

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
MBA EM GESTÃO DE SERVIÇOS DE TELECOMUNICAÇÕES**

LEEW RAFAEL VIEIRA MERTENS

PRIVACIDADE NA INTERNET VIA DISPOSITIVOS MÓVEIS

**CURITIBA – PR
2017**

LEEW RAFAEL VIEIRA MERTENS

PRIVACIDADE NA INTERNET VIA DISPOSITIVOS MÓVEIS

Monografia apresentada à Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista em Gestão de Serviços de Telecomunicações, sob a orientação do(a) Prof. Msc. Alexandre Jorge Miziara

**CURITIBA – PR
2017**



TERMO DE APROVAÇÃO
PRIVACIDADE NA INTERNET VIA DISPOSITIVOS MÓVEIS

Por

LEEW RAFAEL VIEIRA MERTENS

Esta monografia foi apresentada às **19:00 h** do dia **08/12/2017** como requisito parcial para a obtenção do título de Especialista no Curso de MBA em Gestão de Serviços de Telecomunicações, da Universidade Tecnológica Federal do Paraná, **Câmpus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

1		Aprovado
2		Aprovado condicionado às correções Pós-banca, postagem da tarefa e liberação do Orientador.
3		Reprovado

Prof. Msc. Alexandre Szpyro Pereira Cardoso
UTFPR - Examinador

Prof. Msc. Alexandre Jorge Miziara
UTFPR – Orientador

Prof. Msc. Alexandre Jorge Miziara
UTFPR – Coordenador do Curso

- O Termo de Aprovação assinado encontra-se na Coordenação do curso.

Dedico este trabalho à minha esposa A.J.
e a meu filho Z.J.M.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus que me concedeu a vida.

Aos meus familiares que tanto têm me auxiliado e apoiado durante todas as fases de minha vida, principalmente a minha esposa A.J. por aguentar meu mau humor durante essa jornada.

A meu orientador e a instituição pela paciência e compreensão.

Não posso deixar de agradecer a meu filho Z.J.M., por conseguir iluminar qualquer momento com seu sorriso.

Muito obrigado.

RESUMO

MERTENS, Leew Rafael Vieira. **Privacidade na Internet Via Dispositivos Móveis**. 2017. 72fls. Monografia, Especialização em Gestão de Serviços de Telecomunicações – Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

A tecnologia é neutra, pois não é nem boa nem má em si mesma, mas depende do uso que se faz dela. Os usuários de dispositivos móveis estão expostos aos sistemas de segurança pública, mas por outro lado, também podem ser atingidos por meio de assediadores com fins escusos. Os usuários querem criar e armazenar seus próprios dados de busca consciente de localização e podem estar dispostos a compartilhar esses dados com outras pessoas. Os sistemas de busca consciente de localização têm a capacidade de localizar os usuários e outros aplicativos podem acessar seus dados pessoais com ou sem sua autorização. A face criminosa que acompanha o avanço tecnológico pode ser evitada por *softwares* que têm que ser constantemente atualizados para garantir a segurança dos usuários e assegurar sua confiança. As tecnologias dos dispositivos móveis estão em constante atualização exigindo sistemas mais eficazes para garantir segurança. A pesquisa apresentada foi dividida em três partes para que tenha uma melhor objetividade: Referencial Teórico, Desenvolvimento e Considerações Finais. No Referencial Teórico foram apresentados conceitos fundamentais para o embasamento da pesquisa, dentre eles a Segurança e a Privacidade na internet. Na etapa de Desenvolvimento foram apresentadas opiniões de diversos autores a respeito de invasão de privacidade, rastreamento de dispositivos móveis e aplicações baseadas no rastreamento, bem como suas contribuições para a sociedade e o impacto aos usuários. Nas considerações finais foram apresentados os resultados percebidos pela pesquisa e suas implicações no dia a dia dos usuários de dispositivos móveis. O objetivo geral dessa pesquisa é investigar a invasão de privacidade possibilitada por meio dos dispositivos móveis. Como resultados dessa pesquisa, pudemos constatar o empenho dos prestadores de serviços de comunicação móvel em garantir a segurança e a privacidade dos usuários, mas mesmo com esse empenho, o usuário deve estar ciente de que é parte fundamental para a garantia de sua privacidade.

Palavras-chave: Privacidade. Dispositivos Móveis. Segurança. Usuários. Engenharia Social.

ABSTRACT

The technology is neutral, it is neither good nor bad in itself, but depends on the use made of it. The mobile users devices are exposed to public safety systems, but on the other hand may also be achieved by end vested with intruders. Users want to create and store your own data aware location search and may be willing to share that data with others. Systems conscious search location have the ability to locate users and other applications can access your personal data with or without your permission. The criminal face accompanying technological advancement can be avoided by software that must be constantly updated to ensure the safety of users and to ensure your confidence. The technologies of mobile devices are constantly updating demanding more effective systems to ensure safety. The research presented was divided in three parts so that it has a better objectivity: Theoretical Referential, Development and Final Considerations. In Theoretical Referential were presented fundamental concepts for the foundation of the research, including the Security and Privacy on the Internet. At the Development stage, opinions were presented by various authors regarding invasion of privacy, tracking of mobile devices and applications based on traceability, as well as their contributions to society and the impact to users. In the Final Considerations were presented the results perceived by the research and its implications in the day to day of the users of mobile devices. The overall goal of this research is to investigate the invasion of privacy made possible through mobile devices. As a result of this research, we observed the commitment of providers of mobile communications services ensure security and privacy of users, but even with this commitment, the user must be aware that it is a fundamental part of guaranteeing their privacy.

