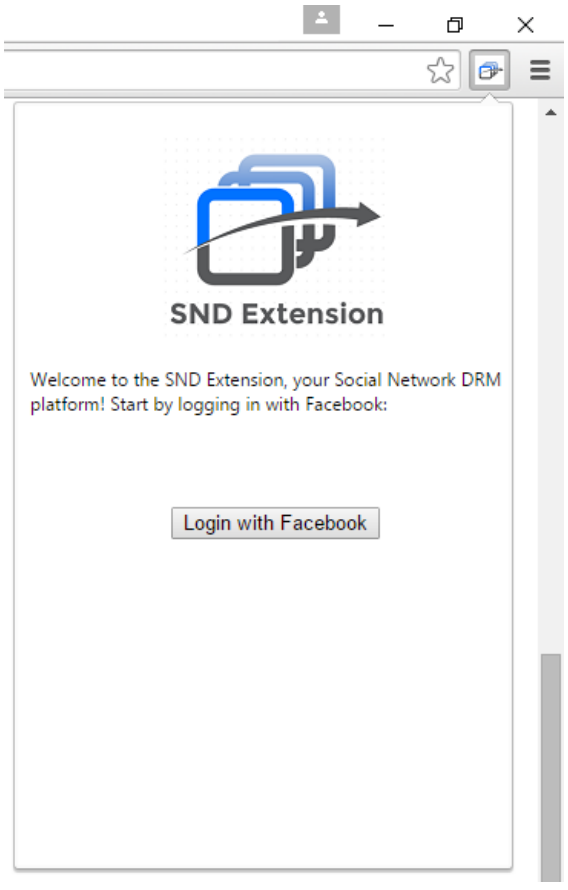



Figura 25 - Ecrã principal da *SND Extension*

Após o utilizador carregar no botão, é exibido um *popup* que pede a este, caso ainda não esteja autenticado nesta rede social, que efectue o seu login.

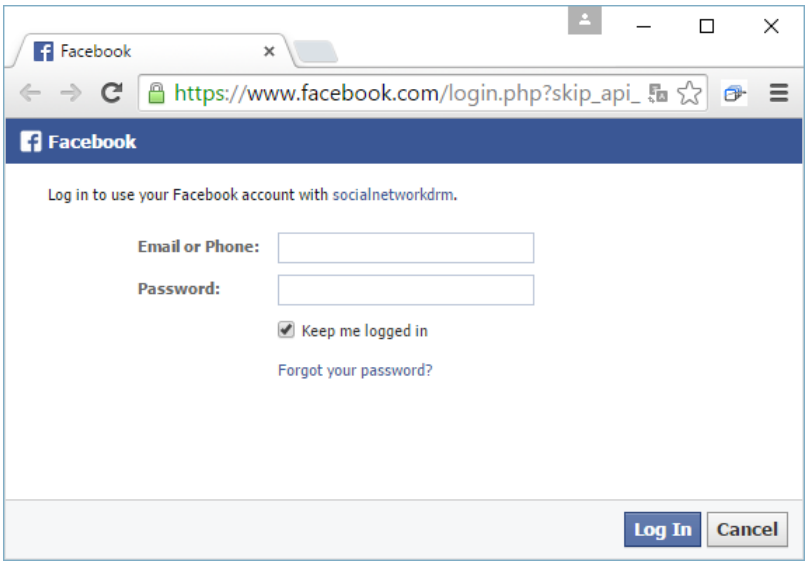



Figura 26 – *Popup* de pedido de autenticação do *SND Extension* via Facebook

Após estar autenticado na rede social, são solicitadas permissões de acesso a informação por parte do Facebook, informação essa que será utilizada pela plataforma, nomeadamente o seu perfil, o seu *email*, e a sua lista de amigos. Este *popup* apenas aparece no primeiro acesso à aplicação, ou quando alguma das permissões não foi concedida por parte do utilizador.

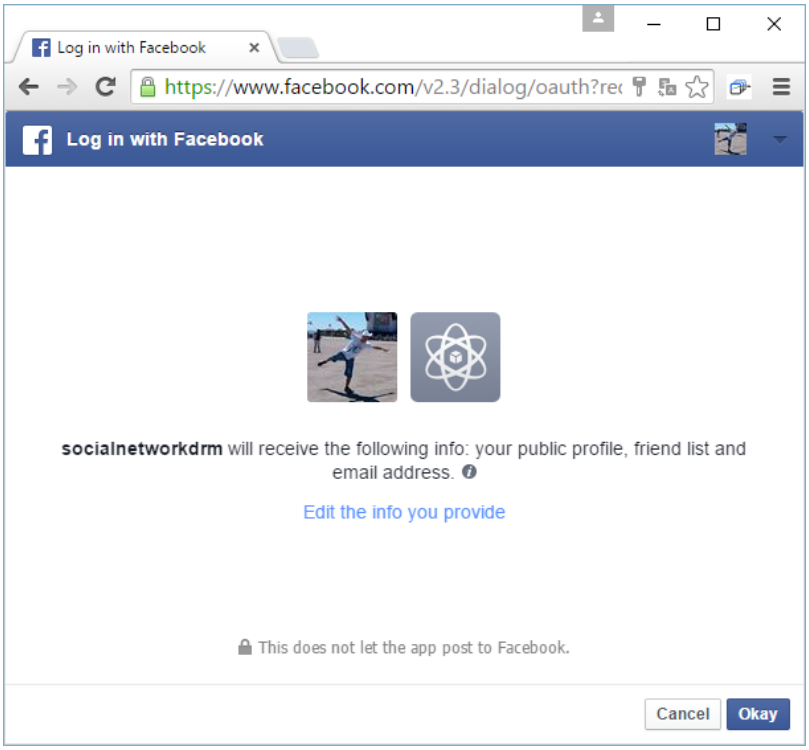



Figura 27 - *Popup* de permissões a serem atribuídas à plataforma

Após devidamente autenticado, é exibido o formulário de registo de conteúdo ao utilizador. Este poderá definir quantas visualizações este poderá ter, e/ou até que data e hora este se encontra disponível (Figura 28). Caso exista alguma restrição que não queira colocar, deverá deixar o campo nos formatos definidos na sua legenda. O utilizador selecciona a imagem que pertende publicar, e terá de carregar no botão *Submit*.

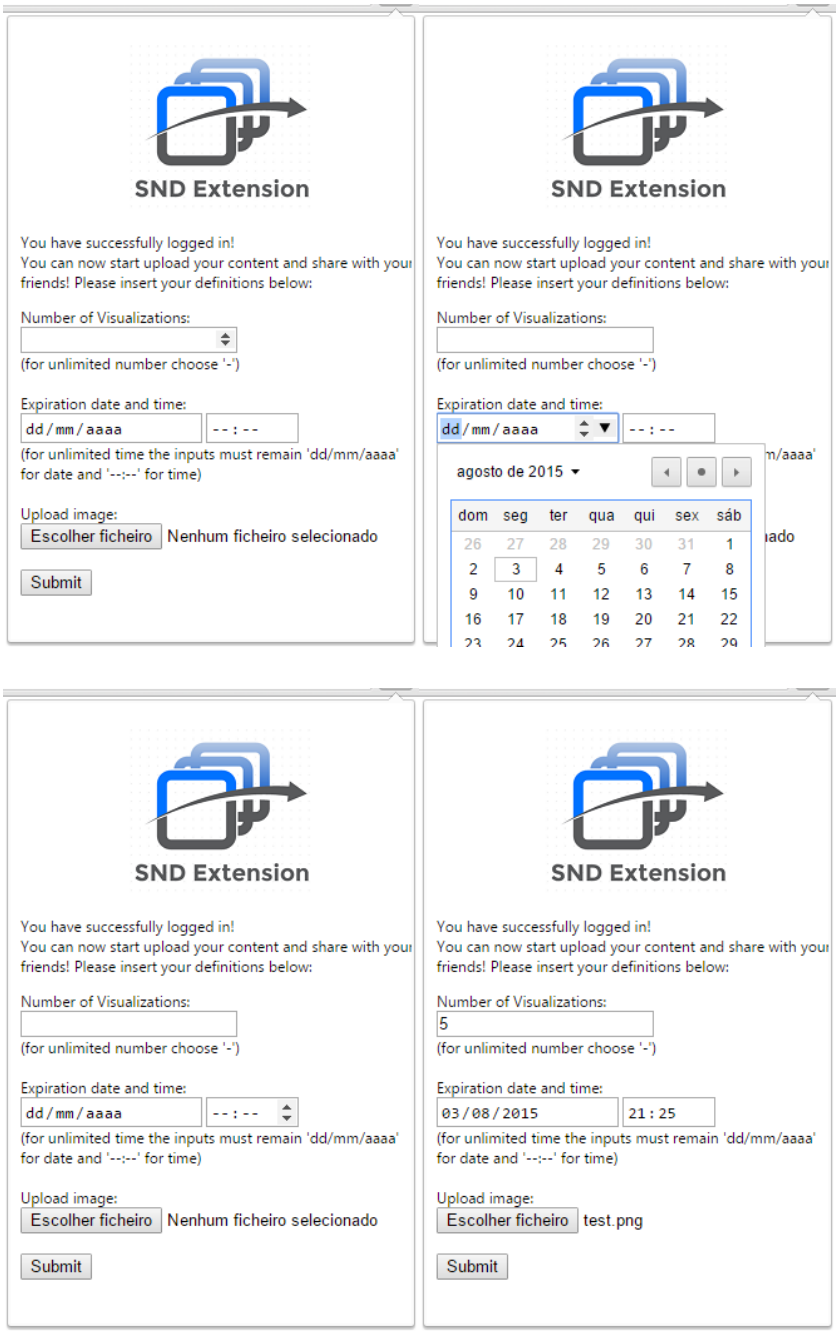



Figura 28 – Formulário de registo de conteúdo (fases de preenchimento)

Caso a submissão seja realizada com sucesso, será enviada para o utilizador uma mensagem de sucesso, juntamente com o link que poderá utilizar para partilhar o seu conteúdo.


Figura 29 - Mensagem de registo do conteúdo com sucesso e respetivo URL

Da perspetiva de uma pessoa que receba o *link*, ao abrir este num *browser*, terá o seguinte aspeto, confirme ilustrado na Figura 30.

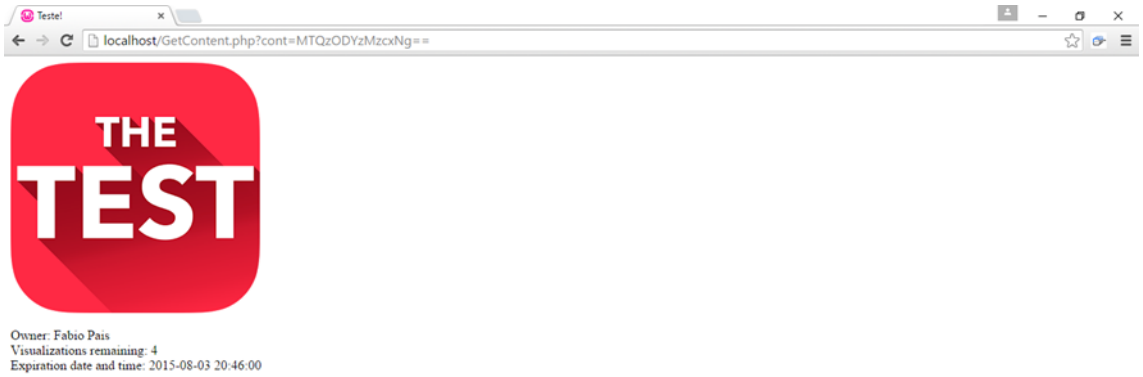



Figura 30 - Página HTML gerada pelo sistema, e acedida através do link partilhado

Caso o conteúdo tenha expirado, a mensagem exibida quando a pessoa acede ao link é a seguinte, conforme ilustrado na Figura 31.


Figura 31 - Mensagem de conteúdo inacessível

# 3. Validação e Avaliação

No âmbito da validação e avaliação da solução proposta, desenvolvida no âmbito desta dissertação, foi necessário perceber quais os hábitos dos utilizadores de redes sociais nestas redes, bem como a sua perceção de segurança e privacidade nestas redes, bem como qual a sua aceitação perante uma solução que lhes permita um maior controlo sobre o seu conteúdo, e assim, averiguar a sua viabilidade. Este estudo ocorre no sentido de responder às questões de investigação colocadas, bem como responder aos objetivos propostos no âmbito deste projeto e assim efetuar as devidas conclusões, servindo assim de instrumentos de validação e recolha de dados.

Para tal, procedeu-se à elaboração de dois inquéritos distintos: um primeiro, que tinha como objetivo perceber os hábitos, segurança e privacidade dos utilizadores de redes sociais, bem como a sua abertura para uma solução de gestão de conteúdos digitais em redes sociais e possíveis requisitos a levantar para a solução, e um segundo, para averiguar a aceitação destes utilizadores da solução, bem como a sua viabilidade, através de um teste ao protótipo desenvolvido.

## 3.1. Inquérito sobre hábitos, segurança e privacidade nas redes sociais

Este inquérito, conforme referido anteriormente, foi elaborado com o principal intuito de perceber quais os hábitos dos utilizadores de redes sociais, e a sua segurança e privacidade nestas redes, isto é, traçar o perfil dos utilizadores de redes sociais, e assim verificar a necessidade do desenvolvimento de um protótipo neste âmbito, considerações a ter em conta e o levantamento de potenciais requisitos, confronto com os resultados dos testes ao protótipo.

O inquérito, que pode ser consultado no Anexo C, é composto por 22 questões, definidas pelos seguintes tipos:

- Três questões de “Sim/Não” ;
- Duas questões de “Sim/Não/Talvez”;
- Quatro questões de escolha mútlipla com diversas respostas assinaláveis;
- Cinco questões de escolha múltipla com uma resposta assinalável;
- Duas questões de escala personalizada (escala de utilização)
- Cinco questões com resposta em escala de Likert de 1 a 10;
- Uma questão de resposta aberta.

O questionário foi disponibilizado online, através da plataforma de formulários do Google Drive, cuja amostragem foi realizada por método de "bola de neve", ou *word-of-mouth*, isto é, partilha do formulário nas redes sociais, por email, e outros mecanismos online, sendo toda a sua divulgação de caracter público, e recolha de dados realizada entre 15 de Maio e 21 de Junho de 2015.

A amostra deste inquérito é constituída por 111 pessoas, seguindo-se a análise às questões realizadas.

