Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

Privacidade em redes sociais centrada no utilizador recorrendo à Gestão de Direitos Digitais

André Filipe Marques Francisco

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Informática e Gestão

Orientador:

Doutor Carlos Serrão, Professor Auxiliar,
ISCTE - IUL

Setembro, 2012

Agradecimentos

Faço uso deste espaço para agradecer a todos aqueles que, de forma directa ou indirecta, contribuíram para que esta dissertação rumasse a bom porto.

Ao meu orientador, Professor Doutor Carlos Serrão, por toda a compreensão e dedicação no auxilio e na disponibilização de todos os instrumentos necessários para que este trabalho fosse produzido com sucesso. O seu contributo foi essencial para todo este projecto.

Aos meus pais, por todo o esforço que ao longo da vida têm feito para que eu me tenha tornado o homem que sou e por todo o apoio incondicional que nunca me faltou durante toda a minha vida e, em especial, no meu percurso académico.

Às minhas irmãs, por toda a compreensão e dedicação nas alturas de maior desânimo. Sempre foram uma alavanca para o meu crescimento como estudante e pessoa.

Á Ana Luísa, por ser uma pessoa muito importante para mim e por nunca, em momento algum, ter vacilado com as dificuldades que tive mesmo quando estas não foram fáceis de gerir. Obrigado pela confiança, apoio e dedicação.

Ao Nuno Filipe, por ser um amigo exemplar e que nunca me negou ajuda quando dela precisei.

A todos os que não referi mas que contribuíram para o sucesso deste trabalho.

A todos os que enumerei o meu profundo e sincero “Obrigado”.

Índice

Índice de Ilustrações

Índice de Tabelas

Termos e Abreviaturas

GDD – Gestão de Direitos Digitais

SGDD – Sistema Gestão de Direitos Digitais

CD – Compact Disc

DVD – Digital Versatile Disc

REL – Rights Expression Language

PRS – Plataformas de Redes Sociais

PC – Personal Computer

XML - Extensible Markup Language

MPEG - Moving Picture Experts Group

COOKIES - Arquivos de texto que se alojam no computador do utilizador onde se encontram registos de dados trocados entre o navegador e servidor

FB - Facebook

IP – Internet Protocol

GPS - Global Positioning System

TW – Twitter

MS – MySpace

GP - Google Plus

URL - Universal Resource Locator

ODRL - Open Digital Rights Language

SGDDRS - Solução de gestão de direitos digitais em redes sociais

OpenSDRM - Open and Secure Digital object Rights Management

IPMP - Intellectual Property Management and Protection

Resumo

As plataformas de redes sociais têm ganho muita popularidade junto dos utilizadores de Internet. Actualmente milhões e milhões de pessoas em todo o mundo interagem com diferentes tipos de redes sociais *online* para que possam partilhar as suas experiências e conteúdos com os seus amigos virtuais com que interagem.

Documentos, vídeos, músicas e fotografias são partilhados na *Web*, confiando muitas das vezes nos controlos de privacidade e segurança oferecidos pelas plataformas de redes sociais, disponibilizando algumas delas algum controlo sobre o conteúdo.

Estes aspectos originam problemas sérios no que diz respeito à privacidade dos utilizadores. O controlo sobre o conteúdo partilhado *online* através das redes sociais está completamente fora do poder de decisão dos utilizadores estando este do lado de quem gere as plataformas de redes sociais.

Este projecto propõe um paradigma diferente para a privacidade da partilha de conteúdos em redes sociais que é centrado no utilizador e não na plataforma onde o conteúdo é partilhado. Posto isto, será apresentada uma arquitectura e um protótipo baseados numa plataforma de gestão de direitos dos utilizadores que irá garantir mecanismos de segurança e privacidade necessários à melhoria dos controlos de privacidade já disponibilizados pelas plataformas de redes sociais.

Para além disto, este documento também apresenta resultados de um questionário onde fica claro que os inquiridos aprovam o propósito deste projecto e que sentem que podem ser dados passos importantes no que diz respeito à melhoria da privacidade nas plataformas sociais.

Palavras-chave: Gestão de Direitos Digitais, Privacidade, Segurança, Redes Sociais e Protecção de conteúdo.

Abstract

Online social networks gained a huge popularity among Internet users. Currently millions and millions of online actors use some kind of social online networks (or multiple) to share their experiences and content with their virtual online friends.

Documents, videos, music and pictures are shared on-line, relying on the privacy and security controls offered by the social network platform, offering little control for the end user. This aspect origins serious privacy concerns, since the control over the content shared on-line on the social network, is out of their hands, and control is passed to the social network.

This document proposes a different paradigm for content privacy shared on social networks that is centered on the user and not on the social network platform. In order to achieve this objective, an architecture and a prototype based on a user rights management platform that will enforce the necessary security and privacy mechanisms that extend the original controls provided by the social network platform, will be presented.

Furthermore, this document also exposes some survey results where is clear that respondents approve the goal of this project, which will increase the privacy of social network user.

Keywords: Digital Rights Management, Privacy, Security, Social Networks and Content Protection.

1. Introdução

1.1. Contexto do tema e problema

O tema principal deste projecto é a "*Privacidade nas redes sociais recorrendo à Gestão de Direitos Digitais*" e da qual se pretende apresentar e clarificar o seu contexto.

Em pleno século XXI, é praticamente impossível ser-se indiferente ao crescente número de plataformas sociais *online* que tem surgido e que tem ganho visibilidade nos últimos anos como o *Facebook*, o *Twitter*, o *Myspace*, entre outras (Boyd & Ellison, 2008). Nessas mesmas plataformas, são criadas redes sociais onde pessoas ou organizações, que apresentem valores e interesses comuns, se relacionam entre si. Essas redes sociais permitem não só reduzir algumas barreiras de comunicação que pudessem existir para a divulgação de informação entre pares ou grupos, mas também optimiza a rapidez com que essa mesma informação é comunicada e partilhada. Esta informação pode incluir o mais variado tipo de conteúdos: música, imagem, informação pessoal, eventos futuros, entre outros. No entanto, a forma como essa informação é distribuída nessas plataformas sociais pode dar origem a problemas relacionados com privacidade, segurança ou mesmo de confidencialidade do próprio utilizador ou organização. Assim sendo, surge um problema, visto ser muito difícil definir qual a visibilidade que pretendemos para os conteúdos que partilhamos e quais os indivíduos que poderão aceder a essa informação. Apesar de algumas dessas plataformas sociais oferecerem alguma protecção de conteúdos, nem todas o fazem.

Todos os utilizadores de plataformas sociais e de *Sites* em geral sejam eles pessoas ou organizações, pretendem que a informação que partilham na *Web* seja canalizada apenas para aqueles a quem se dirigem, sem qualquer tipo de desvio da mesma. Para que tal aconteça, é indispensável que existam mecanismos que tenham em conta essa preocupação e que permitam que a informação seja partilhada nos moldes pretendidos por quem a partilhou.

Neste contexto, torna-se interessante o desenvolvimento de uma solução que permita um aumento da segurança dos conteúdos que são partilhados *online*, podendo isto ser feito através da definição da granularidade de partilha pretendida por cada utilizador para os conteúdos por si divulgados. Com isto pretende-se não só o reforço de segurança, mas também fomentar o respeito pela privacidade de cada utilizador de uma

forma individual. Cada um deve ter a liberdade de decidir o que partilhar e com quem partilhar aquilo que possa entender como privado ou não.

Actualmente, existem sistemas que fazem a monitorização de conteúdos digitais que são divulgados *online*, a essa gestão dá-se o nome de Gestão de Direitos Digitais (GDD), do inglês, *Digital Rights Management* (DRM). A Gestão Direitos Digitais tem como princípio a supervisão e controlo do acesso e da cópia de conteúdos que são partilhados através das plataformas disponíveis na Internet.

1.2. Relevância científica e social

Após a contextualização do tema a abordar e a problemática que o envolve, é importante também referir aquilo que uma solução de gestão direitos digitais em redes sociais *Web* pode trazer para a área científica em estudo e a sua relevância social.

Parece ser de todo o interesse científico que uma abordagem já existente relativa à gestão de direitos digitais possa ser integrada com outro tema também ele já bastante tratado, principalmente na última década, que são as redes sociais *Web*. A gestão de direitos digitais na Internet já possui alguma relevância académica que leva a que se possa pensar em associa-la a outros ramos de investigação. Esta referida gestão, é feita actualmente das mais variadas formas mas, até à data, são poucos os estudos que a sustentam numa perspectiva de partilha de conteúdos e de mecanismos de protecção em redes sociais. Com isto, este trabalho procurará trazer algumas contribuições importantes para a privacidade dos utilizadores de redes sociais para que estes possam fazer uma gestão mais eficaz dos seus conteúdos, salvaguardando a sua privacidade e confidencialidade.

Apresentam-se como principais objectivos académicos os seguintes tópicos:

1. Estudar o problema da gestão de permissões e de partilhas de conteúdos em redes sociais, que afectam a privacidade dos utilizadores;
2. Desenvolver uma ferramenta que seja integrável com um *browser web* que possa ser usada em conjunto com as redes sociais, para melhorar a forma como os conteúdos são partilhados nessas mesmas redes.

Ainda de salientar a importância que este trabalho pode ter no âmbito social, consequência da sua actuação nas redes sociais. Com o desenvolvimento de uma ferramenta potencialmente acessível a todos, e que possa na realidade proteger

conteúdos que são disponibilizados na Internet, podemos afirmar que a privacidade de quem usa esta ferramenta pode vir a ser potencialmente salvaguardada, visto que, se cada um de nós fizer uma protecção adequada dos conteúdos que coloca *online*, estes não terão uma difusão abusiva e que aquilo que é pessoal apenas será exibido a um número muito restrito e limitado de pessoas.

Contudo, a contribuição principal deste projecto é relativa à mudança de paradigma no que diz respeito à privacidade dos utilizadores de redes sociais. O controlo e monitorização que é realizado sobre os conteúdos partilhados nas plataformas de redes sociais é executado apenas do lado de quem gere a rede social, isto é, do lado do servidor. No entanto, este projecto pretende inverter essa realidade fazendo com que se possam dar alguns passos no sentido de capacitar os utilizadores de redes sociais de métodos que permitam salvaguardar a sua privacidade, colocando assim o controlo do conteúdo do lado do utilizador, ou seja, do lado do cliente.

1.3. Objectivos

Como objectivo genérico deste projecto entende-se não só um estudo de toda a temática envolvente à abordagem de gestão de direitos digitais no contexto das redes sociais e no controlo da privacidade, mas também o desenvolvimento de uma solução. Esta solução deve permitir a protecção dos conteúdos dos utilizadores nas diferentes plataformas sociais, através da especificação do grau de direito de acesso aos conteúdos individuais por parte de outros utilizadores.

Os objectivos, de uma forma mais específica, são os seguintes:

- Estudar as diferentes redes sociais *Web* e a forma como os utilizadores partilham a informação e quais são os mecanismos usados para especificar propriedades de partilha de conteúdos, com especial enfoque nas redes sociais mais utilizadas (*Facebook*, *Twitter* e *Google Plus*);
- Definir quais as formas mais eficazes de partilhar e proteger os conteúdos nas redes sociais;
- Analisar, desenhar e desenvolver uma plataforma que permita a partilha efectivamente controlada de conteúdos através das redes sociais;
- Testar e avaliar o sistema em diferentes redes sociais existentes (em particular no *Facebook* e no *Twitter*).

Todos os pontos aqui expostos irão ser abordados ao longo deste documento.

1.4. Formulação do Problema e Hipótese

Todo o conteúdo que é fornecido na *Web* seja a título individual ou organizacional, desde que desprotegido, torna-se vulnerável. Tanto a privacidade como a confidencialidade dos conteúdos que são expostos publicamente pode estar em causa se não existirem mecanismos eficientes que permitam uma real protecção da informação. Mesmo para um utilizador mais preocupado não é fácil proteger tudo o que partilha na Internet, a não ser através das poucas funcionalidades de protecção de privacidade existentes em algumas plataformas sociais presentes na *Web*.

Com tudo isto surge então uma questão que se pretende que seja esclarecida neste projecto:

Em que medida uma solução de gestão direitos digitais associada às redes sociais Web pode afectar a segurança e a privacidade dos utilizadores dessas mesmas plataformas?

Esta questão que é colocada pretende clarificar se o facto de ser produzida uma solução que permita aos utilizadores definir os seus parâmetros de protecção de conteúdos que divulga nas redes sociais existentes na Internet pode afectar esses referidos utilizadores no que diz respeito à sua privacidade e segurança. Por privacidade entenda-se, existir uma menor probabilidade de divulgação alheia daquilo que cada um entende como pessoal e que, neste caso, insere nas redes sociais.

De forma a dar resposta a esta questão que dá origem à investigação apresenta-se a seguinte hipótese:

H – *Uma solução de gestão de direitos digitais aplicada às redes sociais Web aumenta a segurança dos seus utilizadores no que diz respeito à sua privacidade e confidencialidade.*

A hipótese não é mais do que aquilo que se pretende verificar ao longo da investigação a realizar neste projecto e que se defende como resposta à pergunta *supra* elaborada. Esta hipótese de resposta indica a possibilidade de o sistema de gestão de direitos digitais aumentar a privacidade e a confidencialidade.

2. Estado da Arte

Para uma melhor percepção de como se encontram os estudos relativos à gestão de direitos em redes sociais *Web*, na qual se insere o presente projecto, segue-se agora uma clarificação de alguns conceitos indispensáveis para a sua compreensão.

2.1. Conteúdos digitais

2.1.1. O que são conteúdos digitais?

A Internet mudou muitos aspectos do nosso dia-a-dia tanto a nível tecnológico, como económico e até mesmo social. Em particular, permitiu que tivessem sido mudados hábitos e formas de trocar informação (Serrão, Dias, & Delgado, 2006). Em paralelo com a Internet, outros avanços têm ocorrido nas áreas tecnológicas da computação, comunicações e no consumo de bens electrónicos. Estes diferentes avanços tecnológicos tiveram como consequência um aumento do número de conteúdos digitais criados, compartilhados e consumidos por entre os utilizadores dessas mesmas tecnologias. Entende-se como conteúdo digital, qualquer informação que esteja disponível digitalmente que seja processada e acondicionada de forma a ser perceptível. Como exemplos temos o áudio, vídeos, gráficos, animações, imagens, texto ou qualquer outra combinação destes anteriores. Desde a sua criação até à sua utilização por parte do consumidor, os conteúdos seguem um fluxo que nos é mostrado na Ilustração 1 (Subramanya & Yi, 2006).

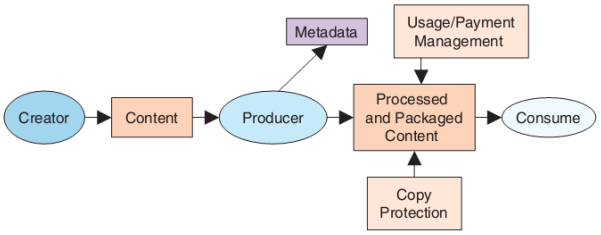


Ilustração 1 - Fluxo de um conteúdo desde o criador até ao consumidor (Subramanya & Yi, 2006)

O criador (*Creator*) é o principal interessado na informação que é inserida no conteúdo (*Content*). Este conteúdo pode ser visto como um conteúdo puro, que por sua vez precisa de ser processado para que a este se possa acrescentar um dado formato, uma adequada integração dos diferentes meios de comunicação, um aperfeiçoamento na qualidade, potenciais efeitos especiais. De seguida o produtor do conteúdo (*Producer*) executa e gera um pacote de conteúdo (*Processed and Packaged Content*) a ser usado.

Após isto, o pacote de conteúdo encontra-se na forma adequada, podendo este ser utilizado e gerido por quem o usa. O consumidor é o último utilizador deste fluxo e que procede ao consumo desse mesmo conteúdo (*Consumer*) (Subramanya & Yi, 2006).

2.1.2. Distribuição de conteúdos

A distribuição de conteúdos divide-se em duas categorias: *offline* e *online*. A distribuição *offline* consiste em distribuir conteúdos em pacotes portáveis, isto é, em suporte físico e limitado no volume de dados. Um exemplo disso é o CD ou DVD. Distribuição *online* pode consistir no envio de conteúdos por correio electrónico para os consumidores ou na inserção desses mesmos conteúdos num servidor para esse efeito, isto é, um servidor de conteúdos. A forma como o servidor de conteúdos distribui a informação que dispõe pode ser realizada de duas maneiras: *download* (descarregamento) ou *streaming* (transmissão). No *download*, o conteúdo é adquirido pelo dispositivo juntamente com os direitos de utilização ou de forma separada. O conteúdo é guardado localmente e apenas é processado mediante o direito de utilização do objecto em causa. No *streaming* não existe um armazenamento integral do conteúdo no dispositivo. Neste caso, o que é transmitido ao consumidor é protegido através de um mecanismo de encriptação da transmissão antes mesmo da sua difusão. A transmissão realizada nestes moldes é descodificada e processada posteriormente no dispositivo que a pretende (Subramanya & Yi, 2006).

Contudo, a distribuição de conteúdos multimédia digitais pode dar origem a alguns problemas sérios. Quando falamos em problemas deste tipo, estamos a falar essencialmente de um que dá pelo nome de pirataria de conteúdos (Serrão, Dias, & Delgado, 2006).

2.2. Gestão de Direitos Digitais

2.2.1. Conceito de Gestão de Direitos Digitais

De forma a contornar alguns problemas originados pelo uso e distribuição não autorizado de conteúdos, algumas medidas tecnológicas foram criadas de forma a contornar essa questão. As mais comuns e simples são a encriptação, o *scrambling* e a marca de água (*watermark*) de conteúdos. Existem, no entanto, medidas tecnológicas mais complexas onde se incluem a definição de regras de uso e de negócio dos conteúdos. Estas são geridas por uma infra-estrutura chamada Gestão de Direitos Digitais (*Digital Rights Management*) (Serrão, Dias, & Delgado, 2006). Por outras

palavras, o termo Gestão de Direitos Digitais refere-se ao conjunto de políticas, técnicas e ferramentas que servem de orientação a um uso adequado dos conteúdos digitais (Subramanya & Yi, 2006).

2.2.2. Sistemas de Gestão de Direitos Digitais

Os sistemas de gestão de direitos digitais (SGDD) gerem os activos digitais de uma forma controlada e seguem os termos que são impostos pelos autores desses conteúdos. Estes sistemas permitem a criação, adaptação, distribuição e consumo de conteúdos multimédia de acordo com as permissões impostas pelos seus criadores e emissores de direitos (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

As principais funcionalidades dos SGDD são a facilidade de empacotamento de conteúdos puros num formato apropriado para uma fácil divulgação e distribuição, a protecção de conteúdos de forma a não poder ser falsificada a sua transmissão, a protecção de conteúdos de uma utilização não autorizada, e a especificação de direitos que determinem o modo como o produto pode ser utilizado.

Os SGDD podem também facilitar a distribuição de conteúdos *offline* (CD ou DVD); a partilha de conteúdos *on-demand* em redes de relação entre pares (*peer-to-peer*), redes empresariais ou na Internet; e oferecer formas de autenticação de conteúdo. Outra funcionalidade igualmente interessante é a capacidade que estes sistemas têm de efectuar pagamentos na Internet para aquisição de direitos de uso, podendo, através deste pagamento, remunerar autores e produtores dos conteúdos que são postos à venda na *Web*. Este tipo de sistema permite monitorizar o uso de conteúdos e assegurar que os mesmos se encontram em concordância com os seus direitos de utilização, a aquisição por faixa e a garantia de que esta compra se encontra de acordo com a utilização que se pretende do conteúdo, e gerir questões de segurança e privacidade apropriadamente (Subramanya & Yi, 2006).

Para além do que já foi referido, os SGDD devem facilitar a personalização de conteúdos adaptando-os de acordo com a preferência dos seus consumidores, ser interoperáveis, permitir diferentes formatos de conteúdos de um modo claro e transparente, e devem igualmente admitir a manipulação de diferentes níveis de granularidade de acesso de conteúdo. Entenda-se por granularidade de um SGDD uma unidade de tamanho (*chunk*) de um conteúdo que pode ser seleccionada, distribuída e consumida de uma forma independente (Subramanya & Yi, 2006). Para uma melhor

compreensão segue-se o exemplo de um álbum de um determinado artista, em formato digital. O artista que criou o conteúdo decidiu, por vontade própria, disponibilizar o seu trabalho completo, isto é, o seu álbum. Contudo, decidiu igualmente disponibilizar cada faixa de forma individual, para que, quem assim o quisesse, pudesse obter apenas algumas das suas faixas. A aquisição de uma ou mais faixas deste artista só seria possível pelo facto de o sistema onde é realizada essa mesma aquisição permitir a compra, ou simplesmente o *download*, de uma unidade de conteúdo (*chunk*).

De entre as características mais desejadas para um SGDD estão a facilidade de utilização por parte dos criadores, produtores e consumidores; robustez na evasão das regras de utilização; politicas justas de uso de conteúdos; transparência no uso de conteúdos para diferentes fornecedores e serviços; justiça na atribuição de tarifas para os variados tipos de consumo de conteúdos; e inovação nas formas de fixação de preços e pagamentos (Subramanya & Yi, 2006).

2.2.3. Componentes típicos de um Sistema de Gestão de Direitos Digitais

Uma das filosofias de desenho utilizadas para sistemas de gestão de direitos digitais baseia-se no princípio de separação entre os conteúdos e os seus direitos. Esta separação permite que os conteúdos possam ser distribuídos ou carregados localmente de um modo livre. Contudo, um dado conteúdo não pode ser utilizado sem que exista uma licença para essa utilização, sendo esta propriedade do próprio objecto que se pretende consumir. Os direitos sobre o conteúdo, ou apenas direitos, determinam em que moldes podem os consumidores fazer uso de um determinado conteúdo. De uma forma mais clara, o mesmo conteúdo pode estar associado a variados tipos de utilização, desde que estes estejam reflectidos no direito que foi especificado para esse mesmo conteúdo (Subramanya & Yi, 2006).

Os dispositivos que são utilizados na GDD podem ser categorizados em dois tipos: os dispositivos portáteis e os dispositivos de rede. Nos dispositivos portáteis mais comuns incluem-se os leitores de áudio (MP3), leitores de DVD, telemóveis, computadores portáteis e PDA. Nos dispositivos de rede temos os receptores de média digital como são televisões de alta-definição com caixas que possibilitam a recepção de conteúdos através da rede. Os dispositivos de interpretação utilizados pelos consumidores de conteúdos têm de suportar os SGDD e estar aptos a interpretar de uma forma apropriada

os direitos especificados na licença de utilização atribuída pelo servidor de licenças (Subramanya & Yi, 2006).

Ainda dentro do âmbito dos SGDD e falando já um pouco de plataformas de redes sociais, existem diferentes iniciativas, tanto *standard* como proprietárias, que especificam elementos que fazem parte desses sistemas ou mesmo um SGDD como um todo. Os componentes que participam num SGDD, comparativamente com os seus homólogos em plataformas sociais, são os seguintes: objectos digitais, expressão de direitos, cumprimento de direitos, ferramentas de protecção de propriedade intelectual, notificação de eventos e os *players* de Gestão de Direitos Digitais (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

O processo de criação de objectos digitais envolve uma combinação entre activos digitais protegidos e metadados associados para originar objectos digitais quem incluem regras de utilização, informação relativa às ferramentas de protecção e outros dados como o autor do produto, entre outros. Nas redes sociais, o conteúdo gerado pelo utilizador não difere muito no que diz respeito à protecção da propriedade intelectual comparando com um conteúdo comutado através de um SGDD, mas as ferramentas que permitem a criação de um conteúdo, e onde se incluem regras de utilização, não são fornecidas, na generalidade dos casos (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

A expressão de direitos administra os activos digitais através de uma cadeia de valor digital. Estes direitos são apresentados aos diferentes intervenientes dessa cadeia de valor como ficheiros XML, também conhecidos como licenças, que são expressos de acordo com uma enriquecida linguagem de expressão de direitos (*Rights Expression Language*). As licenças podem também conter informação protegida como chaves necessárias para decifrar um dado conteúdo digital. Estas são, com frequência, assinadas digitalmente para assegurar a integridade e autenticidade do conteúdo, podendo também conter informação sensível encriptada. Nas plataformas de redes sociais, mas não em todas, os utilizadores podem indicar quem pretendem que seja a sua audiência (amigos, todos, família) mas habitualmente não podem expressar as suas restrições de uma forma tão detalhada como acontecia se o fizessem com uma linguagem de expressão de direitos (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

Os SGDD têm de garantir que os termos definidos na licença que gerem os activos digitais são respeitados pelos utilizadores da cadeia de valor digital. Por esta razão, ferramentas que permitam a autorização são um elemento indispensável nos SGDD. Estas ferramentas de autorização verificam se um utilizador possui uma licença que garanta a operação que pretende executar e se cumpre, como utilizador, as condições especificadas na licença. Nas redes sociais, tudo é baseado na confiança que o utilizador tem na própria plataforma social e em quem faz a sua gestão. Apenas auditores externos podem ter alguma importância neste contexto, mesmo que de uma forma vaga (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

São usadas diferentes técnicas de protecção nos SGDD. Normalmente, os conteúdos digitais são protegidos através de encriptação e técnicas de *scrambling*, enquanto outras técnicas como a marca d'água ou a impressão digital (*fingerprint*) são usadas com o prepósito de rastreio e verificação. Para além disso, a informação sobre as ferramentas usadas para a protecção de recursos digitais é muitas vezes associada aos mesmos no processo de criação de objectos. As plataformas de redes sociais não fornecem ferramentas de protecção pois quem faz a sua monitorização não as entende como necessárias (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

Alguns dos participantes na cadeia de distribuição digital, como produtores ou distribuidores de conteúdos, podem entender como necessária a monitorização do uso do seu material que está licenciado. Assim sendo, alguns dos mecanismos serão necessários para permitir que os sistemas partilhem informação sobre eventos referentes aos conteúdos multimédia. As PRS apenas fornecem informação residual dos eventos: nem sempre é possível, por exemplo, verificar quem viu uma dada fotografia partilhada numa rede social podendo apenas, em algumas plataformas, contabilizarem-se o número de acessos a uma fotografia publicada (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

Os *players* de GDD são aqueles que consomem determinados conteúdos de acordo com os termos e condições especificadas nas licenças associadas ao conteúdo. Então, estes *players* fazem uso de ferramentas de permissão que determinam se os utilizadores estão autorizados a consumir um dado bem digital. Se um utilizador é autorizado, então o conteúdo é desencriptado e concedido. Tipicamente, os *players* de GDD tem um repositório local seguro para armazenamento de licenças, protecção de informação,

operações de *report offline* e outras informações relevantes ou mesmo críticas. Nas redes sociais, a única forma de reproduzir um dado conteúdo é através de um navegador (*Browser*) na própria plataforma da rede social em questão (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

2.2.4. Arquitecturas de gestão de direitos digitais

Existem diferentes tipos de modelos e arquitecturas de GDD que apresentam diferentes implementações, nomes e formas de particularizar o modo como o conteúdo é gerido, isto é, de especificar as regras de uso do conteúdo. Contudo, a base destes sistemas é a mesma e tipicamente envolve quatro partes: o fornecedor de conteúdo ou produtor (*Content Provider*), o distribuidor de conteúdo (*Distributor*), a *Clearinghouse* e o consumidor (*Consumer*). O fornecedor de conteúdo, que pode ser uma produtora de música ou um estúdio de cinema, e que detém os direitos sobre os conteúdos sobre os quais querem garantir o seu cumprimento. O distribuidor fornece canais de distribuição, como são exemplo as lojas *online*. Este recebe o conteúdo digital do fornecedor de conteúdo e cria um catálogo *Web* onde apresenta o próprio conteúdo e os metadados dos direitos para a promoção do conteúdo. Os consumidores são os que usam o sistema para aceder ao conteúdo digital por meio de um canal de distribuição onde fazem *download* ou *streaming* do conteúdo após o pagamento da licença digital. A aplicação usada pelo consumidor encarrega-se de efectuar o pedido de licença à *Clearinghouse* e de fazer cumprir os direitos de uso do conteúdo. A *Clearinghouse* lida com as operações de carácter financeiro. Esta é responsável pela emissão da licença digital para o consumidor e pelo pagamento das taxas de direitos (*royaltys*) ao fornecedor de conteúdos e das taxas de distribuição ao distribuidor de conteúdos, que foram pagas pelo consumidor de acordo com o exigido. Uma tarefa também desempenhada pela *Clearinghouse* mas que não apresenta um propósito financeiro é a de registo de consumo de cada consumidor (Liu, Safavi-Naini, & Nicholas, 2003).

Geralmente, um SGDD é integrado com um sistema de comércio electrónico (*e-commerce)* que lida com transacções financeiras e que acciona a função a desempenhar pela *Clearinghouse*. A figura que se segue (Ilustração 2) mostra os componentes mais comuns de um SGDD baseando-se num sistema comercial típico (Liu, Safavi-Naini, & Nicholas, 2003).

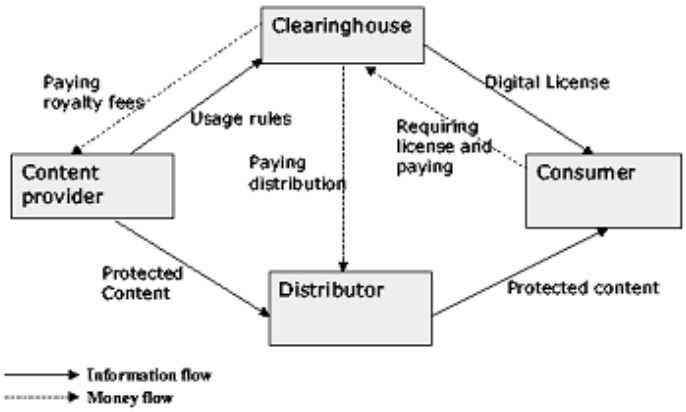


Ilustração 2 - Componentes típicos de um SGDD
(Liu, Safavi-Naini, & Nicholas, 2003)

Numa primeira fase, o fornecedor de conteúdo codifica o mesmo colocando-o num formato quer possa ser suportado pelo SGDD. Os formatos que são admitidos pelos diferentes tipos de SGDD podem variar dependendo dos seus fornecedores e do que estes pretendem que seja suportado pelo sistema por si criado. De seguida, o conteúdo é então encriptado, compactado e preparado tendo por fim a sua distribuição. Os fornecedores de conteúdos podem usar a tecnologia de marca d'água para embutir códigos digitais no interior do seu activo digital que pode identificar o proprietário do conteúdo e as regras de uso do mesmo (Liu, Safavi-Naini, & Nicholas, 2003).