Keywords: *Privacy. Mobiles Device. Safety. Users. Social Engineering.*

LISTA DE TABELAS

Tabela 1 – Conjunto de ameaças a serem consideradas	21
Tabela 2 – Tipos de Intrusos e seus objetivos com a Engenharia Social.....	21
Tabela 3 – Bezuca é um aplicativo Android ou iOS.....	36
Tabela 4 – Regras de privacidade e seus significados – CoPS	45

LISTA DE FIGURAS

Figura 1 – Formas existentes de ataques que podem afetar sistemas	16
Figura 2 – Ilustração sobre o funcionamento do sistema de rastreamento	40
Figura 3 – Arquitetura geral do CoPS	44
Figura 4 – Rede de sensores compartilhada de telefones celulares	57
Figura 5 – Handy Andy arquitetura de computação pervasiva	58

SUMÁRIO

1 INTRODUÇÃO	10
1.1 Problema de Pesquisa.....	11
1.2 Objetivo Geral.....	11
1.3 Objetivos Específicos.....	11
1.4 Justificativa	11
1.5 Metodologia	12
2 REFERENCIAL TEÓRICO.....	13
2.1 Segurança e suas Vulnerabilidades.....	13
2.2 Engenharia Social.....	17
2.3 Privacidade	24
2.4 Uma análise dos pontos positivos e negativos da Internet	32
3 DESENVOLVIMENTO	35
3.1 Invasão de Privacidade.....	35
3.1.1 O Rastreamento e a Privacidade das Pessoas	37
3.1.2 Invasão da Privacidade Via Dispositivos Móveis	43
3.1.3 Modelos conceituais e aplicativos para assegurar privacidade	43
3.1.3.1 O LocServ – serviço de middleware	52
3.1.3.2 O Security-Enhanced Linux (SELinux) para segurança nos smartphones	53
3.1.3.3 Segurança no Android	53
3.1.3.4 Usando SELinux no Android.....	54
3.2 Aplicativos Sociais Baseados em Localização (LBSAS).....	54
3.2.1 Sistema eCall para a União Europeia	58
3.2.2 O crescimento de LBS (Serviços Baseados em Localização)	60
3.2.3 WAZE	601
4 CONSIDERAÇÕES FINAIS	63
REFERÊNCIAS BIBLIOGRÁFICAS	65

1 INTRODUÇÃO

Este trabalho compõe-se de uma pesquisa bibliográfica acerca dos novos hábitos de consumo que têm adentrado a sociedade do conhecimento e criado ou resgatado um novo perfil de consumidores. As organizações estão constantemente procurando compreender os mecanismos e tendências de consumo que os consumidores passaram a expressar por si mesmos nas mídias modernas. (CANONGIA; MANDARINO, 2009)

As tecnologias não são nem boas nem más em si mesmas; depende sim, da utilização que se faça delas para julgar o uso e não a tecnologia em si. As más práticas podem surgir dos mais variados meios de comunicação, mas a comunicação *wi-fi* pode gerar invasão da privacidade dos dados pessoais do usuário.

Neste sentido, procuramos conhecer as más práticas relativas à invasão de privacidade por meio de dispositivos móveis.

O século XXI tem assistido ao crescimento vertiginoso das novas tecnologias sem fio que une as pessoas em grandes nós, cruzando informações, propiciando relações pessoais e profissionais. No entanto, nem todos têm propósitos lícitos nesse meio e surgem as más práticas.

Com a globalização, o acesso às tecnologias informáticas, tais como os *notebooks* com banda larga, smartphones, telefones celulares e demais equipamentos móveis popularizou-se, possibilitando maior uso da internet, por um lado, mas são facilmente rastreáveis por meio da entrada consciente de localização.

Por isso, surgiu o interesse na realização dessa pesquisa para sair do senso comum e adentrar o conhecimento científico sobre essa matéria.

Neste contexto, nos propusemos a investigar sobre a invasão de privacidade possibilitada por meio de dispositivos móveis.

Para explorar este tema, adentramos outros temas paralelos como a segurança na armazenagem de informações e o acesso aos dados pessoais dos usuários de serviços de telefonia móvel.

1.1 PROBLEMA DE PESQUISA

Estamos na era da realidade virtual e da comunicação baseada em altas tecnologias e assim nos perguntamos até que ponto o consumidor pode ter sua privacidade invadida? Os aplicativos que propiciam o rastreamento dos comportamentos dos usuários incorrem em crime contra a Dignidade da Pessoa Humana? Como manter a segurança dos dados pessoais mediante aplicativos tão sofisticados que têm acesso a várias informações dos *smartphones*, *tablets* e outros dispositivos móveis?

1.2 OBJETIVO GERAL

O objetivo geral dessa pesquisa é investigar sobre a privacidade na internet via dispositivos móveis e a sua possível invasão.

1.3 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são: apresentar o uso da localização dos dispositivos móveis para algumas aplicações aos usuários destes dispositivos; investigar sobre os modelos conceituais e aplicativos para assegurar privacidade nos dispositivos móveis; investigar sobre o LocServ (serviço de middleware), Security-Enhanced Linux (SELinux) para segurança nos *smartphones*.

1.4 JUSTIFICATIVA

As tecnologias da informação têm se desenvolvido e evoluído constantemente tornando a internet disponível cada vez mais, por isso a confecção de *softwares* seguros é uma máxima necessária, pois o que está em jogo são a privacidade e a segurança dos usuários e das organizações que trocam informações pela rede mundial de computadores.

1.5 METODOLOGIA

Os critérios que tivemos para este estudo foram no sentido da qualidade das fontes bibliográficas, considerando autores ligados a instituições de ensino com reconhecimento do Ministério da Educação e da Cultura. Também foram utilizadas informações obtidas em *sites* institucionais.

Este estudo caracteriza-se como uma pesquisa descritiva que conforme Andrade (2011, p. 106), é aquele no qual os fatos são observados, registrados, analisados, classificados e interpretados, sem que o pesquisador interfira neles.

Metodologicamente, a pesquisa é do tipo exploratório, pois trata-se de uma pesquisa bibliográfica, que recorre a artigos científicos, dissertações e teses, livros e consultas a *sites* institucionais, tais como do governo, de instituições de ensino; a coleta de dados ocorre por meio de pesquisas realizadas nos materiais bibliográficos impressos ou disponibilizados na internet. A posterior análise dos dados conduzirá aos resultados obtidos nesse estudo pelas leituras e implementações que serão realizadas.

2 REFERENCIAL TEÓRICO

Neste capítulo, serão apresentados os principais conceitos de Segurança da Informação, de vulnerabilidades das redes, os pilares da segurança da informação, principais ameaças e ataques à segurança da informação, incluindo a Engenharia Social, que é uma modalidade recente de prática lesiva à segurança da informação, com base em bibliografia disponível na internet, livros e teses desde 2001 até 2017.