### 3.1.1. Sexo

Dos inquiridos, 39% são do sexo masculino e 61% do sexo feminino, equivalendo a 43 e 88 inquiridos, respetivamente, conforme ilustrado no Gráfico 1.

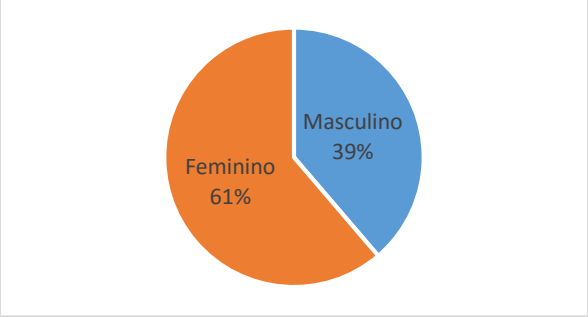



Gráfico 1 – Sexo dos inquiridos

### 3.1.2. Faixa etária

Em termos de faixa etária, 86,49% dos inquiridos situa-se entre os 18 e os 25 anos de idade, conforme representado no Gráfico 2. Seguem-se os inquiridos entre 26 e 39 anos com 11,71%, e os menores de 10 anos e entre 50 e 65 anos com 0,90% cada, sendo que as restantes faixas não apresentam qualquer inquirido.

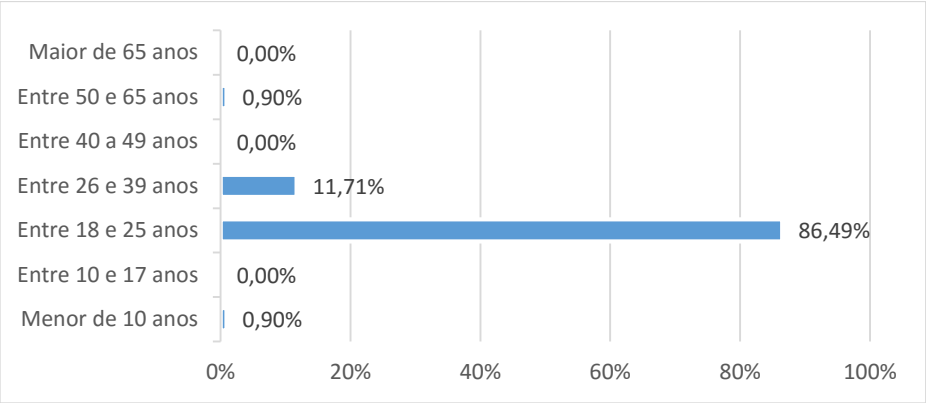



Gráfico 2 - Faixa etária dos inquiridos

### 3.1.3. Habilitações literárias

Conforme ilustrado no Gráfico 3, os inquiridos com licenciatura e ensino secundário são os que apresentam com maior representatividade, com 52,25% e 27,93% da amostra, respetivamente.

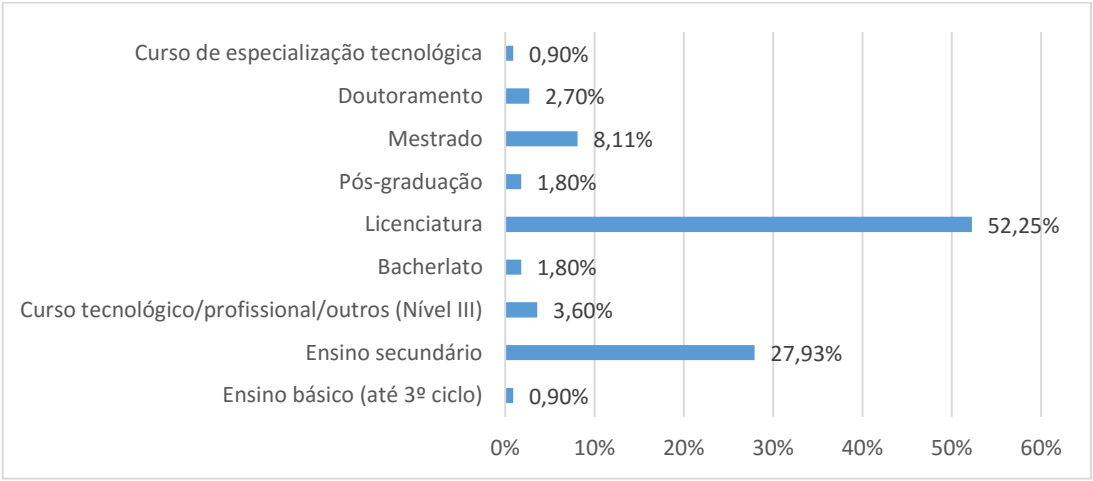



Gráfico 3 - Habilitações literárias dos inquiridos

### 3.1.4. É utilizador regular de redes sociais?

O Gráfico 4 representa a percentagem de utilizadores regulares de redes sociais, pelo que esta representa 99% da amostrágem, nomeadamente 110 inquiridos. Sendo esta a amostragem em estudo, o inquirido que respondeu "Não" terminou assim o seu inquérito, não sendo necessárias mais respostas para este, além das anteriormente referidas.

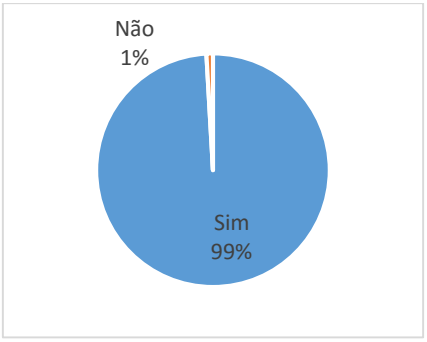



Gráfico 4 - Utilizadores regulares de redes sociais

### 3.1.5. Que redes sociais utiliza?

Entre os inquiridos utilizadores de redes sociais, 41,44% são utilizadores do Facebook, sendo dentro da amostra a rede social mais utilizada. Segue-se o Instagram, com 25,48%, e o Tumblr e Twitter, com 9,89% e 8,37% respetivamente.

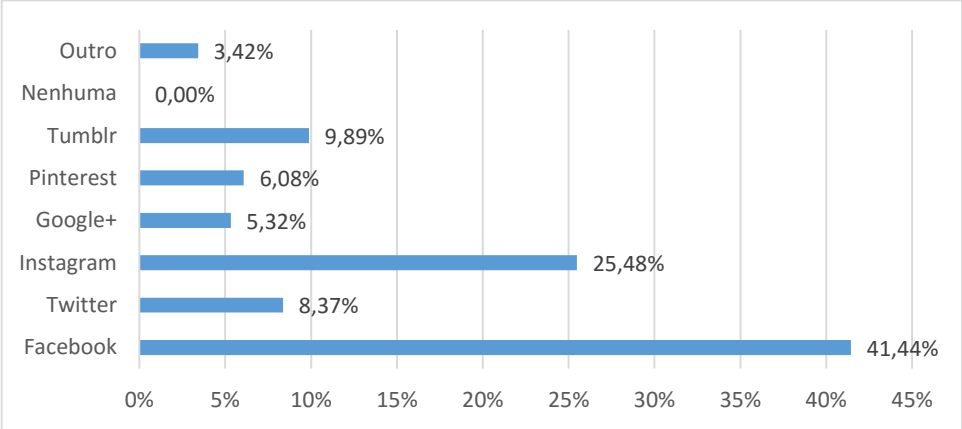



Gráfico 5 - Redes sociais utilizadas pelos inquiridos

### 3.1.6. Qual o dispositivo que mais utiliza para navegar/partilhar nas redes sociais?

Conforme ilustrado no Gráfico 6, o computador e o smartphone são os dispositivos mais utilizados pelos inquiridos para aceder às redes sociais, com 49% e 46% respetivamente.

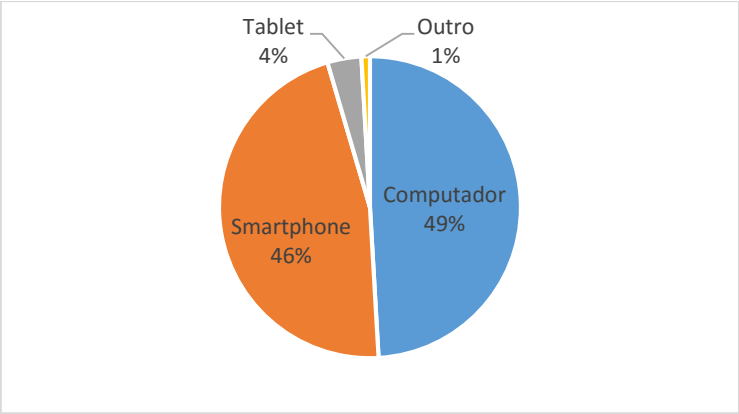



Gráfico 6 - Dispositivos mais utilizados para aceder às redes sociais

### 3.1.7. Das redes sociais que utiliza, com que frequência acede às mesmas?

Dos utilizadores das redes sociais referidas no Gráfico 7, o Facebook é a que apresenta a maior percentagem de acesso várias vezes ao dia, com 85,45% dos utilizadores a acederem com esta frequência, onde ainda, 11,82% afirma que acede pelo menos uma vez por dia. Segue-se o Instagram, onde 37,27% dos inquiridos que utilizam esta rede afirmam que acedem várias vezes ao dia, 13,64% acedem pelo menos uma vez por dia, existindo ainda 37,27% que afirma que nunca ou raramente acede a esta rede social. Os utilizadores das restantes redes, conforme evidenciado pelo gráfico, apresentam maiores percentagens de utilizadores que nunca ou raramente acedem a estas redes sociais.

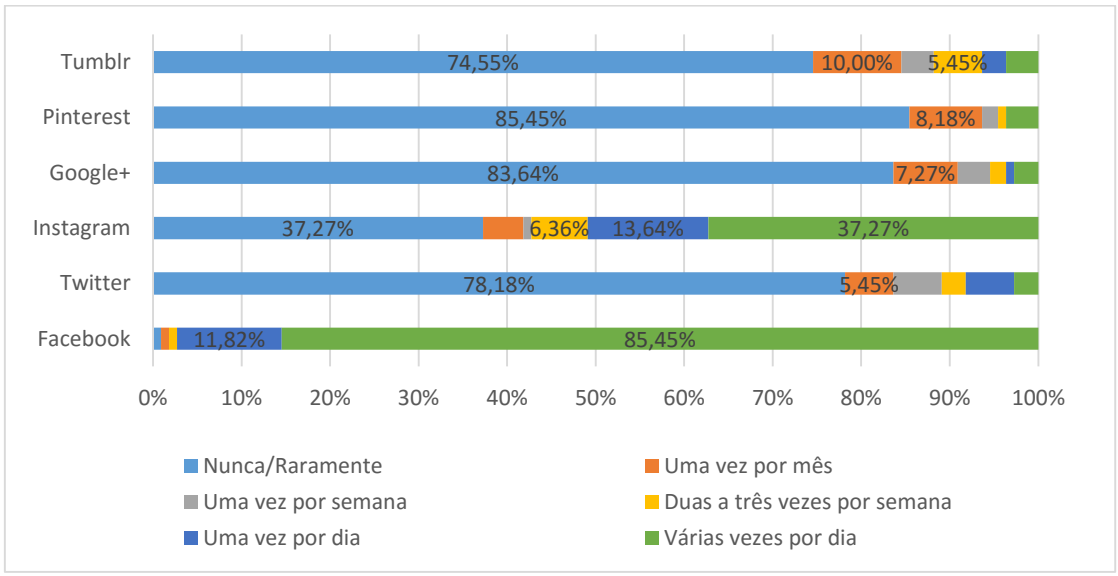



Gráfico 7 - Frequência de utilização das redes sociais

### 3.1.8. Indique, aproximadamente, com que frequência costuma publicar/partilhar o seguinte conteúdo

As fotografias são, para os inquiridos, os conteúdos partilhados com maior frequência, onde 33,64% partilha pelo menos uma vez por mês, 13,64% uma vez por semana, e 11,82% duas a três vezes por semana, conforme evidenciado no Gráfico 8. Os restantes conteúdos apresentam menor percentagem de partilha, sendo que os links de terceiros seguem-se nas frequências de partilha, onde 18,18% afirma partilhar pelo menos uma vez por semana, e 10,91% duas a três vezes por semana. Os vídeos e o texto apresentam características semenhantes em termos de hábitos de frequência de partilha.

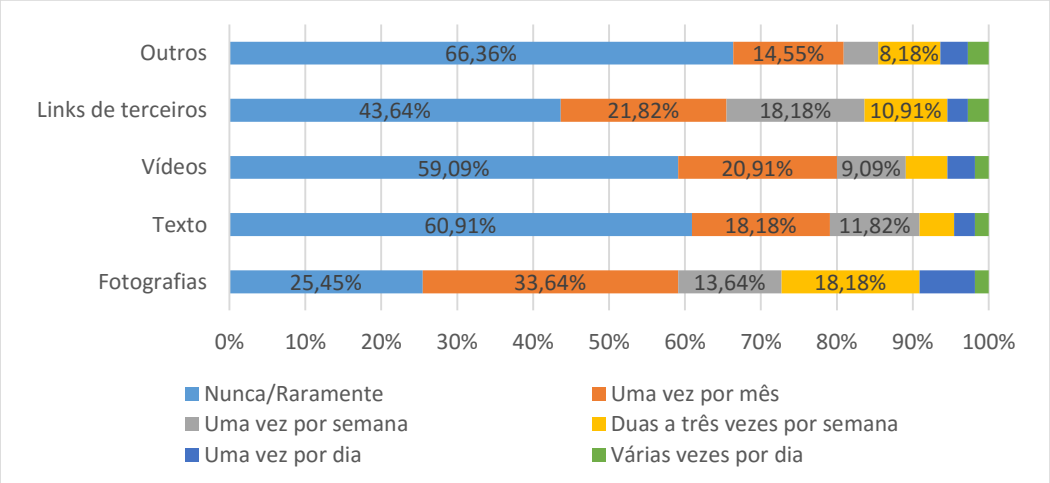



Gráfico 8 - Frequência de publicação/partilha de conteúdo

### 3.1.9. O que entende por privacidade?

Esta questão, de resposta aberta, tem como objetivo perceber o que é para os inquiridos, e utilizadores de redes sociais, o que estes entendem por privacidade. Entre as respostas recolhidas, é de consenso entre os inquiridos que a privacidade é o direito a ter um espaço pessoal, cujo conteúdo apenas diz respeito a quem estes pretendem partilhar, entre os quais família e amigos, sendo também o controlo sobre informações, conteúdos e dados pessoais dos mesmos. É ainda referido por alguns inquiridos que a privacidade é um direito à vida privada e à salvaguarda dos seus interesses relativamente a terceiros.