Na fase seguinte, o conteúdo protegido é transferido para um servidor de distribuição de conteúdo apropriado, por exemplo, um servidor *Web* ou um servidor de *streaming*, para distribuição *online*. A licença digital, que é necessária para a reprodução do conteúdo, contém as chaves de desencriptação do conteúdo e as regras de uso que são enviadas para a *Clearinghouse*. As regras de uso incorporadas na licença especificam como pode o conteúdo ser usado como a permissão de cópia, um aluguer de uma só semana, pagamento para uso, entre outros (Liu, Safavi-Naini, & Nicholas, 2003).

No outro lado do processo, os consumidores efectuam *downloads* de conteúdos digitais de um servidor *Web* ou pedidos de *streaming* de conteúdo a um servidor de *streaming*. Além disto, para que um consumidor possa efectivamente reproduzir um determinado conteúdo protegido este tem de requerer uma licença válida à *Clearinghouse*. Após a recepção da licença, a *Clearinghouse* verifica a identidade do utilizador (por exemplo, pela apresentação de um certificado digital válido por parte do utilizador), carrega a

conta do utilizador com base nas regras de utilização de conteúdo, e gera o relatório de transacção que entrega ao fornecedor de conteúdo.

Finalmente, a licença é entregue ao dispositivo referente ao consumidor depois de o consumidor ter efectuado o pagamento referente ao direito de uso, através de um sistema de pagamento de comércio electrónico. Após o pagamento e aquisição de direitos o conteúdo protegido pode ser desencriptado e utilizado em concordância com os direitos de uso declarados na licença adquirida (Liu, Safavi-Naini, & Nicholas, 2003).

Neste modelo, os consumidores podem, mas apenas se a licença o permitir, passar o seu conteúdo digital recebido para outros indivíduos através da super-distribuição, que permite que vendedores comercializem o seu conteúdo digital para um elevado número de potenciais clientes, sem que para isso haja um envolvimento directo entre comprador-vendedor. Muito embora o conteúdo possa ser distribuído livremente, para utilizar o conteúdo, o beneficiário tem de comunicar com a *Clearinghouse* e fornecer toda a informação necessária ou mesmo o pagamento requerido para que a utilização do conteúdo possa ser efectuada dentro dos termos e condições de utilização (Liu, Safavi-Naini, & Nicholas, 2003).

Tendo agora como referência apenas a distribuição de conteúdo sem controlo de pagamento apresenta-se a seguinte arquitectura (Ilustração 3) de um SGDD (Subramanya & Yi, 2006).

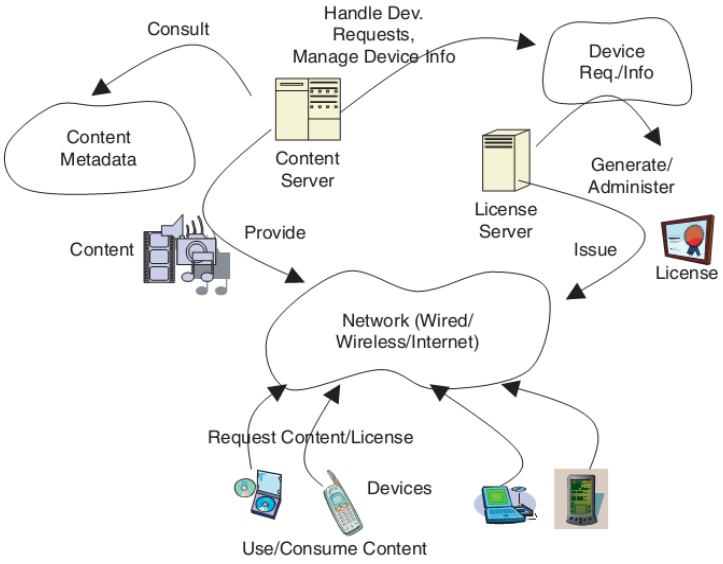


Ilustração 3 - Arquitectura de alto-nível e componentes principais de um SGDD (Subramanya & Yi, 2006)

Nesta arquitectura os dispositivos de interpretação (consumidores) comunicam com o servidor de conteúdos e com o servidor de licenças através de uma rede. O servidor de conteúdos é detentor do pacote de conteúdo que se encontra num formato apropriado para que possa ser reproduzido pelos consumidores. O servidor de licenças gera e monitoriza as licenças de direitos de utilização, indicando quais os direitos que estão associados ao conteúdo e aos utilizadores/dispositivos (Subramanya & Yi, 2006).

Na figura que se segue (Ilustração 4) apresenta-se uma outra proposta alternativa de uma arquitectura de GDD. Esta encontra-se dividida em três elementos Cliente (*Client*), Plataforma de GDD (*DRM Platform*) e *Clearinghouse* (Guth, 2003).

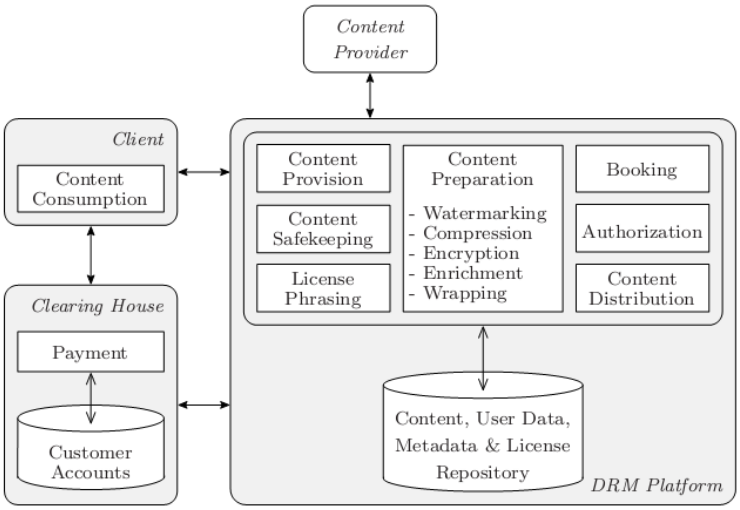


Ilustração 4 - Exemplo de um SGDD

(Guth, 2003)

Neste exemplo de SGDD as funcionalidades são agrupadas em componentes. Os componentes que estão integrados neste exemplo são, como já foi referido, o Cliente (ou consumidor), a *Clearinghouse* e a Plataforma de GDD. O fornecedor de conteúdo (*content provider*) encontra-se também no esquema apresentado mas, como não apresenta uma funcionalidade clara dentro do sistema, apenas será tida em conta a sua interacção. A Plataforma de GDD é o componente chave que controla todo o processo de GDD. Este processo envolve interacções com os diferentes tipos de fornecedores de conteúdos, consumidores e com a *Clearinghouse*. Esta plataforma apresenta funcionalidades no âmbito do aprovisionamento de conteúdo, criação de oferta, protecção de conteúdo, distribuição de conteúdo e reserva de conteúdo (*Booking*). A funcionalidade de pagamento é oferecida pela *Clearinghouse*. Tudo o que diz respeito

ao consumo do próprio conteúdo é tratado pelo componente Cliente deste sistema (Guth, 2003). O aprovisionamento de conteúdo pode ser tecnicamente implementado de diferentes maneiras. Temos como exemplo, o *upload* para um servidor de conteúdos ou então uma partilha de uma pasta num computador que forneça essa mesma partilha. Durante o processo de aprovisionamento, o conteúdo tem de ser protegido do acesso não autorizado pelos mecanismos de segurança. Isso pode ser realizado, por exemplo, através de um canal seguro que utilize o protocolo *Secure Sockets Layer* (SSL) ou de operações de cifra. Quanto aos metadados do conteúdo, estes podem ser fornecidos separadamente (Guth, 2003). No que diz respeito à criação de oferta temos o seguinte. Os fornecedores de conteúdo disponibilizam aquilo que produzem mediante determinados termos e condições. No exemplo aqui apresentado, estas condições não são padronizadas, no entanto, podem ser definidas de forma individual por cada fragmento de conteúdo. A especificação desses termos e condições pode ser considerada como aprovisionamento de direitos de metadados. O aprovisionamento de direitos de metadados resulta numa licença. A funcionalidade da criação de licença tem de ser flexível e para além disso deve suportar diferentes modelos de negócio. Na prática, existe um menu onde o fornecedor de conteúdo define os termos e condições de utilização dos recursos que disponibilizou. Deste processo resulta uma licença que é escrita numa linguagem de expressão de direitos (REL). Funcionando de uma forma semelhante aos metadados de um dado produto, a licença pode tanto ser disponibilizada pelo fornecedor de conteúdo como por um SGDD que saiba quais as condições de atribuição do conteúdo em causa (Guth, 2003).

Quando um conteúdo é disponibilizado este é armazenado num ambiente seguro associado a um repositório de conteúdos. Dependendo da concepção de cada SGDD, o conteúdo é guardado num formato simples ou coberto por um sistema de segurança. Os metadados são armazenados num repositório paralelo igualmente seguro (Guth, 2003). Um pacote seguro é entregue ao provável consumidor através diferentes tipos de canais, podendo estes canais ser redes de comunicação entre pares ou através do envio directo ao receptor registado. Os consumidores podem trocar conteúdos seguros de uma forma privada através da super-distribuição (usa itinerários não estruturados) ou de uma loja de comércio *online* que funcione como canal de distribuição. Estes mercados *online* fornecem muitas vezes informação essencial para a venda de bens digitais sendo também destes a responsabilidade de promover esses conteúdos através dos seus canais

(Guth, 2003). Por fim, quando falamos em reserva de conteúdo é importante ter em conta o seguinte. Quando um consumidor pretende um determinado conteúdo, esse consumidor tem necessariamente de adquirir os direitos que lhe permitam reservar ou comprar um bem digital. Com este propósito, a plataforma de GDD é contactada e o processo requerido pelo consumidor é invocado pelo *software* de cliente de GDD presente no PC do consumidor. Este *software* é responsável por tratar do conteúdo assim como por verificar se o tipo de uso a dar por parte do consumidor está dentro dos termos e condições definidos *a priori* pelo fornecedor de conteúdo. O módulo de reserva do SGDD em causa recebe um pedido de acesso e devolve informação sobre o processo de pagamento ao consumidor (Guth, 2003).

A arquitectura que se segue (Ilustração 5) foi delineada por uma entidade que dá pelo nome de *Open Mobile Alliance* (OMA). A OMA não é mais do que um fórum onde mais de 200 parceiros de indústria definem actividades na área do ambiente de comunicações móveis (Serrão, 2008).

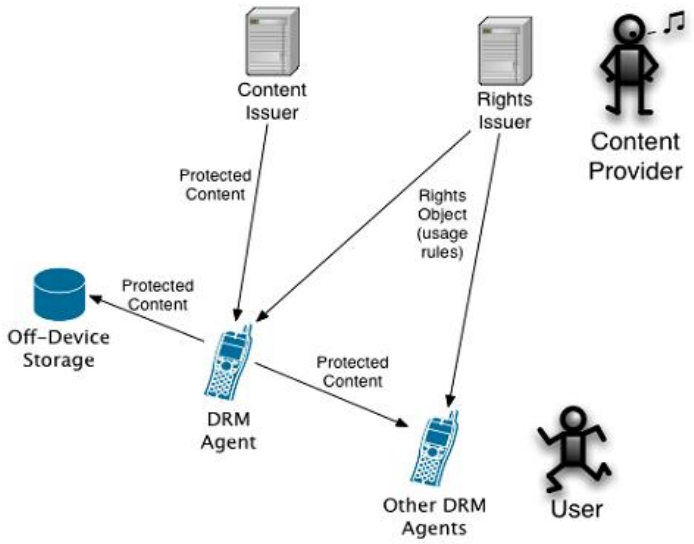


Ilustração 5 - Arquitectura genérica de GDD proposta pela OMA (Serrão, 2008)

O sistema proposto pela OMA apresenta um conjunto de intervenientes e de componentes. No entanto, os mais relevantes são o agente GDD (DRM-A), o emissor de conteúdo (*CI – Content Issuer*), o emissor de direitos (*RI – Rights Issuer*), o utilizador (*User*) e o dispositivo de armazenamento *offline* (*Off-device Storage*).

O agente de GDD representa a entidade de confiança. Esta entidade aplica restrições, monitorização de acesso e de uso que são associadas ao conteúdo que se encontra no sistema. O emissor de conteúdo é o responsável pela entrega do conteúdo de GDD. O sistema proposto pela OMA define o formato a ser entregue ao agente GDD, definindo também a forma como o conteúdo em causa pode ser transportado do emissor de conteúdo até ao agente GDD. Para além disso, neste processo de transmissão, podem ser utilizados diferentes mecanismos alternativos. O emissor de direitos é a entidade que regula a permissão e restrição dos conteúdos GDD do sistema, gerando para isso um objecto de direito ou simplesmente direito. Esse direito de acesso é representado em XML e expressa permissões e restrições associadas ao conteúdo. O utilizador é um humano que pretende usar um conteúdo do sistema e este apenas pode aceder ao conteúdo através do agente de GDD porque apenas este permite um acesso de confiança. O dispositivo de armazenamento *offline* permite salvaguardar o conteúdo com o propósito de criar um *backup* e de libertar memória do próprio dispositivo. Os direitos associados ao conteúdo também podem ser guardados neste espaço (Serrão, 2008).

O SGDD proposto pela OMA permite que ao emissor de conteúdos distribuir conteúdo protegido e ao emissor de direitos expedir direitos de uso para o mesmo conteúdo também ele protegido. O SGDD é independente dos formatos de conteúdo, do sistema operativo utilizado e do ambiente de execução (Serrão, 2008).

2.2.5. Segurança e protecção de conteúdos

Muitos dos esquemas usados em GDD permitem que o conteúdo possa não ser encriptado e, consequentemente, distribuído de uma forma livre. Estes mesmos sistemas garantem de igual forma a legitimidade e a propriedade de uso do conteúdo. No entanto, é igualmente exigida uma utilização de acordo com os direitos desse referido conteúdo.

Existem também outras estruturas que utilizam medidas adicionais de segurança para protecção contra o uso e acesso não autorizado de conteúdos. Uma técnica de protecção simples é a encriptação de conteúdo. Esta encriptação usa um algoritmo e uma chave para combinar a informação. A chave é aquela que permite a recuperação da informação original e que é fornecida aos consumidores que tem autorização para reproduzir o conteúdo. A complexidade do algoritmo de encriptação e o tamanho da chave são adequadamente seleccionadas baseando-se a sua elaboração nos requisitos de cada aplicação em particular. Neste caso, as assinaturas digitais são usadas para garantir a

autenticação tanto dos produtores de conteúdos como dos consumidores. Para clarificar tal situação, demonstra-se a título de exemplo, o seguinte: o cabeçalho de conteúdo e um *hash* desse conteúdo, que não são mais do que dados com um comprimento fixo obtidos após a aplicação de uma função *hash*, poderiam obter uma assinatura digital usando uma chave privada do produtor do conteúdo para gerar essa mesma assinatura. Essa assinatura pode ser verificada quando o emissor da licença entra em contacto com o servidor de licenças para obter uma licença de reprodução do conteúdo que já lhe pertence ou que pretende renovar (Subramanya & Yi, 2006).

2.2.6. Metadados e direitos

Na GDD existe um elemento importante de realçar que são os metadados (*metadata*). Quando falamos em metadados falamos de dados que contém informação relativa ao conteúdo a integrar nos SGDD. Estes dados relativos aos conteúdos contêm informações como o tipo de conteúdo, o identificador (ID), os detalhes de encriptação e informação sobre os direitos associados a esses conteúdos. Os metadados podem ser classificados, num sentido mais lato, em metadados de conteúdo descritivo ou metadados de conteúdo dependente. Os metadados de conteúdo descritivo contêm informações tais como o formato e *layout* dos dados, os vários componentes que constituem o conteúdo e a informação relativa ao autor do conteúdo. Os metadados de conteúdo dependente detêm a informação relativa ao que está no conteúdo. Esta informação engloba, por exemplo, palavras-chave para a cobertura de tópicos de um *e-book* ou de um dado tipo de documentários em vídeo.

Os metadados são usados na gestão de uso de conteúdos. Existem também várias questões relacionadas com o formato e estrutura dos próprios metadados e da sua padronização que têm sido debatidas por diferentes dinâmicas de investigação. Por exemplo têm-se a *Dublin Core Metadata Iniciative* (DCMI), servindo esta iniciativa para reunir recursos com o intuito de reforçar a padronização aplicada aos metadados (Subramanya & Yi, 2006).

Em complementaridade com esta questão é importante fazer igualmente referência a um dos elementos que fazem parte da informação contida nos metadados, os direitos de conteúdo. Na verdade, os direitos de conteúdo, ou somente direitos, especificam de uma forma clara as permissões que dizem respeito a um dado conteúdo indicando a forma como o mesmo pode ser utilizado por consumidores ou dispositivos. Cada um destes

direitos está associado a uma sintaxe e semântica que é especificada por uma linguagem de expressão de direitos (REL). As linguagens de expressão de direitos permitem expressar os termos e condições de uso de um conteúdo de uma maneira clara e inequívoca. Têm sido feitos esforços relevantes no sentido de desenvolver algumas linguagens que permitam expressar direitos. Duas iniciativas a salientar são, por exemplo, a *Open Digital Rights Language* (ODRL) e a *Extensible Rights Markup Language* (XrML). Estes tipos de linguagens permitem que um gestor de direitos seja responsável por criar um objecto-direito, que corresponde a um direito de uso de um conteúdo, e a compactar direitos através de uma chave (Subramanya & Yi, 2006).

Na prática, o conteúdo adere a um formato conhecido como formato de conteúdo de GDD. O conteúdo, juntamente com o direito que lhe está associado, é enviado como uma mensagem GDD. O dispositivo do consumidor origina um conteúdo com uma dada forma baseando-se para isso nos direitos incluídos na mensagem. Se for o caso de não existirem direitos definidos nessa mensagem, são aplicados um conjunto de direitos por definição. O fornecedor de conteúdos pode definir explicitamente os direitos que pretende para os diferentes casos (Subramanya & Yi, 2006)

Existem vários tipos de direitos de uso: data de validade de utilização, que define qual a data sobre a qual o conteúdo não pode ser usado; data de início de utilização, antes da qual o conteúdo não pode ser reproduzido; data de fim de utilização anexada à data de início de utilização, que especifica que o conteúdo é válido por um certo número de dias desde a data da primeira reprodução do mesmo; reprodução contada, onde é especificado o número de vezes que um conteúdo pode voltar a ser reproduzido; tipos de dispositivos, que distingue quais os dispositivos onde o conteúdo pode ser reproduzido; e operações sobre média, estas especificam se um qualquer produto multimédia pode ser transferido para um CD ou para a rede de forma a poder ser transferido para um outro dispositivo (Subramanya & Yi, 2006).

2.2.7. Geração de licenças

As licenças que existem na GDD são aquelas que contém os direitos e onde se incluem os termos e condições relacionados com a reprodução e utilização de conteúdos. As licenças contêm igualmente as chaves que são necessárias para o desbloqueio do conteúdo, no caso de estar protegido. Usando uma chave-semente (*key seed*), que não é mais do que uma chave que é apenas conhecida pelo produtor do conteúdo (*producer*) e

pelo fornecedor de licenças (*manager*), e um identificador da chave (*KEY ID*) a chave é produzida usando-se para isso um processo de geração de chaves. Para além disso, esta chave é utilizada pelo proprietário do conteúdo/produtor (*Producer*) para encriptar o conteúdo quando necessário. A chave é também compactada juntamente com os direitos do conteúdo para gerar uma licença (Subramanya & Yi, 2006).

A figura que se segue (Ilustração 6) demonstra todas as etapas descritas anteriormente (Subramanya & Yi, 2006):

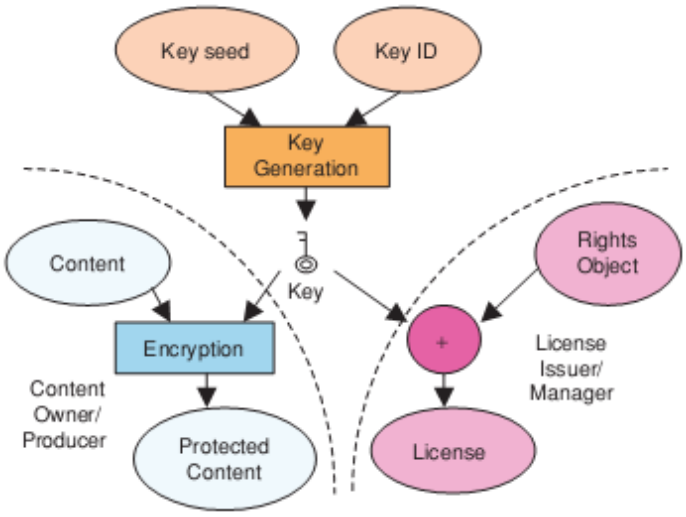


Ilustração 6 - Geração de chaves e uso de chaves na protecção de conteúdos e geração de licenças (Subramanya & Yi, 2006)

É importante também referir que somente após a reunião e cumprimento dos termos e condições indicadas na licença de utilização de um conteúdo é que é validada o uso desse referido conteúdo. A licença pode ser incorporada juntamente com o conteúdo ou enviada em separado. A entrega da licença pode estar implícita, nos casos em que um utilizador não está ciente do processo de entrega da licença, ou explícita nos casos em que o utilizador tem de participar activamente, através, por exemplo, do preenchimento de alguns formulários e fornecendo informações relevantes para que possa obter essa licença. Outras das características do licenciamento é a sua não transferibilidade, isto é, a licença não pode ser transmitida de utilizador em utilizador sem que exista um direito que indique claramente essa hipótese; e a possibilidade de revogação quando os termos e condições de utilização forem violados, tornando assim o conteúdo inutilizável (Subramanya & Yi, 2006).

2.3. Linguagens de expressão de direitos

Nos dias de hoje, as redes comerciais de conteúdo multimédia são baseadas na troca de direitos mas uma das limitações que a tecnologia de GDD têm deve-se à deficiente forma de expressão de direitos. Para colmatar esta questão são necessárias formas de expressão desambiguas, precisas e sem grande complexidade (Polo, Prados, & Delgado, 2004).

Para que possa proteger efectivamente os conteúdos a GDD necessita de tecnologia que cumpra esse propósito. Essa tecnologia, que permite essa segurança de conteúdos, dá pelo nome de linguagem de expressão de direitos (REL). A REL é uma linguagem formal usada para especificar a protecção e segurança dos activos digitais. Esta linguagem formal possibilita a designação de direitos e condições para um dado conteúdo que se encontre em formato digital (Delgado, Prados, & Rodríguez, 2005). Esta expressão de direitos pode ser gerada por qualquer parte que esteja devidamente autorizada a fazê-lo para que, através desta autorização, se possa garantir a correcta permissão de acesso ao conteúdo. Para que uma REL possa ser interpretada por uma máquina deve ter uma sintaxe simples e que possa ser reconhecida (Polo, Prados, & Delgado, 2004).

A REL pode ser utilizada, por exemplo, no controlo do número de vezes que um direito é exercido sobre um dado conteúdo ou expressar *copyrights* associados também sobre um conteúdo. Na prática, consiste na descrição de um acordo entre o produtor e o distribuidor de conteúdo ou entre o distribuidor e o consumidor final (Delgado, Prados, & Rodríguez, 2005).

2.3.1. Linguagem de expressão de direitos MPEG-21

A linguagem de expressão de direitos MPEG é uma linguagem declarativa baseada em XML utilizada para a especificação de condições e direitos de acesso a conteúdos autorizados para distribuição, e que pode ser usado em quaisquer conteúdos, recursos ou serviços. Segue-se um exemplo (Ilustração 7) dessa linguagem (Wang, DeMartini, Wragg, Paramasivam, & Barlas, 2005):

```
license
    grant
        Alice
        play
        whenTheThistleBlooms.mp3
        for 3 weeks
    issuer
        PDQ Records
```

Ilustração 7 - Exemplo de código da linguagem expressão de direitos
(Wang, DeMartini, Wragg, Paramasivam, & Barlas, 2005)

A linguagem de expressão de direitos MPEG pretende dar flexibilidade, mecanismos de interoperabilidade que levem à transparência e fazer crescer o uso de recursos digitais na publicação, distribuição e consumo de conteúdos digitais com o objectivo de proteger o conteúdo e honrar os direitos, condições e taxas específicas de um conteúdo. Entre os referidos conteúdos estão incluídos filmes, música, livros electrónicos, radiodifusão, jogos interactivos, *software* para computadores entre outros conteúdos que possam ser criados em formato digital. É também pretendido que estes sistemas suportem especificação de acesso e controlo de uso para conteúdos digitais nos casos em que não esteja implicada a troca de bens financeiros nas condições de utilização e para ajudar na comutação de informação sensível ou de conteúdo digital privado. Assim sendo torna-se indispensável que esta linguagem seja clara, com a sintaxe bem definida e uma semântica inequívoca (Wang, DeMartini, Wragg, Paramasivam, & Barlas, 2005).

Esta linguagem pode ser usada não só na indústria do entretenimento mas também por empresas ou individuais. Esta mesma linguagem permite a distribuição autorizada e protecção constante de informação importante, conteúdo e recursos de acordo com os requisitos de privacidade e confidencialidade. Quando usada para a protecção da privacidade do consumidor a linguagem MPEG proporciona flexibilidade e mecanismos de interoperabilidade eficientes. Os mecanismos de interoperabilidade permitem aos consumidores, para além de outras coisas, abordar questões de privacidade através da expressão de direitos e condições de uso sobre informação pessoal e assegurar que a informação pessoal é processada de acordo com o especificado nos direitos e condições. Em consequência, torna-se essencial que a linguagem possibilite a existência de um modelo formal de como pode ser concedida uma autorização que esteja em concordância com os direitos expressos na linguagem (Wang, DeMartini, Wragg, Paramasivam, & Barlas, 2005).

Como uma importante tecnologia de desenvolvimento de interoperabilidade através de um SGDD bem como de monitorização de conteúdo e sistemas de gestão de activos digitais, a linguagem MPEG deve ser enriquecida o suficiente para que consiga expressar uma larga variedade de modelos de uso e permitir também a múltipla distribuição e uso de todos os tipos de conteúdos, recursos e serviços em proximidade e centralidade, bem como em ambientes abertos e distribuídos (Wang, DeMartini, Wragg, Paramasivam, & Barlas, 2005).

Esta linguagem apresenta, na sua essência, quatro seguintes elementos: entidade principal, recurso, direito e condição. A entidade principal pode ser uma pessoa, organização ou dispositivo a quem se garantem direitos. Tipicamente, esta informação é associada a mecanismos de autenticação que verificam a autenticidade desta entidade. O recurso é o objecto sobre o qual a entidade principal pretende adquirir o direito de uso. Este recurso pode ser um qualquer trabalho digital, um serviço ou um pedaço de informação. O direito não é mais do que a actividade ou acção que a entidade principal pode efectuar sobre um recurso. Por exemplo, um direito de reprodução. A condição não é mais do que uma ou mais condições que devem ser conhecidas antes do poder de exercício sobre um dado direito. Temos como exemplo, um individuo tem de efectuar o pagamento de uma taxa para exercer um direito de reprodução sobre uma faixa de música (Polo, Prados, & Delgado, 2004).