Define-se segurança da informação como a área do conhecimento que tem a função de salvaguardar os ativos da informação contra ameaças e ataques indevidos, bem como modificações que não foram autorizadas ou colocadas em disponibilidade.

“Segurança da Informação e Comunicações (SIC) são ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações”, inovando e ampliando, portanto, o escopo tradicionalmente conhecido e adotado na segurança da informação. (CANONGIA; MANDARINO, 2009, p. 38)

2.1 SEGURANÇA E SUAS VULNERABILIDADES

Câmara (2010) alerta para a fragilidade de segurança das redes sem fio, pois as redes *wi-fi* que vêm se tornando mais populares e utilizadas ultimamente pela praticidade e mobilidade proporcionadas nos ambientes corporativos vêm acompanhadas por uma série de preocupações por parte dos encarregados da segurança das informações.

A implementação de uma rede sem fio pode trazer várias vantagens e às vezes é até inevitável. Porém, é importante que se compreenda as implicações de segurança de cada decisão tomada. Elas envolvem não somente questões de configurações, mas também de planejamento, projeto e escolha dos equipamentos que possuam as características desejáveis. (CÂMARA, 2010, p. 51)

A vulnerabilidade das redes sem fio é apresentada por Tanenbaum (*apud* CÂMARA, 2010) por meio de situação específica onde ele simula que a espionagem a uma empresa que utilize *wi-fi* pode ser realizada de maneira simples com um notebook que reconheça sinais 802.11 dentro de um carro no próprio estacionamento da empresa por algumas horas, porque nele serão gravadas informações fundamentais no seu disco rígido. Segundo Fiorini (2006), as redes sem fio apresentam maior vulnerabilidade com relação à segurança quando comparadas às redes cabeadas.

A tecnologia *wi-fi* ainda não amadureceu totalmente e, dessa forma, vários de seus padrões e protocolos ainda estão evoluindo e têm falhas. Assim como nas redes cabeadas, as ameaças às redes sem fios precisam ser conhecidas para que seus danos sejam minimizados através das soluções disponíveis e aplicação de boas práticas. (CÂMARA, 2010, p. 51)

Para Alves (2010), a segurança da informação possui três principais pilares sobre os quais ela é edificada e sobre os quais ela enfrenta as potenciais ameaças e enfrenta os ataques reais:

- a) Confidencialidade: É a garantia de que as informações transmitidas chegarão ao seu destino sem que se dissipem para outro lugar onde não deveria passar. Várias tecnologias como, por exemplo, criptografia e autenticações podem ser usadas, desde que mantenham a integridade das informações;
- b) Integridade: É a garantia de que as informações não sofreram nenhuma modificação durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo assim a sua real veracidade após chegarem ao destino.
- c) Disponibilidade: De nada adianta possuir integridade e confidencialidade, se a informação nunca está disponível. Então, o grande desafio é manter essa estrutura de passagem de informações de forma confiável e íntegra sem que haja impossibilidade de captar as informações. (ALVES, 2010, p. 21)

Canongia; Mandarino (2009, p. 38) acrescentaram um item a esses tradicionais pilares da segurança da informação: “d) Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade”.

Segundo Laureano (2005), os riscos à segurança das redes de computadores podem apresentar-se sob a forma de ameaças ou ataques que obtêm maior ou menor eficácia conforme a vulnerabilidade apresentada pela rede visada. Ameaça é designada por um termo da língua inglesa “*threat*” e pode apresentar-se sob várias modalidades como se segue:

- Ameaça Inteligente: Circunstância onde um adversário tem a potencialidade técnica e operacional para detectar e explorar uma vulnerabilidade de um sistema;
- Ameaça: Potencial a violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano;
- Ameaça de Análise: Uma análise da probabilidade das ocorrências e das consequências de ações prejudiciais a um sistema;
- Consequências de uma ameaça: Uma violação de segurança resultado da ação de uma ameaça. Inclui: divulgação, usurpação, decepção e rompimento. (LAUREANO, 2005, p. 15)

A ameaça corresponde a “qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto”, segundo Laureano (2005). Mas as ameaças só existirão se houver alguma vulnerabilidade, porque de outro modo, não gerarão quaisquer prejuízos, porque serão rechaçadas sem causar qualquer problema à rede.

Classifica-se as ameaças de acordo com sua intencionalidade nos seguintes grupos:

- Naturais – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.
- Involuntárias – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados por acidentes, erros, falta de energia, etc.
- Voluntárias – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários. (SÊMOLA *apud* LAUREANO, 2005, p. 15)

Os sistemas de informação podem sofrer ameaças correspondentes aos seguintes eventos: Falhas no hardware ou nos softwares; Ações pessoais; Invasão por meio do terminal de acesso; “Roubo de dados, serviços, equipamentos; Incêndio; Problemas elétricos; Erros de usuários; Mudanças no programa; Problemas de telecomunicação que podem ser originados a partir de fatores técnicos, organizacionais e ambientais, porém as más decisões administrativas podem agravá-los”, segundo Laureano (2005, p. 16).

Por outro lado, o vocábulo da língua inglesa “*attack*” é traduzido por ataque, que também pode apresentar-se sob diferentes roupagens; define-se ataque “como um assalto ao sistema de segurança que deriva de uma ameaça inteligente, isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um