### 3.1.10. Antes de criar uma conta numa rede social, leu a sua respectiva política de privacidade?

Aquando o registo numa rede social, 81% dos inquiridos refere que não leu a política de privacidade, e apenas 19% refere que a leu, conforme ilustrado no Gráfico 9.

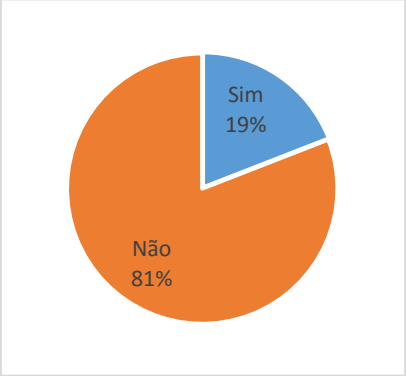
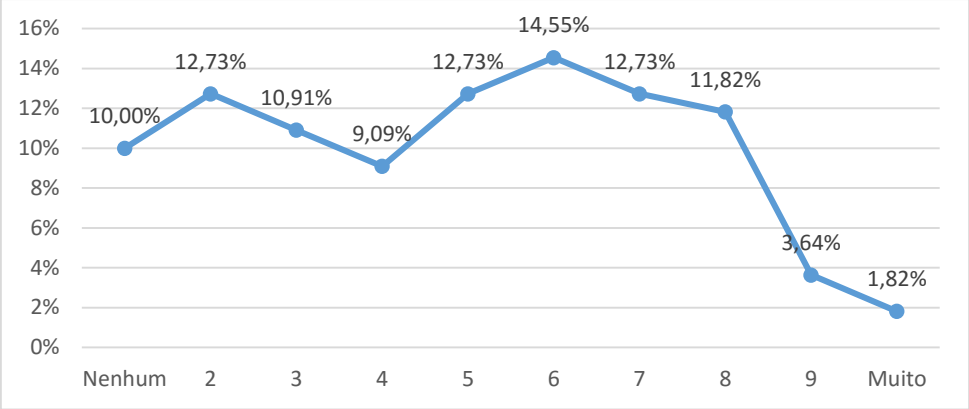



Gráfico 9 - Percentagem de leitura da política de privacidade de uma rede social

### 3.1.11. Qual o grau de conhecimento dos termos de privacidade das redes sociais que utiliza?

Considerando uma escala de Likert, onde "0" corresponde a "Nenhum" e "10" corresponde a "Muito", podemos verificar que 55,45% dos inquiridos tem um conhecimento igual ou inferior a "5", pelo que 10% refere que não tem qualquer conhecimento. Apenas 1,82% refere que o seu grau é "10" ("Muito"), e 3,64% afirma que o seu grau de conhecimento é "9".




**3.1.12.** Gráfico 10 - Grau de conhecimento dos termos de privacidade das redes sociais dos inquiridos**Qual o perfil de privacidade que tem por omissão na(s) rede(s) social(is) que mais utiliza?**

Conforme ilustrado no Gráfico 11, 70,91% dos inquiridos afirma que o seu perfil de privacidade é apenas para amigos. De notar ainda que 12,73% têm um perfil de privacidade personalizado, com as opções de personalização disponibilizadas pela rede social, e que apenas 4,55% tem o perfil como público. Nenhum dos inquiridos afirma desconhecer qual o seu perfil de privacidade por omissão.

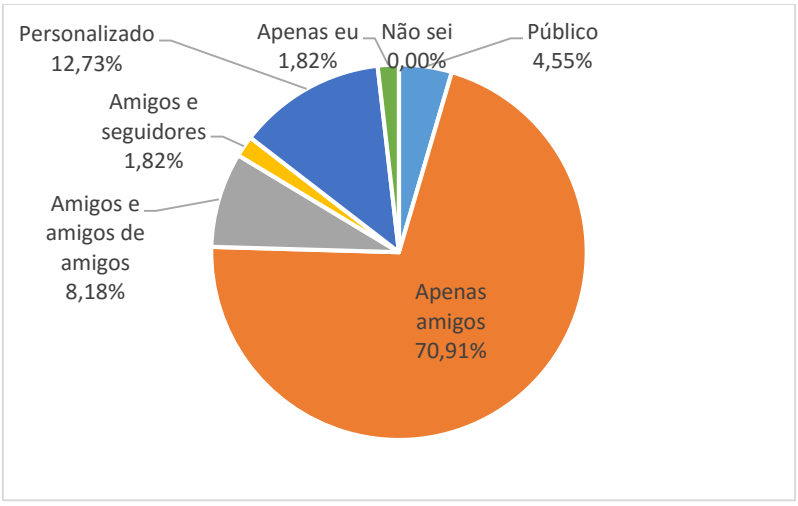



Gráfico 11 - Perfil de privacidade por omissão nas redes sociais dos inquiridos

**3.1.13. Costuma utilizar diferentes permissões de privacidade para publicações individuais?**

Para publicações individuais nas redes sociais, isto é, cada conteúdo publicado por um utilizador destas redes, 62,73% dos inquiridos afirma que utiliza uma diferente permissão de privacidade para os seus conteúdos, e 37,27% refere que não utiliza uma permissão diferente, ou seja, utiliza sempre a configurada por omissão.

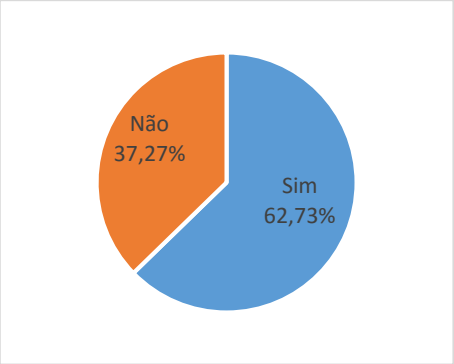



Gráfico 12 - Utilização de diferentes permissões de privacidade para publicações individuais dos inquiridos

### 3.1.14. Que importância tem para si o controlo do conteúdo que publica?

Conforme é possível observar no Gráfico 13, para os inquiridos, é muito importante o controlo do conteúdo publicado pelos mesmos, onde, numa escala de Likert de "1" ("Pouco importante") a "10" ("Muito importante"), 46,36% atribuiram 10 a esta importância, e apenas 3,64% dos inquiridos refere que é "Pouco importante, atribuindo 1 a esta importância.

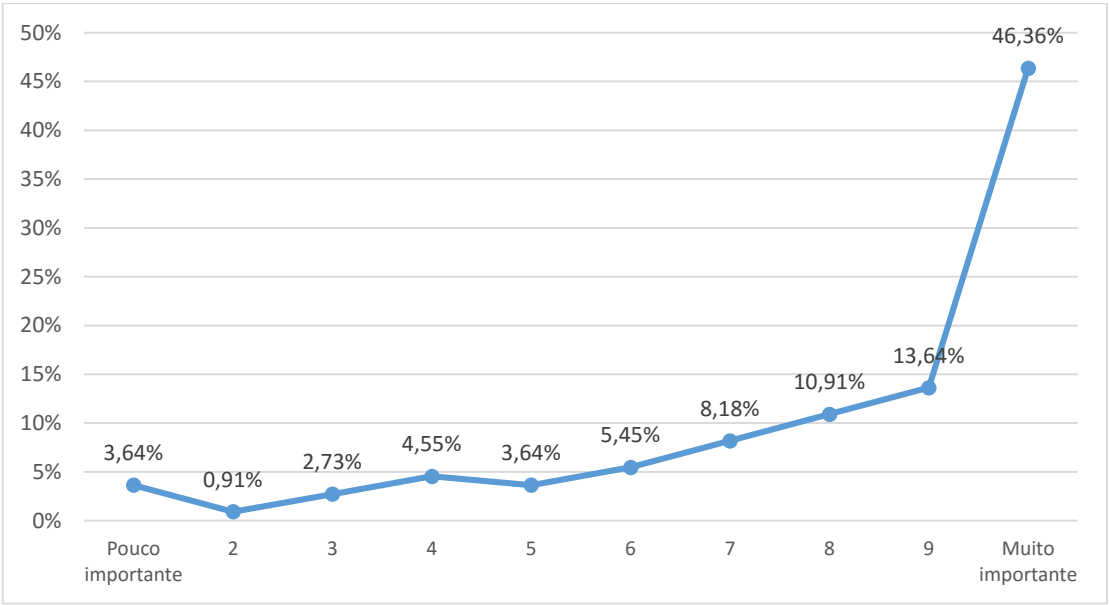



Gráfico 13 – Importância do controlo do conteúdo publicado

### 3.1.15. Qual o grau de importância de controlo e protecção que atribui aos seguintes conteúdos

Conforme é possível observar no Gráfico 14, as fotografias são o conteúdo considerado mais importante em termos de controlo, onde, relativamente a este conteúdo, 57,27% dos inquiridos considera muito importante, atribuindo "10" numa escala de Likert de "1" ("Pouco importante") a "10" ("Muito importante"). Seguem-se os vídeos, onde o nível 10 relativamente a este conteúdo foi atribuido por 38,18% dos inquiridos, posteriormente 25,45% ao texto, 18,18% a outros e 12,73% aos links de terceiros, relativamente ao conteúdo respetivamente.

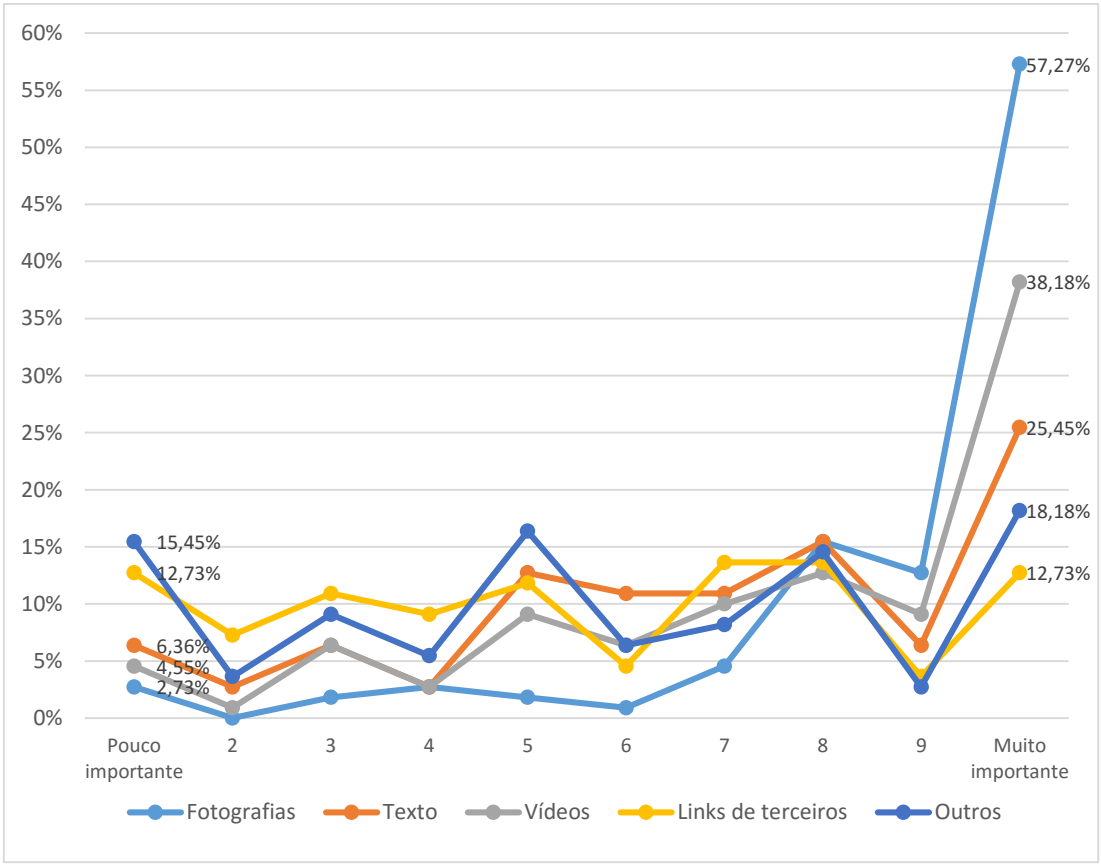



Gráfico 14 – Importância do controlo do conteúdo publicado pelos inquiridos

### 3.1.16. Para si, qual a importância da segurança e privacidade numa rede social?

Conforme é possivel observar no Gráfico 15, 60,55% dos inquiridos consideram que é muito importante a segurança e privacidade numa rede social, atribuindo o valor 10 numa escala de Likert de "1" ("Pouco importante") a "10" ("Muito importante"). De notar ainda as notas 8 e 9 atribuidas, com 11,93% para ambas respetivamente.