A linguagem MPEG tem também uma expressividade muito rica em termos de modelos de negócio e em aplicações potenciais que os suportem. Alguns tipos mais habituais de licenças que esta linguagem pode revelar são as licenças de uso (*Usage license*), oferta (*Offer license*), distribuição (*Distribution license*) e de certificação (*Certificate license*) (Wang, 2004). A licença de uso certifica-se que aquele que a emite autoriza o direito principal de exercício do direito de utilização especificado e que se refere a um determinado recurso digital. Isto é possível apenas e só se as condições estabelecidas sejam integralmente cumpridas. Este tipo de licença contém direitos tais como o de reprodução e de edição do conteúdo. Segue-se um exemplo (Ilustração 8) em que a licença de uso garante à Alice o direito de reprodução de um filme para o mês de Novembro do ano de 2003 (Wang, 2004).

```
license
    grant
        Alice
        play
        oceanWilds.mpg
        during November 2003
    issuer
        Acme Studio
```

Ilustração 8 - Exemplo de uma licença de uso

(Wang, 2004)

Uma licença de oferta expressa que uma entidade tem o direito de poder obter outros direitos mediante o cumprimento de uma série de condições listadas *a priori*. A licença de oferta usa a aquisição como um direito e trata como recursos os outros direitos que são oferecidos sobre a forma de subvenções. No exemplo que se segue (Ilustração 9) a licença concede à Alice uma "oferta" para obter o direito de uso para reprodução de um filme durante o mês de Novembro de 2003 sendo necessário para isso o pagamento de uma taxa de 4 dólares (Wang, 2004).

```
license
    grant
        Alice
        obtain
        grant
            Alice
            play
            oceanWilds.mpg
            during November 2003
        flat fee $4.00
    issuer
        Acme Studio
```

Ilustração 9 - Exemplo de uma licença de oferta

(Wang, 2004)

A licença de distribuição expressa que o seu detentor tem o direito de emitir outros direitos a outras entidades, desde que esta obedeça a determinadas condições. Os proprietários do conteúdo podem usar as licenças de distribuição na sua cadeia de valor de distribuição para permitir que os distribuidores possam de facto distribuir o conteúdo. Por seu lado, os distribuidores podem usar igualmente tais licenças para fazer com que os retalhistas vendam o conteúdo em causa. A figura seguinte (Ilustração 10) mostra que a "*ACME Studio"* concede a uma empresa que dá pelo nome de "*somemoviewarehouse.com"* o direito de emitir a qualquer outra entidade o direito de reprodução de um filme no mês de Novembro de 2003, apenas e só se a empresa pagar uma taxa de 3 dólares para tal emissão (Wang, 2004).

```
license
    grant
        somemoviewarehouse.com
        issue
        grant
            anyone
            play
            oceanWilds.mpg
            during November 2003
        per use fee $3.00
    issuer
        Acme Studio
```

Ilustração 10 - Exemplo de uma licença de distribuição

(Wang, 2004)

A licença de certificação representa a declaração do emissor de que o detentor do direito possui algumas características (papeis e atributos). O direito de possuir uma propriedade caracteriza uma licença de certificado. Em muitos casos, o titular é forçado a deter este tipo de licença antes de lhe serem garantidos outros direitos. Temos como exemplo a figura que se segue (Ilustração 11) onde o emissor atesta que a Alice é membro de um dado clube de vídeo (Wang, 2004).

```
license
    grant
        Alice
        possessProperty
        movieClubMembership
    issuer
        Acme Studio
```

Ilustração 11 - Exemplo de uma licença de certificado

(Wang, 2004)

2.3.2. Linguagem de expressão de direitos ODRL

A *Open Digital Rights Language* (ODRL) é uma linguagem de expressão de direitos, que utiliza como base a linguagem XML, proposta pela comunidade de GDD para a padronização da expressão de direitos de informação sobre o conteúdo. O ODRL pretende dar flexibilidade e mecanismos de interoperabilidade para permitir a transparência e um uso inovador de recursos digitais na publicação, distribuição e consumo de bens electrónicos sejam eles imagens, áudio, vídeo, *software*, entre outros.

A ODRL foca-se muito na semântica da linguagem de expressão de direitos digitais. Esta linguagem pode ser usada dentro de sistemas de confiança ou não e em activos digitais ou físicos (Polo, Prados, & Delgado, 2004). Existem três entidades essenciais que se relacionam com as licenças de GDD: a parte interessada, o direito e o activo.

A parte interessada inclui consumidores finais e titulares de direitos. A parte interessada pode ser tanto uma pessoal individual como uma organização a quem os direitos podem ser atribuídos.

O direito inclui permissões, que podem conter restrições, requisitos e condições. As permissões referem-se à utilização ou actividades exercidas sobre os activos (por exemplo, a edição). As restrições são limites às permissões (por exemplo, exibir um livro três vezes). Requisitos são obrigações necessárias exercício da permissão. As condições especificam excepções que, no caso de se tornarem verdadeiras, expiram as permissões e a renegociação torna-se necessária.

O activo inclui qualquer conteúdo. Este activo deve ser um identificador único deve ser constituído por subpartes e ser de diferentes formatos. Também podem ser considerados activos expressões não tangíveis (Delgado, Prados, & Rodríguez, 2005).

A linguagem ODRL inclui um dicionário de dados. Este é formado por elementos que definem permissões, direitos, restrições e requisitos de isso que estão inseridos numa licença de ODRL. Todos estes elementos formam a base da linguagem e podem ser alargados através da adição de novos elementos. Por exemplo, considerando um livro em formato digital que é entregue a um consumidor (Alice) que pode ser publicado três vezes. A licença ODRL tem um ponto que refere que a Alice pode fazer a publicação do livro apenas três vezes. Neste caso, a Alice é a parte interessada, o livro o activo a publicação o direito e as “três vezes” a restrição incluída no direito (Delgado, Prados, & Rodríguez, 2005). A imagem que se segue (Ilustração 12) clarifica e mostra a licença de ODRL para este exemplo (Polo, Prados, & Delgado, 2004):

```
<?xml version="1.0" encoding="UTF-8" ?>
<o-ex:rights xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:o-dd="http://odrl.net/1.1/ODRL-DD"
        xsi:schemaLocation="http://odrl.net/1.1/ODRL-EX ../schemas/ODRL-EX-11.xsd
        http://odrl.net/1.1/ODRL-DD ../schemas/ODRL-DD-11.xsd">
  <o-ex:asset>
    <o-ex:context>
      <o-dd:uid>urn:ebook.world/999999/ebook/rossi-000001</o-dd:uid>
      <o-dd:name>Why Cats Sleep and We don't</o-dd:name>
    </o-ex:context>
  </o-ex:asset>
  <o-ex:permission>
    <o-dd:print>
      <o-ex:constraint>
        <o-dd:count>3</o-dd:count>
      </o-ex:constraint>
    </o-dd:print>
  </o-ex:permission>

  <o-ex:party>
    <o-ex:context>
      <o-dd:name>Alice</o-dd:name>
    </o-ex:context>
  </o-ex:party>
</o-ex:rights>
```

Ilustração 12 - Exemplo de uma licença ODRL

(Polo, Prados, & Delgado, 2004)

2.3.3. Linguagem de expressão de direitos MPEG-21 vs ODRL

As linguagens MPEG-21 e ODRL são bastante semelhantes: sintacticamente ambas são baseadas em XML e estruturalmente ambas têm em conta os princípios axiomáticos de *Stefik* de modelação de direitos (Polo, Prados, & Delgado, 2004). A diferença entre estas linguagens é que a ODRL parece mais adaptada às transacções actuais que ocorrem nos ambientes comerciais enquanto a linguagem MPEG-21 foi desenhada numa perspectiva de aplicabilidade vertical. A ODRL apresenta também termos que são encontrados no mundo comercial real (Polo, Prados, & Delgado, 2004).

Tanto a linguagem MPEG-21 como a ODRL são amplamente utilizadas, então é muito importante permitir a interoperabilidade entre diferentes sistemas. Ambas tem o mesmo propósito e começaram com a mesma base de partida. Apresentam diferentes entidades mas tentam representar a mesma informação. Após uma análise de ambas as linguagens, Polo, Prados e Delgado (2004), concluíram que existem quatro entidades essenciais em ambas as licenças:

Sujeito: elemento que actua e efectua algumas operações sobre o conteúdo. Na ODRL, é representado pela parte interessada e na linguagem MPEG-21 como a entidade principal.

Direito: aquilo que um sujeito pode exercer sobre o objecto. Na ODRL é dado o nome de permissão (direito) e no linguagem MPEG-21 o nome de direito.

Objecto: conteúdo que sofre a actuação do sujeito. Na ODLR é o activo e na linguagem MPEG-21 o recurso.

Condição: descreve quando um direito pode ser exercido. Na ODRL é a restrição que é incluída no direito e na linguagem MPEG-21 a condição (Polo, Prados, & Delgado, 2004).

2.4. Privacidade e controlo de conteúdo

Torna-se importante fazer referência, no âmbito deste projecto, à privacidade tanto no contexto *Web* em geral como no contexto mais específico das redes sociais.

2.4.1. Privacidade do utilizador e de dados

Dentro da definição de utilizadores *Web* incluem-se pessoas, aplicações e outros serviços *Web*. Em muitos casos, aos utilizadores que interagem na *Web* são lhes solicitadas informações com alguma relevância e de caracter sensível tais como número de segurança social, número de cartão de crédito, morada de residência, entre outras informações. Estes utilizadores podem, contudo, definir diferentes níveis de privacidade de acordo com a sua própria definição de "informação sensível". Temos como exemplo um utilizador que exige uma privacidade mais apertada sobre informação médica do que sobre o seu histórico como trabalhador. A percepção de privacidade do utilizador depende também de quem recebe a informação e da forma como essa informação é usada e com que propósito (Rezgui, Ouzzani, Bouguettaya, & Medjahed, 2002).

A todo o conjunto de preferências privadas aplicáveis a uma informação de um dado utilizador dá-se o nome de "perfil de privacidade do utilizador". Um perfil de privacidade do utilizador é tipicamente definido por um utilizador mas pode também ser uniformemente definido para um grupo de pessoas individuais. Os perfis privados são dinâmicos, isto é, os utilizadores podem criar, ver, actualizar ou mesmo apagar dentro do perfil pessoal. As arquitecturas *Web* devem permitir todas estas operações dinâmicas de forma a evitar problemas legais associados à perda/quebra de privacidade. Podem também ser definidas credenciais privadas para os utilizadores que funcionem como assinatura e que é habitualmente anexada a qualquer acção que o utilizador pretenda efectuar na plataforma *Web*. Isto possibilita a delimitação do âmbito da privacidade do utilizador. O âmbito de privacidade para um dado utilizador define a informação que um serviço *Web* pode divulgar sobre um utilizador em particular. Por exemplo, um governante que acede a uma plataforma governamental deve deter credenciais que

permitam provar que está autorizado a aceder a essa plataforma, visto que estas incluem informações relevantes e confidenciais sobre os cidadãos que não podem ser apresentadas publicamente (Rezgui, Ouzzani, Bouguettaya, & Medjahed, 2002).

Um determinado objecto que contém informação pode ser acedido por diversos serviços *Web*. Os diferentes serviços disponibilizados na *Web* podem pretender aceder a informação distinta apesar de o objecto que detêm a informação ser o mesmo. Isto é, o mesmo objecto de informação pode ser fonte para diferentes serviços *Web*. Por cada objecto de informação, podem ser definidos "perfis de privacidade de informação" que especificam o acesso à informação que é exposta nas diferentes plataformas *Web*.

Além disso, os objectos que contém informação que tenham perfis de privacidade semelhantes formam aquilo a que se chama um c*luster* de privacidade. A motivação essencial do *clustering* de informação é a de que as leis e políticas de privacidade são tipicamente aplicáveis a vastos segmentos de população, como por exemplo, um país ou região (Rezgui, Ouzzani, Bouguettaya, & Medjahed, 2002).

2.5. Plataformas de redes sociais Web

2.5.1. Características e definição de plataformas de redes sociais Web

Desde a sua origem, as plataformas sociais, como o *MySpace, Facebook* ou *Twitter*, têm atraído milhões de utilizadores. Estes utilizadores têm de tal forma presentes estas redes na sua vida que o acesso às plataformas, onde podem aceder a essas referidas redes, é algo que já faz parte do quotidiano de muitos. Existem centenas de plataformas de redes sociais com a mais variada tecnologia tendo por base diferentes tipos de interesses e praticas. Enquanto as características tecnológicas chave destas foram sendo consolidadas, os mais variados tipos de culturas foram surgindo em redor das PRS (Boyd & Ellison, 2008).

A figura seguinte (Ilustração 13) permite perceber a evolução das PRS entre os anos de 1997 e 2006 (Boyd & Ellison, 2008).

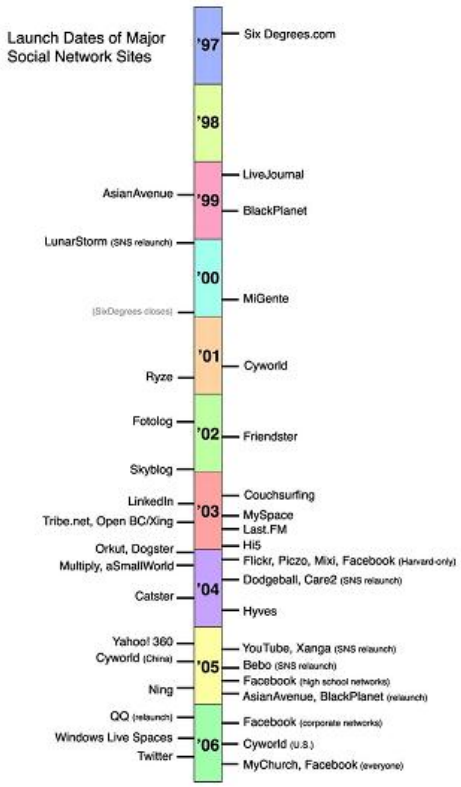


Ilustração 13 - Linha temporal com datas de lançamento das maiores PRS e datas de reedição (Boyd & Ellison, 2008)

Muitos destes *sites* permitem a manutenção de redes sociais que já tenham sido criadas anteriormente, fazendo com que apenas seja facilitada a sua comunicação interna, mas existem outras que ajudam os seus utilizadores a criar relação com indivíduos estranhos à sua vida quotidiana baseada na partilha de interesses, pontos de vista políticos ou actividades comuns. Algumas destas plataformas atraem audiências dos mais variados tipos, enquanto outras cativam pessoas baseando-se no princípio de uma língua comum ou partilha racial, sexual, religiosa, ou mesmo pela pertença ao mesmo país de origem. Estes *sites* incorporam muitas das vezes novas ferramentas de comunicação e de informação, como é o caso da relação de conectividade entre dispositivos móveis, o *blogging* e partilha de vídeos/fotos (Boyd & Ellison, 2008). De uma forma simples e clara, as redes sociais *Web* são serviços disponibilizados *online* que permitem a um indivíduo criar um perfil público ou semipúblico dentro de um sistema limitado, articular uma lista de outros utilizadores com quem este partilha uma ligação, e visualizar a sua lista de ligações e aquilo que é realizado por outros dentro desse sistema. A forma como os utilizadores se relacionam e mesmo a nomenclatura usada pode variar de plataforma para plataforma (Boyd & Ellison, 2008).

O que torna estes espaços *online* tão únicos não é o facto de permitirem a cada um conhecer pessoas estranhas ao seu quotidiano, mas sim o de dar a possibilidade aos seus utilizadores de articular e tornar visível a sua rede social, isto é, o grupo de amigos que tem à sua volta. Este fenómeno dá origem a conexões entre pares que de outro modo não poderiam existir. Contudo, este tipo de relação não é o objectivo principal de muitos, visto que o propósito de partilha é muitas vezes a relação entre pessoas com quem já têm ligações fora do contacto feito *online*. Por outras palavras, a conectividade entre pares é muitas vezes feita entre pessoas que já se conheceram pessoalmente no passado. Em grande parte das PRS, os seus participantes não procuraram necessariamente conhecer pessoas novas, em vez disso, estes procuram primariamente estabelecer um contacto com as pessoas que já fazem parte da sua rede social comum (Boyd & Ellison, 2008).

Embora as PRS vão implementando ao longo do tempo mais funcionalidades, a sua base consiste na visualização do perfil de um utilizador da plataforma que é articulado com uma lista de "Amigos" do mesmo. Neste contexto, os "Amigos" não são mais do que outros utilizadores do sistema com o qual o proprietário do perfil se relaciona. Os "Perfis", que existem neste tipo de plataformas, são páginas únicas que pertencem a um dado utilizador e onde são inseridas informações sobre o seu titular. Quando um determinado utilizador se regista numa PRS são colocadas várias questões tendo em vista a obtenção de informação individual. O perfil desse utilizador é então gerado usando como conteúdo as respostas dadas nessa fase de registo, onde estão incluídas, tipicamente, informações como a idade, localização, interesses culturais, desportos de eleição, uma zona onde são descritas algumas características que o utilizador considere importantes denominada de "Sobre mim", entre outras. A grande maioria deste tipo de plataformas encoraja também os seus utilizadores a carregarem algumas fotos, a adicionarem conteúdos multimédia ou mesmo a mudar o visual e estrutura da página, tudo isto com o argumento de completar e personalizar o seu perfil. Algumas plataformas, como o *Facebook*, permitem que os proprietários dos perfis possam adicionar módulos ("Aplicações") igualmente com o argumento de melhorar o perfil e a sua usabilidade (Boyd & Ellison, 2008). Entre estas aplicações encontram-se questionários sobre figuras de cinema, jogos, calendários com alertas, e outras de aplicações dos mais variados tipos.

A visibilidade dos perfis criados nas PRS pode variar de plataforma para plataforma e de acordo com a discrição que os seus utilizadores entendam como necessária. Vejamos a forma como é gerida a visibilidade dos perfis nas seguintes plataformas: *Friendster*, *LinkedIn*, *Myspace* e *Facebook*.

Por definição, perfis criados no *Friendster* são encontrados nos motores de busca e visíveis a todos, independentemente se quem vêm detêm conta na plataforma ou não. Alternativamente, o *LinkedIn* controla aquilo que pode ser visto baseando-se no facto de um utilizador ter conta paga na plataforma. Plataformas como o *Myspace* permitem que os utilizadores seleccionem se pretendem que o seu perfil seja público ou se pretendem que o mesmo seja visível apenas pelos seus amigos ("Só amigos"). O *Facebook* apresenta uma abordagem diferente. Por definição, os utilizadores que façam parte da mesma rede de "Amigos" podem visualizar perfis de outros, a menos que o proprietário de um dado perfil indique explicitamente que não permite a visualização do seu perfil por parte de outros utilizadores que não pertençam à sua rede. Esta variação entre estruturas de visibilidade e de acesso aos perfis é um dos elementos diferenciador entre PRS (Boyd & Ellison, 2008). Para além de tudo isto, depois de integrarem estas plataformas os utilizadores são convidados a procurar e identificar outros utilizadores com os quais já tenham algum tipo de relação anterior. Dependendo da plataforma, a terminologia utilizada pode igualmente variar. Entre os termos mais populares estão "Amigos", "Fãs" ou "Contactos". Muitas das PRS implicam necessariamente uma confirmação de amizade bidireccional, por outras palavras, uma confirmação feita tanto por quem convida como por quem é convidado para ser "Amigo". No entanto, isto não acontece em todas as plataformas visto que algumas delas apresentam-se como sendo unidireccionais. Dentro destes convites unidireccionais, e quanto à terminologia, as pessoas com quem se estabelece uma relação desse tipo são rotuladas de "Fãs", "Seguidores" ou mesmo de "Amigos" em casos menos frequentes. O termo "Amigos" pode ser enganador, visto que é possível estabelecer uma comunicação entre pares mesmo que não exista uma relação real de amizade. Uma ligação deste tipo pode ter os mais variados propósitos (Boyd & Ellison, 2008).

A exibição das conexões estabelecidas nestas plataformas é um componente crucial das PRS. As listas de amigos permitem aceder a outros perfis levando a que se possa navegar por entre os vários perfis de utilizador sendo para isso necessário apenas um *click* dentro dessa lista e dentro dos diferentes perfis visitados. Em muitos casos, esta

lista de amigos é visível a todos os que tem permissão para visualizar um perfil, muito embora existam excepções. Por exemplo, tanto o *Myspace* como o *Facebook* tem como opção a omissão da lista de amigos (Boyd & Ellison, 2008).

Embora as PRS sejam conhecidas como plataformas largamente acessíveis, muitas atraem populações homogenias numa fase inicial, por isso não é invulgar encontrar grupos que utilizem estas plataformas para criar grupos segmentados por nacionalidade, idade, nível educacional ou outros factores que tipicamente dividem a sociedade (Boyd & Ellison, 2008).

2.5.2. Privacidade vs. Plataformas Redes Sociais

O sucesso das redes sociais que foram surgindo *online* durante os últimos anos tem tido como consequência um aumento do volume de informação que os utilizadores destas plataformas partilham na *Web* e de aplicações de gestão de redes sociais. Neste contexto, o essencial é assegurar a privacidade da informação pessoal, isto é, de conteúdos e dados pessoais, nas plataformas onde ser criam essas referidas redes sociais (Rodríguez, Rodríguez, Carreras, & Delgado, 2009).

No que diz respeito à relação entre privacidade e a acção de uma pessoa nas redes sociais esta pode ser multifacetada. Isto é explicado da seguinte forma. Em certas ocasiões pretende-se que a informação sobre nós próprios seja apenas conhecida por pessoas de um círculo muito restrito de amigos próximos e não por estranhos. Por outro lado, muitos utilizadores estão dispostos a revelar informações pessoais a pessoas alheias mas não para aqueles que os conhecem melhor (Gross & Acquisti, 2005). A privacidade nas redes sociais é muitas vezes aquilo que não esperamos que seja ou mesmo algo que não está claramente definido. Na verdade, as PRS, e ao contrário do que muitas vezes se pensa, registam todas as interacções e utilizam-nas de forma a potenciar a actividade social através do uso de tecnologia de *Data Mining* (procura de padrões num grande volume de dados). Fora de um ambiente que envolva a Internet, muitas das actividades sociais e comportamentos não deixam qualquer tipo de rasto. Esta carência de registo é um elemento passivo da privacidade social. Dentro deste contexto, o grande desafio para estas plataformas é a necessidade de explicitar políticas e mecanismos de protecção a fim de igualar o nível de privacidade social que existe na interacção *offline* (Dwyer, Hiltz, & Passerini, 2007).

2.6. Controlo de privacidade nas plataformas de redes sociais

As PRS existentes *online* disponibilizam e oferecem oportunidades de interacção e de comunicação muito interessantes. Contudo, o crescimento associado a essa oferta leva também a um aumento de novos desafios no que diz respeito à privacidade (Acquisti & Gross, 2006). Neste contexto, torna-se importante perceber como lidam as PRS que apresentam um maior número de utilizadores com a privacidade e como é feito o seu controlo.

Para análise foram seleccionadas as quatro redes sociais que apresentam uma grande adesão por parte dos utilizadores, neste momento, em Portugal, sendo estas o *Facebook*, o *Twitter*, o *Myspace* e o *Google+*.

2.6.1. Facebook

O *Facebook* (FB) é uma PRS caracterizada por ter uma forte presença de membros do ensino secundário e superior. De todas as redes sociais o FB destaca-se por três razões principais: por ser um sucesso entre as multidões estudantis, por deter uma vasta quantidade e qualidade de informação pessoal de cada utilizador disponível a todos os seus utilizadores e o facto de a informação contida na plataforma ser identificada pessoalmente, o que não acontece em outras plataformas destinadas a jovens estudantes.

O FB tornou-se um fenómeno nos Estados Unidos da América tendo-se espalhado entre os alunos do ensino superior atraindo mais de 9 milhões de utilizadores nos seus primeiros tempos de existência. A penetração do FB é impressionante: esta PRS atraiu quase 80% da população estudantil jovem americana em apenas um ano de existência. A quantidade e qualidade da informação oferecida é igualmente impressionante não só pela existência de perfis com informação pessoal inserida pelo próprio mas também pelo facto de oferecer informação como moradas ou números de telemóvel que não se encontram disponíveis de uma forma simples em condições normais (Acquisti & Gross, 2006).

Os utilizadores do FB podem partilhar os mais diversos conteúdos com outros utilizadores. Este tipo de informação pode compreender contactos pessoais, informação pessoal como o género, data de nascimento, cidade de residência; informação sobre interesses musicais, livros, filmes e desportos; estado de relacionamento e orientação política. Esta informação pode ser actualizada pelo utilizador a qualquer dia e a qualquer hora (Govani & Pashley, 2005).

Globalmente, no último mês de 2011 e nos primeiros cinco meses de 2012, esta plataforma apresenta a seguinte distribuição (Ilustração 14) no número de utilizadores (Portugal Facebook Statistics, 2012).

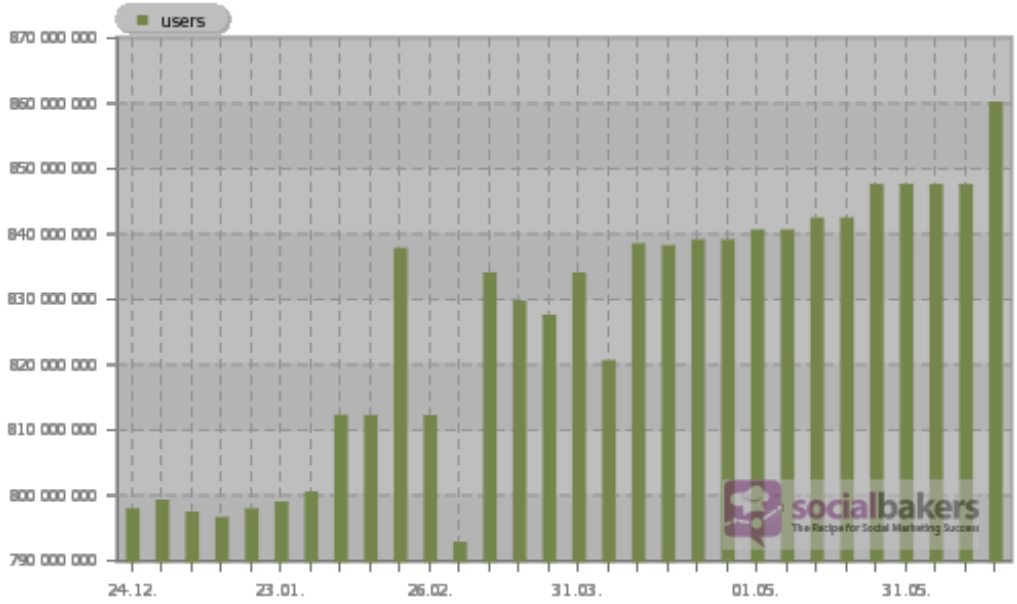


Ilustração 14 - Distribuição mundial dos utilizadores de Facebook entre Dezembro de 2011 e Maio de 2012 (Portugal Facebook Statistics, 2012)

Tal como é verificável no quadro anterior, no mês de Maio de 2012 o número de utilizadores do FB a nível mundial atingia os 860 717 180 de utilizadores.

Em Portugal no mês de Maio de 2012, o número de utilizadores do FB ascendia aos 4 380 420 estando no número 38 no ranking mundial de utilizadores desta plataforma. A sua taxa de penetração junto da população é de 40.80%, mais que duplica esse valor quando falamos de população *online*, chegando aos 84.75% (Portugal Facebook Statistics, 2012).

O gráfico que se segue (Ilustração 15) apresenta a distribuição etária dos utilizadores de FB em Portugal (Portugal Facebook Statistics, 2012).

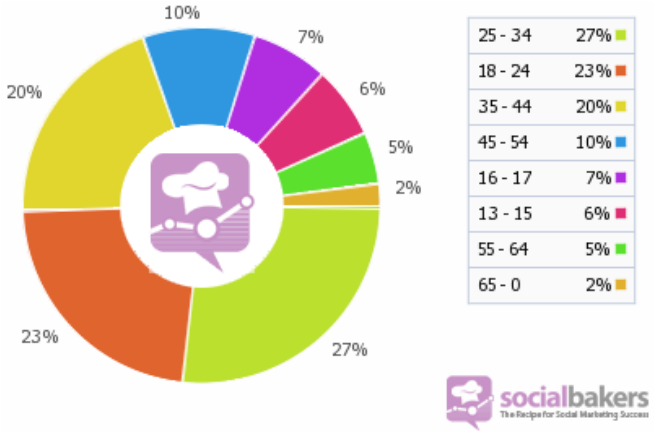


Ilustração 15 - Faixas etárias por percentagem dos utilizadores de Facebook em Portugal (Portugal Facebook Statistics, 2012)

Como podemos verificar, o maior número de utilizadores desta PRS encontram-se nas faixas etárias entre os 18 e os 24 anos e os 25 e os 34 anos de idade.

2.6.1.1. Política de privacidade e de utilização de dados do Facebook

O FB armazena tipos de informação pessoal de vários tipos: informação de registo, informação de partilha do utilizador, informação que outros utilizadores partilham sobre o utilizador em questão e ainda outras informações não voluntárias na utilização da plataforma (Facebook: Política de Utilização de Dados, 2011).

No registo do utilizador a informação que é guardada é aquela que é disponibilizada directamente pela pessoa que se está a registar na plataforma, isto é, nome, correio electrónico, data de nascimento e sexo.

Da informação que é partilhada na plataforma, o FB conserva no seu sistema todos os registos de actualizações de estado, carregamento de fotos ou comentários a outros perfis. Neste pacote de informação retida está incluída informação relativa a acções do próprio utilizador como são exemplo a adesão de um amigo ao grupo de "Amigos" do perfil, a "Gostos" (sinónimo de preferência por uma dada página, grupo, foto, etc.) realizados pelo utilizador, a informação de localização cedida pelo utilizador, a adesão de um amigo por sugestão do sistema ou importação através dos contactos de correio electrónico e a indicação de relacionamento do utilizador do perfil do FB. Dentro deste tópico a plataforma arquiva também as fotos inseridas como fotos de perfil e as redes de partilha. A data de nascimento do utilizador permite direccionar conteúdo e anúncios directamente para o utilizador através da procura de preferências (Facebook: Política de Utilização de Dados, 2011).

Relativamente à informação que outros utilizadores partilham sobre o utilizador, esta plataforma retêm informação através do sistema de identificação em fotos, locais ou grupos. Nestes grupos um utilizador pode ser adicionado por outros sendo essa informação registada. A plataforma recebe também informação sobre jogos ou aplicações adicionadas por um dado utilizador.

O FB guarda também outras informações relativas a interacções como a visualização de perfis de outros utilizadores, envio de mensagens a outros, pesquisas feitas na plataforma ou num anúncio seleccionado. Existem metadados que são armazenados pela plataforma como a hora, data, local onde foi feita uma acção em concreto. A localização GPS, endereço IP, tipo de navegador usado ou páginas visitadas pelo utilizador são informações também elas retiradas do computador, dispositivo ou telemóvel dependendo do aparelho utilizado para aceder à plataforma. Quando existe uma localização por GPS esta é associada a informação já existente nos sistemas do FB.

Os dados que o FB recebe são fornecidos a parceiros publicitários ou clientes depois de removidas informações pessoalmente identificáveis de forma a não haver associação ao utilizador de uma forma pessoal e directa. Os dados recebidos por clientes e fornecedores publicitados são armazenados 180 dias e depois desse período são combinados com outros dados para que não sejam associados pessoalmente (Facebook: Política de Utilização de Dados, 2011).