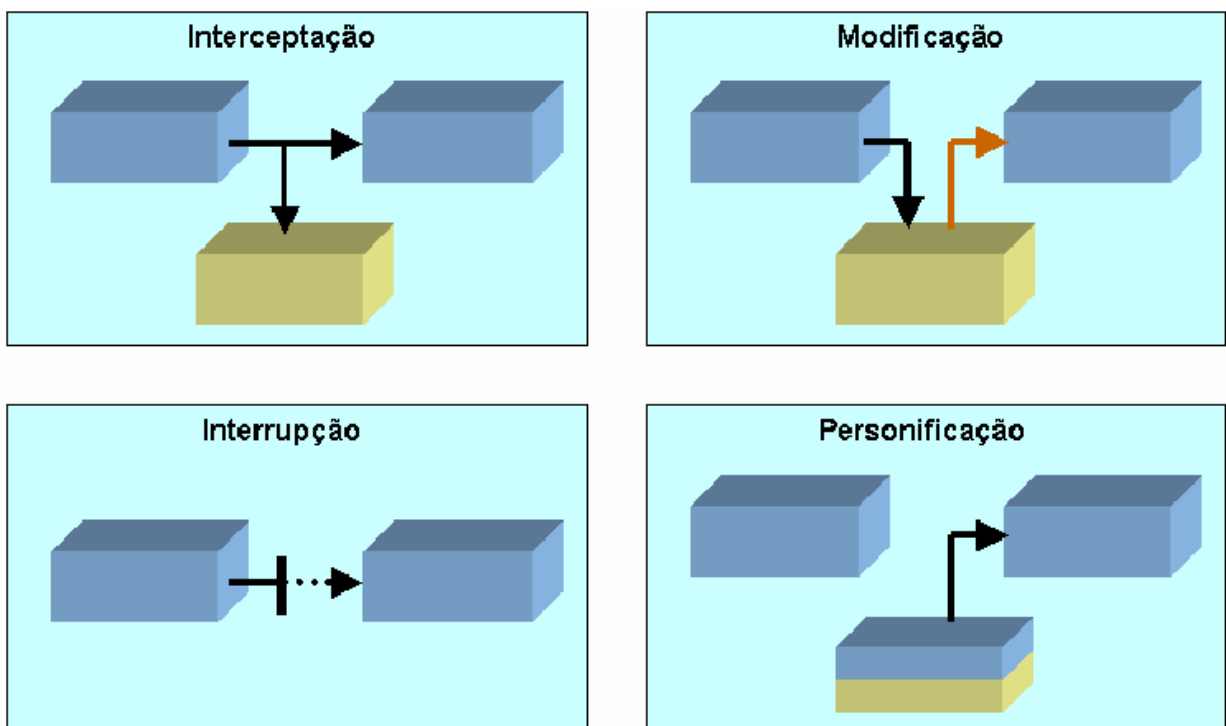
método ou técnica) para invadir serviços de segurança e violar as políticas do sistema”, segundo Laureano (2005, p. 16).

O ataque é ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios citados anteriormente. Um ataque pode ser *ativo*, tendo por resultado a alteração dos dados; *passivo*, tendo por resultado a liberação dos dados; ou *destrutivo* visando à negação do acesso aos dados ou serviços. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. (LAUREANO, 2005, p. 16)

Como asseveramos anteriormente, a vulnerabilidade é que determinará o sucesso ou insucesso dos ataques direcionados ao sistema; também contam as contramedidas existentes para evitá-los. Os mecanismos de segurança dependem do nível de conhecimento que se pode ter dos potenciais ataques, que são os seguintes:

- **Interceptação:** considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).
- **Interrupção:** pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
- **Modificação:** consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
- **Personificação:** considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade. (LAUREANO, 2005, p. 16)

Figura 1 – Formas existentes de ataques que podem afetar sistemas



Fonte: Laureano, 2005

As tecnologias da informação têm se desenvolvido e evoluído constantemente tornando a internet disponível cada vez mais, por isso a confecção de softwares seguros é uma máxima necessária, pois o que está em jogo são a privacidade e a segurança dos usuários que ficam expostos “por meio de softwares na rede mundial de computadores”, segundo Rego (2011, p. 8).

Isoni; Vidotti (2007) apresenta o perfil de dois tipos de atacantes contra a segurança das redes das organizações: 1- as de origem do meio interno que vêm da própria organização, empresa ou instituição; 2- os que se originam do meio externo, correspondendo a atacantes externos, que provêm, na maior parte das vezes, da WWW – *World Wide Web* (Rede Mundial de Computadores).

O atacante interno é dotado de um comportamento mais complexo, demonstrando na maioria das vezes a mesma motivação dos crimes regulares: cobiça, obtenção ilegal de dinheiro, lucro, riqueza, ou até mesmo ligados a revanches pessoais ou vingança. (ISONI; VIDOTTI, 2007, p. 8)

Uma pesquisa realizada nos Estados Unidos, aos cuidados da CSI – *Computer Security Institute* em parceria com o FBI – *Federal Bureau of Investigations* (*Departamento da Computer Intrusion Squad*) levantou informações sobre as características dos crimes cibernéticos que ocorrem nas organizações, demonstrando que na maioria dos casos em que os ataques geram perdas financeiras há a participação ativa ou cooperação de algum funcionário da própria organização vítima dos ataques. (ISONI; VIDOTTI, 2007)

Os ataques internos e externos seguem padrões bem definidos, que mantêm uma sequência de eventos, onde se pode traçar perfis e modelos de comportamento, que segundo Isoni; Vidotti (2007, p. 9) seguem uma metodologia simplista que consiste em “rastrear a rede, ou o computador alvo, buscando vulnerabilidades específicas e estabelecer uma base de dados de endereços IP que possam ser atacados”.

2.2 ENGENHARIA SOCIAL

A expressão Engenharia Social foi forjada pelo ex-hacker dos anos 90, Kevin Mitnick, que tornou-se escritor e consultor de segurança após o cumprimento de

prisão pelos prejuízos causados às empresas que ele burlou o sistema de segurança por “esporte”. A expressão cabe às práticas que utilizam a psicologia de maneira anti-ética para a obtenção de informações sigilosas das organizações, das pessoas e dos sistemas de informação junto às próprias pessoas (muitas vezes funcionários das empresas). As pessoas são ludibriadas para fornecerem informações que possibilitem o roubo de informações ou bens, causar prejuízos, extorquir. Uma definição é:

Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos. (ALVES, 2010, p. 14)

Engenharia Social é o termo aplicado às diversas técnicas utilizadas por pessoas externas ao sistema com o intuito de obter “acesso não autorizado a informações privadas e usá-las contra um alvo”, segundo Cavalcanti Jr. (2011). A peculiaridade das estratégias utilizadas pelos praticantes dessa forma ilícita denominada engenharia social é o fato de usarem psicologia¹ contra o alvo com o intuito de conseguir as informações que precisam para a prática de atos ilícitos. (CAVALCANTI JR, 2011, p. 24).