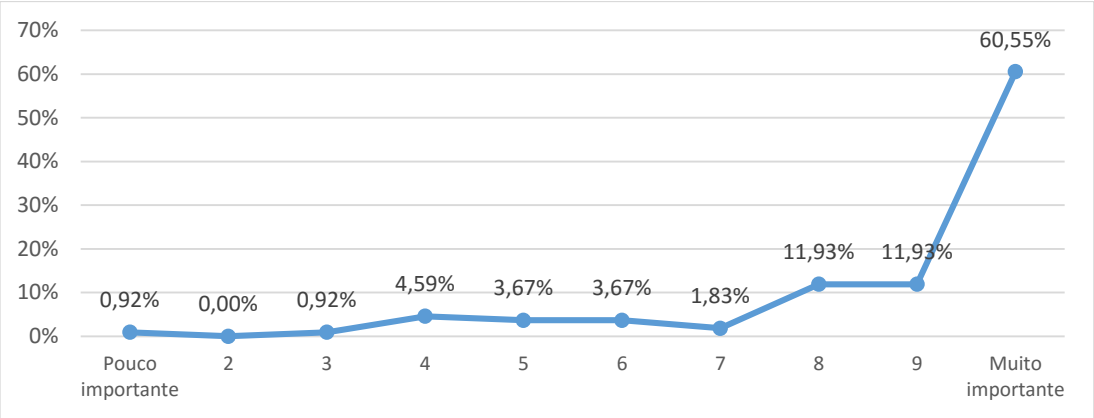



Gráfico 15 – Importância da segurança e privacidade numa rede social

### 3.1.17. Quando publica um determinado conteúdo numa rede social, como se sente em termos de proteção do mesmo?

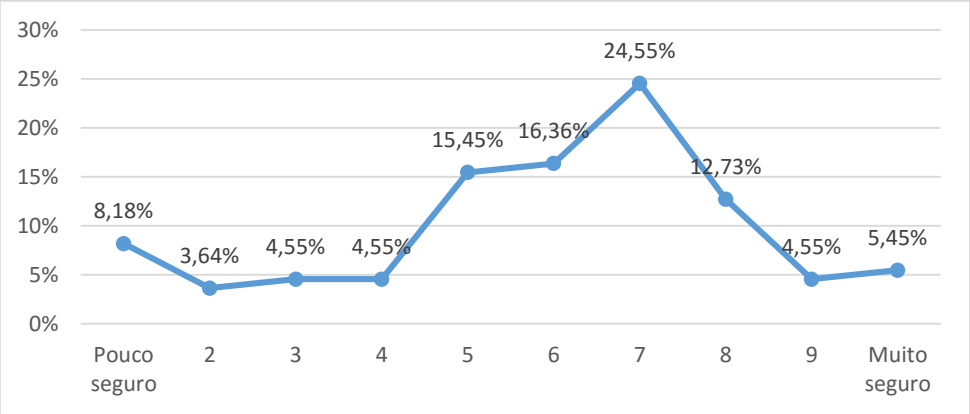



Gráfico 16 – Segurança dos inquiridos na publicação de conteúdo numa rede social

Os inquiridos revelam ter segurança na publicação dos seus conteúdos nas redes sociais, onde 24,55% dos inquiridos atribui o valor 7 numa escala de Likert de "1" ("Pouco seguro) a "10" ("Muito seguro"), notando ainda que os valores 5, 6 e 8 correspondem a 15,15%, 16,36% e 12,73% da opinião dos inquiridos, respetivamente. No entanto, é importante referir que 8,18% dos inquiridos sente-se pouco seguro, atribuindo o valor 1 na segurança da publicação de conteúdos nestas redes.

### 3.1.18. Que mecanismo preferia de forma a dar uma maior proteção às suas partilhas nas redes sociais?

De forma a perceber a preferência dos utilizadores no que toca à utilização de mecanismos para uma maior proteção dos seus conteúdos partilhados nas redes sociais, segue-se a seguinte questão. Conforme se pode observar no Gráfico 17, 36,25% dos utilizadores preferia utilizar uma aplicação da rede social com mais funcionalidades. De notar ainda que 26,88% dá preferência à utilização de grupos privados dentro da rede social, 18,75% prefere a utilização de uma extensão para browser e 10,63% utilizaria uma aplicação para computador. No entanto, 6,25 dos inquiridos referem que não têm nenhuma preferência pela utilização de mecanismos para a proteção dos seus conteúdos.

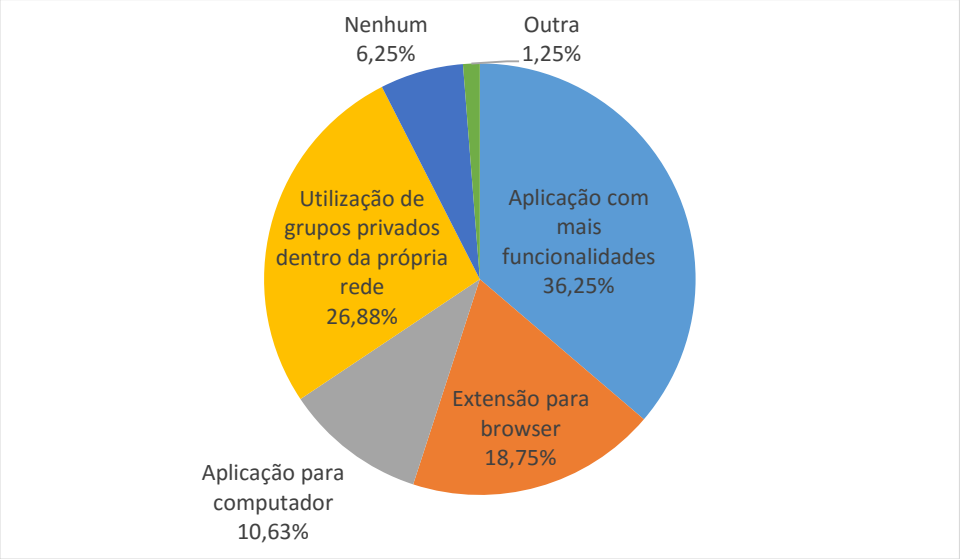



Gráfico 17 - Mecanismos de maior preferência para a proteção de conteúdos nas redes sociais

### 3.1.19. Utilizaria um *plugin* ou aplicação que permitisse um maior controlo dos seus conteúdos?

Conforme é possível observar no Gráfico 18, 60,91% dos inquiridos mostram interesse na utilização de um *plugin* ou aplicação que lhes permitisse um maior controlo dos seus conteúdos, respondendo "Sim". De referir ainda que 36,36% dos inquiridos afirma que talvez utilizasse o *plugin*, sendo que apenas 2,73% não mostra nenhum interesse na sua utilização.

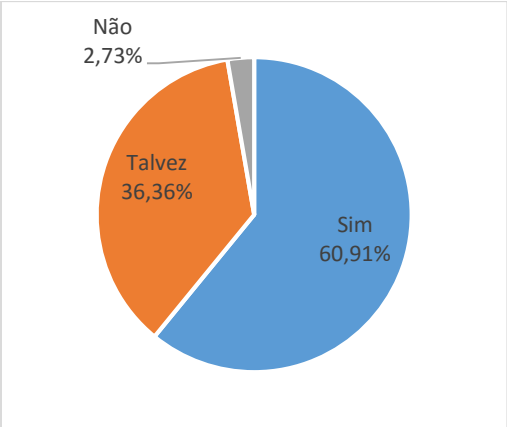



Gráfico 18 - Interesse dos inquiridos em utilizar um *plugin* ou aplicação para maior controlo dos seus conteúdos nas redes sociais

### 3.1.20. Utilizaria o *plugin* para o seu *browser*, mesmo que este fosse feito por terceiros (isto é, não desenvolvido pela própria rede), mas que garantisse a proteção dos seus dados?

Na situação do *plugin* ser desenvolvido por terceiros, existe alguma incerteza na sua utilização, onde 53,27% dos inquiridos afirmam que talvez utilizem a solução. No entanto, 39,25% dos inquiridos afirma que utilizaria o *plugin*, e apenas 7,48% diz que não utilizaria de todo, conforme ilustrado no Gráfico 19.

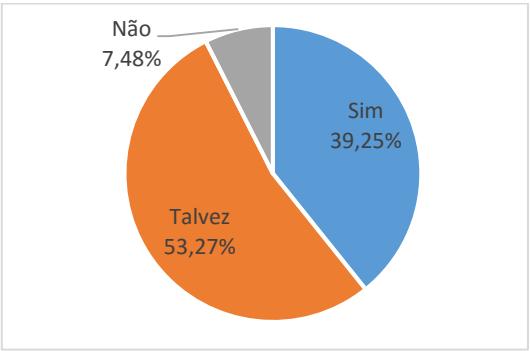



Gráfico 19 – Interesse dos inquiridos na utilização de um *plugin* feito por terceiros

### 3.1.21. Que funcionalidades gostaria de ver no *plugin*?

Dos inquiridos interessados na utilizaçao do plugin, 58,50% gostariam de utilizar uma funcionalidade para limitar o conteúdo para um determinado grupo de pessoas, conforme

ilustrado no Gráfico 20. De notar ainda que 26,53% gostaria de poder limitar o conteúdo por tempo disponivel e 10,88% gostaria de limitar o seu conteúdo por número de visualizações.

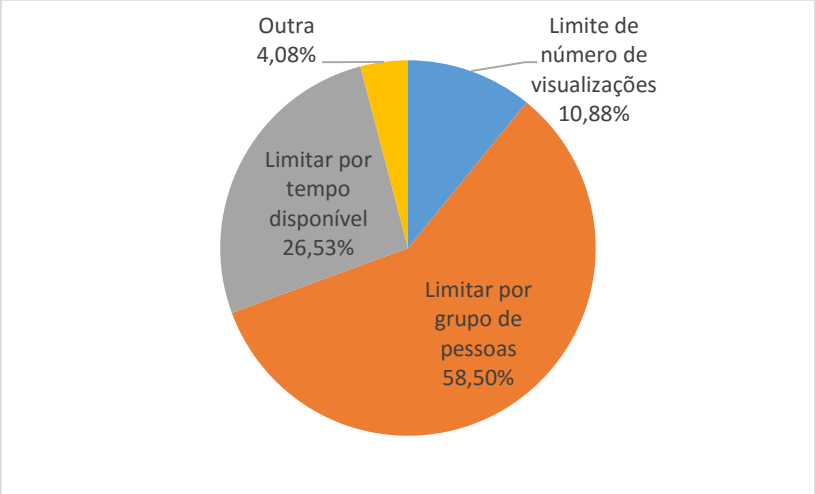



Gráfico 20 - Funcionalidades que os inquiridos gostariam de ver no *plugin*

### 3.1.22. Porque não estaria interessado na utilização do *plugin*?

Dos inquiridos que não estão interessados na utilização do *plugin*, 33,33% não acha a solução segura ou não sente necessidade. 16,67% dos inquiridos não quer instalar aplicações de terceiros, ou refere outra razão para não utilizar o *plugin*.

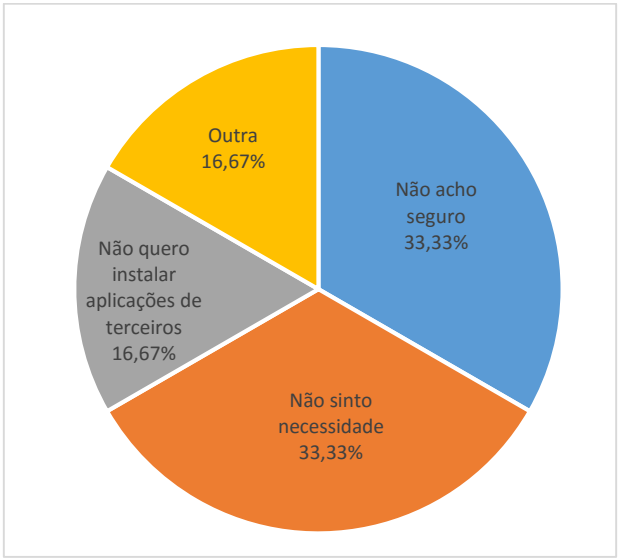



Gráfico 21 - Razões dos inquiridos que não estão interessados na utilização do *plugin*

### 3.1.23. Conclusões

Através do inquérito realizado, é possível concluir que existe preocupação por parte dos utilizadores pelas questões de segurança, privacidade, e controlo de conteúdos nas redes sociais. No entanto, existe ainda alguma falta de conhecimento relativamente às políticas de privacidade destas redes, pelo que o desconhecimento do tratamento da informação fornecida pelos utilizadores destas redes poderá implicar uma falta de proteção dos seus conteúdos ou desconhecimento de procedimentos que poderão aumentar o seu controlo pelos seus conteúdos.

Em termos de conteúdos gerados pelos utilizadores, isto é, conteúdos pessoais, as fotografias são sem dúvida o conteúdo mais privilegiado pelos inquiridos, sendo estes os que têm especial atenção aquando da sua publicação, a sua segurança, e a quem deverão ser partilhados. Os vídeos também têm bastante relevância na sua segurança.

Em geral, embora não totalmente, os inquiridos sentem-se seguros na utilização das suas redes sociais. No entanto, ainda existe algum receio quanto à segurança e proteção dos seus conteúdos nestas redes.

Tudo isto abre espaço para a criação de soluções que permitam uma maior gestão e controlo de conteúdos digitais dos utilizadores destas redes. Os inquiridos revelam bastante interesse na utilização de uma solução com estas caracteristicas. No entanto, mostram algum receio em relação ao facto de esta ser desenvolvida por terceiros, isto é, não descartando ainda a sua utilização, pois apenas uma percentagem residual afirmou que não utilizaria de algum modo a solução.

## 3.2. Inquérito de feedback sobre a *SND Extension*

De forma a validar esta solução, isto é, avaliar o protótipo desenvolvido, e estudar a viabilidade da solução concebida, foram realizados testes com 50 pessoas, tendo estes sido escolhidos de forma aleatória.

Os testes foram realizados de forma acompanhada, com um primeiro *briefing* ao tema da tese e ao funcionamento da solução desenvolvida no âmbito da mesma, bem como uma explicação passo-a-passo das suas interações com a extensão e todo o processo que estava a ocorrer por de trás, de forma a que os utilizadores compreendessem corretamente o seu funcionamento e eventuais esclarecimentos de dúvidas e questões colocadas pelos mesmos.

De referir que os *testers* foram devidamente informados de que o que iriam testar seria apenas um protótipo com algumas das funcionalidades propostas, e que se encontrava num ambiente controlado, isto é, instalado em apenas um computador, que serviu igualmente de servidor.

Após o teste de utilizadores, os testers realizaram um inquérito, de forma individual, com o objetivo de avaliarem o uso da extensão - pontos positivos, pontos negativos, possíveis sugestões e verificar se utilizariam, ou não, uma versão final do protótipo.

O inquérito, que pode ser consultado no Anexo D, é composto por 11 questões, definidas pelos seguintes tipos:

- Duas questões com resposta em escala de Likert de 1 a 10, divididas da seguinte forma:
    - Uma com 8 frases, de "Discordo completamente" a "Concordo completamente;
    - Uma com 3 frases, de "Muito difícil" a "Muito fácil";
- Três questões de resposta aberta
- Três questões de "Sim/Não/Talvez";
- Três questões de escolha múltipla com uma resposta assinalável;

O questionário foi realizado precencialmente através de um formulário online, através da plataforma de formulários do Google Drive, cuja recolha de dados foi realizada entre 14 e 30 de Junho.

### 3.2.1. Sexo

Dos utilizadores que testaram o protótipo desenvolvido, 46% são do sexo masculino e 54% do sexo feminino, conforme ilustrado no Gráfico 22.