A informação recebida pela plataforma FB é utilizada, segundo o próprio FB da seguinte forma (Facebook: Política de Utilização de Dados, 2011):

- ✓ Para manter a segurança da própria plataforma;
- ✓ Para fornecimento de funcionalidades e serviços de localização aos utilizadores;
- ✓ Para medição e compreensão da eficácia dos anúncios publicitados;
- ✓ Para alimentação do sistema de sugestões de amigos, páginas ou grupos;
- ✓ Para inovação de serviços e funcionalidades oferecidas aos utilizadores.

O FB apresenta garantias de privacidade afirmando que partilha informação recebida do utilizador apenas e só se receberem a permissão do utilizador, se o utilizador for notificado ou se o utilizador eliminar o nome ou qualquer informação pessoalmente identificável (Facebook: Política de Utilização de Dados, 2011).

2.6.2. Twitter

O *Twitter* (TW) é uma PRS de *microblogging* fundada em 2006 com o propósito de permitir aos seus utilizadores partilhar mensagens de texto com outros que são designadas por *tweets*. Originalmente este sistema foi criado para partilha de texto via SMS (*Short Message Service*) e por isso tem como limite máximo de dimensão de cada *tweet* 140 caracteres. Na verdade, este serviço evoluiu muito para além das mensagens escritas, no entanto, acabou por persistir ao longo do seu desenvolvimento a limitação dos 140 caracteres.

A criação do TW permitiu combinar redes sociais com a actividade de um *blog* mas com algumas diferenças. Quando falamos da parte de rede social estamos a falar das redes que se geram em torno de um utilizador. Os perfis relacionam-se entre si, originando as referidas redes, mas estas ligações não são directamente reciprocas. Isto é, um utilizador pode querer aceder a conteúdos de outro, carregando na opção *Follow* ("Seguir"), mas o utilizador que está a ser acompanhado pode não desejar o inverso. O TW é também em parte um *blog* na medida em que os utilizadores mostram os seus *tweets* por ordem cronológica invertida mas não apresenta a possibilidade de comentar o texto publicado como acontece nos *blogs*.

Muito embora as pessoas possam interagir directamente através desta plataforma, existem também algumas aplicações disponíveis. Tanto em dispositivos móveis como em computadores pessoais existem ferramentas que permitem aos clientes do *Twitter* seguir os tópicos mais populares, saber quem segue quem e visualizar quão populares os utilizadores são (Boyd, Golder, & Lotan, 2010).

Na figura que se segue (Ilustração 16) podemos verificar quais os utilizadores com mais seguidores a nível mundial até ao mês de Maio de 2012.

#	Screen name	Following	Followers ▼
1.	Lady Gaga (@ladygaga)	138 572	25 931 039
2.	Justin Bieber (@justinbieber)	123 106	23 608 752
3.	Katy Perry (@katyperry)	97	21 575 547
4.	Rihanna (@rihanna)	818	20 961 145
5.	Britney Spears (@britneyspears)	415 055	17 818 152
6.	Barack Obama (@BarackObama)	676 742	16 740 830
7.	Shakira (@shakira)	66	16 629 887
8.	Taylor Swift (@taylorswift13)	80	15 299 929
9.	Kim Kardashian (@KimKardashian)	176	15 050 615
10.	YouTube (@YouTube)	423	13 948 500

Ilustração 16 - Ranking mundial de utilizadores do Twitter por número de seguidores (Twitter Statistics, 2012)

Como é verificável, o número de utilizadores desta plataforma ascendem às dezenas de milhões mundialmente. Neste caso, a figura pública mundial Lady Gaga ascende aos 25 931 039 seguidores dos seus *tweets* (Twitter Statistics, 2012).

2.6.2.1. Política de Privacidade do Twitter

O *Twitter* é uma PRS que define uma série de políticas e procedimentos quanto à forma como recolhe, usa e divulga a informação que retira da sua plataforma. O *Twitter* recebe informações através de *sites* da Internet, SMS, API (*Application Programming Interfaces*), aplicativos e de serviços comuns e de terceiros (Política de Privacidade do Twitter, 2011).

Informação recolhidas durante o registo: Quando uma conta é criada no *Twitter* cada utilizador fornece informações pessoais como nome, nome de utilizador, apelido, senha e correio electrónico. Algumas das informações (como o nome e nome de utilizador) são listadas no serviço do *Twitter* estando também incluído na página de perfil do utilizador e nos resultados de busca da plataforma.

Informação adicional: Esta plataforma sugere também a recolha de informação adicional como biografia da pessoal, localização, número de telemóvel ou uma foto. Esta informação é utilizada de forma a disponibilizar serviços e divulgar produtos ao utilizador. Todas estas informações pessoais são de caracter opcional.

Informação pública: Grande parte da informação compartilhada no *Twitter* tem de ter o consentimento do próprio utilizador para se tornar pública. A informação pública referida inclui a informação de cada *tweet* e os metadados fornecidos com esse mesmo

tweet. Para além disso, estão dentro deste pacote também listas criadas pelo utilizador, o grupo de seguidores (*Followers*), os *tweets* favoritos, os *retweets* e outros pedaços de informação. Por comportamento padrão o TW é em grande maioria das vezes a divulgação de informação de forma pública apesar de oferecer opções de configuração (Política de Privacidade do Twitter, 2011).

Informação de localização: Os utilizadores podem definir a localização em cada *tweet* que fazem podendo o TW utilizar essa informação recolhida de forma exacta para melhoria do serviço. Os servidores do TW registam de forma imediata os chamados dados de registo. Os dados de registo incluem informação relevante como endereços IP, tipo de navegador, domínio referente, páginas visitadas, operadora de dispositivo móvel, o próprio dispositivo móvel, identificadores de aplicativos e históricos de busca. Interacções na plataforma em si ou através de anúncios e aplicativos podem também ser incluídas nos dados de registo. O TW compromete-se a apagar este tipo de registos após 18 meses.

Ligações: O TW pode acompanhar as interacções do utilizador através de *links* e regista-las incluindo-as nos serviços a terceiros, clientes ou através de outros meios.

Cookies: Esta plataforma pode usar tanto *cookies* de sessão como *cookies* persistentes e retirar destes informação sobre interacção com a plataforma TW mas também pretende monitorizar o uso agregado pelos utilizadores da plataforma e verificar o tráfego efectuado. O TW justifica sempre este tipo de decisões como sendo para melhoria de serviço.

Serviços de terceiros: O TW utiliza serviços de terceiros que podem utilizar a informação que lhes é fornecida pela plataforma TW como *cookies* ou informação sobre IPs.

O TW determina também alguns pontos importantes relativos à divulgação de informação que recolhe dos seus utilizadores e serviços.

Existe informação que pode ser compartilhada com o consentimento do utilizador e que é disponibilizada quando um dado utilizador decide aceder ao TW através de terceiros e não pela própria plataforma. No entanto, existem informação não pessoal ou agregada que o TW pode divulgar como *tweets* públicos ou número de utilizador que interagiram com um dado *tweet*, por exemplo. No que diz respeito a questões legais e transferência

comerciais, o TW pode fornecer informação pessoal para cumprimento de lei, regulamentação ou solicitação legal, reservando-se igualmente no direito de transferência de informação em caso de alienação (Política de Privacidade do Twitter, 2011).

2.6.3. MySpace

A plataforma *MySpace* (MS) é uma rede social que surgiu com o propósito de aumentar a interacção entre o público jovem em torno do entretenimento e da ligação destes mesmo jovens à música, celebridades, televisão, filmes e jogos. Esta oferta é disponibilizada através da plataforma própria do MS ou dispositivos móveis (MySpace: Acerca de Nós, 2012).

Dentro do MS existe uma oferta de um catálogo de áudio e vídeo alimentado pelos próprios utilizadores e em constante crescimento que é oferecido de forma gratuita a quem acede a um dado perfil do MS. Neste contexto, fornece-se a possibilidade tanto aos grandes artistas como a artistas independentes e não editados, as ferramentas necessárias para divulgação do seu conteúdo artístico para o público em geral (MySpace: Acerca de Nós, 2012).

2.6.3.1. Política de privacidade do MySpace

O MS define na sua política de privacidade um conjunto de dados a que chama de informação pessoalmente identificável (IPI) e um outro a que dá o nome de informação não pessoalmente identificável (INPI). Entre o grupo de IPI estão informações como nome completo, endereço de correio electrónico, endereço postal, número de telefone ou número de cartão de crédito e que são atribuídos de forma voluntária pelo utilizador. Ainda referente a este tipo de dados, o MS afirma que notifica os utilizadores da plataforma para que se possa certificar de que esse utilizador está consciente da sua acção. Quanto à INPI o MS define esta informação como sendo de carácter não privado e onde inclui endereços de IP, dados de utilizador agregados e o tipo de navegador utilizado. Este tipo de dados é recolhido com o propósito de melhorar o serviço e para fins de segurança dos seus utilizadores.

O MS recolhe IPI através da acção de registo do utilizador e pela adesão do mesmo a actividades promocionais, sondagens ou sorteios. Quanto à INPI, o utilizador pode também inserir informação como a data de nascimento, interesses, tempos livres, opções de vida, grupos aos quais estejam afiliados, vídeos e/ou imagens, mensagens privadas,

recados ou declarações pessoais. Esta informação é cedida apenas com o consentimento do utilizador não sendo de caracter obrigatório (MySpace: Política de Privacidade, 2010).

A PRS MS utiliza os *cookies* para identificar o navegador utilizado, armazenar preferências dos utilizadores e verificar se o utilizador tem *software* instalado que permita aceder aos serviços do MS. O MS faz uso de *cookies* e ferramentas semelhantes para personalização do conteúdo e publicidade que recebe de acordo com a informação fornecida pelo utilizador.

No que diz respeito à utilização de dados recolhidos, o MS pode divulgar IPI nas seguintes situações: protecção ou defesa de direitos legais da empresa ou afiliadas, protecção da segurança dos utilizadores do seu serviço, na protecção contra fraudes ou de gestão de risco e para efeitos de cumprimento de processos legais e da própria lei. O MS também fornece a IPI a terceiros nos casos em que o utilizador tenha optado por receber determinada informação e que tenha sido notificado de que a execução desse pedido requer a partilha da referida IPI (MySpace: Política de Privacidade, 2010).

No campo da segurança o MS emprega medidas comerciais, técnicas, pessoais e físicas para protecção da IPI e de números de cartão de crédito. Para além disso, cumpre com o *Safe Harbor Framework* (quadro de segurança entre os EUA e a UE) garantindo que cumpre todos os princípios de privacidade referentes à notificação, escolha, transferência para jusante, segurança, integridade de dados, acesso e aplicação de informação (MySpace: Política de Privacidade, 2010).

2.6.4. Google Plus

O *Google Plus* (GP) é uma plataforma onde são criadas redes sociais de utilizadores criada pela empresa *Google*. O GP permite a ligação entre diferentes pessoas na Internet parecida com uma interacção no mundo real. Esta plataforma permite partilhar ideias, páginas, fotos ou "Círculos". No GP os círculos tem como base um conjunto de pessoas diferentes que partilham conteúdos, isto é, um círculo pretende simular os círculos pessoais que todos nós criamos no nosso quotidiano tendo em conta a especificidade de cada pessoa que conhecemos. Podemos, por exemplo, distinguir o nosso chefe do nosso amigo de infância colocando-os em "Círculos" distintos para que o conteúdo que é enviado para um não seja enviado para o outro e vice-versa (Google Plus: Visão Geral, 2011).

O GP apresenta outras funcionalidades como os *Hangouts*, jogos, pesquisa, carregamento instantâneo de fotos e *chat* de conversação.

O serviço de *Hangouts* na prática não é mais do que um serviço de conversação por *chat* de vídeo onde um grupo de pessoas pode interagir sem sair de casa, sendo para isso apenas necessário uma *webcam*. Com este serviço o utilizador pode comunicar com pessoas dos seus "Círculos" sem que seja necessária a sua deslocação física. Para além disto, o GP apresenta no seu sistema alguns jogos que todos os utilizadores podem jogar sem que seja necessária instalação do mesmo. A pesquisa de amigos também é permitida nesta plataforma.

Para os acessos através de dispositivos móveis o GP oferece um serviço de carregamento de fotos instantâneo para o perfil do utilizador e ainda um serviço de *chat* para que o utilizador possa conversar com os seus "Círculos" bastando para isso ter acesso à Internet (Google Plus: Visão Geral, 2011).

Quanto aos utilizadores do GP, estes ainda apresentam valores baixos sinónimo de pouca adesão por parte dos utilizadores deste tipo de plataformas. Isto justifica-se com o facto de esta PRS ser uma criação recente do *Google*. Na imagem que se segue (Ilustração 17) podemos verificar que em Maio de 2012 o utilizador mais seguido a nível mundial (Britney Spears) não ultrapassa os três milhões e meio de utilizadores (Google+ statistics, 2012).

#	Name	Following	Followers ▼
1.	Britney Spears	4 468	3 493 196
2.	Snoop Dogg	33	3 012 543
3.	Ashley Tisdale	N/A	2 773 420
4.	Usher	1	2 663 639
5.	Tom Anderson	N/A	2 584 429
6.	Trey Ratcliff	1 522	2 576 982
7.	Hugh Jackman	1	2 554 833
8.	Thomas Hawk	2 525	2 550 451
9.	Felicia Day	N/A	2 508 145
10.	Tyra Banks	11	2 470 842

Ilustração 17 - Ranking mundial de utilizadores do Google Plus por número de seguidores (Google+ statistics, 2012)

2.6.4.1. Recolha e tratamento de informação do Google Plus

O GP recolhe informação dos seus utilizadores de duas formas: através do fornecimento directo do utilizador ou através da informação que é retirada dos serviços que são disponibilizados pela plataforma.

A quando do registo o GP exige que o utilizador insira alguns dados que são imediatamente tratados. Entre estes dado está o nome do utilizador, endereço de correio electrónico, número de telefone ou de cartão de crédito. Para a criação do perfil do *Google* é também muitas vezes solicitada uma foto que também é igualmente armazenada (Google Plus: Política de Privacidade, 2012).

Quanto às informações retiradas a partir da utilização dos serviços do *Google* estas incluem serviços que são usados, o modo como são usados e visitas a *web sites* que utilizam os serviços de publicidade (visualização ou interacção anúncios e conteúdos *Google*).

Informações de aparelhos: O GP retém informação de dispositivos tais como modelo do *hardware*, versão do sistema operativo, identificadores únicos do aparelho e informações relativas à rede de telemóvel, incluindo números de telemóvel. Para além destas o GP recolhe automaticamente as seguintes informações: (i) detalhes sobre como são utilizados os serviços *Google*; (ii) informações de registo telefónico como o número de telemóvel, número de destino, número e informações de encaminhamento, hora e data das chamadas, duração e tipo de chamadas; (iii) endereço IP; (iv) informações de eventos do aparelho tais como falhas e actividade do sistema, definições de *hardware*, tipo de navegador, idioma do navegador, data e hora do pedido e URL (*Universal Resource Locator*) de referência; (v) *cookies* que permitem a identificação do navegador ou conta *Google* do utilizador.

Informações de localização: O GP recolhe informações de localização como sinais de GPS, informação sobre pontos de acesso *Wi-Fi* e torres de rede de telemóvel.

Números de aplicações exclusivos: Alguns serviços incluem um número de aplicação exclusivo. Este número, as informações sobre o tipo de sistema operativo e o número de versão da aplicação são recolhidos pelo GP.

Armazenamento local: O GP armazena dados relativos a informações (incluindo dados pessoais) localmente no aparelho do utilizador usando o armazenamento feito pelo navegador e caches de dados de aplicações.

***Cookies* e identificadores anónimos:** O GP envia, em muitas situações, *cookies* ou identificadores anónimos (cadeia de caracteres aleatória) para o aparelho utilizado para aceder às plataformas para recolha de informação (Google Plus: Política de Privacidade, 2012).

O GP utiliza todas as informações recolhidas com o intuito de disponibilizar, manter, proteger e melhorar os serviços e desenvolver outros, bem como para proteger a empresa em si e os seus utilizadores. As informações recolhidas a partir de *cookies* e de outras tecnologias são processadas para apresentação de conteúdos e anúncios personalizados. Não existe associação desses referidos *cookies* a categorias pessoais e sensíveis como raça, religião, orientação sexual ou saúde.

O GP combina informações pessoais, ou outras, com informação de outros serviços da *Google* de forma a facilitar a partilha de itens com pessoas conhecidas do utilizador. Não são combinadas informações retiradas de *cookies* com informações de caracter pessoal, salvo mediante consentimento do utilizador (Google Plus: Política de Privacidade, 2012).

2.7. Comparação entre os diferentes controlos de privacidade

As PRS analisadas apresentam-se como sendo similares em diversos aspectos, começando pelo facto de serem, em todos os casos, plataformas que têm como intuito principal o estabelecimento de comunicação entre pessoas através de uma comunidade que apresenta um padrão de interesses comuns.

Para além disso, estas quatro redes sociais apesar de algumas delas terem propósitos distintos são semelhantes no que diz respeito ao público-alvo, à criação de perfis de utilizador e à partilha de conteúdo digital.

Todas as PRS descritas apresentam um público-alvo preferencial comum apesar de algumas delas não o referirem explicitamente. Estas redes sociais pretendem uma adesão por parte dos utilizadores que se encontram na faixa etária entre os 16 e os 30 anos, visto que grande parte dos serviços que estas plataformas disponibilizam estão mais acessíveis a pessoas que se encontrem entre estas idades. Isto não invalida o facto

de existirem também um grande número de utilizadores que estejam fora deste intervalo de idades.

A criação de perfis pessoais de utilizador é também algo presente nestas quatro plataformas. Em qualquer delas, o utilizador tem necessariamente de criar um perfil, individual ou de grupo, para que possa interagir e usufruir de tudo o que é disponibilizado. Estes perfis contêm informação pessoal, parte dela de inclusão opcional, como nome e apelido, endereço de correio electrónico ou foto.

Algo comum a todas estas plataformas é também a partilha de conteúdo. O *Twitter* e o *MySpace* definem claramente o conteúdo que pretendem divulgar pequenos textos e música e vídeo, respectivamente. Já o *Facebook* e o *Google Plus* promovem conteúdos dos mais diferentes tipos, sem que exista um foque específico. Muito embora existam estas diferenças, todas elas existem com o propósito de possibilitar a partilha de conteúdos em comunidade, independentemente do tipo de conteúdo.

Para uma melhor compreensão da forma como as redes sociais em análise gerem o conteúdo foram definidos os seguintes critérios: conteúdo directo e conteúdo de actividade. A definição destes critérios foi elaborada tendo em conta a distinção que as próprias plataformas fazem nas suas políticas de privacidade entre o conteúdo que é inserido pelo utilizador e aquele que é consequência da sua actividade.

O Conteúdo Directo compreende toda a informação que é disponibilizada à plataforma de forma directa e consciente por parte do utilizador da mesma. Por exemplo, quando se efectua um registo em qualquer das plataformas é necessário o preenchimento do campo referente ao endereço de correio electrónico que é escrito directamente pelo utilizador na plataforma.

O Conteúdo de Actividade é todo aquele que não é entregue à plataforma de forma directa mas em consequência da utilização dos serviços por parte dos utilizadores. Temos como exemplo o endereço IP. Esta informação é disponibilizada de forma indirecta pelos utilizadores que não fornecem de uma forma directa o seu endereço de rede.

Segue-se uma tabela (Tabela 1) comparativa entre o conteúdo armazenado pelas quatro PRS em análise segundo os critérios já referidos:

		Redes Sociais			
		Facebook	**Twitter**	**MySpace**	**Google Plus**
Critérios	**Conteúdo Directo**	Informação de registo (dados pessoais e interesses), conteúdo partilhado e informação de outros utilizadores (identificação em fotos).	Informação de registo (dados pessoais), adicional (interesses) e pública (*Tweets*).	Informação de registo (dados pessoais), adicional (*hobbie*), contéudo partilhado, actividades promocionais, sondagens e sorteios.	Informação de registo (dados pessoais), conteúdo partilhado e foto de perfil.
	Conteúdo Actividade	Informação não voluntária (IP, GPS, tipo navegador, páginas visitadas, visualizações, mensagens, pesquisas e anuncios).	Informação de localização (IP, GPS, tipo navegador), ligações (interacções), *cookies* (trafego e uso agregado) e serviços externos.	*Cookies* (tipo de navegador, preferências e personalização), endereços IP e dados agregados.	Informação de aparelhos (IP, tipo utilização, registos telefónicos e tipo de navegador), localização (GPS, Wi-Fi), armazenamento local (Caches), e *cookies* e identificadores anónimos.

Tabela 1 - Comparação entre conteúdos armazenados pelas PRS

Quanto ao Conteúdo Directo as quatro plataformas armazenam informações relativas ao registo efectuado pelo utilizador apesar de muita dessa informação de preenchimento obrigatório poder não ser a mesma, podendo esta variar de plataforma em plataforma. Para além disso, todas estas plataformas registam igualmente o conteúdo que é inserido na sua plataforma e que é partilhado directamente pelo utilizador. Se compararmos o conteúdo directo pedido, por exemplo, pelo *Facebook* e pelo *Google Plus*, que são duas plataformas com princípios semelhantes, podemos verificar que a informação que é pedida directamente ao utilizador é em maior número no *Facebook*. O *Google Plus* não dá uma importância tão grande ao que outros utilizadores realizam relativamente a um dado utilizador como acontece no *Facebook*. O *Myspace*, ainda sobre o critério de Conteúdo Directo, destaca-se pelo facto de recolher directamente do utilizador informação em actividades promocionais, sondagens e sorteios. Em nenhuma outra PRS acontece o mesmo.

No que diz respeito ao Conteúdo de Actividade, existem um conjunto dados que são registados por todas as PRS em análise. Entre estes dados estão endereços IP e o tipo de navegador utilizado para acesso à plataforma. Existe também outro tipo de informação que é retirada da utilização por algumas mas não pela totalidade das plataformas. Esta informação inclui: coordenadas de GPS recolhidas pelo *Facebook, Twitter* e *Google Plus*; *cookies* utilizadas pelo *Twitter*, *Myspace* e *Google Plus*; registo de páginas visitadas realizado pelo *Facebook, Twitter* e *Google Plus*; e dados de utilização agregados recolhidos pelo *Twitter* e *Myspace*.

Por outro lado, o que protege o conteúdo do utilizador das redes sociais? Que garantia é que o utilizador têm de que, uma vez removido o conteúdo da plataforma, que o conteúdo é realmente removido em definitivo?

As plataformas sociais, como o *Facebook*, *Twitter*, *Google+*, disponibilizam aos utilizadores "configurações de privacidade". Por outras palavras, os utilizadores podem especificar quais os outros utilizadores (ou grupos) que podem aceder ao seu conteúdo. Para cada categoria de conteúdo, o proprietário da conta pode definir a granularidade de acesso a uma *Access Control List* (ACL). Esta estratégia baseia-se na confiança que a plataforma oferece e no acesso controlado do utilizador aos seus dados. Além disso, os utilizadores precisam de confiar no serviço, não só para restringir os acessos aos seus conteúdos, através da ACL, mas também para poder fazer uma gestão dos mesmos (Francisco, Marques, & Serrão, 2012).

Os provedores de redes sociais *online* são incentivados a proteger o conteúdo do utilizador, uma vez que o contrário poderia manchar sua reputação e/ou resultar em acções judiciais. Por exemplo, os termos de uso do *Facebook* classificam todos os conteúdos dos utilizadores como "público", por definição, o que pode levantar algumas suspeitas sobre a privacidade e que devem ser analisadas por algumas instâncias, como por exemplo, da Comissão de Comércio Federal dos EUA. O conteúdo armazenado nas referidas plataformas está sujeito a um potencial acesso indevido ou a ataques internos, sobre os quais as entidades competentes depositam atenção (por exemplo, durante a investigação WikiLeaks) (Francisco, Marques, & Serrão, 2012).

Os riscos de privacidade são agravados pela prática comum de armazenamento *offline* ou em *cache* de conteúdo, mesmo depois que de os utilizadores exprimirem explicitamente a intenção de excluir o conteúdo. Assim sendo, a ameaça à privacidade dos utilizadores torna-se real. Estas plataformas têm de facto a preocupação de cuidar dos interesses de seus utilizadores?

Informações sobre utilizadores e sobre a sua privacidade podem ser valiosas. Existem duas formas de utilizar a informação recolhida nas redes sociais: para uso de terceiros ou para uso próprio. A informação privada é realmente atraente para venda quando se retêm um grande lucro dessa acção. É muito atraente para as redes sociais cair nesta “teia” visto que detêm muita informação sobre os mais diferentes tipos de utilizadores. Um dos exemplos mais famosos é o de uma entidade que dá pelo nome de "Internet

Grátis", que é acusada por venda de endereços de correio electrónico de utilizadores dos seus serviços (Francisco, Marques, & Serrão, 2012).

Além disso, as lojas *online* podem, através deste tipo de informações, fazer pesquisas para marketing e publicidade. Com isto, pode não só existir uma invasão da privacidade dos utilizadores, mas também originar uma competição desleal comparativamente com outros prestadores desse tipo de serviço (Francisco, Marques, & Serrão, 2012).

2.8. SmartRM

No mercado actual existe uma plataforma que apresenta o intuito de aplicar a GDD ao conteúdo individual, através da PRS *Twitter*, que tem o nome de *SmartRM*.

A plataforma *SmartRM* é uma extensão para o navegador *Mozzila Firefox* que permite proteger o conteúdo *Web* de uma forma individual, isto é, uma protecção de conteúdo partilhado definida por cada utilizador. Esta plataforma tem como principais atributos (SmartRM Home, 2010):

- Proteger conteúdo digital individual;
- Enviar conteúdo protegido por correio electrónico a amigos;
- Enviar conteúdo seguro a amigos que utilizem o *Twitter*;
- Reproduzir ficheiros no formato MPEG-21 (.mp21).

O *SmartRM* é uma extensão criada para ser utilizada no navegador *Mozilla Firefox*. No entanto, esta plataforma carece de actualização. A extensão *SmartRM* não se encontra disponível para versões do *Firefox* mais recentes como a actual 11.0, sendo para isso necessário instalar uma versão próxima da versão 3.5 para que esta extensão possa ser utilizada.

2.8.1. Funcionamento da plataforma SmartRM

Para utilizar o *SmartRM* é necessário efectuar um registo de modo a que o utilizador possa ser identificado e fazer a gestão dos seus conteúdos. Para além disso, é ainda necessária a associação da conta do *SmartRM* à conta que o utilizador possa ter no *Twitter* através da importação de contactos desta plataforma, caso o utilizador queira divulgar conteúdo directamente no *Twitter*. Segue-se então uma clarificação do funcionamento do *SmartRM*.

No ecrã inicial de contactos, apresentado abaixo (Ilustração 18), o utilizador pode escolher quais os contactos a quem pretende enviar um dado conteúdo e pode fazê-lo bastando para isso fazem um clique no botão do lado direito do rato (SmartRM: Create protected content for your contacts, 2010).

Ilustração 18 - Ecrã de contactos do SmartRM
(SmartRM: Create protected content for your contacts, 2010)

Posto isto, é necessário que o utilizador indique qual a directoria do conteúdo que se encontra guardado localmente. No entanto, os tipos de ficheiros que se podem partilhar são limitados. Existe ainda a possibilidade de acrescentar outros contactos adicionais para partilha do ficheiro em questão. A imagem abaixo (Ilustração 19) ilustra essas opções:

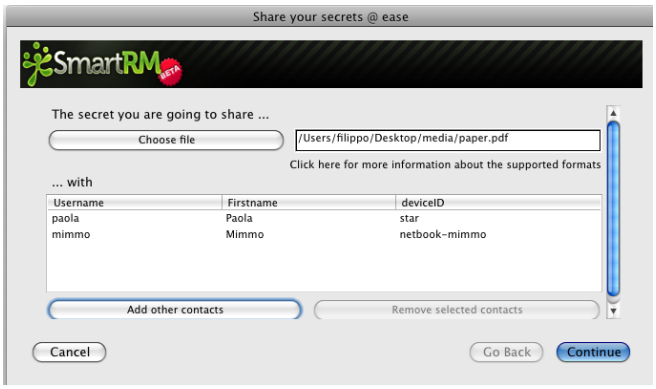


Ilustração 19 - Ecrã de escolha de conteúdo do SmartRM
(SmartRM: Create protected content for your contacts, 2010)

Antes disso é solicitado ao utilizador que indique qual o nome que quer dar ao ficheiro e a sua respectiva descrição. De seguida, o utilizador que pretende partilhar o seu conteúdo deve definir quais são os seus limites de acesso ao conteúdo em questão. Entre

estes parâmetros que limitam o acesso estão: o tipo de utilização (leitura, edição ou leitura e edição), opção de uso *online* ou *offline*, data de início de uso, data de fim de uso, duração permitida de uso e o número de vezes que esse conteúdo pode ser utilizado. A figura que se segue (Ilustração 20), mostra como são definidos os limites de acesso referidos (SmartRM: Create protected content for your contacts, 2010):

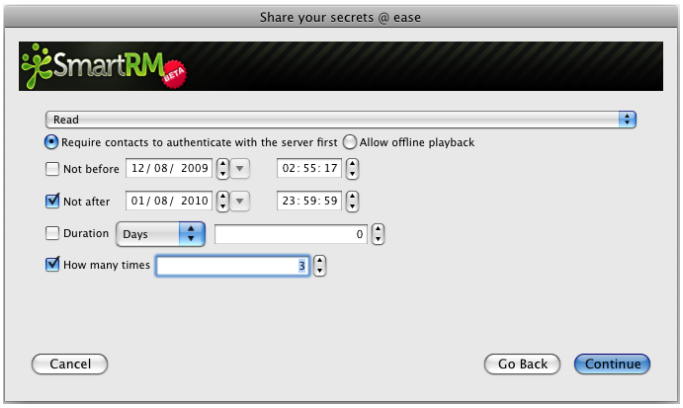


Ilustração 20 - Ecrã de limites de acesso ao conteúdo no SmartRM
(SmartRM: Create protected content for your contacts, 2010)

Após todo este processo o conteúdo pode ser partilhado directamente no *Twitter*, como anexo de uma mensagem de correio electrónico, ou através de um qualquer suporte de conteúdo físico (Memória USB).