O exemplo dos falsos sequestradores simplifica esse conceito: de posse de informações públicas e privadas, criminosos ligavam para as vítimas *simulando* um sequestro para conseguir um resgate. Não há sequestro propriamente dito e toda a simulação não passa de um engodo psicológico contra a vítima, que é reforçada pela posse de informações até então consideradas privadas. (CAVALCANTI JR, 2011)

O ataque de engenharia social não requer a aproximação do atacante aos computadores e sistemas do alvo desejado, porque vale-se da vulnerabilidade humana, que é um dos pontos mais relevantes para os ataques dos engenheiros sociais. Dessa forma:

[...] a engenharia social explora duas questões: a personalidade de um indivíduo e seu ambiente de trabalho. Os funcionários gostam de ser cordiais com outros, na maior parte das vezes. Na minha experiência pessoal, em 95% das vezes a engenharia social é bem sucedida para um hacker (ANDRADE; CUNHA, 2008, p. 18).

¹ É preciso esclarecer que os engenheiros sociais dominam os recursos psicológicos/emocionais de forma a extorquir informações das pessoas.

No âmbito das organizações, os colaboradores têm que estar atentos às possibilidades de serem confrontados com engenheiros sociais a todo o momento e para tanto, precisam ser treinados com simulação de situações em que as informações poderiam ser solicitadas ou copiadas sem o seu conhecimento. No âmbito das redes sociais, a atenção é de cada usuário que deve resguardar seus dados pessoais para não ser alvo de roubo de informações, de bens materiais e de lesão de sua intimidade com prejuízos incalculáveis. Vale lembrar que o principal objetivo do engenheiro social é manipular a vulnerabilidade humana.

Há engenharia social que podemos classificar como lesiva e não lesiva, ou ainda, lesiva sempre ela é, no entanto, pode não lesar o patrimônio de uma organização, mas expor suas informações por meio de burla do sistema.

A vulnerabilidade humana é o que possibilita mais a ação da engenharia social, porque as pessoas deixam-se envolver por diversas razões e acabam por deixar escapar informações aos engenheiros sociais.

O engenheiro social não tem um perfil definido e é mais interessante definir a postura e o comportamento, porque pode ser qualquer pessoa. Todos somos, em determinada proporção um engenheiro social conforme afirma Kevin Mitnick, porque podemos usar de engenharia social² para nos aproximarmos de alguém com interesse de relacionamento (uma ‘cantada’ é uma atitude de engenharia social); os vendedores profissionais utilizam de engenharia social: “quando se deseja vender um produto, você tem que convencer a pessoa do que ela precisa e do quanto o produto é importante e vai fazer a diferença, isto é engenharia social”. (ANDRADE; CUNHA, 2008, p. 19)

Kevin Mitnick (*ex-hacker*), em seu livro *A Arte de Enganar* demonstra várias situações de utilizar a vulnerabilidade humana para extorquir informações por meio da engenharia social. De posse das informações privadas é possibilitado o acesso aos dados sigilosos.

Em um dos exemplos, ele cita a situação na qual uma pessoa obtém acesso à intranet de uma empresa, mas que é protegida por uma senha que muda diariamente. Para descobrir a senha, ele aguarda por um dia de chuva forte, liga para empresa fingindo ser um empregado preso em casa por conta da tempestade e convence o operador a revelar a senha daquele dia. (CAVALCANTI JR., 2011, p. 24)

² O engenheiro social não é um profissional específico, ele pode ser qualquer pessoa com segundas intenções. Como o alvo principal é o usuário dos sistemas e não o hardware ou o software, ferramentas de hardware e software dificilmente preveem o ataque. (ANDRADE; CUNHA, 2008)

Os métodos são muito variados, dependendo do estilo do criminoso, mas mantendo um ponto em comum que é focar no psicológico da vítima. Mitnick cumpriu 5 anos de detenção pelos crimes de obtenção de informações para invadir sistemas, causando prejuízos às organizações. Apesar de não retirar dinheiro das empresas, causou-lhes muitos transtornos. Seu método era a engenharia social onde, normalmente, passava-se por alguém para conseguir informações privilegiadas, segundo Cavalcanti Jr. (2011).

Para Reis; Pereira; Souza (2010), as antigas redes de computadores limitavam-se a pequenos espaços, normalmente, circunscritos a um laboratório de informática e poderiam apenas operar por cabeamento e, por isso ficavam restritas a esse espaço físico. Com o crescente emprego de equipamentos, de redes heterogêneas, de tecnologias móveis para acesso à Internet e do aumento do número de usuários, as soluções têm que ser continuamente repensadas e reorganizadas.

Em sentido lato, as redes são agrupamentos, por isso são fenômenos coletivos cuja dinâmica implica o inter-relacionamento entre os grupos, as pessoas, as organizações ou as comunidades, que são chamados de atores. A existência das redes propiciam relações distintas que podem incluir o trabalho, o estudo, as amizades, mas normalmente passam despercebidas, segundo Tomaél; Alcara; Di Chiara (2005).

Segundo Santaella; Lemos (2010), as redes são sistemas que contém grande dinamicidade e complexidade, que por sua vez, é marcada pela auto-organização e pela emergência. Apesar das redes sociais antecederem ao surgimento da Internet, sua alavancagem deu-se a partir dela, pois o fenômeno conhecido como Web 2.0 marcou a revolução das redes sociais digitais, que hoje encontram-se na versão Web 3.0 que congregam o *Facebook*, *LinkedIn*.

Segundo Martins (2012), o ambiente virtual é acometido constantemente por tentativas de atacantes ou intrusos, que têm distintas intenções desde a mera especulação e teste de sua habilidade em burlar a segurança de sistemas até o prejuízo de pessoas e empresas. Essas últimas podem ter seus dados destruídos ou publicadas informações que são essenciais à empresa, podendo utilizar sua estrutura para gerar a invasão de outras empresas.