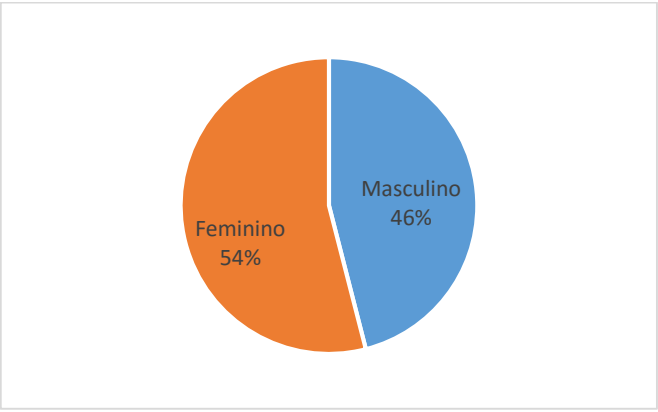



Gráfico 22 - Sexo dos utilizadores

### 3.2.2. Faixa etária

Em termos de faixa etária, 84% dos utilizadores situa-se entre os 18 e os 25 anos de idade, conforme representado no Gráfico 23. Seguem-se os inquiridos entre 26 e 39 anos com 12%, entre 40 e 49 anos e entre 50 e 65 anos com 2% cada.

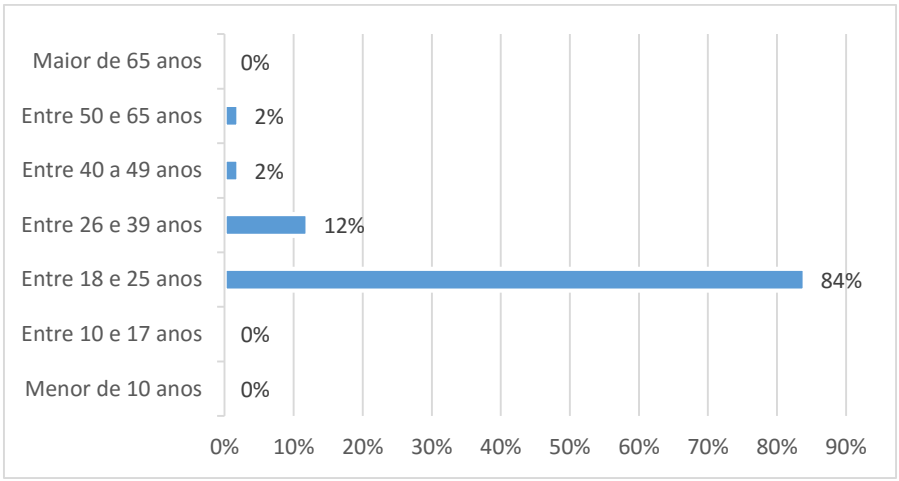



Gráfico 23 - Faixa etária dos inquiridos

### 3.2.3. Habilitações literárias

Conforme ilustrado no Gráfico 24, os utilizadores com ensino secundário e licenciatura são os mais representados, correspondendo a 40% e 44% dos utilizadores, respetivamente. De notar ainda que 6% dos utilizadores revela ter Mestrado e 10% um Curso de Nível III.

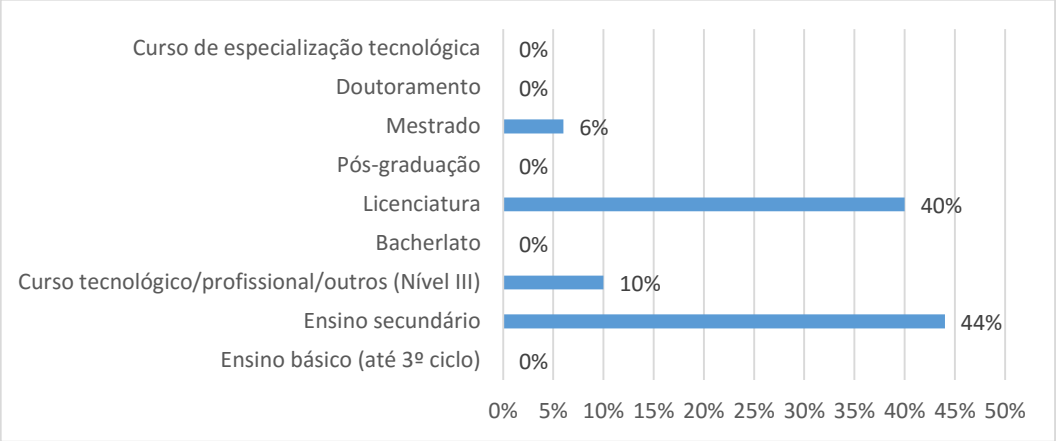



Gráfico 24 - Habilitações literárias dos utilizadores

### 3.2.4. Indique, numa escala de 1 (Discordo completamente) a 10 (Concordo completamente), o quão concorda com as seguintes frases

De modo a obter de uma forma mais quantitativa a opinião dos testers, realizou-se a questão recorrendo à escala de Likert, de "1" a "10", a oito frases. De forma a facilitar a análise, definiram-se os seguintes grupos de frases, identificados pelos seus respectivos gráficos:

#### 3.2.4.1. Utilização do protótipo

Conforme é possível observar no Gráfico 22, a concordância com as frases é positiva, pelo que 40% dos utilizadores concordam que a aplicação é simples de utilizar, atribuindo o valor "10", sendo ainda que o conjunto entre os valores "8" e "9" corresponde a 54% dos utilizadores. Os utilizadores consideram ainda que a aplicação é intuitiva, sendo que 24% atribui o valor "8", 36% atribui "9" e 18% atribui "10". Quanto ao interesse por parte dos utilizadores de redes sociais na aplicação, os utilizadores também concordam, com 38% a atribuir o valor "10" e 34% a atribuir o valor "9".

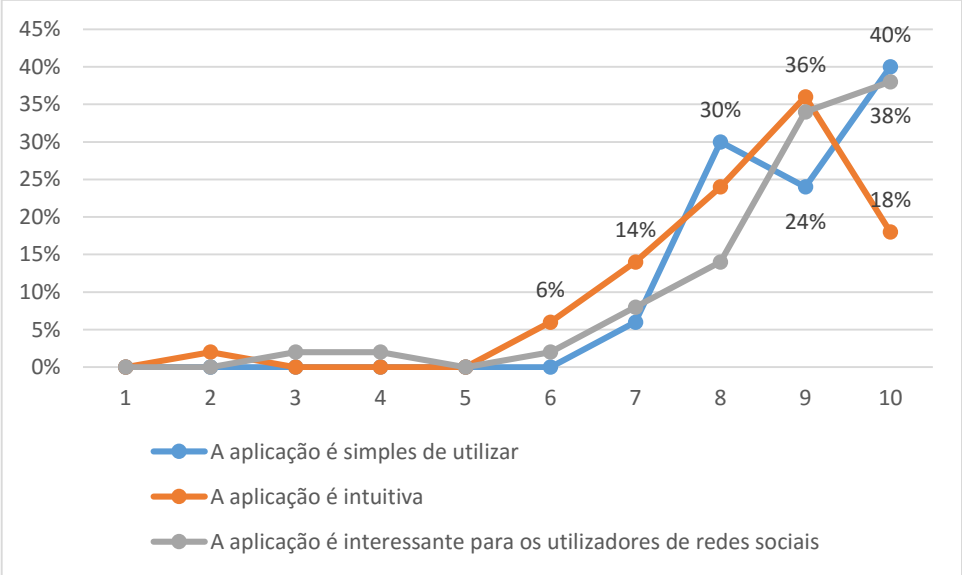



Gráfico 25 – Concordância com as frases em termos de utilização do protótipo

#### 3.2.4.2. Segurança e controlo de conteúdo no protótipo

Em termos de segurança e controlo de conteúdo na utilização do protótipo, conforme ilustrado no gráfico 23, os utilizadores sentiram-se seguros na sua utilização, onde 22% atribuiu o valor "8" e 38% atribuiu "9", mas, no entanto, o valor "10" desce para 26%. Relativamente à

privacidade, os utilizadores concordam muito com a frase, onde 40% atribuiu o valor "10" e 32% atribuiu "9". Os utilizadores também concordam muito relativamente ao controlo do seu conteúdo, onde igualmente 40% atribuiu o valor "10", 26% atribuiu "9" e 24% atribuiu "8".

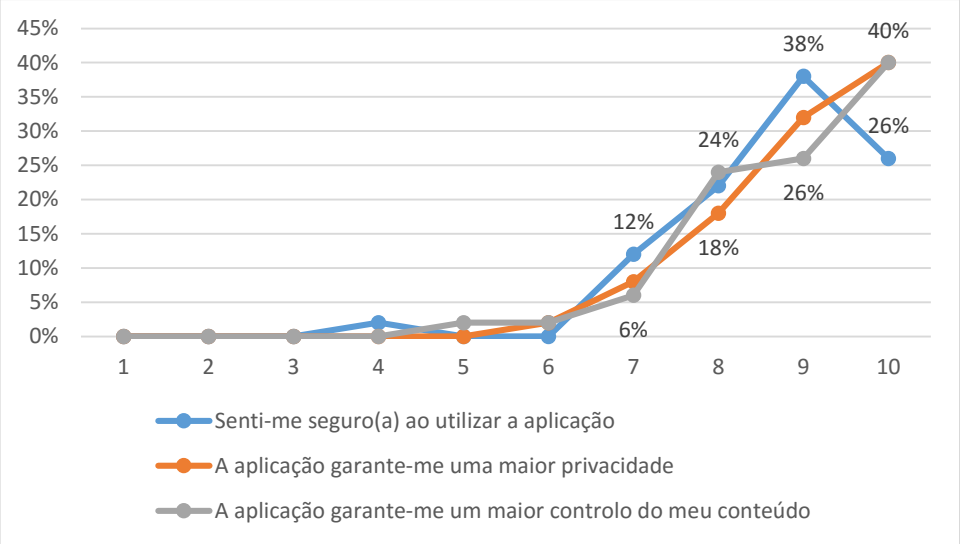



Gráfico 26 - Concordância com as frases em termos de segurança e controlo de conteúdo na utilização do protótipo

### 3.2.4.3. Dificuldades do protótipo

Quanto a dificuldades em perceber o protótipo e a sua utilização, alguns utilizadores revelaram que a aplicação é demasiado técnica, onde 14% atribuiu o valor "7" em termos de concordância, e 6% atribuiu "6" e "8" respetivamente. No entanto, 16% não concordou com a frase, atribuindo o valor "1", 22% atribuiu "2" e 18% atribuiu "3". Quanto à dificuldade em aceder à aplicação, os utilizadores discordam da existência da mesma, onde 36% atribui o valor "1", 20% o valor "2" e 18% o valor "3". É de referir que, no entanto, ainda existe uma percentagem relevante de utilizadores que concordam com a dificuldade no seu acesso, com 10% a atribuir o valor "10" em termos de concordância com esta afirmação.

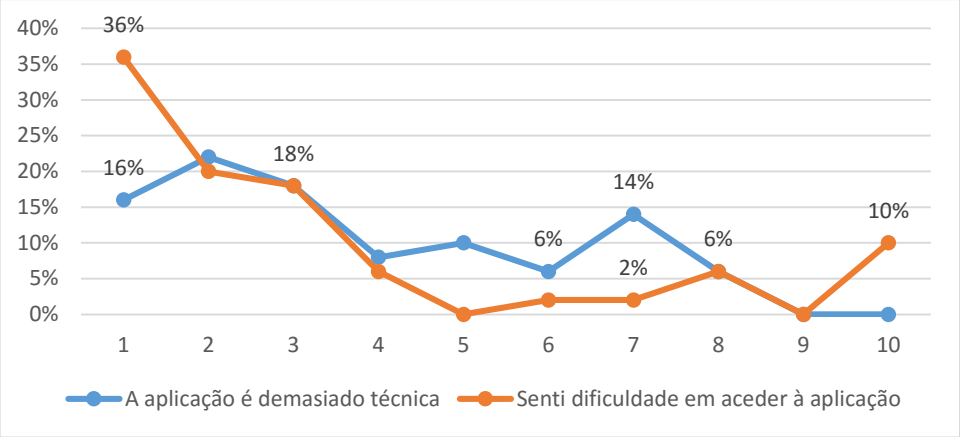



Gráfico 27 - Concordância com as frases em termos de dificuldades utilização do protótipo

### 3.2.5. Indique, numa escala de 1 (Muito difícil) a 10 (Muito fácil), a utilização das funcionalidades que testou

Com o intuito de perceber a facilidade de utilização das funcionalidades testadas na utilização do protótipo, o utilizador avaliou, numa escala de Likert de "1" ("Muito difícil") a "10" ("Muito fácil") as frases representadas no seguinte gráfico:

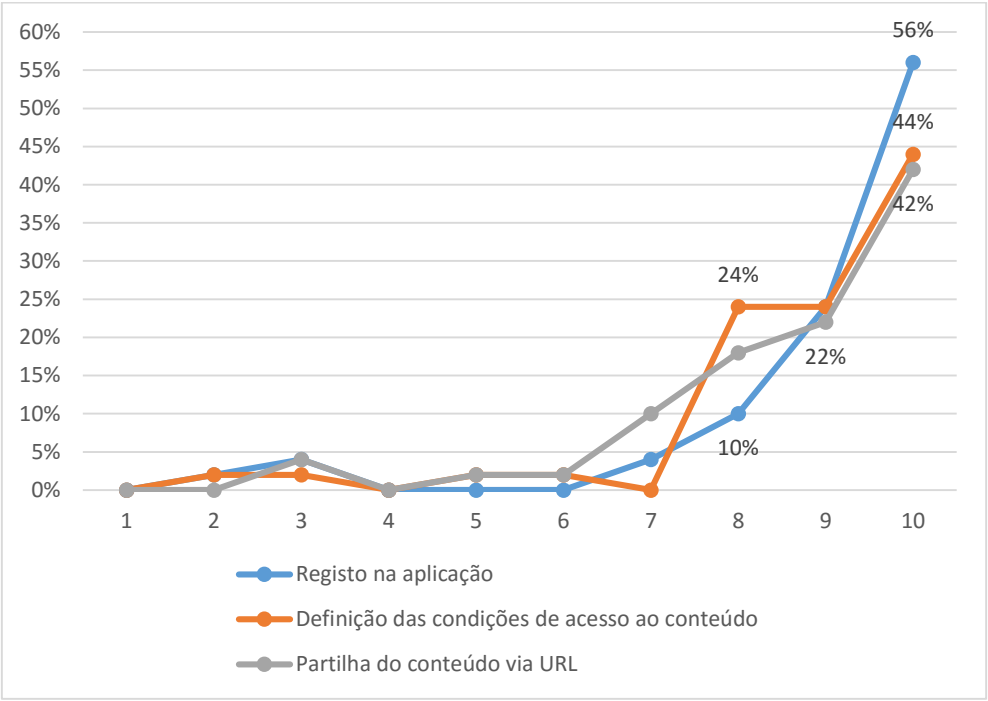



Gráfico 28 – Facilidade de utilização das funcionalidades do protótipo

Conforme é possível observar no Gráfico 25, os utilizadores consideram que o protótipo é muito fácil de utilizar, onde 56%, 44% e 42% atribuiram o valor "10" ao registo na aplicação, definição das condições de acesso ao conteúdo, e partilha do conteúdo via URL, respetivamente. É importante ainda referir que os valores 8 e 9 foram ainda bastante atribuidos às afirmações.