3. Metodologia

Para um melhor esclarecimento da forma como se pretende que este projecto de pesquisa seja orientado, é necessária a exposição de todo o conjunto de regras e linhas condutoras a obedecer para que este referido projecto possa ser concluído com sucesso.

Estando este projecto relacionado com a criação de uma solução que possa ser testada por cada pessoa de forma individual, toda a pesquisa terá de ser baseada em estudos descritivos. Por outras palavras, visto que este projecto tem o propósito de conceber uma solução que seja benéfica para os utilizadores de redes sociais *Web*, estudando um dado número de utilizadores, é necessária uma pesquisa onde a descrição desse benefício seja clara e verificável.

Algo também muito importante a referir quando falamos em metodologia é precisamente o método a utilizar nesta análise. O método quantitativo é aquele que melhor se insere no âmbito deste projecto, visto que se pretende a procura da relação entre as variáveis em estudo e a sua relação causa-efeito.

Para ser feita uma avaliação entende-se como necessária a realização de questionários ao utilizador da solução. Ao serem retirados dados dos questionários de resposta fechada, salvo casos específicos em que se entenda como necessária algumas perguntas abertas, a realizar aos que pretendam testar a solução de gestão de conteúdos digitais, que se encontram registados em redes sociais *Web,* estes poderão mostrar se a ideia de criar um sistema deste tipo terá para eles uma utilidade prática na realidade. Pretende-se através desses mesmos questionários tirar conclusões que podemos assumir como gerais para a população em estudo a partir de um dado grupo de indivíduos.

No que diz respeito aos questionários, estes pretendem-se que sejam aplicados a um grupo de pessoas que usem redes sociais no seu quotidiano, que se irão assumir como parte do universo em estudo, ou seja, a amostra deste estudo será uma amostra de conveniência. Dentro do domínio de indivíduos que utilizam as redes sociais *Web*, este estudo pretende inquirir apenas algumas pessoas desse grupo, dependendo sempre a amostra da disponibilidade dos inquiridos e do tempo existente no projecto para questionários. Os dados produzidos após o termo dos inquéritos irão passar por uma análise estatística de onde irá resultar informação relevante e a ser tida em conta para validar a aceitação ou não por parte dos utilizadores da solução.

Segue-se o conjunto de fases a realizar neste projecto:

1. Enquadramento escrito do âmbito do tema a abordar no projecto.
2. Procura e tratamento de documentos teóricos para estudo de redes sociais e seus mecanismos de gestão de conteúdos.
3. Pesquisa documental de arquitecturas de gestão de conteúdos a utilizar na solução.
4. Desenho e construção da solução a desenvolver para uso na *Web*.
5. Realização de questionários de resposta fechada para validação da solução.
6. Análise estatística dos questionários realizados.
7. Escrita de conclusões estatísticas e finais do estudo.

Numa fase inicial, pretende-se definir um enquadramento de todo o tema a tratar neste projecto com o intuito de perceber qual o problema que pretende resolver, clarificar os pontos teóricos mais relevantes e definir linhas de orientação do projecto. De seguida, inicia-se o processo de procura de conteúdos teóricos necessário ao aprofundamento dos tópicos relativos às plataformas de redes sociais e à gestão de direitos digitais, como por exemplo, a teoria relativa aos mecanismos usados para proteger conteúdos em plataformas sociais *Web* já existentes. Para a construção da solução decidir-se-á qual a arquitectura a utilizar e o desenho e a forma de desenvolvimento da mesma. Posto isto, irá proceder-se à recolha e análise de questionários para verificar a aceitação da solução por parte dos potenciais utilizadores e uma análise estatística dos referidos questionários. Por fim, serão elaboradas tanto as conclusões dos questionários como as conclusões do projecto como um todo.

Todas estas fases terão de ser executadas para que os objectivos a que este projecto se propõe sejam cumpridos de forma clara.

4. Solução de gestão de direitos digitais em redes sociais Web

4.1. Introdução

A proposta de criação de uma solução de gestão de direitos digitais em redes sociais (SGDDRS) surge com o intuito de possibilitar o aumento da privacidade dos utilizadores de redes sociais e também de evoluir toda a temática em redor do estudo da GDD.

Um elemento indispensável para toda esta temática é um sistema que dá pelo nome de OpenSDRM. Este sistema foi criado em 2005 com o intuito de disponibilizar uma plataforma que permitisse a gestão de conteúdos digitais áudio e que apresentasse igualmente uma arquitectura genérica que fosse adaptável a outros cenários, também eles ligados à GDD (Torres, Serrão, Dias, & Delgado, 2008).

O OpenSDRM apresenta uma base de construção que assenta no conceito de Gestão de Direitos Digitais e que foi elaborada inicialmente com o propósito de possibilitar diferentes modelos de negócio, daí a escolha deste sistema como base.

O OpenSDRM torna-se preponderante nesta proposta visto que é o sistema que, como referido, servirá de base para a arquitectura a propor no contexto de GDD aplicado às redes sociais e sobre o qual se pretende desenvolver esta nova proposta.

Este tópico pretende, após o estudo de toda a envolvente da GDD associada às PRS, definir a concepção e análise da solução de GDD pretendida. Estas irão incidir sobre os seguintes tópicos:

- ✓ Arquitectura conceptual da solução – apresentação da estrutura global da solução;
- ✓ Sistema OpenSDRM – como funciona o sistema que faz a gestão de conteúdo dentro da arquitectura genérica;
- ✓ Análise de requisitos da solução – definição dos requisitos que devem ser satisfeitos pela solução;
- ✓ Arquitectura da solução de gestão de direitos digitais – elaboração da arquitectura de gestão de conteúdos tendo em conta os requisitos da solução.

Todos estes tópicos apresentam-se como essenciais para que o desenvolvimento da solução proposta possa ser realizado com sucesso.

4.2. Arquitectura conceptual da solução proposta

Para uma melhor compreensão da forma como se pretende que a SGDDRS pretendida funcione e seja desenvolvida segue-se a seguinte arquitectura conceptual (Ilustração 21):

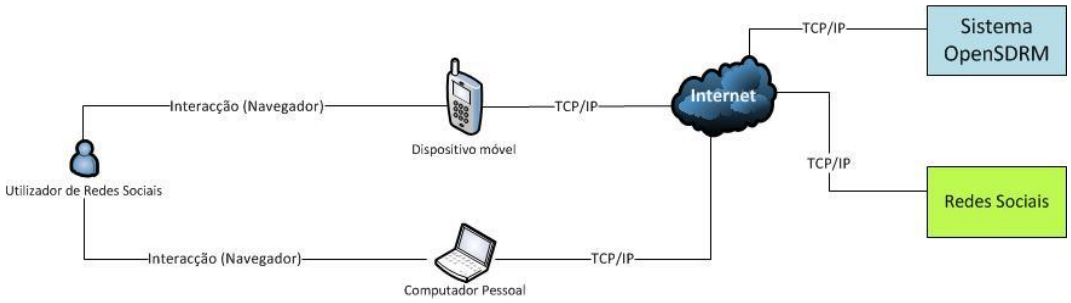


Ilustração 21 - Arquitectura conceptual da solução

Esta arquitectura apresenta as interacções e elementos que efectuam essas mesmas interacções pretendidas nesta proposta de solução. Os elementos principais são os utilizadores de redes sociais, os dispositivos de comunicação (dispositivo móvel e computador pessoal), o Sistema OpenSDRM e as Redes Sociais (*Facebook*, *Twitter*, entre outros).

Os utilizadores de redes sociais são os beneficiários directos do sistema proposto, isto é, são aqueles que, através do navegador, podem aceder ao OpenSDRM e proteger os seus conteúdos. Os dispositivos de comunicação são aqueles que permitem ao utilizador interagir com as PRS e com o sistema OpenSDRM para protecção dos seus conteúdos. Os ficheiros a carregar no OpenSDRM devem estar alojados localmente nestes dispositivos. As Redes Sociais são aquelas com o que o utilizador interage para que possa partilhar o seu conteúdo. Por outras palavras, é a plataforma que disponibiliza todos os elementos necessários para a actividade social *online*, actividade essa em que o utilizador poderá proteger o seu conteúdo. O sistema OpenSDRM é aquele que é responsável por toda a gestão de conteúdos a integrar nas PRS. Para além disso, é sobre este sistema que se pretende propor uma arquitectura de GDD a implementar.

Torna-se igualmente importante perceber como é que o utilizador interage dentro desta arquitectura e quais as actividades que pode realizar. Para clarificar este ponto segue-se um diagrama de actividades (Ilustração 22).

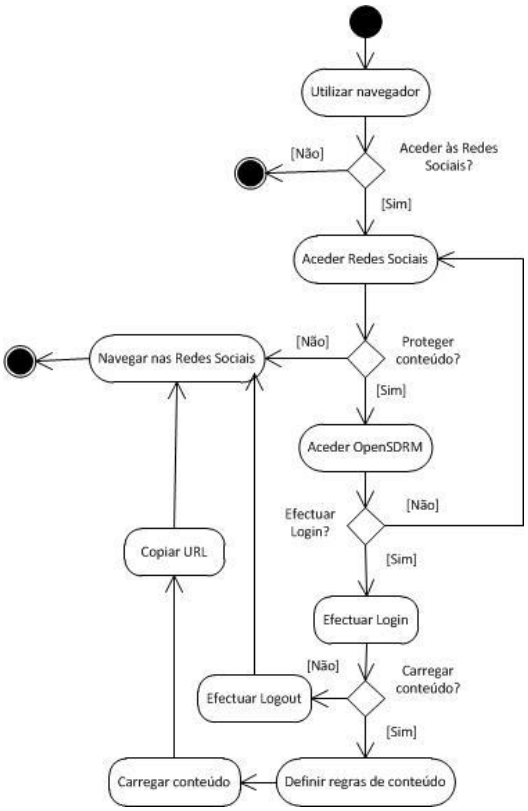


Ilustração 22 - Diagrama de actividades do utilizador na SGDDRS

O utilizador para que possa utilizar esta solução tem obrigatoriamente aceder a um navegador que lhe permita aceder tanto às PRS como, através de uma extensão, ao sistema OpenSDRM. Quando o utilizador acede a uma rede social e se pretender que o seu conteúdo seja protegido deve aceder ao sistema OpenSDRM. Já dentro do referido sistema, o utilizador deve carregar o conteúdo para que possa ser monitorizado e armazenado pelo sistema. O OpenSDRM deve devolver ao utilizador um URL que o utilizador deve colar na PRS em que está a navegar. Deste modo, pretende-se que o utilizador partilhe conteúdo mas que apenas este possa ser usado mediante as regras e condições definidas pelo utilizador. Em caso de incumprimento das condições de utilização, o acesso é negado pelo gestor de conteúdos OpenSDRM.

Como referido anteriormente, é sobre o sistema OpenSDRM que será feita uma proposta de arquitectura base para esta solução. Assim sendo, é importante perceber como funciona e quais os principais componentes deste sistema.

4.3. Sistema OpenSDRM

O sistema OpenSDRM (Open and Secure Digital object Rights Management) é um SGDD que lida com direitos digitais e não com ferramentas ou mecanismos de

protecção de cópia. Por outras palavras, o propósito deste sistema não é contribuir para a proibição da cópia mas sim permitir a monitorização de conteúdos áudio. Este sistema é independente de mecanismos de protecção de conteúdo (Torres, Serrão, Dias, & Delgado, 2008).

A plataforma OpenSDRM é composta por um conjunto de componentes distribuídos que comutam mensagens padrão sobre redes abertas (como a Internet). Este sistema apresenta uma arquitectura conceptual que define um cenário capaz de lidar com uma multiplicidade de diferentes modelos de negócio para distribuição de conteúdos.

A arquitectura conceptual que se segue (Ilustração 23) está dividida em três blocos: os papéis de utilizador (*the user roles*), as entidades externas ao sistema de gestão de conteúdos em si e as entidades internas do sistema que disponibilizam as funcionalidades de GDD (Torres, Serrão, Dias, & Delgado, 2008).

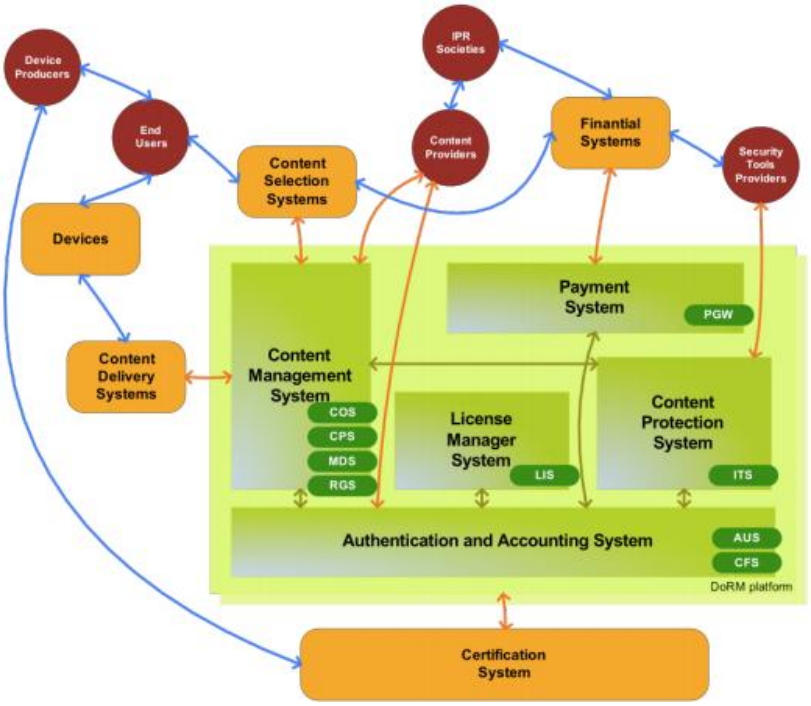


Ilustração 23 - Arquitectura conceptual do sistema OpenSDRM
(Torres, Serrão, Dias, & Delgado, 2008)

4.3.1. Papéis de utilizador

Estes são os papéis que são representados por diversas entidades na cadeia de valor. É importante não confundir estes papéis de utilizador com os papéis do utilizador-final. A *framework* do OpenSDRM identifica os seguintes papéis (Torres, Serrão, Dias, & Delgado, 2008):

- ✓ Sociedades gestoras de direitos de autor (*Author/Owner Societies*): estas sociedades são responsáveis pela defesa dos direitos de propriedade de conteúdo e, em alguns casos, garantir o pagamento de direitos;
- ✓ Fornecedores de conteúdo (*Content Providers*): representam os autores de um bem que foi criativamente produzido e distribuído de forma digital. Estes autores de conteúdo são também responsáveis por definir os termos e condições sobre as quais o conteúdo pode ou não ser usado;
- ✓ Produtores de dispositivos (*Device Producers*): estes representam os fabricantes de dispositivos (*hardware*, *software* ou ambos) que produzem dispositivos capazes de aplicar funções de gestão e protecção de conteúdo. Estes fabricantes de dispositivos podem ser certificados pela plataforma de GDD;
- ✓ Fornecedores de ferramentas de segurança (*Security Tools Providers*): estas entidades disponibilizam meios tecnológicos aos dispositivos de processamento para que possam adaptar as suas características de segurança para o tipo de tecnologia de protecção aplicada sobre o conteúdo;
- ✓ Utilizadores Finais (*End Users*): representam os utilizadores finais que pretendem seleccionar e fazer uso de um dado conteúdo.

4.3.2. Entidades externas

Estas entidades apoiam as funções que não se destinam à gestão de conteúdo nesta arquitectura. As entidades referidas são (Serrão, Dias, & Delgado, 2006):

- ✓ Infra-estrutura de pagamento (*Payment Infrastrusture*): entidade externa que é responsável por todas as transacções financeiras e por garantir que todos os intervenientes recebem a recompensa que lhes é devida;
- ✓ Módulos de selecção de conteúdo (*Content Selection Modules*): entidade ou módulo externo que pode ser usado para encontrar, procurar ou seleccionar conteúdo;
- ✓ Dispositivos (*Devices*): os dispositivos são mecanismos que permitem ao consumidor final reproduzir o conteúdo que obteve;
- ✓ Servidores de distribuição de conteúdo (*Content Delivery Server*): esta entidade representa os servidores que disponibilizam conteúdos aos utilizadores finais ou a dispositivos;

- ✓ Sistema de certificação (*Certification System*): esta é a entidade externa (muito embora possa ser interna) que lida com questões relativas às credenciais dos componentes de certificação.

4.3.3. Entidades do sistema

Estas entidades, que se encontram dentro da arquitectura conceptual, fornecem os elementos que permitem o funcionamento do sistema de GDD. Tanto no lado do servidor como no lado do cliente estes elementos disponibilizam as funcionalidades necessárias à protecção do conteúdo e suporte de direitos associados ao conteúdo e ao utilizador. Estas entidades são o sistema de gestão de conteúdo (*Content Management System*), o módulo de entrada de pagamento (*Payment Gateway Module*), o sistema de gestão de licenças (*License Management System*), o sistema de ferramentas de protecção de conteúdo (*Content Protection Tools System*) e o sistema de conta e autenticação (*Authentication and Accounting System*) (Serrão, Dias, & Delgado, 2006).

4.3.4. Descrição da arquitectura técnica

O OpenSDRM apresenta uma arquitectura distribuída. Todos os serviços que compõem a arquitectura comunicam entre si através do uso de um conjunto de interfaces bem conhecidos, estes encontram-se sobre a forma de WSDL (*Web Services Description Language*). Toda a infra-estrutura foi desenhada com o intuito de ser adaptada e aplicada a todos os tipos de conteúdos e modelos de negócio.

Na arquitectura conceptual é mostrada a complexidade da intercomunicação entre os diferentes elementos da plataforma (Serrão, Marques, Dias, & Delgado, 2006).

4.3.4.1. Componentes e interfaces externos

Apresentam-se agora os componentes e actores externos que interagem com o OpenSDRM, sendo eles o utilizador (*user*), o fornecedor de ferramentas IPMP (*IPMP Tools Provider*), o fornecedor de conteúdo (*Content Provider*), a infra-estrutura de pagamento (*Payment Infrastructure*) e a autoridade de certificação (*Certification Authority*) (Serrão, Marques, Dias, & Delgado, 2006).

- ✓ Utilizador: representa uma pessoa que deseje consumir um dado conteúdo. Este conteúdo pode ou não ser protegido. Muito embora, a forma de acesso e de exibição como conteúdo pode requerer o uso de dispositivos protegidos, *software* e licenças;

- ✓ Fornecedor de ferramentas protecção de conteúdo: representa uma qualquer organização que produza ferramentas e tecnologias de encriptação, *scrambling*, marca d'água e outras que possam servir como protecção para o conteúdo. Estas ferramentas necessitam de seguir algumas linhas orientadoras. Estas são traduzidas para uma relação de negócio que deve existir entre o fornecedor de conteúdo e o fornecedor de ferramentas protecção de contéudo, na maior parte das vezes, um produtor e/ou distribuidor de conteúdo quer escolher que tipo de protecção pretende e as ferramentas que podem ser aplicadas ao conteúdo que pretende oferecer;
- ✓ Fornecedor de conteúdo: refere-se a um qualquer criador de conteúdo multimédia que alimenta o OpenSDRM com o seu conteúdo e metadados opcionais;
- ✓ Infra-estrutura de pagamento: esta facilita a parte comercial do OpenSDRM disponibilizando serviços de fornecimento para pagamentos electrónicos. O interface entre o OpenSDRM e a infra-estrutura de pagamento é genérico e independente do método de pagamento, permitindo uma multiplicidade de sistemas de pagamento;
- ✓ Autoridade de certificação: é a autoridade responsável por receber pedidos de credenciais para as entidades. Estas credenciais são usadas por essas entidades se autenticarem a si mesmas e a outras, permitindo o estabelecimento de canais de comunicação seguros e autenticados entre as entidades (Serrão, Marques, Dias, & Delgado, 2006).

4.3.4.2. Componentes e interfaces internos

Seguem-se os componentes internos da plataforma OpenSDRM responsáveis por toda a gestão relativa a conteúdos dentro do sistema. Entre estes estão (Serrão, Fonseca, & Dias, 2006):

- ✓ Servidor de preparação de conteúdo (*CPS – Content Preparation Server*): é o servidor é responsável por toda a preparação do conteúdo. Este recebe o conteúdo no seu estado puro de uma dada fonte ou fontes e codifica-o para um formato específico, adiciona metadados e protege-o. O conteúdo recebido é codificado no formato MPEG-4, de acordo com um modelo pré-estabelecido. Este modelo permite a criação de ficheiros MPEG-4 que contêm músicas no

formato MP3 ou ACC em conjunto com algumas imagens sobre o álbum do artista;

- ✓ Portal de pagamento (*PGW - Payment Gateway*): é um servidor responsável por verificar e validar os métodos de pagamento fornecidos pelo utilizador vindos do servidor comercial;
- ✓ Servidor Comercial (*COS – Comercial Server*): é o servidor que fica responsável pela negociação do conteúdo com os utilizadores. O conteúdo é escolhido pelo utilizador através do navegador, podendo ser consultados alguns metadados genéricos, informação sobre o preço e as condições de utilização que tem de ser claramente aceites e estabelecidas por ambas as partes. Esta última apresenta-se como uma das especificidades mais relevantes relativas ao conteúdo.
- ✓ Servidor de distribuição multimédia (*MDS – Media Delivery Server*): é o servidor responsável pelas trocas de partes do conteúdo com o cliente do sistema. Este servidor implementa um protocolo específico (*download*: FTP, HTTP ou outro; *streaming*: RTSP ou outro) para efectuar trocas de conteúdo protegido com a aplicação de multimédia (*Media Application*).
- ✓ Servidor de Registo (*RGS - Registation Server*): é o componente do tipo servidor cujo papel é o de atribuir identificadores únicos e registar metadados relativos a um conteúdo específico inserido no OpenSDRM. Esta arquitectura foi desenhada tendo em conta, o mais possível, dos padrões ISO e portanto, utiliza os referidos identificadores únicos. O OpenSDRM segue as directivas MPEG-21 sobre identificação de itens digitais (*DII – Digital Item Identification*), usando uma versão reduzida do MPEG-21 sobre identificação de itens digitais e identificadores de objectos digitais - *MPEG-21 DII Digital Object Identifiers (DOI)*.
- ✓ Servidor de licenças (*LIS – License Server*): é um servidor responsável pela manutenção de regras associadas a um utilizador, a um conteúdo e ao correspondente direito de acesso. Este componente aceita as conexões de um cliente reprodutor de multimédia autenticado que se destinam ao *download* de licenças, licenças que são aplicadas a conteúdo protegido através de uma ferramenta IPMP apropriada. As licenças apresentam-se em formato XML usando o *Open Digital Right Language* (*ODRL/ OMA profile*) ou a linguagem de expressão de direitos (*REL – Rights Expression Language*), desenvolvida pela MPEG-21.

- ✓ Servidor de ferramentas de protecção de conteúdos (*ITS – IPMP tools server*): é o servidor responsável pelo registo de novas ferramentas de protecção de conteúdos e por receber pedidos do *software* de aplicação multimédia (*Media Application*) de um cliente autenticado que pretenda efectuar *download* de uma ferramenta de protecção de conteúdos específica. É igualmente responsável por disponibilizar ferramentas de protecção de conteúdos ao servidor de preparação de conteúdo (CPS) para permitir a protecção de conteúdo.
- ✓ Aplicação de multimédia (*MPL – Media Application*): este componente representa o *software* que é utilizado para ceder o conteúdo. Este é um componente genérico com a particularidade de ser capaz de exibir/reproduzir o conteúdo para que os *codecs* de áudio/vídeo necessários possam ser disponibilizados (se estes *codecs* não estiverem disponíveis pode ser realizado o *download* do mesmo de um servidor remoto seguro). Esta aplicação multimédia pode trabalhar com uma ou mais ferramentas de protecção de conteúdos com o intuito de controlar a forma como um dado utilizador acede a um conteúdo. Este componente trabalha no lado do cliente dentro da arquitectura genérica. Contudo, este realiza alguns papéis importantes nas funções de GDD (Serrão, Fonseca, & Dias, 2006).

4.4. Análise de requisitos da solução proposta

Para melhor compreender quais as características desejáveis para a SGDD a desenvolver seguem-se um conjunto de requisitos que devem ser tidos em conta aquando do desenvolvimento da solução.

4.4.1. Stakeholders

Existem dois *stakeholders* relevantes para esta nova solução de gestão de direitos digitais aplicados ao sistema OpenSDRM, sendo estes o utilizador de redes sociais e o gestor do sistema de gestão de conteúdo digital. O utilizador de redes sociais é, como o próprio nome indica o utilizador de PRS que faz uso do sistema e é o principal beneficiário do sistema visto que os conteúdos a ser protegidos pelo sistema são os deste tipo de utilizador. O gestor do sistema é o elemento responsável por realizar tarefas de monitorização e de controlo do sistema. Este gestor funciona igualmente como moderador do sistema de forma a prevenir violações de direitos e excessos por parte dos utilizadores.

Segue-se um diagrama (Ilustração 24) de *use-case* que clarifica as acções destes *stakeholders* no SGDDRS:

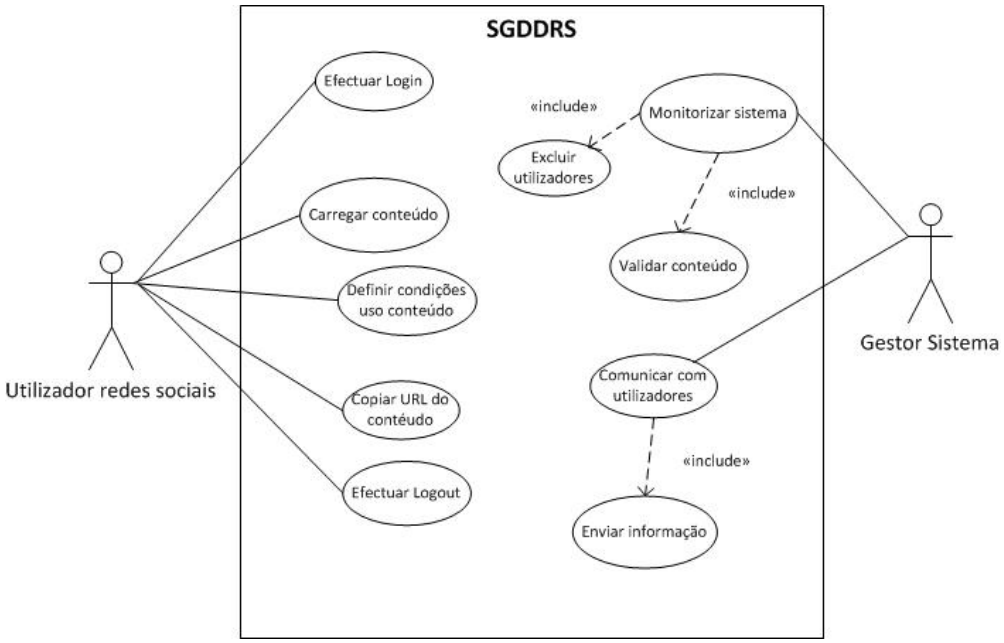


Ilustração 24 - Diagrama de Use-Case do SGDDRS

4.4.2. Categorias de requisitos

Os requisitos de produto são tipicamente classificados em duas categorias: requisitos funcionais (RF) e não-funcionais (RNF). Os requisitos funcionais são serviços que devem ser fornecidos pela solução. Indicam como o sistema deve reagir a um *input* particular e como o sistema se deve comportar numa situação em particular. Os requisitos não-funcionais são condições de serviço ou funcionalidades oferecidas pelo sistema Estes incluem condições temporais, condições de desenvolvimento, processo e de padrão. Em grande parte das situações, este tipo de requisitos são aplicados ao sistema como um todo (Sommerville, 2007).

4.4.3. Tabela de requisitos da solução

Na tabela que se segue (Tabela 2) são listados os requisitos a ter em conta a quando do desenvolvimento da solução. Os requisitos incluem categoria (funcional ou não-funcional), identificador e descrição.

Todos estes requisitos têm de ser cumpridos para que o sistema possa funcionar correctamente e dentro do que se pretende para a solução. Em anexo (Anexo A) encontra-se a tabela completa relativa igualmente a estes requisitos.

Categoria	Requisitos	
	ID	**Descrição**
RF	1	Para aceder ao sistema é necessário acesso à Internet.
RF	2	O utilizador deve aceder ao sistema através de uma extensão de um navegador *web*.
RF	3	O sistema deve estar acessível tanto a computadores pessoais como a dispositivos móveis.
RF	4	O sistema deve permitir o *login* e *logout* do utilizador.
RF	5	O sistema deve permitir o registo e criação de conta de utilizador na plataforma.
RF	6	O sistema deve permitir ao utilizador o carregamento de conteúdos na plataforma.
RF	7	O sistema deve criar um URL do conteúdo que possa ser copiado pelo utilizador
RF	8	O sistema deve permitir ao utilizador a definição das condições de utilização do conteúdo.
RF	9	O sistema deve permitir ao gestor do sistema banir utilizadores que tenham uma conduta imprópria.
RF	10	O sistema deve permitir o envio de notificações ao utilizador.
RF	11	O gestor do sistema deve ter credenciais únicas e que o distinga dos demais para que este possa monitorizar o sistema.
RF	12	A remoção da conta de um utilizador por vontade própria deve ser permitida pelo sistema.
RNF	13	Para que o utilizador possa usar a plataforma deve ser utilizador de redes sociais.