- a. Falsificação de Identidade – Se passar por outra pessoa usando seu login e senha para executar tarefas e acessar sistemas ou locais restritos. Por exemplo enviar e-mail com mensagens falsas e fazer com que pacotes de autenticação sejam executados. Esses ataques podem ser feitos usando senhas deixadas embaixo do teclado.
- b. Violação - É a alteração de dados que pode ser feita durante uma transmissão.
- c. Repudição – Feita na finalização do ataque pois é a negação do que foi feito, ou seja, apagar qualquer sinal de que você esteve ali, que acessou aquele sistema ou que entrou naquela sala.
- d. Divulgação das Informações – um ataque que pode custar muito caro com consequências irreversíveis e tão grave quanto a “Negação de Serviço” que é divulgação de informações confidenciais. Informações que deveriam estar protegidas e que agora estão nas mãos de pessoas não autorizadas. Um exemplo pode ser expor mensagens de erro ou expor código em sites.
- e. Negação de Serviço – paralisar algum serviço. Pode ser feito “inundando” o DHCP Server Local com solicitações de IP, fazendo com que nenhuma estação com IP dinâmico obtenha endereços IP. O alvo pode ser um Web Server que contem o site da empresa. Outro exemplo seria “inundar” uma rede com pacotes SYN (Syn-Flood); “inundar” uma rede com pacotes ICMP forçados.
- f. Elevação de Privilégios – quando o usuário não autorizado consegue ter privilégios de forma ilegal. Acessando uma máquina onde o Administrador da rede fez logon e esqueceu, deixando-a desbloqueada. Ele pode simplesmente adicionar sua própria conta como administrador do domínio ou dar privilégio como acesso remoto, o que permitira fazer o que quiser de onde estiver.

Tabela 1 – Conjunto de ameaças a serem consideradas
 Fonte: Nakamura; Geus (*apud* ANDRADE; CUNHA, 2008)

INTRUSOS	OBJETIVOS
Estudantes	Vasculhar mensagens de e-mail alheias por diversão ou curiosidade.
Crackers	Quebrar sistemas de segurança e roubar informações.
Representantes Comerciais	Encontrar planilhas referentes a preços ou cadastro de clientes.
Executivos	Descobrir plano estratégico dos seus concorrentes.
Espiões	Descobrir planos militares.
Terroristas	Causar pânico pela rede e roubar informações estratégicas
Contadores	Desfalques financeiros.
Corretores de valores	Adulterar informações para obter lucro com o valor das ações.
Ex-funcionários	Causar prejuízos apenas por vingança.
Vigaristas	Roubar informações, como senhas e números de cartões de crédito

Tabela 2 – Tipos de Intrusos e seus objetivos com a Engenharia Social
 Fonte: Popper; Brignoli (*apud* ALVES, 2010)

Kevin Mitnick, o ex-hacker que, após o cumprimento de sua pena, tornou-se muito conhecido mundialmente pela publicação de livros sobre segurança na Internet, entende que todos os colaboradores de uma organização devem passar por treinamentos para formar um senso de suspeita e de cuidados no momento em que são contactados por pessoas desconhecidas, especialmente, quando uma pessoa solicita algum dado de acesso à rede ou a um computador da empresa. O ser humano tem por natureza a tendência de confiar nos outros, “mas como dizem os japoneses, os negócios são uma guerra. Os seus negócios não podem permitir que você baixe a guarda. A política de segurança corporativa deve definir claramente o comportamento apropriado e inapropriado”. (ANDRADE; CUNHA, 2008, p. 38)

Dentre os processos que exigem conhecimento está o monitoramento do fluxo de informações de negócios que implica analisar o ambiente externo e interno às organizações e, conseqüentemente, interagir com todos os atores e variáveis que afetam o negócio da organização.

Os conhecimentos organizacionais permitem a visualização das etapas dos que dizem respeito, por exemplo, às áreas envolvidas e suas responsabilidades dentro do processo para garantir eficácia na disseminação da informação para agilizar a formação do capital intelectual necessário à organização.

No caso da utilização de informações é importante conhecer os produtos que representam novos investimentos financeiros para empresas e quais os atores envolvidos para fins de aquisição e fusão de informações.

O fator mais importante do uso de tecnologias informacionais é o uso inteligente das informações armazenadas nos bancos de dados da empresa. É fundamental o processamento da informação para a utilização na abordagem correta dos processos. Saber lidar com a informação é uma grande estratégia das organizações. Nesse universo de mudanças econômicas que influenciam as incertezas, a formação de capitais intelectuais favorece o sucesso no mercado.

As empresas precisam de estratégias políticas e tecnológicas para buscar formas alternativas para enfrentar a competitividade e manter seus produtos no mercado com qualidade.

A estratégia do monitoramento permanente do fluxo de informações que se processam no ambiente externo e interno de negócios e envolvem vários processos dinâmicos entre pessoas, instituições e organizações, possibilitam uma dinâmica

interativa entre setores operacionais e administrativos se tornam viáveis a partir do fluxo de informações. Essa interação é extremamente dinâmica em sua conjuntura produtiva.

Um dos aspectos positivos do fluxo de informações diz respeito ao seu uso para tomada de decisões e redução do tempo em relação às respostas provenientes de pesquisas do ambiente externo, a fim de transformar em inteligência, as informações mediante a rápida avaliação dos problemas de níveis operacionais e administrativos.

As informações são hierarquizadas a partir de dados de informações mais básicas e quantitativas. Assim, a informação agrega conhecimentos e favorece a tomada de decisões.

Com a implementação de sistemas de informatização a empresa tem condições efetivas de realizar a atividade de gestão estratégica da informação que tem por finalidade contribuir para o monitoramento competitivo e operacional. A coleta de informação proporciona à organização do conhecimento facilidade de conhecer melhor as oportunidades e os riscos externos.

A vantagem competitiva é processo de ação que envolve posturas frente ao conhecimento. Entende-se, portanto, que o capital intelectual atua como um radar para a empresa, proporcionando-lhe o conhecimento das oportunidades e ameaças identificadas no ambiente, que poderá instruir suas tomadas de decisão, visando à conquista de vantagem competitiva. (BUFREM, 2010)

A informação qualitativa e as necessidades reais do setor organizacional são um dos desafios atuais, já que é fundamental, utilizar a informação em sua extensão delimitada para ser utilizada de acordo com os objetivos da organização. Neste processo, o conhecimento intelectual é importante para que os colaboradores saibam discernir como utilizar as informações nas decisões da organização e de suas necessidades; a coleta de informação apropriada; a análise da informação e geração de inteligência e a disseminação do conhecimento.