### 3.2.6. Que pontos positivos considerou na aplicação?

Dentro dos pontos positivos considerados pelos utilizares, os mais recorrentes centram-se na privacidade alcançada pelo protótipo e personalização através da criação de licenças e gestão do mesmo conteúdo. A fácil utilização e o facto da informação ser efetivamente apagada quando a licença do conteúdo expira são também pontos importantes referidos pelos *testers*, bem como permitir a autenticação através das redes socials, nomeadamente o Facebook, e a sua fácil partilha através do *link* gerado.

### 3.2.7. Que pontos negativos considerou na aplicação?

Entre os pontos negativos mais referidos encontra-se o design do protótipo, que deveria estar mais desenvolvido, alguma limitação de utilização por estar restringido a uma extensão de *browser* (nomeadamente o Google Chrome), alguma dificuldade na partilha do *link* gerado, e possível complexidade na percepção do seu funcionamento, bem como o facto de ainda se tratar de um protótipo. É de referir ainda que 18 dos 50 utilizadores que testaram o protótipo não têm nenhum ponto negativo a apontar.

### 3.2.8. Que funcionalidades gostaria que fossem implementadas?

Relativamente a novas funcionalidades a implementar, os utilizadores referem a partilha com amigos em específico, ligação por via de outras redes sociais para além do Facebook, o *link* ser automáticamente copiado para o *clipboard* de forma a facilitar a sua partilha, a partilha de outros tipos de conteúdos multimédia, como vídeos ou documentos, a recepção de um email sempre que um conteúdo expira, e botões automáticos de partilha com as diversas redes sociais. De notar que 12 dos 50 utilizadores afirmam não ser necessário acrescentar mais funcionalidades.

### 3.2.9. Considera a integração de uma solução deste tipo no navegador de Internet diferenciador?

Relativamente ao fator de diferenciação, 82% dos utilizadores consideram que a solução apresentada é diferenciadora por ser integrada num *browser*. Apenas 2% consideram este fator como não sendo diferenciador, e 16% afirma que talvez contribua para a sua diferenciação.

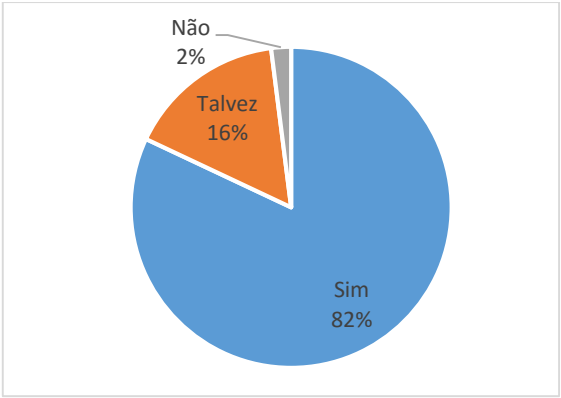



Gráfico 29 – Concordância com diferenciação da solução pela integração num navegador de Internet

### 3.2.10. Considera que esta aplicação atinge o objetivo a que se propõe?

De forma unânime, os utilizadores do protótipo afirmam que a solução proposta atinge o objetivo a que se propõe, isto é, garantir uma maior proteção e privacidade dos conteúdos digitais gerados pelos utilizadores, bem como a sua definição de condições de acesso a estes.

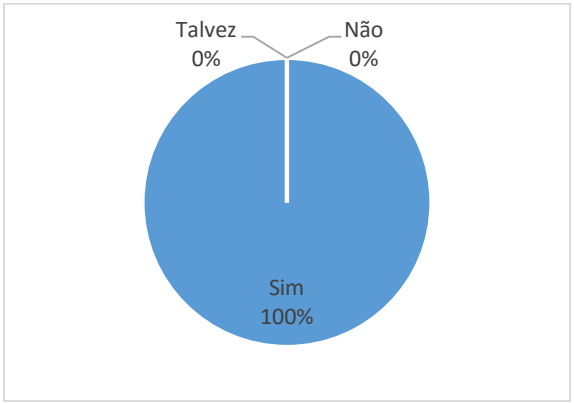



Gráfico 30 – Concordância quanto ao objetivo a que a solução proposta se propõe

### 3.2.11. Utilizaria o produto final da aplicação que testou?

Relativamente à utilização do produto final do protótipo testado, as respostas foram também positivas, onde 80% afirma que utilizaria o mesmo, 18% afirma que tavez utilize, e apenas 2% refere que não o utilizaria.

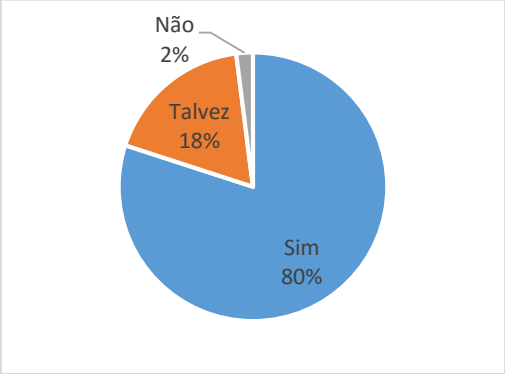



Gráfico 31 - Utilização do produto final do protótipo testado

### 3.2.12. Conclusões

O *feedback* dos utilizadores que testaram o protótipo foi bastante positivo, onde vários destes afirmaram que utilizariam um produto final resultante desta solução. É, no entanto, importante garantir a privacidade dos utilizadores, a integridade e segurança do conteúdo, e deixar bem claro qual o intuito da solução, bem como a sua forma de funcionamento. Deve ser de fácil utilização, intuitiva e com um design apelativo, mas ao mesmo tempo minimalista. O facto de ser uma extensão para um *browser* é visto como um fator diferenciador, mas ao mesmo tempo, poderá ser uma limitação à própria utilização do sistema.

Durante os testes de utilização, foi referido aos utilizadores que a solução ainda era um protótipo, pelo que esta apenas tinha implementadas as funcionalidades base e um design ainda em bruto, mas que garantisse a percepção do seu funcionamento e facilidade de utilização, bem como o seu funcionamento "por trás", isto é, aquele que não é visualizado normalmente pelo utilizador e que não necessita interacção deste, nomeadamente o registo do conteúdo e a sua eliminação após a sua licença ter expirado.

Embora tenham sido referidos alguns pontos negativos, grande parte devem-se ao facto da solução ainda ser apenas um protótipo, explicado durante o teste da aplicação, mas ainda um número considerável de utilizadores não tem pontos negativos a referir, nomeadamente 18 dos 50 utilizadores que testaram o protótipo. Os pontos referidos, servem portanto como formas a melhorar no sistema.

As sugestões referidas pelos utilizadores podem ser consideradas pertinentes, sendo que algumas delas já estão consideradas na solução, e outras poderão ser implementadas, garantindo assim ainda mais costumização à aplicação.

O facto de todos os utilizadores revelarem que a solução cumpre o objetivo a que se propõe, e a sua elevada taxa de aceitação, levam a concluir que existe interesse no desenvolvimento da solução e na sua utilização.

# Conclusão

O desenvolvimento e a proliferação de redes sociais, bem como a massificação do seu uso, levanta o problema da privacidade e proteção dos conteúdos gerados pelos utilizadores destas redes, que se apoiam nas mesmas para a partilha desses mesmos conteúdos. O desconhecimento de muitos utilizadores da política de privacidade das redes, como a utilização e disponibilização dos seus conteúdos, ou até mesmo questões relativas à remoção do seu conteúdo, pode não salvaguardar a sua proteção, pelo que foi nesse sentido que se levantou o problema a ser resolvido por esta dissertação.

Cada rede social tem a sua forma de funcionamento e um determinado público-alvo. Mesmo com as opções disponibilizadas por estas redes, referentes à gestão de permissões de acesso aos conteúdos publicados pelos utilizadores das mesmas, estas podem não cobrir todos os conteúdos e não impedem a disponibilização para terceiros, conforme referenciado nas respetivas políticas de privacidade, mesmo garantindo que estes podem estar mascarados. O utilizador perde, no momento que publica o seu conteúdo, grande parte do poder sobre este. Embora deva existir consciência perante os conteúdos publicados por parte dos utilizadores, atendendo às redes em que estão inscritos, a existência de ferramentas que permitam um maior controlo sobre os seus conteúdos é vista como uma mais-valia na sua partilha, conforme evidenciado nos testes e inquéritos realizados.

Torna-se então fundamental a Gestão de Direitos Digitais, que se refere ao conteúdo de políticas, técnicas e ferramentas que servem de orientação para um uso adequado dos conteúdos digitais (Subramanya & Yi, 2006), de forma a perceber como um sistema do género poderá estar aliado às redes sociais. A existência de sistemas como o OpenSDRM, como plataforma de gestão de direitos digitais, e ferramentas já existentes neste âmbito, como o Phantom, revelam que existe uma preocupação em oferecer algo mais a estes utilizadores em prol do controlo pelos seus conteúdos. E nesse sentido, surge o desenvolvimento de uma arquitetura conceptual com vista a uma solução de gestão de direitos digitais para plataformas de redes sociais, nomeadamente a Social Network DRM (SND).

A plataforma desenvolvida foi testada com utilizadores e permitiu efetivamente comprovar a necessidade da existência destas ferramentas. É necessário garantir a simplicidade no seu uso, bem como a segurança dos seus conteúdos, onde uma plataforma desde género deve cumprir com o que se compromete, de forma a ganhar confiança por parte de utilizadores de redes sociais.

A solução apresentada e o protótipo desenvolvido foram bem recebidos junto dos utilizadores, o que levou à viabilidade deste desenvolvimento. Portanto, com a análise realizada, podemos afirmar que os objetivos definidos para esta dissertação foram atingidos, bem como a resposta às perguntas levantadas, nomeadamente *"Será possível o desenvolvimento e aplicação de mecanismos que permitam melhorar a confidencialidade e privacidade de conteúdos gerados pelos utilizadores (fotos, vídeos, e outros) e partilhados nas redes sociais?"* e *"Qual será a aceitação do mesmo junto dos utilizadores?"*.

Em termos de trabalho futuro, podemos considerar interessantes os desafios sugeridos pelos utilizadores que testaram o protótipo desenvolvido, bem como uma melhor integração deste tipo de sistemas com redes sociais e maior robustez no seu desenvolvimento.

O facto das redes sociais estarem em constante mudança, bem como as suas políticas de privacidade e o uso dos conteúdos gerados pelos utilizadores torna importante a adaptação da solução perante a realidade presente. A existência de soluções apresentadas e da solução desenvolvida, bem como a sua referida aceitação, são bons pontos de partida para a continuidade deste tema. A criação de uma política de privacidade para a solução apresentada também deverá ser tida em conta de forma a informar devidamente aos seus utilizadores do seu funcionamento, recolha de dados e o seu processamento.

É necessário também acompanhar as tendências tecnológicas, com vista à melhoria da plataforma. A crescente revelação de informação confidencial torna fundamental o acompanhamento das mais recentes medidas de segurança, sendo essa uma parte fulcral nestes sistemas, e sob o qual estes se baseiam. O uso de *feedback* dos utilizadores é igualmente importante para o crescimento destes serviços, pois é necessário ir ao encontro do que estes pretendem com estas plataformas. Os testes deverão ser estendidos a um maior número de utilizadores, ser mais exaustivos e o desenvolvimento deverá ser realizado em conformidade com os mesmos, pois são estes os principais beneficiados com estas plataformas.

# Bibliografia

Reinier L. Dohmen. 2012. Facebook: befriending and social capital. *Social Cosmos* 3, 2 (2012), 145–152.

E. De Cristofaro, C. Soriente, G. Tsudik, & A. Williams. 2012. Hummingbird: Privacy at the Time of Twitter. In *2012 IEEE Symposium on Security and Privacy (SP)*. 285–299. DOI:http://dx.doi.org/10.1109/SP.2012.26

Danah M. Boyd & Nicole B. Ellison. 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13, 1 (2007), 210–230. DOI:http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x

Joaquim Marques & Carlos Serrão. 2014. Improving user content privacy on social networks using rights management systems. *Ann. Telecommun.* 69, 1-2 (February 2014), 37–45. DOI:http://dx.doi.org/10.1007/s12243-013-0388-1

Ralph Gross & Alessandro Acquisti. 2005. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. WPES '05. New York, NY, USA: ACM, 71–80. DOI:http://dx.doi.org/10.1145/1102199.1102214

*Facebook Data Use Policy*. (13 de Novembro de 2013). Obtido em 23 de Dezembro de 2014, de Facebook: https://www.facebook.com/about/privacy/your-info

*Company Info | Facebook Newsroom*. (30 de Setembro de 2014). Obtido em 29 de Dezembro de 2014, de Facebook: http://newsroom.fb.com/company-info/

*Twitter Privacy Policy*. (8 de Setembro de 2014). Obtido em 23 de Dezembro de 2014, de Twitter: https://twitter.com/privacy

*About Twitter, Inc. | About*. (2014). Obtido em 29 de Dezembro de 2014, de Twitter: https://twitter.com/privacy

*Política de Privacidade – Privacidade e Termos de Utilização – Google*. (19 de Dezembro de 2014). Obtido em 23 de Dezembro de 2014, de Google: http://www.google.com/intl/pt-PT_ALL/policies/privacy/

*Instagram Privacy Policy*. (19 de Janeiro de 2013). Obtido em 23 de Dezembro de 2014, de Instagram: http://instagram.com/about/legal/privacy/

*Press Page - Instagram*. (Dezembro de 2013). Obtido em 29 de Dezembro de 2014, de Instagram: http://instagram.com/press/

*Phantom~Photos can't be misused – Android Apps on Google Play*. (7 de Agosto de 2014). Obtido em 29 de Dezembro de 2014, de Google Play: https://play.google.com/store/apps/details?id=org.phantom&hl=en

S.R. Subramanya & B.K. Yi. 2006. Digital rights management. *IEEE Potentials* 25, 2 (March 2006), 31–34. DOI:http://dx.doi.org/10.1109/MP.2006.1649008

V. Torres, C. Serrão, M.S. Dias, & J. Delgado. 2008. Open DRM and the Future of Media. *IEEE MultiMedia* 15, 2 (April 2008), 28–36. DOI:http://dx.doi.org/10.1109/MMUL.2008.38

Qiong Liu, Reihaneh Safavi-Naini, & Nicholas Paul Sheppard. 2003. Digital Rights Management for Content Distribution. In *Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003 - Volume 21*. ACSW Frontiers '03. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 49–58.