Tabela 2 - Tabela de requisitos da SGDDRS

4.5. Arquitectura da solução proposta integrada no OpenSDRM

Como já foi referido anteriormente, pretende-se que a solução proposta possa resolver o problema da privacidade associada à GDD, decorrente do uso da PRS, seja integrada com o sistema já existente, o OpenSDRM. Este sistema apresenta, já por si, uma arquitectura muito interessante, sobre a qual é feita a proposta de arquitectura a desenvolver que se segue.

Posto isto, e tendo em conta toda a análise efectuada ao longo de todo este projecto, apresenta-se a seguinte proposta de arquitectura (Ilustração 25) para a solução de GDD enquadrada com a temática das PRS a desenvolver:

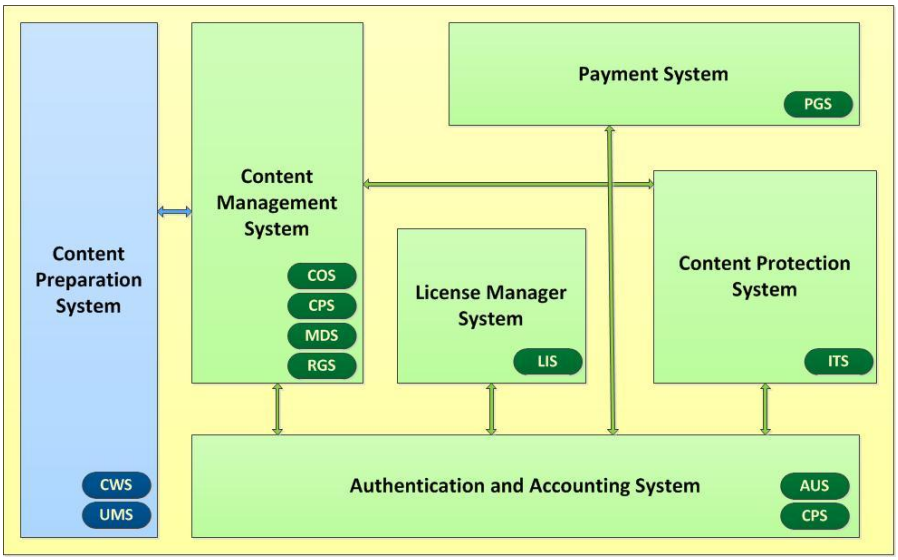


Ilustração 25 - Arquitectura proposta para o SGDDRS

Nesta arquitectura, os sistemas internos (*Content Management System, Payment System, License Manager System, Content Protection System* e *Authentication and Accouting System*) são aqueles que já fazem parte do sistema OpenSDRM. O *Content Preparation System* é o sistema proposto para que todo este em conjunto de sistemas possa efectuar a monitorização de conteúdos nas PRS.

O sistema interno aqui proposto dá pelo nome de sistema de preparação de conteúdo (*Content Preparation System*). Este sistema tem como principal função a preparação do conteúdo, que se pretende controlar, tanto para acção interna como para acção externa. Por outras palavras, compõe o conteúdo para que este possa ser monitorizado dentro do sistema e para que seja possível a integração do referido conteúdo nas PRS que se encontram fora do sistema.

Como é igualmente visível na arquitectura proposta existem dois servidores *Web* que se entendem como necessários para que a preparação do conteúdo possa ser realizada: o servidor de acondicionamento de conteúdo e o servidor de monitorização de URL.

- ✓ Servidor de acondicionamento de conteúdo (*CWS - Content Wrapper Server*): É o servidor responsável pela preparação e integração do conteúdo que é carregado pelo utilizador no sistema. Este recebe o conteúdo e atribui-lhe um formato interno ao sistema para que possa ser gerido internamente independentemente do formato exterior que apresente. Com esta funcionalidade tornasse possível gerir qualquer conteúdo no sistema sem que exista a preocupação de qual o formato do conteúdo, seja ele JPEG, MP3, ou outro.
- ✓ Servidor de monitorização de URL (*UMS – URL Monitoring Server*): Este servidor existe com o intuito de preparar o conteúdo que foi carregado no sistema para que este possa ser inserido nas redes sociais através de um URL. O servidor de monitorização de URL processa o conteúdo da seguinte forma: recebe o conteúdo no formato interno ao sistema, cria um URL para que este conteúdo possa ser exibido na PRS e atribui ao conteúdo o formato inicial para que seja possível a sua reprodução.

Com a adição destas alterações ao sistema OpenSDRM poderemos considerar que o SGDDRS está preparado para dar o seu contributo para aumento da privacidade dos utilizadores de PRS.

De seguida é descrita a arquitectura tendo em conta a comunicação entre os diferentes componentes do sistema, tendo sido excluído o sistema de preparação de conteúdo (*Content Preparation System*).

A arquitectura proposta (Ilustração 26), como já foi referido, é baseada numa plataforma genérica de gestão de direitos digitais que dá pelo nome de OpenSDRM. O *Open and Secure Digital Rights Management system* (OpenSDRM) é uma arquitectura (Torres, Serrão, Dias, & Delgado, 2008) adaptável à GDD. Esta arquitectura pode ser configurada para uma utilização que implique diversos modelos de negócios e diferentes tipos de conteúdo. OpenSDRM implementa uma solução de GDD comum que permite a protecção dos direitos de conteúdo e que pode ser aplicada na divulgação e comercialização de conteúdo digital multimédia (Francisco, Marques, & Serrão, 2012).

A arquitectura do *OpenSDRM* é baseada em extensões do MPEG-4 IPMP. São também utilizados componentes de identificação de itens digitais (MPEG-21 DII - *Digital Item Identification*). Esta solução de GDD é constituída por vários elementos opcionais que cobrem todas as fases da cadeia de valor de distribuição, desde a produção do conteúdo até ao uso desse conteúdo. Esta abrange vários aspectos importantes da distribuição de conteúdo e sua comercialização como a produção de conteúdo, a preparação de conteúdo e registo, a distribuição de conteúdo interactivo, a negociação de conteúdo e aquisição, a autenticação de utilizador e a visualização condicional/reprodução. Esta infra-estrutura foi projectada para ser adaptável e aplicável a todos os tipos de modelos de conteúdo e de negócios (tanto para *download*, *streaming* ou mesmo a *broadcasting*).

É importante referir a capacidade de modularidade presente no *OpenSDRM* e a abertura que este sistema tem de ser facilmente adaptável a outros cenários. Esta modularidade do *OpenSDRM* só é possível através de um conjunto de componentes independentes que são implementadas através de uma abordagem orientada a serviços (Francisco, Marques, & Serrão, 2012).

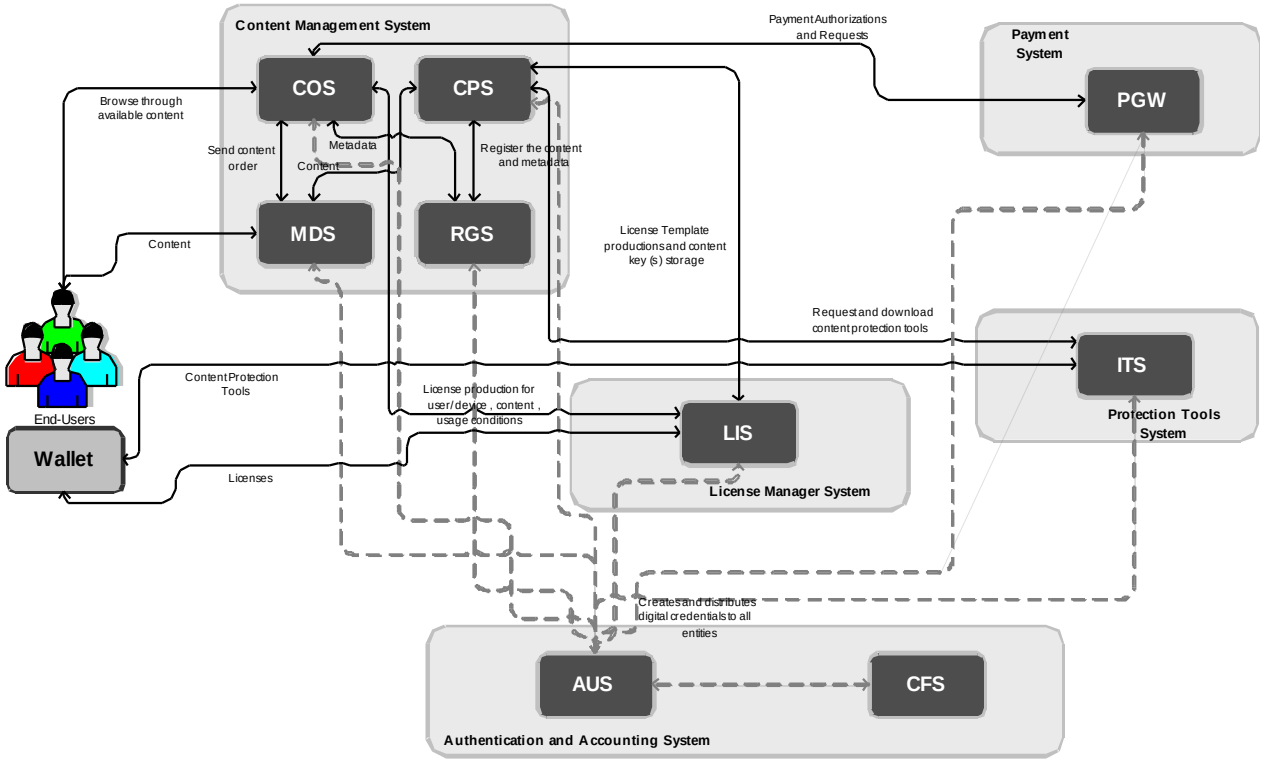


Ilustração 26 - A framework OpenSDRM

(Francisco, Marques, & Serrão, 2012)

Alguns dos componentes referidos *OpenSDRM* apresentam uma maior importância. Além disso, no lado do cliente (*client-side*) é implementada uma extensão de um navegador específico que permite que um qualquer utilizador de redes sociais possa registar-se na plataforma OpenSDRM, fazer *upload* de um conteúdo para a plataforma que o quer compartilhar *online*, definir as regras de controlo de acesso para todos os outros utilizadores registados para que possam aceder ao conteúdo publicado, e monitorizar o acesso ao referido conteúdo.

É importante ainda referir algumas notas e pressupostos: todos os componentes da plataforma são confiáveis, não foram modificados e comportam-se exactamente como o esperado; todas as mensagens componentes de câmbio através de um canal seguro e autenticado. Cada componente tem seu próprio par de chaves que é usado para estabelecer uma ligação: $K_{pub}^{Component}$, $K_{priv}^{Component}$; e todos os componentes que compõem a *framework* (ou um subconjunto da *framework*, de acordo com o cenário implementado) estão registados na AUS e tem uma credencial AUS válida: $Cert^{AUS}_{Component}$. Seguem-se os vários passos seguidos por esta arquitectura no registo do utilizador, na partilha de conteúdo, na definição de regras de partilha e no acesso ao conteúdo (Francisco, Marques, & Serrão, 2012).

4.5.1. Registo do utilizador

O registo de utilizador segue o seguinte protocolo (Francisco, Marques, & Serrão, 2012):

- O "Wallet" cria um par de chaves para o utilizador: K_{pub}^{U}, K_{priv}^{U};
- O utilizador gera uma *passphrase* para o "Wallet". Sobre esta *passphrase* é aplicado um hash, resultando numa chave que será posteriormente utilizada para criar um repositório seguro (base de dados): $K_{SecureStorage}$ = SHA1 (*passphrase*). A K_{priv}^{U} é armazenada de forma segura. O *passphrase* não é armazenado e apenas o utilizador o conhece;
- O "Wallet" requere alguma informação adicional do utilizador final, confirma o endereço de correio electrónico do utilizador e envia toda a informação ao componente AUS: $K_{pub}^{AUS}\{U_{ID}$, informação do utilizador + $K_{pub}^{U}\}$;
- O AUS confirma o registo do utilizador e todas as questões relacionadas com as credenciais do utilizador: $Cert^{AUS}_{U}$. Estas credenciais são usadas para autenticar o utilizador de outros serviços dentro da *framework* do *OpenSDRM*.

4.5.2. Partilha de conteúdo na plataforma

A partilha de conteúdo segue o seguinte protocolo (Francisco, Marques, & Serrão, 2012):

- O utilizador selecciona a extensão do navegador. Se o utilizador ainda não tiver sessão iniciada, ou se a sessão expirou, este tem de entrar através de *login* usando a sua *passphrase* secreta;
- O sistema valida o utilizador através do componente AUS do *OpenSDRM*. Se o utilizador tiver as credenciais que lhe permitem o acesso e se este estiver autenticado no sistema, o utilizador pode iniciar a sessão;
- Os conteúdos são carregados pelo utilizador (*Content*) para o *OpenSDRM* através do MDS (*Media Delivery Service*). Para além disso, o utilizador também preenche alguma informação relativa aos dados (*Metadata*) que descreve o conteúdo carregado;
- O *Content* é carregado para o CPS (*Content Preparation Service*). O CPS é responsável por preparar o conteúdo para que este possa ser partilhado nas plataformas sociais. Isto pode incluir o *re-packaging*, *scrambling* e protecção. Dependendo do método de protecção usado, o conteúdo pode ser protegido de várias formas. Para simplificar vamos assumir que o conteúdo é encriptado;
- Dependendo do mecanismo de protecção usado, o CPS pode necessitar de obter as ferramentas de protecção apropriadas, caso ainda não as tenha. Para que isto possa acontecer o CPS comunica com o ITS (*Protection Tools Service*) e faz *download* das ferramentas apropriadas;
- O CPS contacta o RGS (*Registration Service*) e regista o conteúdo e os seus metadados. O RGS assina com um identificador de registo único (C_{ID}) o conteúdo e devolve o mesmo ao CPS, assinando: $K_{pub}{}^{CPS}\{K_{priv}{}^{RGS}[C_{ID}]\}$;
- O CPS cria uma chave de conteúdo (C^{EK}) que é usada para cifrar o conteúdo carregado pelo utilizador. Este C^{EK} é enviado para o LIS (*License Service*) sendo anexado a este o identificador de conteúdo: $K_{pub}{}^{LIS}\{K_{priv}{}^{CPS}[C^{EK}, K_{priv}{}^{RGS}[C_{ID}]]\}$;
- O CPS protege o conteúdo do utilizador cifrando-o usando a ferramenta de protecção seleccionada e o CEK: $C^{EK}\{Content\}$. O resultado é devolvido ao MDS em conjunto com um identificador único do conteúdo: $K_{pub}{}^{MDS}\{K_{priv}{}^{CPS}[K_{priv}{}^{RGS}[C_{ID}]]\}$, $K_{priv}{}^{CPS}[C^{EK}\{Content\}]$. O MDS guarda o conteúdo protegido;

- Depois o MDS cria um URL especial que contêm o identificador de conteúdo único e após isto devolve-o ao utilizador final. Este URL é um *shortcut* global que permite o acesso ao conteúdo localizado na plataforma *OpenSDRM*.

4.5.3. Definição de regras de partilha

A definição de regras de partilha segue o seguinte protocolo (Francisco, Marques, & Serrão, 2012):

- O CPS contacta o LIS e requere uma lista de *templates* de licenças disponíveis. Um *template* de licença é um documento XML (de formato específico) que tem no seu interior a definição de uma expressão específica de direitos. O *template* contém campos que podem ser adaptados para situações particulares de expressão de direitos;
- Os *templates* de licença são apresentados ao utilizador final pelo MDS e o utilizador pode seleccionar aquele que entende como o mais apropriado para o seu caso em particular. Se o utilizador entender que o *template* não é suficiente, então o sistema oferece a oportunidade ao utilizador de definir o seu próprio *template*;
- Um *template* típico apresenta a seguinte estrutura:
    - ID do utilizador (U_{ID}), ID de múltiplos utilizadores ($U_{ID}^{1}..U_{ID}^{n}$), ID de grupo (G_{ID}): estes campos representam identificadores únicos de uma pessoa ou utilizador com quem o conteúdo será partilhado. Neste caso, o conteúdo pode ser partilhado com um utilizador único, com vários utilizadores ou com um grupo que é definido previamente pelo utilizador;
    - Identificador único de conteúdo - *Content unique identifier* (C_{ID}): este é o identificador único obtido nos passos anteriores do RGS;
    - Número de visualizações ($Condition^{1}..Condition^{n}$): este é um componente da licença que, caso exista, irá limitar o número de visualizações do conteúdo pelo utilizador ou por um grupo de utilizadores;
    - Data de validade (*Validity*): se existente, este elemento irá definir o período de tempo durante o qual a licença é valida;
    - Chaves de encriptação de conteúdo ($C_{EK}^{1}..C_{EK}^{n}$): este elemento é a chave de encriptação do conteúdo que é usado para proteger o mesmo. A chave

de encriptação é protegida por uma chave-pública do utilizador: ($K_{pub}^{U}\{C_{EK}^{1}..C_{EK}^{n}\}$);

- Assinatura de licença - *License signature*: os conteúdos da licença são assinados pelo LIS: *License* = $K_{priv}^{LIS}[U_{ID}|U_{ID}^{1}..U_{ID}^{n}|G_{ID}$, C_{ID}, $Condition^{1}..Condition^{n}$, *Validity*, $C_{EK}^{1}..C_{EK}^{n}$, $K_{pub}^{U}\{C_{EK}^{1}..C_{EK}^{n}\}]$.

- Os utilizadores criam licenças com os parâmetros apropriados e esta licença é guardada no LIS.

4.5.4. Acesso ao conteúdo

O acesso ao conteúdo segue o seguinte protocolo (Francisco, Marques, & Serrão, 2012):

- O utilizador autentifica-se no sistema através da extensão do navegador;
- Enquanto selecciona o URL, a extensão do navegador verifica se o utilizador tem alguma licença para o conteúdo identificado (C_{ID}) representado pelo URL. Se uma licença existir o sistema faz o seguinte:
  - A extensão verifica a licença de conteúdos, valida a assinatura da licença (fazendo uso do K_{pub}^{LIS}), e verifica o C_{ID};
  - Se o C_{ID} é o certo, a validade (*Validity*) é verificado e as condições ($Condition^{1}..Condition^{n}$) analisadas;
  - Se as condições forem conhecidas, o conteúdo é desencriptado. O CEK é recuperado da licença ($K_{priv}^{U}\{ K_{pub}^{U}\{C_{EK}^{1}..C_{EK}^{n}\}\}= C_{EK}^{1}..C_{EK}^{n}$) e usado para libertar o conteúdo ($C^{EK}\{Content\}$);
  - O conteúdo é então disponibilizado para divulgação nas redes sociais. O conteúdo é cedido enquanto as condições de licenciamento forem cumpridas.
- Se o navegador do utilizador ainda não tiver uma licença válida para o C_{ID} que está a tentar visualizar, são realizados os seguintes passos:
  - O MDS contacta o LIS, passa o U_{ID}, as respectivas credenciais AUS ($Cert^{AUS}{}_{U}$) e o C_{ID}: $K_{pub}LIS\{K_{priv}^{MDS}[U_{ID}, Cert^{AUS}{}_{U}, C_{ID}]\}$;
  - O LIS recebe e valida a informação enviada pelo MDS. Usando o U_{ID} e o C_{ID} o LIS verifica a existencia de uma Licença e devolve a licença ao utilizador através do MDS e da extensão do navegador;
  - A licença é guardada de forma segura pela extensão: $K_{SecureStorage}\{License\}$;

- A extensão verifica a licença de conteúdos, validando a assinatura digital da licença (usando o K_{pub}^{LIS}), e verificando o C_{ID};
- Se o C_{ID} for o correcto, o *Validity* é verificado e as suas condições (*Condition*^{1}..*Condition*^{n}) analisadas;
- Se as condições forem conhecidas, o conteúdo é desencriptado. O CEK é recuperado a partir da licença ($K_{priv}^{U}\{ K_{pub}^{U}\{C_{EK}^{1}..C_{EK}^{n}\}\}= C_{EK}^{1}..C_{EK}^{n}$) e utilizador para desencriptar o conteúdo ($C^{EK}\{Content\}$);
- O conteúdo é então exposto na página da rede social. O conteúdo é disponibilizado apenas durante o período em que as condições o permitem.

4.6. Protótipo

No desenrolar de todo o processo de investigação foi criado um protótipo de um sistema de gestão de direitos digitais centrado no utilizador para protecção de conteúdos partilhados nas redes sociais.

Neste protótipo foram desenvolvidas algumas das funcionalidades pretendidas para um sistema deste tipo, e que cumprem com os objectivos que haviam sido propostos.

O desenvolvimento de um protótipo neste contexto teve os seguintes propósitos: em primeiro lugar o de tornar real a possibilidade dos utilizadores de redes sociais de experimentar um sistema que demonstrasse algumas funcionalidades de protecção de conteúdos partilhados nas redes sociais; e em segundo lugar, para que fosse possível uma avaliação real do trabalho desenvolvido no âmbito deste projecto, nomeadamente, através de questionários de validação, por parte dos utilizadores.

A implementação, como já foi referido, seguiu uma abordagem baseada em prototipagem que fez com que foi possível criar algumas das funcionalidades e onde fosse igualmente possível demonstrar as potencialidades de um sistema de gestão de direitos em conteúdos digitais aos utilizadores de redes sociais.

As funcionalidades presentes neste protótipo são as seguintes:

- Acesso ao sistema através de uma extensão do navegador *Google Chrome*;
- Registo do utilizador no sistema;
- Página de utilizadores com o perfil próprio;
- Definição de condições de acesso ao conteúdo:

  - Número de visualizações permitidas;
  - Utilizador registado com permissão de acesso ao conteúdo.
- Criação de um URL único por cada utilizador para partilha de conteúdos;
- Validação do acesso ao conteúdo do utilizador.

O protótipo desenvolvido é baseado nas linguagens PHP, HTML e SQL, tendo sido utilizado durante o seu desenvolvimento a ferramenta XAMPP (servidor independente e *open source*).

4.7. Exemplo de utilização

Para melhor compreender o funcionamento do protótipo vamos utilizar um exemplo de utilização.

O primeiro contacto que o utilizador tem com o protótipo é através da extensão do *Google Chrome* (Ilustração 27). Aqui o utilizador pode inserir o seu *Username* e a sua *Password* para aceder ao sistema ou então, caso ainda não esteja registado, proceder ao registo através do botão *Registar*.

Ilustração 27 - Extensão do Google Chrome de acesso ao SGRS

Se o utilizador preferir aceder directamente através do *site* do SGRS (http://sgrs.adetti.pt/index.php) também o pode fazer e ser-lhe à apresentada o seguinte ecrã (Ilustração 28):

Ilustração 28 - Página inicial de acesso SGRS

Neste ecrã estão presentes os botões de *Registar*, *Contactos* e *Quem somos*. Se o utilizador carregar no botão *Registar* aparece o seguinte ecrã (Ilustração 29) onde pode efectuar o seu registo preenchendo todos os campos.

Ilustração 29 - Página de Registo no SGRS

No caso de o utilizador já estar registado e após se ter acedido ao sistema surge o seguinte ecrã (Ilustração 30):

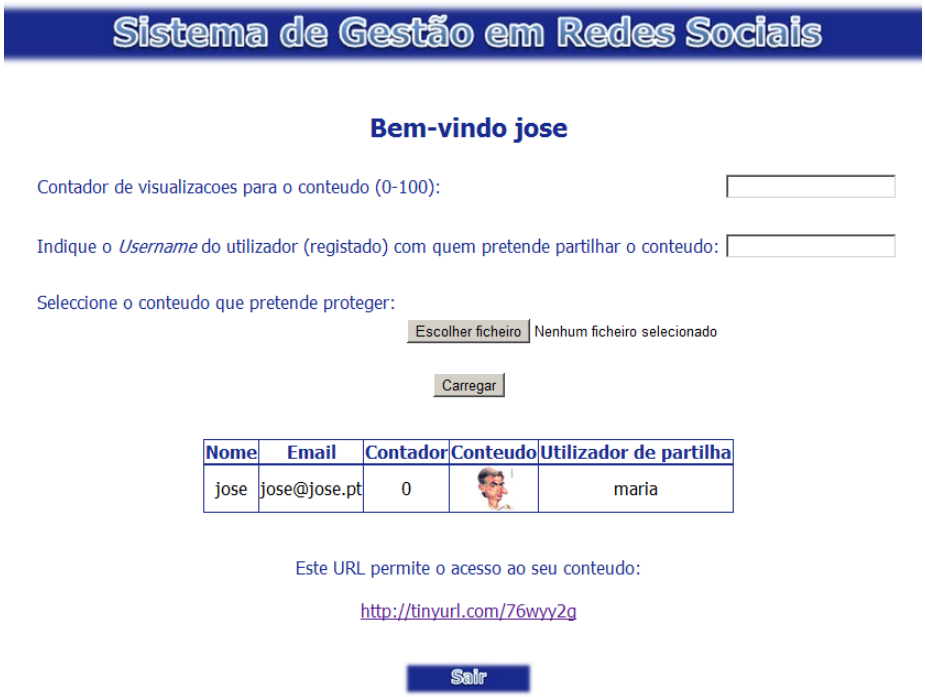


Ilustração 30 - Página de perfil do utilizador (Após o Login)

Nesta situação o utilizador registado é o *José*. Após efectuar o *Login* o *José* pode fazer uma de três coisas:

- Definir os parâmetros de partilha de conteúdo, isto é, pode atribuir um número de visualizações máximo para a imagem que pretende partilhar, indicar qual o utilizador registado com quem pretende partilhar o conteúdo e seleccionar a imagem que pretende partilhar;
- Visualizar os seus parâmetros actuais como o seu nome de registo, email, contador de visualizações actual, o conteúdo actual de partilha e o nome do utilizador com quem está a fazer a partilha (neste caso a *maria*);
- Copiar o URL gerado pelo sistema e partilha-lo nas redes sociais.

Se a *maria* pretender aceder ao conteúdo terá de seleccionar o URL que lhe foi fornecido pelo *José* e confirmar a sua *password* de registo no sistema de forma a poder visualizar o conteúdo (Ilustração 31).

Ilustração 31 - Página de acesso ao conteúdo (Confirmação de identidade)

No caso de um outro utilizador tentar aceder ao conteúdo e errar na introdução da *password* surgirá o ecrã que se segue (Ilustração 32).

Ilustração 32 - Página de aviso em casos de impossibilidade de acesso (Acesso negado)

No caso de ser de facto a *maria* a quer aceder ao conteúdo, este surgirá no ecrã. Caso seja a *maria* e o número de visualizações permitidas pelo *José* ter sido excedido, a *maria* irá depara-se com este ecrã (Ilustração 33).

Ilustração 33 - Página de notificação em casos de esgotamento do número de visualizações

No ecrã principal (Ilustração 28) existem também os botões *Contactos* (Ilustração 34) e *Quem somos* (Ilustração 35). No primeiro botão são apresentados ao utilizador os contactos de correio electrónico (fictícios). No segundo botão é feito um pequeno enquadramento de como surgiu o SGRS.

Ilustração 34 - Página de contactos (Contactos fictícios)

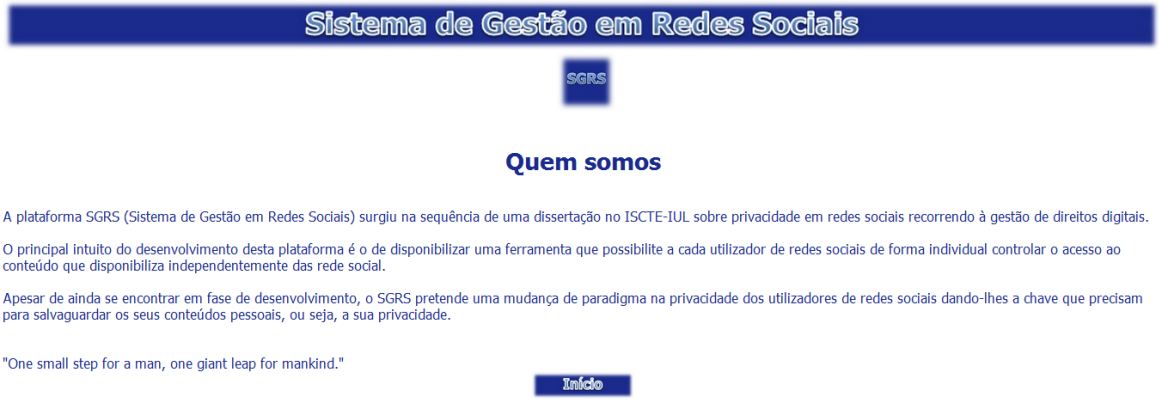


Ilustração 35 - Página "Quem somos"

5. Validação e Avaliação

5.1. Introdução

Para a validação e avaliação do protótipo da solução desenvolvido no âmbito deste projecto entendeu-se como necessária a elaboração de um questionário (ver Anexo B) a utilizadores de redes sociais. Este questionário permite avaliar qual a percepção dos utilizadores de redes sociais em relação às plataformas estudadas (*Facebook*, *Twitter*, *MySpace* e *Google Plus*) no âmbito deste projecto, qual o perfil de utilizador destas plataformas e se os referidos utilizadores estariam dispostos utilizar uma ferramenta que tivesse por base o protótipo desenvolvido. Com este questionário pretendeu-se chegar a um número considerável de utilizadores de redes sociais tentando, na sua divulgação, que a amostra fosse o mais aleatória possível.

Os questionários foram disponibilizados, *online* e foi fornecido a cada um dos inquiridos, um manual de utilização do protótipo (SGRS) e o respectivo questionário de resposta (ver Anexo B), para que estes pudessem fazer uso do protótipo de forma correcta e para que pudessem igualmente tirar proveito de todas as funcionalidades do mesmo.

5.1.1. Instrumento de validação e recolha de dados

Este questionário foi elaborado com o intuito principal de validar se o objectivo a que este projecto se tinha proposto teria sido atingido. O questionário foi construído tendo em conta uma divisão em dois tipos de questões: um primeiro grupo de questões que permitissem traçar o perfil do utilizador inquirido e um segundo onde fossem colocadas questões relativas à utilização do protótipo desenvolvido.