Na atualidade os recursos humanos nas organizações precisam dominar a gestão da informação e do conhecimento, o capital intelectual, as vantagens competitivas e tecnologia da informação e seu uso mais abrangente e sistemático dependem de como usar esse capital intelectual.

Hoje, com a globalização, a Internet e a evolução das telecomunicações, as organizações podem definir a metodologia do compartilhamento de informações

para atingir a melhor forma de compartilhar conhecimentos. Essa é uma estratégia de atuação perante a concorrência, mas envolvem posturas, investimentos e formação intelectual para a produção de mudanças políticas, econômicas, sociais e tecnológicas capazes de garantir uma vantagem competitiva.

2.3 PRIVACIDADE

Maria Helena Diniz (2010), ao referir-se ao direito de imagem do empregado, leciona que trata-se de um atributo da pessoa e por isso deve ser preservada, cabendo sanções ao empregador no caso de explorar a imagem do empregado para publicidade, por exemplo, sem o seu explícito consentimento, porque trata-se de uma “lesão a um interesse que visa a satisfação ou gozo de um bem jurídico extra patrimonial contido nos direitos da personalidade [...] ou nos atributos da pessoa”. (DINIZ, 2010, p. 94).

O Inciso X, do art. 5º da Constituição Federal de 1988 dispõe, *in verbis*: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 2017)

O Art. 20º do Código Civil de 2002 corrobora a previsão constitucional, demonstrando que há garantias ao direito e preservação da imagem nas normas infraconstitucionais, como o Código Civil:

Art. 20 do CC - Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais. (grifo nosso) (DINIZ, 2010, p. 94)

O Direito é um instituto dinâmico que tem que adaptar-se às inovações pelas quais passa a sociedade, contribuindo para o bem-estar e para a manutenção da ordem e da justiça. Atualmente, os vínculos estreitos existentes entre o Direito e a Informática desperta a ocorrência de situações que impõem situações inéditas que exigem soluções que demandam estudos e reinterpretações desafiadoras aos profissionais do direito. (PAIVA, 2002)

As novas tecnologias são desenvolvidas de forma veloz impedindo o devido acompanhamento simultâneo dos juristas no sentido de elaborar leis e estudos que viabilizem um regular manuseio dos instrumentos eletrônicos. Assim atestamos um abismo profundo entre o fático e o jurídico - e o conseqüente debate que isso provoca - em virtude da existência de outros e novos institutos jurídicos, pelo surgimento de realidades (o fato) antes desconhecidas; o revigoramento e adaptação de enfoques outrora consolidados sobre alicerces que se modificam permanentemente; a presença de direitos e valores que - hoje se enfrentam em outra esfera (no mundo virtual) e que requerem definições jurídicas, sejam de origem legal ou judicial. (PAIVA, 2002, p. 1)

Há uma crescente preocupação em se preservar os direitos da personalidade do empregado no ambiente de trabalho da sociedade atual, pois o trabalhador é possuidor dos direitos fundamentais que a Constituição Federal dá garantias. (BURMANN, 2011)

Com o uso intensivo da tecnologia que permite maior controle das ações no ambiente de trabalho, a privacidade, que se constitui um direito da personalidade e está ligada aos valores morais humanos vem despertando as atenções das entidades trabalhistas e dos especialistas em direito, pois é preciso estabelecer especificamente até onde pode ir o controle e a fiscalização do empregador sobre o empregado para a manutenção de um ambiente favorável para o desenvolvimento das atividades laborais, segundo Burmann (2011).

Entretanto, apesar desta preocupação, não há como negar, em razão de o empregado estar inserido na estrutura empresarial, ter a sua atividade subordinada ao empregador e poder praticar atos capazes de afetar direitos fundamentais dos seus colegas de trabalho e de terceiros, que poderão existir situações em que haverá necessidade de limitação da privacidade do trabalhador. Diante desse cenário, a grande discussão que se estabelece é se é possível garantir a concretização do direito à privacidade do trabalhador sem afastar a característica principal da relação de emprego e, principalmente, sem afrontar outros direitos fundamentais de maior ou igual relevância. (BURMANN, 2011, p. 2)

Burmann (2011) entende que há possibilidade de estabelecer regras que preservem a privacidade da pessoa, apesar de não estar estabelecida por lei de modo específico.

O direito à intimidade e à privacidade explicitado na Carta Magna do país é motivo de polêmica judicial devido à interpretação dessa questão em circunstâncias específicas. Poderíamos nos questionar até que ponto é invasão da intimidade em um local de trabalho, a instalação de câmeras de vigilância.

Alvarenga (2013, p. 9), sobre esta questão apresenta o seguinte parecer:

A intimidade atua como uma espécie dos Direitos de Personalidade do empregado e compreende um direito humano fundamental assegurado ao mesmo de não ter a revelação de aspectos pessoais da sua intimidade e dos seus sentimentos e/ou pensamentos a terceiros.

O artigo 5^a da Constituição respalda a vida íntima do indivíduo de modo que sua violação incorre em desrespeito aos direitos fundamentais constitucionais e aos direitos da dignidade da pessoa humana, que são universais.

Segundo Diniz (2010), dano patrimonial, denominado também como dano material, é aquele que repercute no patrimônio do lesado, entendendo-se o patrimônio, de forma restrita, como o conjunto das relações jurídicas de uma pessoa, apreciáveis em dinheiro.

É a lesão concreta que afeta um interesse relativo ao patrimônio da vítima, consistente na perda ou deteriorização, total ou parcial, dos bens materiais que lhe pertencem, sendo suscetível de avaliação pecuniária e de indenização pelo responsável.

São patrimoniais os danos consistentes em prejuízos de ordem econômica suportados pelo ofendido. Entretanto, nem sempre o dano patrimonial resulta da lesão de bens ou interesses patrimoniais. A violação de bens personalíssimos pode refletir no patrimônio da vítima, gerando perda de receitas ou realização de despesas. (DINIZ, 2010, p. 55)

É possível distinguir-se, no âmbito dos danos, a categoria dos danos patrimoniais ou materiais, de um lado, dos chamados danos morais, de outro; respectivamente, o verdadeiro e o próprio prejuízo econômico, e o sofrimento psíquico ou moral, as dores, etc.