Eva Rodríguez, Víctor Rodríguez, Anna Carreras, & Jaime Delgado. 2009. A Digital Rights Management approach to privacy in online social networks. In *Workshop on Privacy and Protection in Web-based Social Networks (within ICAIL'09), Barcelona*.

Big Data Working Group. 2013. Expanded Top Ten Big Data Security and Privacy Challenges. (Abril de 2013). Cloud Security Alliance.

André Filipe Marques Francisco. 2012. Privacidade em redes sociais centrada no utilizador recorrendo à gestão de direitos digitais. (Setembro de 2012). Lisboa: ISCTE-IUL, 2012. Dissertação de mestrado.

Logan Kugler. 2015. Online privacy: regional differences. *Communications of the ACM* 58, 2 (Janeiro 2015), 18–20. DOI:http://dx.doi.org/10.1145/2693474

H. Liu and P. Maes. Interestmap: Harvesting social network profiles for recommendations. *In Beyond Personalization – IUI*. 9 (Janeiro 2005), San Diego, California, USA, 2005.

Madejski, M., Johnson, M. L., & Bellovin, S. M. (2011). The failure of online social network privacy settings. Obtido em 31 de Julho de 2015, de Columbia University Academic Commons: http://academiccommons.columbia.edu/catalog/ac:135406

King, J., & Kudumakis, P. (2002). MPEG-4 IPMP Extensions. In T. Sander (Ed.), *Security and Privacy in Digital Rights Management* (Vol. 2320, pp. 126–140). Berlin, Heidelberg: Springer Berlin Heidelberg. Obtido de http://link.springer.com/10.1007/3-540-47870-1_8

Burnett, I. S. (Ed.). (2006). The MPEG-21 book. Hoboken, NJ: Wiley.

Balestri, M., Barker, T., Carruthers, A., Hong, J. W., Mattavelli, M., & Serrão, C. (2002, January 3). MOSES - MPEG Open Security for Embedded Systems. Obtido em 16 de Setembro de

2015, de http://www.ist-world.org/ProjectDetails.aspx?ProjectId=7233d7ddbbbd46d590b9938ef15cd80b

*Facebook Developers*. (2015). Obtido em 3 de Agosto de 2015, de https://developers.facebook.com/

*JavaScript APIs - Google Chrome*. (2015). Obtido em 3 de Agosto de 2015, de https://developer.chrome.com/extensions/api_index

Walker, D. G. (2014, 4 de Agosto). *phpJobScheduler - scheduling PHP scripts to run at set intervals your replacement for cron jobs - cron script*. Obtido a 3 de Setembro de 2015, de http://www.phpjobscheduler.co.uk/

Bourdon, R. (2015). *WampServer, la plate-forme de développement Web sous Windows - Apache, MySQL, PHP*. Obtido a 3 de Setembro de 2015, de http://www.wampserver.com/en/

JetBrains. (2015). *PHP IDE :: JetBrains PhpStorm*. Obtido a 3 de Setembro de 2015, de https://www.jetbrains.com/phpstorm/

Oracle Corporation. (2015). *MySQL :: MySQL Workbench*. Obtido a 3 de Setembro de 2015, de https://www.mysql.com/products/workbench/

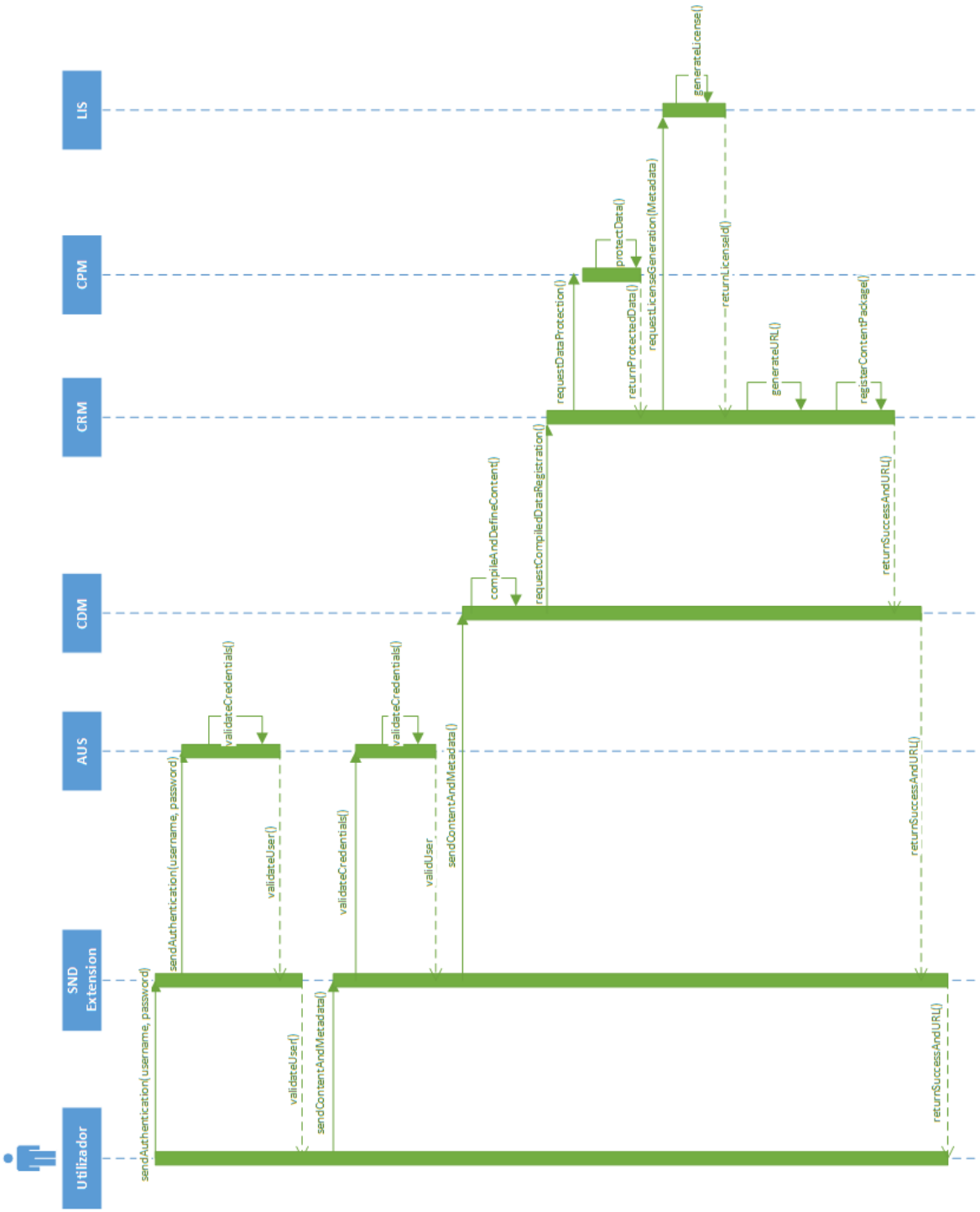
# Anexos

## A. Tabela completa de requisitos

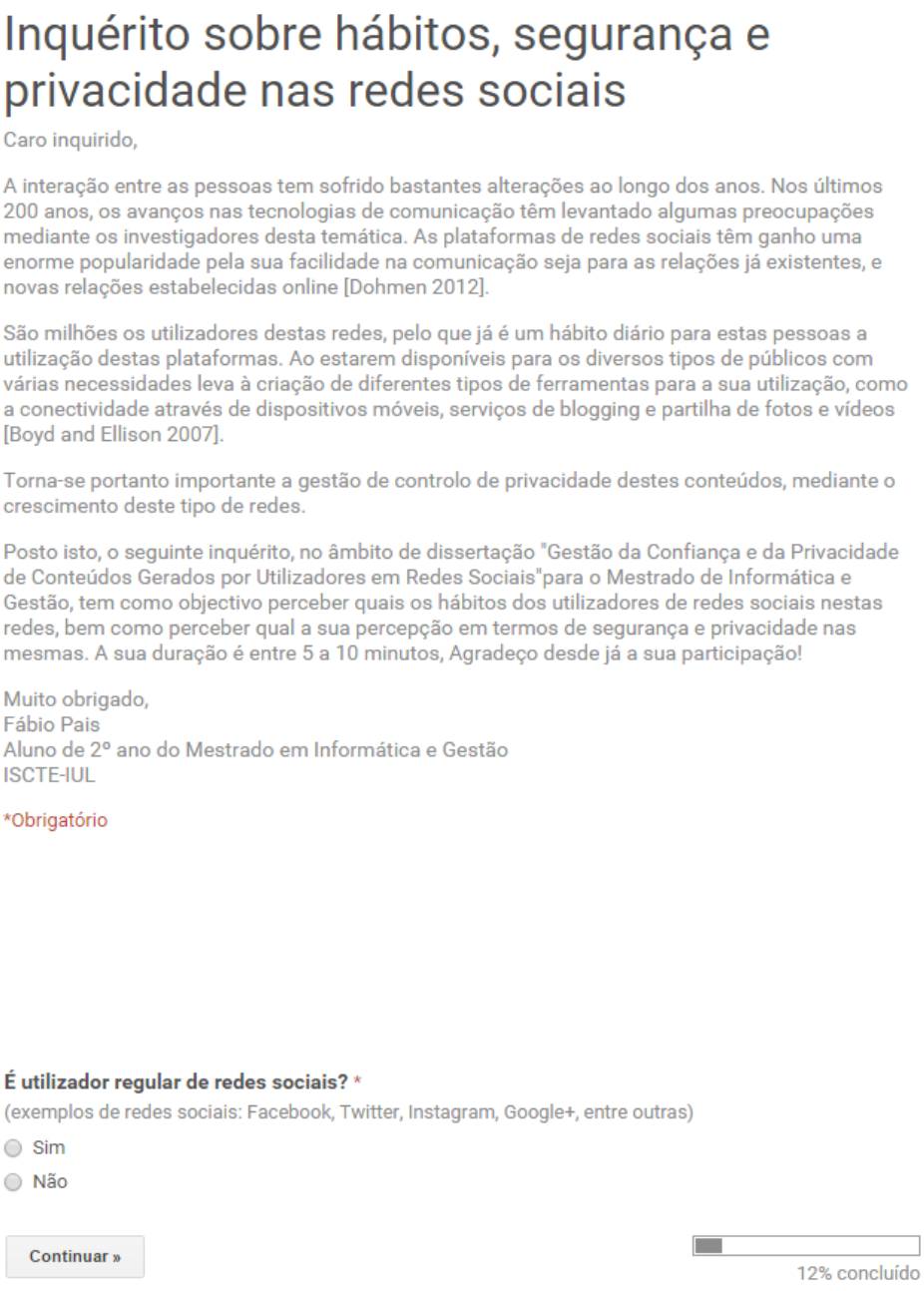
| Stakeholder | Categoria | Requisitos | | Critério de aceitação |
|---|---|---|---|---|
| | | ID | Descrição | |
| Utilizador de redes sociais | RF | 1 | O utilizador deve ter acesso à internet para aceder à plataforma. | Acesso à Internet. |
| Utilizador de redes sociais | RF | 2 | O utilizador deve aceder à plataforma através de uma extensão de um navegador web. | O utilizador acede a partir de um navegador web. |
| Utilizador de redes sociais | RF | 3 | O sistema deve permitir o registo e criação de uma conta de utilizador. | O utilizador pode registar-se no sistema. |
| Utilizador de redes sociais | RF | 4 | O sistema deve permitir ao utilizador autenticar-se através de uma rede social. | O utilizador pode registar-se no sistema através de uma rede social. |
| Utilizador de redes sociais | RF | 5 | O sistema deve permitir ao utilizador efectuar o login e o logout da sua conta. | O utilizador efectua o login e o logout. |
| Utilizador de redes sociais | RF | 6 | O sistema deve permitir o upload de conteúdos pelo utilizador. | O sistema realiza o upload do conteúdo do utilizador. |
| Utilizador de redes sociais | RF | 7 | O sistema deve permitir a configuração de condições de utilização do conteúdo ao utilizador. | O sistema fornece ao utilizador os campos necessários para configurar o acesso ao conteúdo. |
| Utilizador de redes sociais | RF | 8 | O sistema deve gerar um URL do conteúdo que permita a partilha do mesmo pelo utilizador | O sistema gera o URL a ser utilizado pelo utilizador |
| Utilizador de redes sociais | RF | 9 | O sistema deve permitir a eliminação de conteúdo por parte do utilizador. | O sistema permite que o utilizador pode remover o seu conteúdo em qualquer momento. |
| Utilizador de redes sociais | RF | 10 | O utilizador deve poder remover a sua conta do sistema. | O sistema permite que o utilizador apague a sua conta quando este o solicita. |

| | | | | |
|---|---|---|---|---|
| Gestor do sistema | RF | 11 | O sistema deve permitir a sanção de utilizadores que tenham uma conduta imprópria na plataforma. | O sistema permite a remoção de utilizadores pelo gestor do sistema. |
| Gestor do sistema | RF | 12 | O sistema deve permitir o envio de notificações ao utilizador. | O sistema permite que o gestor do sistema envie mensagens ao utilizador. |
| Utilizador de redes sociais | RNF | 13 | O utilizador deve ser utilizador de redes sociais para poder utilizar a plataforma. | O utilizador está registado em pelo menos uma plataforma de redes sociais. |
| Gestor do sistema | RNF | 14 | O sistema deve garantir que os dados estão protegidos de acessos não autorizados. | Os dados devem estar encriptados no sistema. |

## B. Diagrama de estados da partilha de conteúdo na plataforma SND (Maior resolução)



# C. Inquérito sobre hábitos, segurança e privacidade nas redes sociais



## Inquérito sobre hábitos, segurança e privacidade nas redes sociais

Caro inquirido,

A interação entre as pessoas tem sofrido bastantes alterações ao longo dos anos. Nos últimos 200 anos, os avanços nas tecnologias de comunicação têm levantado algumas preocupações mediante os investigadores desta temática. As plataformas de redes sociais têm ganho uma enorme popularidade pela sua facilidade na comunicação seja para as relações já existentes, e novas relações estabelecidas online [Dohmen 2012].