Este questionário é constituído por 35 questões dos seguintes tipos:

- Seis questões de “Sim”/”Não” e três questões de “Sim”/”Não”/”Talvez”;
- Quatro questões com diversas respostas assinaláveis;
- Quatro questões de escolha múltipla;
- Dezassete questões com resposta em escala de Likert (Likert, 1932) de 1 a 5;
- Uma questão de resposta aberta.

Como já foi referido, este questionário foi disponibilizado *online* tendo sido utilizada a tecnologia *Google Docs* para o efeito.

A recolha de dados foi efectuada entre os dias 26 de Julho de 2012 e o dia 16 de Agosto de 2012. O questionário foi divulgado através de canais *online* como o correio electrónico ou redes sociais e através da divulgação *word-of-mouth*, sendo toda a divulgação de caracter público.

5.2. Caracterização da amostra

A amostra é constituída por 43 utilizadores de redes sociais que se encontram distribuídos geograficamente pelo território nacional.

De seguida serão exibidas as questões que foram colocadas aos inquiridos e as respectivas respostas mediante duas categorias: características pessoais e utilização da solução (protótipo).

5.2.1. Características pessoais

As questões que se seguem foram colocadas aos inquiridos com o propósito de definir o perfil dos elementos da amostra.

Questão 1: *Qual o seu sexo?*

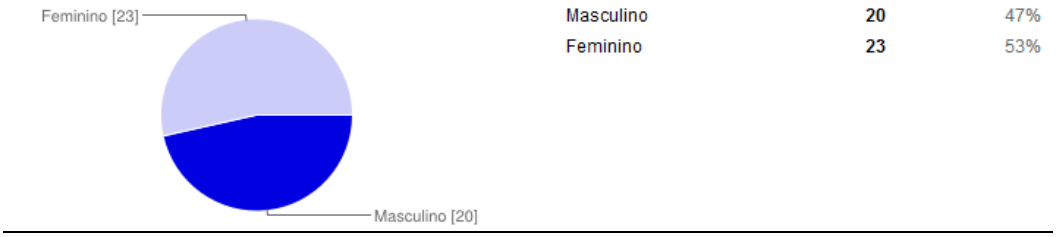


Ilustração 36 - Sexo dos inquiridos

De um total de 43 inquiridos, 47% destes são do sexo masculino sendo os restantes 53% do sexo feminino, o que equivale a 20 e 23 inquiridos, respectivamente.

Questão 2: *Qual a sua faixa etária?*

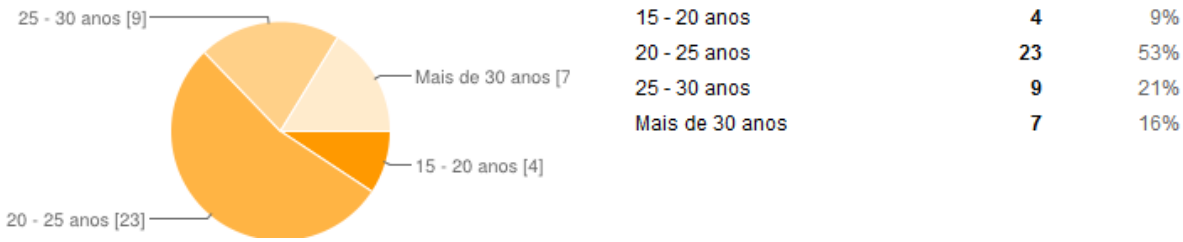


Ilustração 37 - Faixa etária dos inquiridos

Dos inquiridos, 53% encontra-se na faixa etária entre os 20 e os 25 anos, 21% entre os 25 e os 30 anos, 16% tem mais de 30 anos e 9% apresenta-se numa idade entre os 15 e os 20 anos.

Questão 3: *Qual o seu grau de escolaridade?*

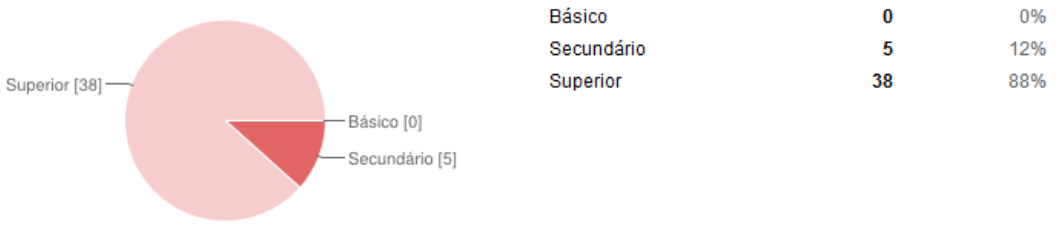


Ilustração 38 - Escolaridade dos inquiridos

Dentro dos inquiridos, 88% tem como grau de escolaridade o ensino superior. Dos restantes, apenas foram inquiridas pessoais com formação de ensino secundário o que corresponde a 12% do total de inquiridos.

Questão 4: *Com que frequência acede a redes sociais?*

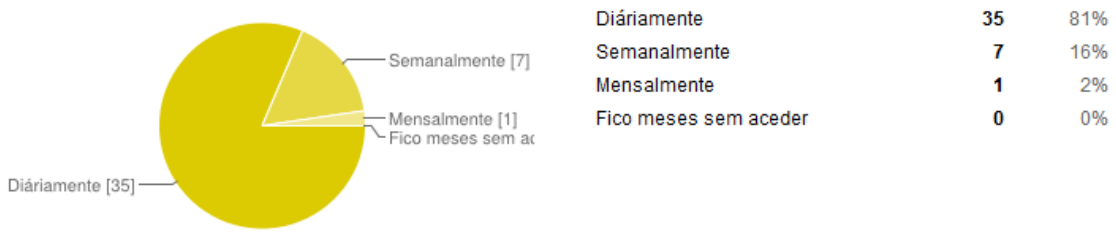
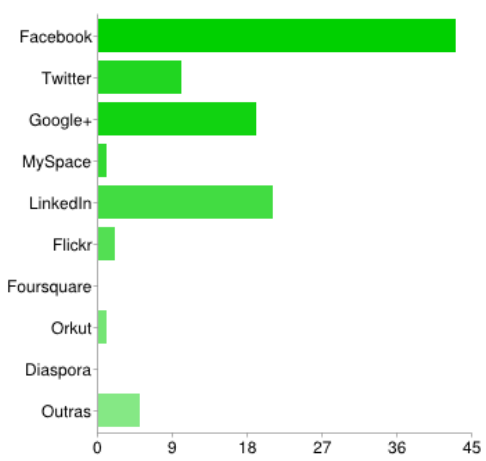


Ilustração 39 - Frequência de acesso a redes sociais por parte dos inquiridos

No total dos inquiridos, 81% acede diariamente a plataformas de redes sociais sendo esta percentagem correspondente a 35 do total de 43 inquiridos. Ainda de referir que 16% dos inquiridos acede semanalmente a redes sociais e que apenas 2% o faz mensalmente. Nenhum dos inquiridos fica mais de um mês sem aceder à sua rede social.

Questão 5: *Quais as redes sociais onde se encontra actualmente registado(a)?*



Facebook	43	100%
Twitter	10	23%
Google+	19	44%
MySpace	1	2%
LinkedIn	21	49%
Flickr	2	5%
Foursquare	0	0%
Orkut	1	2%
Diaspora	0	0%
Outras	5	12%

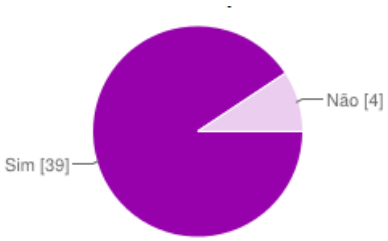
É possível seleccionar mais de uma caixa de verificação, pelo que as percentagens podem somar mais de 100%.

Ilustração 40 - Redes sociais em que os inquiridos se encontram registados

Quando questionados sobre quais as redes sociais em que se encontravam registados, 100% dos inquiridos afirmou que se encontrava registado na plataforma *Facebook*. Outra plataforma com grande adesão por parte desta amostra é o *LinkedIn* correspondendo a 49% do total de inquiridos. Muito próximo dos valores de adesão do *LinkedIn* encontra-se o *Google+* que apresenta uma adesão de 44% dos inquiridos.

As restantes plataformas de redes sociais sugeridas apresentam valores bastante mais baixos de adesão dentro desta amostra com excepção do *Twitter* que apresenta uma adesão de 23%, ainda esta significativamente mais elevada que o *Flickr* que tem uma adesão de 5% dos inquiridos. As plataformas *MySpace* e *Orkut* têm apenas 2% dos seus utilizadores dentro desta amostra. Um número não menos relevante é o da categoria "*Outras*" que se refere a outras plataformas sociais que não se encontram nesta lista e que representa 12% do total dos inquiridos.

Questão 6: *Tem por hábito inserir conteúdos pessoais nas redes sociais?*



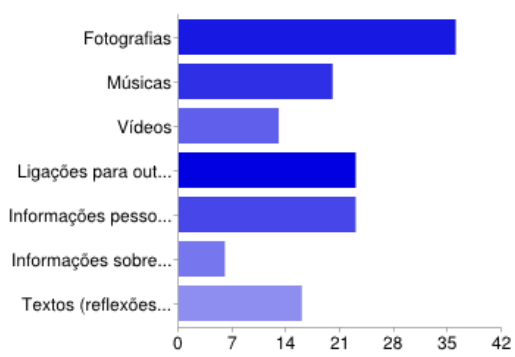
Sim	39	91%
Não	4	9%

Ilustração 41 - Inquiridos que inserem conteúdos nas redes sociais

Quando questionados se tem por hábito inserir conteúdos em plataformas de redes sociais, 91% dos inquiridos afirma que "*Sim*", correspondendo estes a 39 do total dos

inquiridos. Os restantes 9% dos inquiridos afirmam que não insere conteúdos nas redes sociais habitualmente.

Questão 7: *Se sim* (insere conteúdos nas redes sociais), *a que tipo de conteúdos se refere?*



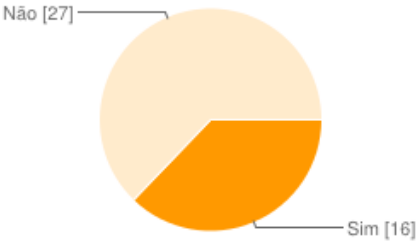
Fotografias	**36**	92%
Músicas	**20**	51%
Vídeos	**13**	33%
Ligações para outros sites	**23**	59%
Informações pessoais (localidade, data de nascimento,etc)	**23**	59%
Informações sobre localização	**6**	15%
Textos (reflexões, pensamentos,etc)	**16**	41%

É possível seleccionar mais de uma caixa de verificação, pelo que as percentagens podem somar mais de 100%.

Ilustração 42 - Tipos de conteúdos inseridos pelos inquiridos em redes sociais

Os conteúdos mais vezes inseridos pelos utilizadores de redes sociais que foram inquiridos são as "*Fotografias*" com 92%, "*Ligações para outros sites"* e "*Informações pessoais"* com 59% e "*Músicas*" com o valor de 51% de respostas. Com percentagens inferiores mas também relevantes encontram-se os "*Textos*" com 41%, "*Vídeos*" com 33% e "*Informações sobre localização*" com 15% de respostas.

Questão 8: *Protege os seus conteúdos antes de os colocar nas redes sociais?*



Sim	**16**	37%
Não	**27**	63%

Ilustração 43 - Percentagem de inquiridos que protegem os seus conteúdos

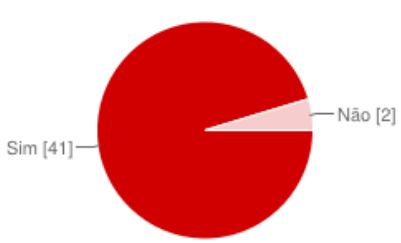
Dos inquiridos, 63%, correspondendo a 27 dos inquiridos, afirmam que não protegem os seus conteúdos antes dos inserir nas redes sociais, contrapondo com os restantes 37%, correspondendo a 16 dos inquiridos, que afirmam que protegem os seus conteúdos antes de os disponibilizarem *online*.

Questão 9: *Se sim, indique como protege os seus conteúdos.*

Esta questão era colocada como tendo resposta aberta. Os inquiridos, na sua essência, fizeram referência às configurações de protecção de conteúdos existentes em algumas

plataformas de redes sociais como forma de protecção de conteúdo que permitem uma restrição no acesso apenas para um número limitado de utilizadores.

Questão 10: *Considera-se uma pessoa preocupada com a sua privacidade?*

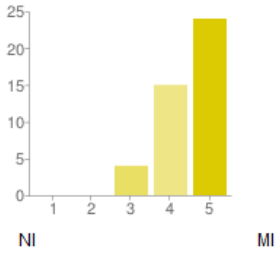


Sim	**41**	95%
Não	**2**	5%

Ilustração 44 - Percentagem de inquiridos que se preocupam com a sua privacidade

A esta questão 95% dos inquiridos afirmou-se como sendo uma pessoa preocupada com a sua privacidade, contrapondo com os restantes 5% de inquiridos que se afirmam como pessoas pouco preocupadas com a sua privacidade.

Questão 11: *Em geral, qual o grau de importância da privacidade nas redes sociais para si?*

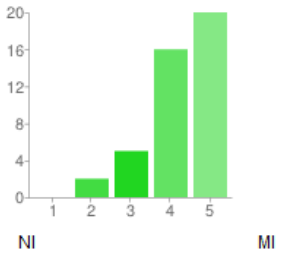


1 - Nada Importante	**0**	0%
2	**0**	0%
3	**4**	9%
4	**15**	35%
5 - Muito Importante	**24**	56%

Ilustração 45 - Grau de importância da privacidade nas redes sociais para os inquiridos

Numa escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade nas redes sociais, 56% dos inquiridos consideraram a sua privacidade de nível 5. Dos restantes, 35% considerou a importância no nível 4 e 9% no nível 3 desta escala.

Questão 12: *Tendo em conta a partilha de fotografias que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das fotografias?*

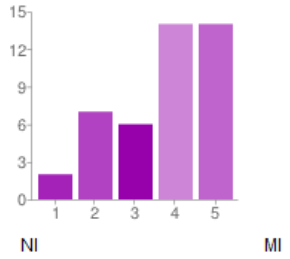


1 - Nada Importante	0	0%
2	2	5%
3	5	12%
4	16	37%
5 - Muito Importante	20	47%

Ilustração 46 - Grau de importância da privacidade das fotografias nas redes sociais para os inquiridos

Numa escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade das fotografias nas redes sociais, 47% dos inquiridos consideraram a privacidade das suas fotografias de nível 5 e 37% de nível 4. Em proporções mais pequenas temos os níveis 3 e 2 com 12% e 5%, respectivamente.

Questão 13: *Tendo em conta a partilha de vídeos que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade dos vídeos?*

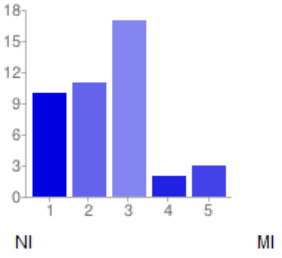


1 - Nada Importante	2	5%
2	7	16%
3	6	14%
4	14	33%
5 - Muito Importante	14	33%

Ilustração 47 - Grau de importância da privacidade dos vídeos nas redes sociais para os inquiridos

Numa escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade dos vídeos nas redes sociais, os níveis 4 e 5 apresentam 33% de resposta por parte dos inquiridos. Os restantes níveis apresentam-se distribuídos por percentagens mais pequenas tendo os níveis 2, 3 e 1 as percentagens 16%, 14% e 5%, respectivamente.

Questão 14: *Tendo em conta a partilha de músicas que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das músicas?*

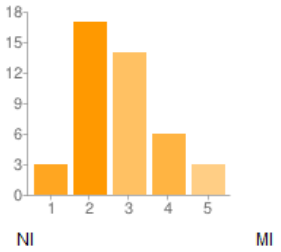


1 - Nada Importante	10	23%
2	11	26%
3	17	40%
4	2	5%
5 - Muito Importante	3	7%

Ilustração 48 - Grau de importância da privacidade das músicas nas redes sociais para os inquiridos

Nesta questão temos também uma escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade das músicas nas redes sociais, 40% dos inquiridos, que corresponde a 17 de um total de 43, optou pelo nível 3 para definir o seu grau de importância da privacidade no que diz respeito às músicas. Os níveis 2 e 1 apresentam valores de resposta de 26% e 23%, respectivamente, sendo que para os referidos 23% dos inquiridos da amostra não se torna relevante a privacidade neste contexto. Ainda de referir que o nível 4 obteve 5% de respostas e que 7% da amostra considerou a privacidade das músicas como sendo muito importante.

Questão 15: *Tendo em conta a partilha de ligações para outros sites que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das ligações para outros sites?*

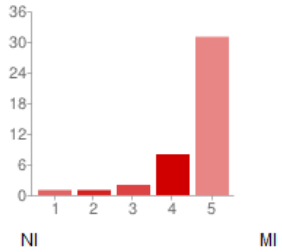


1 - Nada Importante	3	7%
2	17	40%
3	14	33%
4	6	14%
5 - Muito Importante	3	7%

Ilustração 49 - Grau de importância da privacidade das ligações para outros sites nas redes sociais para os inquiridos

Numa escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade das ligações para outros sites nas redes sociais, 40% dos elementos que constituem esta amostra definiram o nível 2 como grau de importância da privacidade de este tipo de conteúdo. Os níveis 3 e 4 de importância apresentam valores relevantes sendo estes 33% e 14% respectivamente. Os níveis de extremo como o 1 e o 5 apresentam uma adesão de resposta de 7% em ambos os casos.

Questão 16: *Tendo em conta a partilha de informações pessoais (localidade, data de nascimento, etc) que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das informações pessoais?*

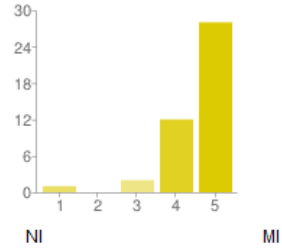


1 - Nada Importante	1	2%
2	1	2%
3	2	5%
4	8	19%
5 - Muito Importante	31	72%

Ilustração 50 - Grau de importância da privacidade das informações pessoais nas redes sociais para os inquiridos

Tendo em conta novamente uma escala de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), e sendo esta referente à importância da privacidade de informações pessoais nas redes sociais, a grande maioria dos inquiridos definiu o nível 5 como opção, 72%. O nível 4 foi a escolha de 19% dos inquiridos tendo os níveis 3, 2 e 1 apresentado valores significativamente mais baixos: 5%, 2% e 2%, respectivamente.

Questão 17: *Tendo em conta a partilha de informações de localização que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das informações de localização?*

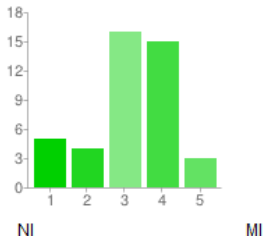


1 - Nada Importante	1	2%
2	0	0%
3	2	5%
4	12	28%
5 - Muito Importante	28	65%

Ilustração 51 - Grau de importância da privacidade das informações de localização nas redes sociais para os inquiridos

Quanto às informações de localização, tendo em conta novamente uma escala de importância de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), 65% dos elementos desta amostra considerou muito importante a privacidade das informações sobre a sua localização. O nível 4 obteve o valor de 28% das respostas e os níveis 3 e 1 as percentagens de 5% e 2%, respectivamente. Ainda de salientar que nenhum dos inquiridos definiu a sua importância como sendo de nível 2.

Questão 18: *Tendo em conta a partilha de textos (reflexões, pensamentos, etc) que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade de textos publicados?*

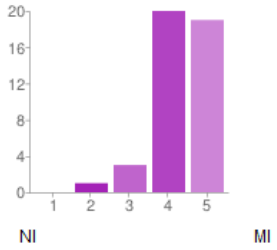


1 - Nada Importante	5	12%
2	4	9%
3	16	37%
4	15	35%
5 - Muito Importante	3	7%

Ilustração 52 - Grau de importância da privacidade de textos nas redes sociais para os inquiridos

No que diz respeito à partilha de textos nas redes sociais, tendo em conta uma escala de importância de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), 37% dos inquiridos considerou este tipo de conteúdo de nível 3 de importância de privacidade. O nível 4 também teve um número de respostas de interessante tendo chegado aos 35%. Os níveis 1, 2 e 5 apresentaram respostas com percentagens de 12%, 9% e 7%.

Questão 19: *Tendo em conta a plataforma Facebook, qual o grau de importância da privacidade nesta rede social para si?*

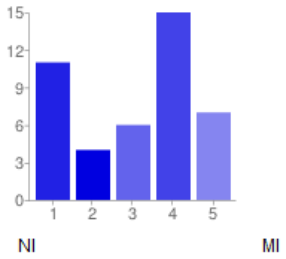


1 - Nada Importante	0	0%
2	1	2%
3	3	7%
4	20	47%
5 - Muito Importante	19	44%

Ilustração 53 - Grau de importância da privacidade no Facebook para os inquiridos

Focando-nos agora na avaliação que os inquiridos fazem sobre as redes sociais em estudo nesta dissertação começamos pelo *Facebook*. Utilizando uma escala de importância de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante") podemos verificar que para 47% dos inquiridos a privacidade é de nível 4 para esta rede social. Outros 44% dos inquiridos afirmaram como sendo muito importante a sua privacidade dentro desta plataforma social, nível 5. Nos restantes níveis os valores são consideravelmente mais baixos pertencendo as percentagens de 7%, 2% e 0% aos níveis 3, 2 e 1, respectivamente.

Questão 20: *Tendo em conta a plataforma Twitter, qual o grau de importância da privacidade nesta rede social para si?*

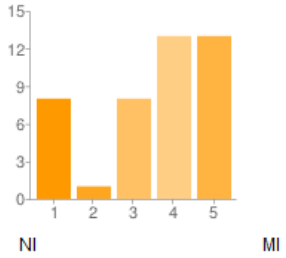


1 - Nada Importante	11	26%
2	4	9%
3	6	14%
4	15	35%
5 - Muito Importante	7	16%

Ilustração 54 - Grau de importância da privacidade no Twitter para os inquiridos

No que diz respeito à plataforma *Twitter*, tendo em conta uma escala de importância de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), 35% dos elementos da amostra considerou como resposta o nível 4 mostrando alguma preocupação com a privacidade nesta plataforma. Dos inquiridos 26% não considerou importante a privacidade desta rede social. Os restantes níveis, isto é, os níveis 5, 3 e 2, apresentam valores de 16%, 14% e 9%, respectivamente.

Questão 21: *Tendo em conta a plataforma Google+, qual o grau de importância da privacidade nesta rede social para si?*

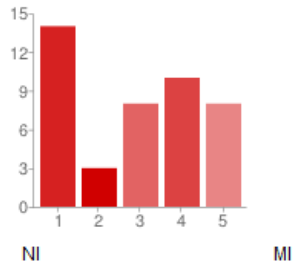


1 - Nada Importante	8	19%
2	1	2%
3	8	19%
4	13	30%
5 - Muito Importante	13	30%

Ilustração 55 - Grau de importância da privacidade no Google Plus para os inquiridos

Quando questionados quanto à privacidade no *Google Plus* e colocando a sua resposta numa escala de importância de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante"), 30% dos inquiridos considerou muito importante a sua privacidade nesta plataforma. Igualmente com 30% de respostas está o nível 4. Os dois maiores valores de importância nesta escala representam 60% dos inquiridos. Os níveis 3 e 1 apresentam percentagens de 19% e o nível 2 foi a opção de 2% dos inquiridos.

Questão 22: *Tendo em conta a plataforma MySpace, qual o grau de importância da privacidade nesta rede social para si?*

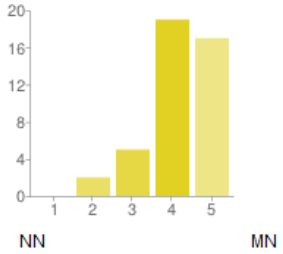


1 - Nada Importante	**14**	33%
2	**3**	7%
3	**8**	19%
4	**10**	23%
5 - Muito Importante	**8**	19%

Ilustração 56 - Grau de importância da privacidade no MySpace para os inquiridos

Numa escala de importância da privacidade de 1 a 5 (onde 1 é "Nada Importante" e 5 é "Muito Importante") e tendo em conta a plataforma MySpace, 33% dos elementos da amostra considerou como irrelevante a importância da privacidade nesta rede social. Dos inquiridos, 23% considerou a sua privacidade neste contexto de nível 4 e 19% foi a resposta aos níveis 5 e 3 em ambos os casos. A resposta de nível 2 representa apenas 7% do total de inquiridos.

Questão 23: *Na sua opinião, qual o grau de necessidade de melhoria da privacidade nas redes sociais?*



1 - Nada Necessário	**0**	0%
2	**2**	5%
3	**5**	12%
4	**19**	44%
5 - Muito Necessário	**17**	40%

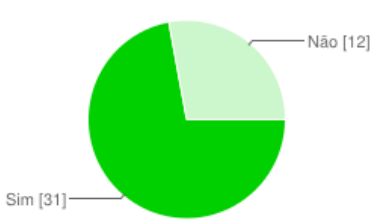
Ilustração 57 - Grau de necessidade de melhoria da privacidade em redes sociais para os inquiridos

Quando questionados quanto ao grau de necessidade de melhoria da privacidade em redes sociais, numa escala de necessidade de 1 a 5 (onde 1 é "Nada Necessário" e 5 é "Muito Necessário"), 44% dos inquiridos considerou o nível 4 de resposta e 40% considerou o nível máximo de 5 para definir a necessidade de melhoria da privacidade no contexto referido. Somando os dois maiores níveis, i.e. os níveis 4 e 5, temos um total de 84% dos inquiridos. Os níveis 3 e 2 apresentam valores de resposta de 12% e 5%, respectivamente. Importante também referir que nenhum dos inquiridos considerou o nível 1 na sua resposta.

5.2.2. Utilização da solução

O conjunto que questões que se seguem foram colocadas aos inquiridos após experimentarem o protótipo desenvolvido no âmbito deste projecto.

Questão 24: *Considera a solução visualmente apelativa?*

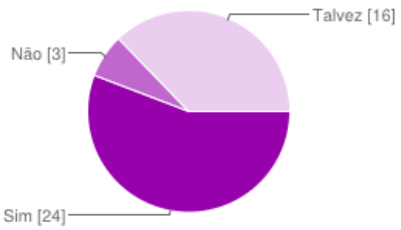


Sim	**31**	72%
Não	**12**	28%

Ilustração 58 - Percentagem de inquiridos que consideram a solução (protótipo) apelativa

Quando questionados relativamente ao interesse visual do protótipo desenvolvido 72%, correspondendo a 31 dos 43 elementos da amostra, considerou a solução apelativa, contrapondo com os restantes 28% (12 inquiridos) que considerou que o protótipo não é apelativo.

Questão 25: *Considera a integração de uma solução deste tipo no navegador de Internet algo diferenciador?*

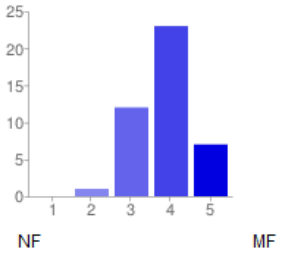


Sim	**24**	56%
Não	**3**	7%
Talvez	**16**	37%

Ilustração 59 - Percentagem de inquiridos que consideram a integração num navegador algo diferenciador

Do total de inquiridos, 56% considerou a integração do protótipo num navegador de Internet como elemento diferenciador. Dos restantes, 37% considerou que talvez fosse elemento diferenciador e apenas 7% considerou que não seria relevante este tipo de integração.

Questão 26: *Como classificaria este sistema em termos de facilidade de utilização?*

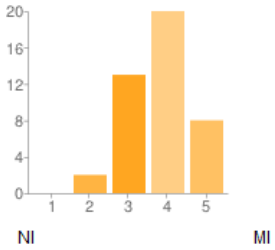


1 - Nada Fácil	0	0%
2	1	2%
3	12	28%
4	23	53%
5 - Muito Fácil	7	16%

Ilustração 60 - Grau de facilidade de uso do protótipo para os inquiridos

Quando questionados quanto ao grau de facilidade de utilização do protótipo, numa escala de facilidade de 1 a 5 (onde 1 é "Nada Fácil" e 5 é "Muito Fácil"), 53% dos inquiridos considerou o nível 4 na sua resposta. Dos inquiridos, 28% considerou uma facilidade de nível 3 e 16% de nível 5. O nível 2 teve uma percentagem de resposta de 2% e o nível 1 não teve qualquer tipo de resposta.

Questão 27: *Como classificaria este sistema em termos de interesse para utilizadores de redes sociais?*

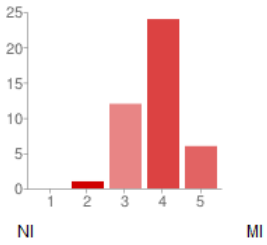


1 - Nada Interessante	0	0%
2	2	5%
3	13	30%
4	20	47%
5 - Muito Interessante	8	19%

Ilustração 61 - Grau de interesse do sistema para os utilizadores de redes sociais segundo os inquiridos

Quando questionados quanto ao grau de interesse do sistema para utilizadores de redes sociais, numa escala de interesse de 1 a 5 (onde 1 é "Nada Interessante" e 5 é "Muito Interessante"), 47% considerou o nível 4 na sua resposta. O nível 3 obteve 30% das respostas e o nível máximo de interesse teve uma percentagem de resposta de 19%. Os restantes 5% apenas consideraram o nível 2 como resposta.

Questão 28: *Como classificaria este sistema no que diz respeito à forma de registo dos utilizadores?*

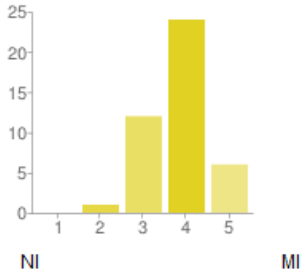


1 - Nada Interessante	0	0%
2	1	2%
3	12	28%
4	24	56%
5 - Muito Interessante	6	14%

Ilustração 62 - Grau de interesse da forma de registo do sistema segundo os inquiridos

Quando questionados quanto ao grau de interesse da forma de registo de utilizadores no sistema, numa escala de interesse de 1 a 5 (onde 1 é "Nada Interessante" e 5 é "Muito Interessante"), 56% considerou o nível 4 e 28% considerou o nível 3 na sua resposta. Os restantes 16% de respostas encontram-se distribuídos pelos níveis 5 e 2 tendo o primeiro 14% e o segundo 2% de respostas.

Questão 29: *Como classificaria este sistema no que diz respeito à forma como define as suas condições de acesso ao conteúdo?*



1 - Nada Interessante	0	0%
2	1	2%
3	12	28%
4	24	56%
5 - Muito Interessante	6	14%

Ilustração 63 - Grau de interesse da forma como são definidas as condições de acesso ao conteúdo segundo os inquiridos

Considerando novamente uma escala de interesse de 1 a 5 (onde 1 é "Nada Interessante" e 5 é "Muito Interessante"), 56% dos elementos da amostra consideraram o nível 4 na sua resposta quando questionados sobre a forma de definição de condições de acesso ao conteúdo. Os níveis 3 e 5 apresentam valores interessantes de resposta: 28% e 14%, respectivamente. As restantes respostas incidem apenas sobre o nível 2 correspondendo a 2% do total de inquiridos.

Questão 30: *Considera a cópia de um URL para as redes sociais uma forma simples de partilhar conteúdos?*

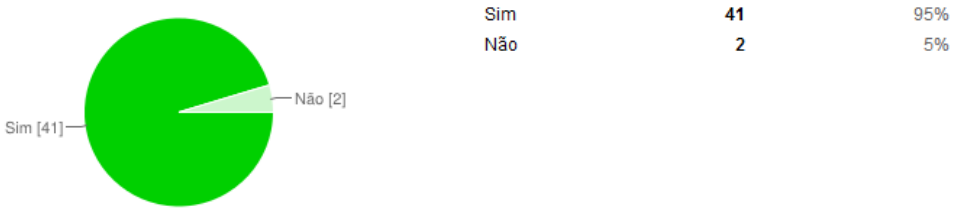


Ilustração 64 - Percentagem de inquiridos que consideram a cópia de um URL uma forma simples de partilha

Quando questionados sobre a simplicidade de partilha de conteúdos pela geração de um URL, 95% dos inquiridos considerou a cópia de um URL para as plataformas sociais uma forma simples de partilha. No entanto, os restantes 5% consideraram o oposto.

Questão 31: *Partindo do princípio que era utilizador(a) desta solução, quais são para si os pontos positivos a assinalar?*

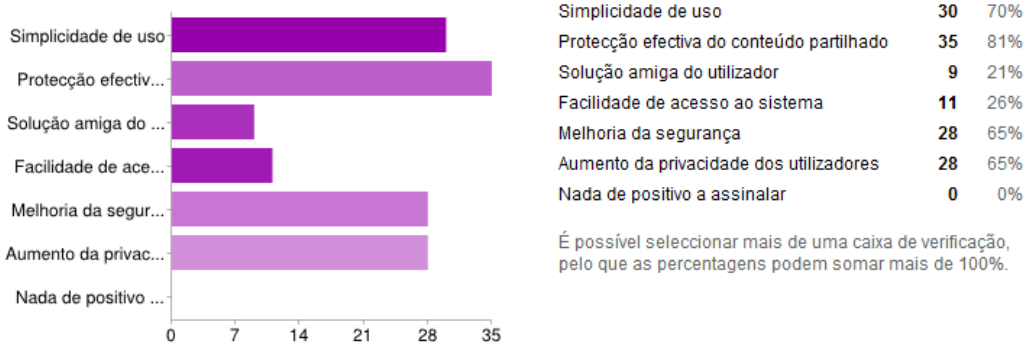


Ilustração 65 - Pontos positivos da solução/protótipo

Quando confrontados com os pontos positivos a assinalar relativamente ao protótipo testado, 81% dos inquiridos considerou que existe uma "Protecção efectiva do conteúdo partilhado" e 70% considerou a "Simplicidade de uso" um ponto positivo. A "Melhoria da segurança" e o "Aumento da privacidade dos utilizadores" foram ambos seleccionados por 65% dos elementos desta amostra. Importante referir que nenhum dos inquiridos considerou na sua resposta a opção "Nada de positivo a assinalar".

Questão 32: *Partindo do princípio que era utilizador(a) desta solução, quais são para si os pontos negativos a assinalar?*

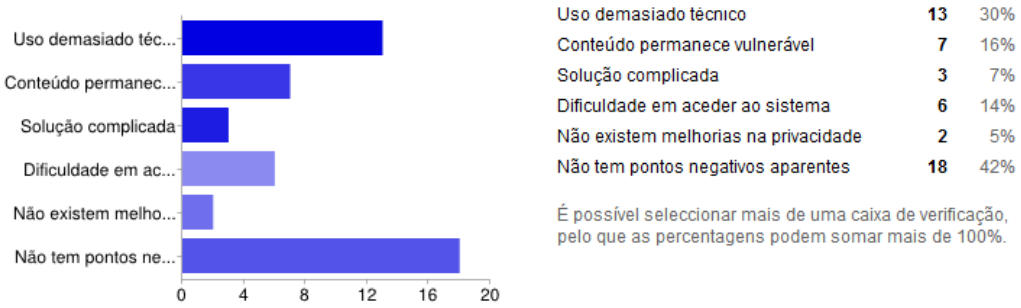


Ilustração 66 - Pontos negativos da solução/protótipo

Entre os pontos negativos a assinalar, 42% dos inquiridos seleccionou a opção "Não tem pontos negativos aparentes", correspondendo estes a 18 dos 43 elementos que constituem esta amostra. O "Uso demasiado técnico" foi o ponto negativo mais assinalado com 30% dos inquiridos a assinalar esta opção. O ponto "Conteúdo permanece vulnerável" foi a resposta de 16%. A "Dificuldade em aceder ao sistema" também foi um ponto negativo indicado tendo este sido assinalado por 14% do total de inquiridos.

Questão 33: *Considera que esta ferramenta atingiria o objectivo a que se propõe?*

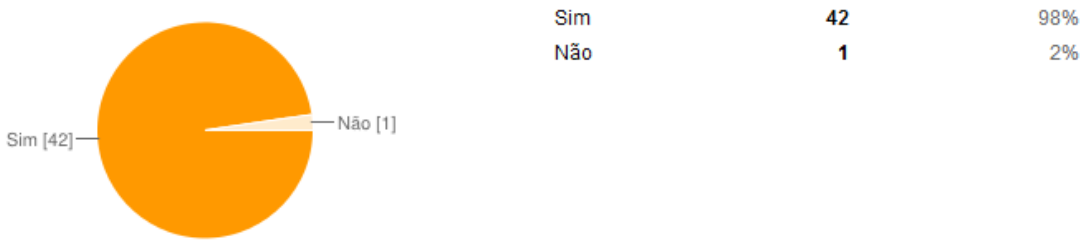
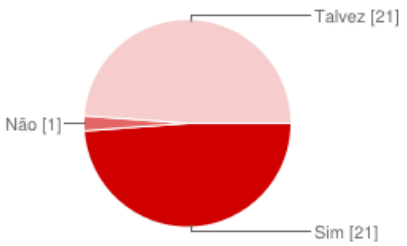


Ilustração 67 - Percentagem de inquiridos que considera que o protótipo atinge o seu objectivo

Quando questionados quanto ao facto de este protótipo atingir o objectivo de aumentar a privacidade dos utilizadores de redes sociais, a esmagadora maioria considerou que "Sim" reflectindo-se no valor de 98% de respostas afirmativas. Apenas 2% dos inquiridos afirmou o contrário.

Questão 34: *Sentir-se-ia mais protegido na sua privacidade se utilizasse uma solução como esta?*

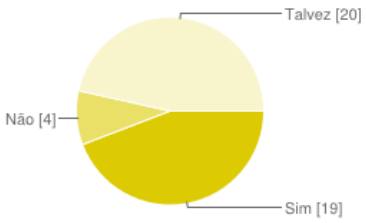


Sim	**21**	49%
Não	**1**	2%
Talvez	**21**	49%

Ilustração 68 - Percentagem de inquiridos que considera que se sentiria mais protegido com esta solução

Quando questionados se como utilizadores se sentiriam mais protegidos com uma solução deste tipo, 49% dos inquiridos afirma que "Sim". Dos restantes, 49% não exclui a possibilidade de uma protecção real da sua privacidade e apenas 2% dos inquiridos se considera mais protegido com uma ferramenta deste tipo.

Questão 35: *Utilizaria esta ferramenta caso fosse disponibilizada?*



Sim	**19**	44%
Não	**4**	9%
Talvez	**20**	47%

Ilustração 69 - Percentagem de inquiridos que utilizaria uma solução como esta caso estivesse disponível

Como resposta à esta questão, 47% dos inquiridos não exclui a possibilidade de usar esta ferramenta caso fosse disponibilizada. Entre os outros elementos que constituem esta amostra, 44% afirma que utilizaria esta ferramenta e apenas 9% afirma que não faria uso de uma solução deste tipo.

5.3. Conclusões

Depois de toda a análise estatística efectuada no ponto anterior, torna-se relevante descrever as conclusões que se podem tirar dos resultados do questionário realizado aos utilizadores de redes sociais. Seguem-se as conclusões a reter:

- As plataformas de redes sociais são utilizadas maioritariamente por pessoas com idades compreendidas entre os 20 e os 30 anos, por pessoas com formação académica superior e de ambos os sexos;
- Os utilizadores acedem às redes sociais diariamente e as redes sociais com maior adesão no estudo são o *Facebook*, *LinkedIn* e *Google Plus*;

- Nas redes sociais são partilhados conteúdos não protegidos como fotografias, informações pessoais e de localização;
- Os utilizadores de redes sociais dizem sentir-se protegidos pelo facto de restringirem o acesso ao seu conteúdo a um número limitado de outros utilizadores. Isto torna-se preocupante, visto que na realidade os utilizadores não protegem o conteúdo com uma ferramenta independente mas sim com serviços disponibilizados pelas próprias plataformas onde partilham conteúdos;
- Os utilizadores consideram-se preocupados com a sua privacidade principalmente quando falamos de conteúdos que revelam informações mais pessoais como são as fotografias, vídeos, informações pessoais e de localização;
- Das redes sociais analisadas neste projecto os utilizadores mostram-se mais preocupados com a sua privacidade nas plataformas *Facebook*, *Google Plus* e *Twitter*, sendo o *MySpace* menos preocupante para os utilizadores quando falamos em privacidade;
- Grande parte dos utilizadores sente que as redes sociais deveriam ter uma maior preocupação com a privacidade dos seus utilizadores;
- A maioria dos utilizadores inquiridos considerou que o protótipo é visualmente apelativo e que a sua integração num navegador *Web* é um elemento diferenciador;
- O protótipo é visto como fácil de usar e com interesse real para os utilizadores de redes sociais;
- O protótipo desenvolvido foi visto com muito interesse por parte dos utilizadores de redes sociais pois é uma ferramenta com uma forma de registo e com uma definição de condições de acesso ao conteúdo interessante;
- A partilha de conteúdos através de um URL é uma forma simples de partilha para os utilizadores;
- Os pontos positivos mais assinalados foram a protecção efectiva do conteúdo e a simplicidade de uso do protótipo;
- Uma parte significativa dos utilizadores inquiridos considerou que o protótipo não apresenta pontos negativos aparentes;
- Ainda relativamente ao protótipo, os utilizadores consideraram que a ferramenta atinge o seu propósito (aumento da privacidade em redes sociais), que se sentiriam mais protegidos ao utiliza-la e que vêem com bons olhos a possibilidade de uma ferramenta como esta ser disponibilizada.

6. Conclusão

Com o desenvolvimento das plataformas de partilha de através de redes sociais surge um problema que será necessário solucionar. Como pode a privacidade dos utilizadores e dos conteúdos que partilham em redes sociais ser salvaguardada tendo as plataformas o controlo sobre o mesmo? Foi no sentido de dar os primeiros passos para a resolução deste problema que surgiu esta dissertação.

Através da análise do contexto através do Estado da Arte foi possível perceber o contexto dos tópicos mais importantes para este trabalho. A Gestão de Direitos Digitais como uma das tecnologias onde se incluem a definição de regras de uso e de negócio dos conteúdos digitais (Serrão, Dias, & Delgado, 2006), associada às plataformas de redes sociais que são serviços disponibilizados *online* que permitem a um indivíduo criar um perfil dentro de um sistema limitado, articular uma lista de outros utilizadores, e visualizar a sua lista de ligações e aquilo que é realizado por outros dentro desse sistema (Boyd & Ellison, 2008), permitiram desenvolver um trabalho em torno da segurança e privacidade em redes sociais. Ainda dentro do Estado da Arte, foram descritas linguagens de expressão de direitos (MPEG-21 e ODRL) como ferramenta para o licenciamento, uma ferramenta existente para GDD (*SmartRM*) que carece de desenvolvimento e uma comparação entre quatro redes sociais que foram igualmente descritas: *Facebook*, *Twitter*, *MySpace* e *Google Plus* onde, através de dois critérios diferentes, se compararam as formas de controlo de cada uma destas plataformas.

Foi também desenhada e analisada uma arquitectura conceptual para uma solução de gestão de direitos digitais, que se enquadrasse com as plataformas de redes sociais, tendo como base o conceito e a arquitectura de uma ferramenta que lida com direitos digitais que dá pelo nome de *OpenSDRM*. Foi tendo por base este sistema, que foi definida uma tabela de requisitos, uma análise dos *stakeholders* envolvidos e uma arquitectura como proposta para desenvolvimento de uma solução de gestão de direitos digitais que fosse centrada no utilizador e que recorresse a gestão de direitos. Ainda dentro deste tópico foi desenvolvido um protótipo que foi construído de forma independente e que permitisse aos utilizadores de redes sociais guardar um conteúdo no sistema. Este conteúdo tem acesso condicionado e o sistema permite que um utilizador registado partilhe um conteúdo próprio com um outro utilizador também ele registado, impondo o primeiro condições de acesso, como o limite do número de acessos ao conteúdo.

Foi também elaborado um questionário a diversos utilizadores de redes sociais, após estes terem experimentado o protótipo desenvolvido, onde foi possível verificar que estes utilizadores são pessoas preocupadas com a sua privacidade, que não protegem conteúdos antes de os publicar e que apenas tem presente a preocupação de restringir a visibilidade dos referidos conteúdos. Estes utilizadores analisados são também da opinião de que existe uma necessidade real de melhorar a privacidade dos utilizadores de redes sociais e de que este protótipo desenvolvido pode ser o primeiro passo nesse sentido. Importante também referir que a esmagadora maioria dos inquiridos não exclui a possibilidade de vir a instalar uma ferramenta semelhante ao protótipo caso fosse disponibilizada aos utilizadores em geral. Os utilizadores inquiridos validaram o propósito deste projecto de forma clara.

Por fim, podemos afirmar que os objectivos gerais e específicos desta dissertação foram atingidos. Podemos igualmente afirmar que a hipótese defendida neste projecto afirma que: "*Uma solução de gestão de direitos digitais aplicada às redes sociais Web aumenta a segurança dos seus utilizadores no que diz respeito à sua privacidade e confidencialidade*", tem uma resposta afirmativa dado que depois de todo este trabalho os indicadores apontam para um aumento da segurança dos utilizadores de redes sociais.

Para trabalho futuro e de continuidade surgem alguns desafios interessantes sendo eles o desenvolvimento de um sistema que suporte um maior número de utilizadores para partilha, que seja mais robusto relativamente ao licenciamento e à autenticação de utilizadores podendo este estar associado à autenticação através do sistema *OpenID*.

Ao longo desta dissertação foi elaborado um artigo com o tema "*User-centric content privacy control for Social Networks*", que foi submetido para o *"Information Security Technical Report Journal"* da *Elsevier*.

7. Bibliografia

MySpace: Política de Privacidade. (7 de Dezembro de 2010). Obtido em 13 de Março de 2012, de MySpace: http://www.myspace.com/Help/Privacy

SmartRM Home. (2010). Obtido em 30 de Março de 2012, de SmartRM: http://www.smartrm.com/home

SmartRM: Create protected content for your contacts. (2010). Obtido em 30 de Março de 2012, de SmartRM: http://www.smartrm.com/learn_more/create_protected_content

Facebook: Política de Utilização de Dados. (23 de Setembro de 2011). Obtido em 12 de Março de 2012, de Facebook: https://www.facebook.com/about/privacy/

Google Plus: Visão Geral. (2011). Obtido em 15 de Março de 2012, de Google Plus: http://www.google.com/intl/pt-BR/+/learnmore/

Política de Privacidade do Twitter. (23 de Junho de 2011). Obtido em 13 de Março de 2012, de Twitter: https://twitter.com/privacy

Google Plus: Política de Privacidade. (1 de Março de 2012). Obtido em 15 de Março de 2012, de Google Plus: http://www.google.com/intl/pt-PT/policies/privacy/

Google+ statistics. (2012). Obtido em 20 de Junho de 2012, de Socialbakers: http://www.socialbakers.com/google-plus-statistics/

MySpace: Acerca de Nós. (2012). Obtido em 14 de Março de 2012, de MySpace: http://www.myspace.com/Help/AboutUs

Portugal Facebook Statistics. (2012). Obtido em 20 de Junho de 2012, de Socialbakers: http://www.socialbakers.com/facebook-statistics/portugal

Twitter Statistics. (2012). Obtido em 20 de Junho de 2012, de Socialbakers: http://www.socialbakers.com/twitter/

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Proceedings from Privacy Enhancing Technologies Workshop* (pp. 36-58). Cambridge, Reino Unido: Springer.

Boyd, D. M., & Ellison, N. B. (2008). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communications 13*, 210-230.

Boyd, D., Golder, S., & Lotan, G. (2010). Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. *Hawaii International Conference on System Sciences* (pp. 1-10). Honolulu, Hawaii, EUA: IEEE 2010.

Delgado, J., Prados, J., & Rodríguez, E. (2005). A new approach to interoperability between ODRL and MPEG-21 REL. *ODRL 2nd International Workshop.* Lisboa, Portugal.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and Myspace. *Americas Conference on Information Systems.* Keystone, Colorado, EUA: Citeseer.

Francisco, A., Marques, J., & Serrão, C. (2012). *User-centric content privacy control for Social Networks through Rights Management Systems.* Lisboa, Portugal.

Govani, T., & Pashley, H. (2005). *Student awareness of the privacy implications when using Facebook.* Pittsburgh, Pensilvânia, EUA: Carnegie Mellon University.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. *Workshop on Privacy in the Electronic Society* (pp. 71-80). Alexandria, Virginia, EUA: ACM.

Guth, S. (2003). A Sample DRM System. *Lecture Notes in Computer Science 2770*, 150-161.

Likert, R. (1932). *A Technique for the Measurement of Attitudes.* Archives of Psychology.

Liu, Q., Safavi-Naini, R., & Nicholas, S. P. (2003). Digital Rights Management for Content Distribution. *Australasian Information Security Workshop.* Adelaide, Australia: Australian Computer Society Inc.

Polo, J., Prados, J., & Delgado, J. (2004). Interoperability between ODRL and MPEG-21 REL. *First International ODRL Workshop*, (pp. 1-12). Viena, Áustria.

Rezgui, A., Ouzzani, M., Bouguettaya, A., & Medjahed, B. (2002). Preserving Privacy in Web Services. *Web Information and Data Management* (pp. 56-62). McLean, Virginia, EUA: ACM.

Rodríguez, E., Rodríguez, V., Carreras, A., & Delgado, J. (2009). A Digital Rights Management approach to privacy in online social networks. *International Conference on Artificial Intelligence.* Barcelona.

Serrão, C. (2008). *iDRM - Interoperability Mechanisms for Open Rights Management Platforms.*

Serrão, C., Dias, M., & Delgado, J. (2006). Bringing DRM interoperability to digital content rendering applications. In K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, & M. Karim, *Advances in Computer, Information, and Systems Sciences, and Engineering* (pp. 323-329). Dordrecht: Springer.

Serrão, C., Dias, M., & Delgado, J. (2006). Using Service-oriented Architectures towards Rights Management interoperability. *Proceedings of the International*

Joint Conferences on computer, Information and Systems Sciences and Engineering (CISSE06). Universidade de Bridgeport, EUA.

Serrão, C., Fonseca, P., & Dias, M. (2006). The Web-Services growing importance for DRM interoperability. *IADIS International Conference WWW/Internet 2006.* Múrcia, Espanha.

Serrão, C., Marques, J., Dias, M., & Delgado, J. (2006). Open-Source Software as a Driver for Digital Content E-Commerce and DRM interoperability. *Proceedings of the Europe-China Conference on Intellectual Property in Digital Media – Optimisation of Intellectual Property in Digital Media (IPDM06).* Xangai, China.

Sommerville, I. (2007). *Software Engineering 8.* Essex, Inglaterra: Addison Wesley.

Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. *IEEE Potentials Magazine March/April*, 31-34.

Torres, V., Serrão, C., Dias, M. S., & Delgado, J. (2008). Open DRM and the Future of Media. *IEEE MultiMedia vol. 15 no. 2*, 28-36.

Wang, X. (2004). MPEG-21 Rights Expression Language: Enabling Interoperable Digital Rights Management. *IEEE Computer Society: October - December*, 84-87.

Wang, X., DeMartini, T., Wragg, B., Paramasivam, M., & Barlas, C. (2005). The MPEG-21 Rights Expression Language and Rights Data Dictionary. *IEEE Transactions on multimedia, Vol.7, No 3*, 408-417.

8. Anexos

A. Tabela completa de requisitos do SGDDRS

Nome do projecto	Solução gestão de conteúdos digitais em redes sociais

Stakeholder	**Categoria**	**Requisitos**		**Critério de aceitação**
		ID	**Descrição**	
Utilizador de Redes Sociais	RF	1	Para aceder ao sistema é necessário acesso à Internet.	Acesso à Internet.
Utilizador de Redes Sociais	RF	2	O utilizador deve aceder ao sistema através de uma extensão de um navegador *web*.	O utilizador acede a partir de um qualquer navegador *web*.
Utilizador de Redes Sociais	RF	3	O sistema deve estar acessível tanto a computadores pessoais como a dispositivos móveis.	O sistema está acessível a partir de um computador pessoal.
Utilizador de Redes Sociais	RF	4	O sistema deve permitir o *login* e *logout* do utilizador.	O sistema permite o *login* do utilizador.
Utilizador de Redes Sociais	RF	5	O sistema deve permitir o registo e criação de conta de utilizador na plataforma.	O utilizador pode registar-se no sistema.
Utilizador de Redes Sociais	RF	6	O sistema deve permitir ao utilizador o carregamento de conteúdos na plataforma.	O sistema carrega o conteúdo insetido pelo utilizador.
Utilizador de Redes Sociais	RF	7	O sistema deve criar um URL do conteúdo que possa ser copiado pelo utilizador	O sistema produz o URL a ser copiado pelo utilizador.
Utilizador de Redes Sociais	RF	8	O sistema deve permitir ao utilizador a definição das condições de utilização do conteúdo.	O sistema oferece pelo menos um campo onde o utilizador pode condicionar o acesso ao conteúdo.
Gestor do Sistema	RF	9	O sistema deve permitir ao gestor do sistema banir utilizadores que tenham uma conduta imprópria.	O sistema permitir a remoção de utilizadores pelo gestor do sistema.
Gestor do Sistema	RF	10	O sistema deve permitir o envio de notificações ao utilizador.	O sistema permitir o envio de uma mensagem ao utilizador.
Gestor do Sistema	RF	11	O gestor do sistema deve ter credenciais únicas e que o distinga dos demais para que este	O gestor de sistema possuir credenciais únicas e que os distinga de outros utilizadores.

			possa monitorizar o sistema.	
Utilizador de Redes Sociais	RF	12	A remoção da conta de um utilizador por vontade própria deve ser permitida pelo sistema.	O utilizador poder apagar a sua conta.
Utilizador de Redes Sociais	RNF	13	Para que o utilizador possa usar a plataforma deve ser utilizador de redes sociais.	O utilizador ter uma conta em pelo menos uma plataforma de redes sociais.

B. Questionário sobre privacidade em redes sociais

1. Características pessoais (Definição de perfil)

Questionário sobre privacidade em redes sociais

*Obrigatório

Características pessoais

De seguida são colocadas algumas questões que permitem definir o seu perfil de utilizador de redes sociais.

Qual o seu sexo? *
- Masculino
- Feminino

Qual a sua faixa etária? *
- 15 - 20 anos
- 20 - 25 anos
- 25 - 30 anos
- Mais de 30 anos

Qual o seu grau de escolaridade? *
- Básico
- Secundário
- Superior

Com que frequência acede a redes sociais? *
- Diáriamente
- Semanalmente
- Mensalmente
- Fico meses sem aceder

Quais as redes sociais onde se encontra actualmente registado(a)? *
- Facebook
- Twitter
- Google+
- MySpace
- LinkedIn
- Flickr
- Foursquare
- Orkut
- Diaspora
- Outras

Tem por hábito inserir conteúdos pessoais nas redes sociais? *
- Sim
- Não

Se sim, a que tipo de conteúdos se refere?
- Fotografias
- Músicas
- Vídeos
- Ligações para outros sites
- Informações pessoais (localidade, data de nascimento,etc)
- Informações sobre localização
- Textos (reflexões, pensamentos,etc)

Protege os seus conteúdos antes de os colocar nas redes sociais? *
- Sim
- Não

Se sim, indique como protege os seus conteúdos.

Considera-se uma pessoa preocupada com a sua privacidade? *

- Sim
- Não

Em geral, qual o grau de importância da privacidade nas redes sociais para si? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de fotografias que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das fotografias? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de vídeos que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade dos vídeos? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de músicas que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das músicas? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de ligações para outros sites que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das ligações para outros sites? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de informações pessoais (localidade, data de nascimento, etc) que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das informações pessoais? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de informações de localização que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade das informações de localização? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a partilha de textos (reflexões, pensamentos, etc) que se disponibilizam nas redes sociais, qual é para si o grau de importância da privacidade de textos publicados? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a plataforma Facebook, qual o grau de importância da privacidade nesta rede social para si? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a plataforma Twitter, qual o grau de importância da privacidade nesta rede social para si? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a plataforma Google+, qual o grau de importância da privacidade nesta rede social para si? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Tendo em conta a plataforma MySpace, qual o grau de importância da privacidade nesta rede social para si? *

1 - Nada importante (NI); 5 - Muito importante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Na sua opinião, qual o grau de necessidade de melhoria da privacidade nas redes sociais? *

1 - Nada necessário (NN); 5 - Muito necessário (MN)

	1	2	3	4	5	
NN	○	○	○	○	○	MN

2. *Utilização do protótipo da solução*

Utilização da solução

De seguida serão colocadas questões relacionadas com a utilização do protótipo da solução a desenvolver e que pretende melhorar a privacidade dos utilizadores de redes sociais.

Importante referir que só poderá responder às questões seguintes após ter utilizado o protótipo.

Considera a solução visualmente apelativa? *
- ○ Sim
- ○ Não

Considera a integração de uma solução deste tipo no navegador de Internet algo diferenciador? *
- ○ Sim
- ○ Não
- ○ Talvez

Como classificaria este sistema em termos de facilidade de utilização? *
1 - Nada fácil (NF); 5 - Muito fácil (MF)

	1	2	3	4	5	
NF	○	○	○	○	○	MF

Como classificaria este sistema em termos de interesse para utilizadores de redes sociais? *
1 - Nada interessante (NI); 5 - Muito interessante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Como classificaria este sistema no que diz respeito à forma de registo dos utilizadores? *
1 - Nada interessante (NI); 5 - Muito interessante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Como classificaria este sistema no que diz respeito à forma como define as suas condições de acesso ao conteúdo? *
1 - Nada interessante (NI); 5 - Muito interessante (MI)

	1	2	3	4	5	
NI	○	○	○	○	○	MI

Considera a cópia de um URL para as redes sociais uma forma simples de partilhar conteúdos? *
- ○ Sim
- ○ Não

Partindo do principio que era utilizador(a) desta solução, quais são para si os pontos positivos a assinalar? *
- ☐ Simplicidade de uso
- ☐ Protecção efectiva do conteúdo partilhado
- ☐ Solução amiga do utilizador
- ☐ Facilidade de acesso ao sistema
- ☐ Melhoria da segurança
- ☐ Aumento da privacidade dos utilizadores
- ☐ Nada de positivo a assinalar

Partindo do principio que era utilizador(a) desta solução, quais são para si os pontos negativos a assinalar? *
- ☐ Uso demasiado técnico
- ☐ Conteúdo permanece vulnerável
- ☐ Solução complicada
- ☐ Dificuldade em aceder ao sistema
- ☐ Não existem melhorias na privacidade
- ☐ Não tem pontos negativos aparentes

Considera que esta ferramenta atingiria o objectivo a que se propõe? *
Objectivo: Aumentar a privacidade de utilizadores de redes sociais.
- ○ Sim
- ○ Não

Sentir-se-ia mais protegido na sua privacidade se utilizasse uma solução como esta? *
- ○ Sim
- ○ Não
- ○ Talvez

Utilizaria esta ferramenta caso fosse disponibilizada? *
- ○ Sim
- ○ Não
- ○ Talvez

Enviar

Tecnologia do Google Docs

Denunciar abuso - Termos de Utilização - Termos adicionais