São milhões os utilizadores destas redes, pelo que já é um hábito diário para estas pessoas a utilização destas plataformas. Ao estarem disponíveis para os diversos tipos de públicos com várias necessidades leva à criação de diferentes tipos de ferramentas para a sua utilização, como a conectividade através de dispositivos móveis, serviços de blogging e partilha de fotos e vídeos [Boyd and Ellison 2007].

Torna-se portanto importante a gestão de controlo de privacidade destes conteúdos, mediante o crescimento deste tipo de redes.

Posto isto, o seguinte inquérito, no âmbito de dissertação "Gestão da Confiança e da Privacidade de Conteúdos Gerados por Utilizadores em Redes Sociais"para o Mestrado de Informática e Gestão, tem como objectivo perceber quais os hábitos dos utilizadores de redes sociais nestas redes, bem como perceber qual a sua percepção em termos de segurança e privacidade nas mesmas. A sua duração é entre 5 a 10 minutos, Agradeço desde já a sua participação!

Muito obrigado,
Fábio Pais
Aluno de 2º ano do Mestrado em Informática e Gestão
ISCTE-IUL

*Obrigatório

**É utilizador regular de redes sociais?** *

(exemplos de redes sociais: Facebook, Twitter, Instagram, Google+, entre outras)

- Sim
- Não

Continuar »

12% concluído

**Que redes sociais utiliza?** *

- [ ] Facebook
- [ ] Twitter
- [ ] Instagram
- [ ] Google+
- [ ] Pinterest
- [ ] Tumblr
- [ ] Nenhuma
- [ ] Outra:

**Qual o dispositivo que mais utiliza para navegar/partilhar nas redes sociais?** *

- ( ) Computador
- ( ) Smartphone
- ( ) Tablet
- ( ) Outra:

**Das redes que utiliza, com que frequência acede às mesmas?** *

| | Nunca/Raramente | Uma vez por mês | Uma vez por semana | Duas a três vezes por semana | Uma vez por dia | Várias vezes por dia |
|---|---|---|---|---|---|---|
| Facebook | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Twitter | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Instagram | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Google+ | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Pinterest | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Tumblr | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |

**Indique, aproximadamente, com que frequência costuma publicar/partilhar o seguinte conteúdo:** *
(considere o seu próprio conteúdo, produzido por si)

| | Nunca/Raramente | Uma vez por mês | Uma vez por semana | Duas a três vezes por semana | Uma vez por dia | Várias vezes por dia |
|---|---|---|---|---|---|---|
| Fotografias | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Texto | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Vídeos | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Links de terceiros (sites, blogs, outros) | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |
| Outros | ( ) | ( ) | ( ) | ( ) | ( ) | ( ) |

« Anterior  Continuar »

25% concluído

**O que entende por privacidade?** *

Dê uma breve descrição sobre, o que para si, a privacidade.

**Antes de criar uma conta numa rede social, leu a sua respectiva política de privacidade?** *

- ○ Sim
- ○ Não

**Qual o grau de conhecimento dos termos de privacidade das redes sociais que utiliza?** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Nenhum | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Muito |

**Qual o perfil de privacidade que tem por omissão na(s) rede(s) social(is) que mais utiliza?** *

- ○ Público
- ○ Apenas amigos
- ○ Amigos e amigos de amigos
- ○ Amigos e seguidores
- ○ Personalizado
- ○ Apenas eu
- ○ Não sei

**Costuma utilizar diferentes permissões de privacidade para publicações individuais?** *

Nota: É possível em algumas redes sociais personalizar o tipo de partilha para uma publicação individual, permissões essas disponíveis, como por exemplo, o Google+ e o Facebook.

- ○ Sim
- ○ Não

« Anterior | Continuar »

37% concluído

**Que importância tem para si o controlo do conteúdo que publica?** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pouco importante | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Muito importante |

**Qual o grau de importância de controlo e protecção que atribui seguintes conteúdos** *

Considere a escala de 1, como "pouco importante", a 10 como "muito importante"

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Fotografias | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Texto | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Vídeos | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Links de terceiros (sites, blogs, outros) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Outros | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Para si, qual a importância da segurança de privacidade numa rede social?** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pouco importante | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Muito importante |

**Quando publica um determinado conteúdo numa rede social, como se sente em termos de protecção do mesmo?** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pouco seguro | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Muito seguro |

**Que mecanismo preferia de forma a dar uma maior protecção às suas partilhas nas redes sociais?** *

- ☐ Aplicação com mais funcionalidades
- ☐ Extensão para browser
- ☐ Aplicação para computador
- ☐ Utilização de grupos privados dentro da própria rede
- ☐ Nenhum
- ☐ Outra: _____

« Anterior  Continuar »

50% concluído

As perguntas que se seguem têm como objectivo aferir o seu interesse na utilização de um plugin para um browser, cujo objectivo é dar um maior controlo e protecção ao conteúdo publicado pelo utilizador.

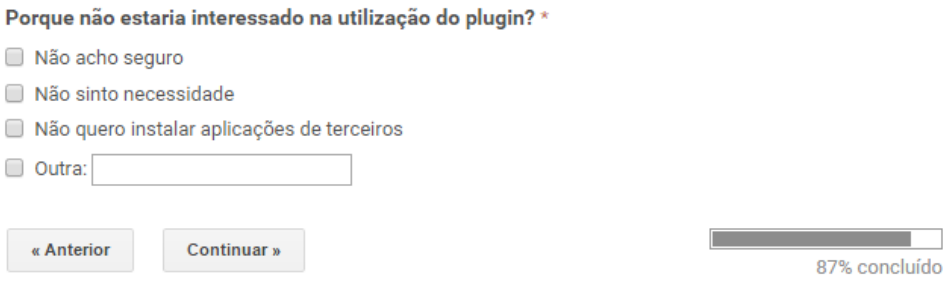
Um plugin, ou extensão, é um pequeno programa que adiciona novas funcionalidades ao seu browser (navegador web) e personalizam a sua experiência de navegação [definição adaptada de Chrome Web Store]. A sua utilização é por norma feita no próprio browser, isto é, integrada no mesmo.

**Utilizaria um plugin ou aplicação que permitisse um maior controlo dos seus conteúdos?** *

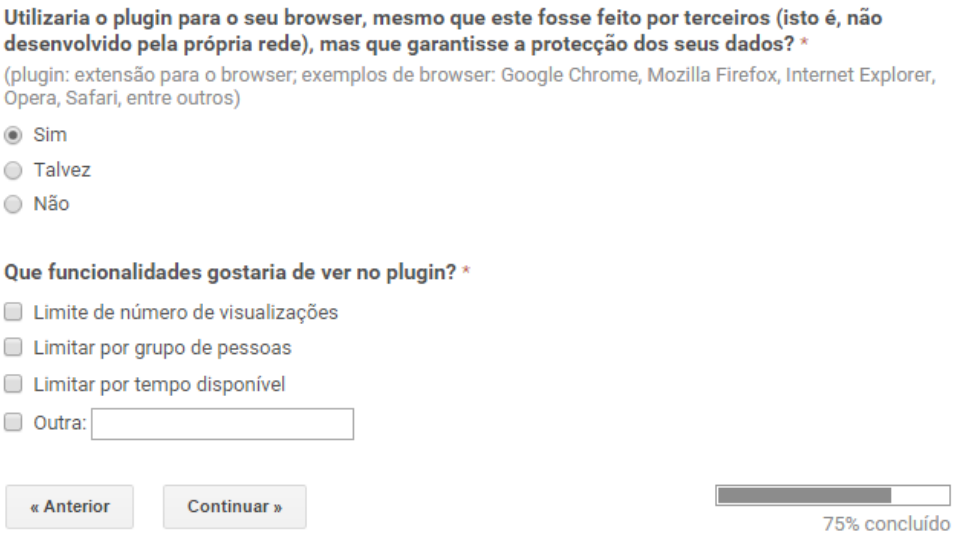
- ○ Sim
- ○ Talvez
- ○ Não

« Anterior  Continuar »

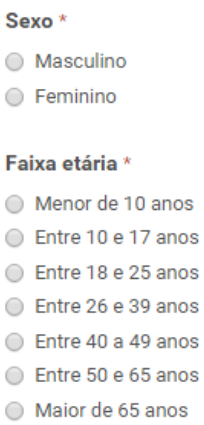
62% concluído

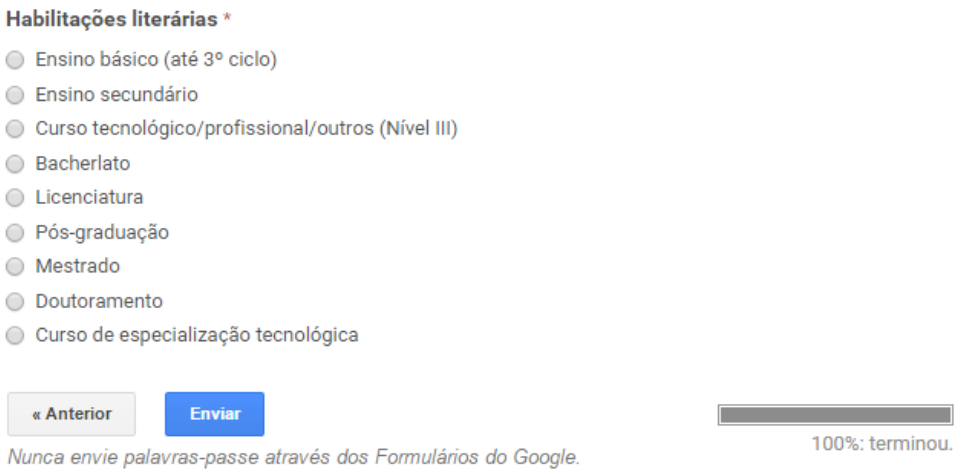



(nota: questão apenas colocada a quem respondeu "Não" na pergunta "*Utilizaria um plugin ou aplicação que permitisse um maior controlo dos seus conteúdos?*")




(nota: questão apenas colocada a quem respondeu "Sim" ou "Talvez" na pergunta "*Utilizaria um plugin ou aplicação que permitisse um maior controlo dos seus conteúdos?*")





**Habilitações literárias** *

- ○ Ensino básico (até 3º ciclo)
- ○ Ensino secundário
- ○ Curso tecnológico/profissional/outros (Nível III)
- ○ Bacherlato
- ○ Licenciatura
- ○ Pós-graduação
- ○ Mestrado
- ○ Doutoramento
- ○ Curso de especialização tecnológica

« Anterior  Enviar

100%: terminou.

*Nunca envie palavras-passe através dos Formulários do Google.*

# D. Inquérito de *feedback* sobre a SND Extension

## Inquérito de feedback sobre a SND Extension

Caro inquirido,

A SND Extension é uma aplicação/extensão para o Google Chrome com o intuito de oferecer aos seus utilizadores um maior controlo sobre o conteúdo que publicam nas redes sociais, dando mais opções e garantias quanto à protecção do mesmo.

O seguinte inquérito, no âmbito de dissertação "Gestão da Confiança e da Privacidade de Conteúdos Gerados por Utilizadores em Redes Sociais" para o Mestrado de Informática e Gestão, surge na sequência do teste da aplicação/extensão para o Google Chrome, nomeadamente a SND Extension, e tem como objectivo recolher a sua opinião acerca da mesma. De referir que a aplicação encontra-se numa fase alfa (produto em desenvolvimento).

O inquérito não deverá demorar mais de 5 minutos.

Agradeço desde já a sua colaboração no teste da aplicação, bem como na resposta desde inquérito.

Muito obrigado,
Fábio Pais
Aluno de 2º ano do Mestrado em Informática e Gestão
ISCTE-IUL

*Obrigatório

**Indique, numa escala de 1 (Discordo completamente) a 10 (Concordo completamente), o quão concorda com as seguintes frases:** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| A aplicação é simples de utilizar | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| A aplicação é intuitiva | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| A aplicação é interessante para os utilizadores de redes sociais | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Senti-me seguro(a) ao utilizar a aplicação | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| A aplicação garante-me um maior controlo do meu conteúdo | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| A aplicação é demasiado técnica | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Senti dificuldade em aceder à aplicação | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| A aplicação garante-me uma maior privacidade | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Indique, numa escala de 1 (Muito difícil) a 10 (Muito fácil), a utilização das funcionalidades que testou:** *

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Registo na aplicação | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Definição das condições de acesso ao conteúdo | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Partilha do conteúdo via URL | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

Continuar »

**Que pontos positivos considerou na aplicação?** *

Escreva a sua resposta por tópicos. Considere apenas as funcionalidades que testou.

**Que pontos negativos considerou na aplicação?** *

Escreva a sua resposta por tópicos. Considere apenas as funcionalidades que testou.

**Que funcionalidades gostaria que fossem implementadas?** *

Escreva a sua resposta por tópicos.

« Anterior  Continuar »

**Considera a integração de uma solução deste tipo no navegador de Internet diferenciador?**

- Sim
- Talvez
- Não

**Considera que esta aplicação atinge o objectivo a que se propõe?**

- Sim
- Talvez
- Não

**Utilizaria o produto final da aplicação que testou?** *

- Sim
- Talvez
- Não

« Anterior  Continuar »

**Sexo:** *

- Masculino
- Feminino

**Faixa etária** *

- Menor de 10 anos
- Entre 10 e 17 anos
- Entre 18 e 25 anos
- Entre 26 e 39 anos
- Entre 40 a 49 anos
- Entre 50 e 65 anos
- Maior de 65 anos

**Habilitações literárias** *

Indique o seu último grau completo.

- Ensino básico (até 3º ciclo)
- Ensino secundário
- Curso tecnológico/profissional/outros (Nível III)
- Bacherlato
- Licenciatura
- Pós-graduação
- Mestrado
- Doutoramento
- Curso de especialização tecnológica

« Anterior  Enviar