A caracterização do dano extrapatrimonial tem sido deduzida na doutrina sob a forma negativa, na sua contraposição ao dano patrimonial, ou seja, “dano patrimonial é o dano que atinge o patrimônio do ofendido; dano não patrimonial é o que, só atingindo o devedor (sic) como ser humano, não lhe atinge o patrimônio”. (SILVA, 2012, p. 2)

Magalhães ainda afirma que os danos morais podem ser variados, mas os principais citados pela doutrina trazem prejuízo “à reputação, à integridade física, como o dano estético, ao direito moral do autor, ao direito de uma pessoa ao nome, às convicções de alguém, às pessoas que a vítima do dano tem afeto”, a exemplo da morte de um filho, “à integridade da inteligência, à segurança e tranquilidade, à honra, ao cônjuge por aquele que ocasionou o divórcio, à liberdade, aos sentimentos afetivos de qualquer espécie, ao crédito, etc”.

O dano moral também pode ser ressarcido em caráter coletivo, pois empresas têm sido condenadas a pagar indenização por danos morais coletivos, em ações civis públicas, ajuizadas pelo Ministério Público do Trabalho. Ações essas que estão relacionadas “ao meio ambiente do trabalho, ao trabalho análogo à condição de escravo, ao trabalho infantil, à discriminação de toda ordem (sexo, idade, raça, deficiência física), à revista íntima e à terceirização ilícita por meio de cooperativa de trabalho, entre outras”. (TARCITANO; GUIMARÃES, 2004)

A definição de pessoa pública apresentada por Alcides Leopoldo Silva Junior é bastante esclarecedora, porque conceitua pessoa pública como a que se “dedica à vida pública ou que a ela está ligada, ou exerce cargos políticos, ou cuja atuação dependa do sufrágio popular ou do reconhecimento das pessoas ou a elas é voltado, ainda que para entretenimento ou lazer”. (SILVA JUNIOR, 2012, p. 89) Tal reconhecimento público pode ter ou não objetivo de lucro ou eminentemente social. Nestas categorias estão incluídos vários perfis de pessoas: modelos como Gisele Bündchen; cantores como Roberto Carlos; políticos como Dilma Rousseff; atores como Murilo Benício ou Alinne Moraes; apresentadores como Sílvio Santos e Faustão; executivos como Maria das Graças Foster (ex-presidente da Petrobras) ou Bill Gates; Barac Obama.

Pessoa pública é aquela que, em determinado momento de sua carreira ou fato marcante de sua vida, passa a figurar com notoriedade perante aos meios de comunicação de massa como o futebolista Neymar ou mesmo em círculos mais restritos como o Ministro do STF Joaquim Barbosa. Essas personalidades “devido à sua atividade ou fatos marcantes de sua vida, passam a desfrutar de notoriedade, despertando a atenção generalizada do público, sofrendo uma limitação ao seu direito à vida privada”, segundo Garcia (2002, p. 228).

Tal reconhecimento pode ser a nível regional, nacional ou internacional, dependendo das atividades exercidas ou cargos ocupados pela pessoa pública.

As pessoas que não têm destaque e não possuem notoriedade podem ser consideradas pessoas privadas. Assim, toda pessoa pública tem sua notoriedade e assuntos que são relevantes à imprensa, no entanto, sua vida privada tem que ser preservada para não gerar danos morais e patrimoniais. Podemos classificar como pessoas públicas os atores e atrizes de cinema, novelas, teatro, circo; *socialites* que são pessoas que se destacam por suas fortunas, títulos honoríficos, executivos de

grandes corporações; esportistas (com destaque a futebolistas); modelos, políticos. (GARCIA, 2002)

Um caso ocorrido com pessoa pública que teve seus dados e arquivos pessoais vasculhados por um profissional da informática seguida de divulgação de fotos de sua intimidade na imprensa serviu para acelerar o processo de aprovação da Lei nº 12.737, de 30 de novembro de 2012 que dispõe sobre a tipificação criminal de delitos informáticos. A pessoa pública envolvida neste processo foi a atriz Carolina Dieckman, que teve 30 fotos publicadas na internet após a invasão de seu e-mail por *hackers* que exigiram o pagamento de um resgate no valor de R\$ 10.000,00 para retirar as fotos de circulação. Esta lei alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, conhecido como Código Penal, acrescentando-lhe os seguintes artigos, *in verbis*:

Art. 154- A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

A invasão de dispositivo informático danificou a imagem da atriz e acelerou a aprovação do novo texto do Código Penal para coibir e punir os crimes eletrônicos que burlam a segurança de computadores pessoais e de empresas com invasões que causam danos morais e patrimoniais.

Há uma verdade encartada em um ditado popular “A minha liberdade vai até onde começa a do outro” que pode servir de baliza na veiculação e uso da imagem sem a autorização. A punição ao uso indevido da imagem decorre da Constituição Federal que prevê a indenização por danos morais e materiais. (BRASIL, 1988)

Na medida em que as pessoas públicas extrapolam a esfera da vida privada e adentram no âmbito da coletividade, sua imagem passa a ser relativizada, o que não significa que as celebridades ou pessoas notórias não possam ter sua imagem violada, consequência da veiculação fora dos padrões éticos e morais, sem que atendam ao interesse da coletividade. No caso de pessoas públicas, a necessidade de autorização para veiculação da imagem sofre limitações, ou seja, é flexibilizada.

As disposições legais preceituam que a veiculação da imagem, excetuando os casos previstos em lei, necessita de autorização prévia dos titulares. Isso ocorre

até mesmo em escolas, quando os responsáveis assinam termo de cessão de imagem à instituição.

A era da informação exige que as lideranças adquiram uma nova competência, isto é, a capacidade de planejar e estimular a adesão da organização a uma maneira determinada num ritmo mais rápido para acompanhar as mudanças. As estratégias de conhecimento informacional tendem a exigir um tratamento das informações, de forma a organizar, transmitir e selecionar as informações a fim de satisfazer as necessidades da organização e de seus colaboradores. Segundo Santos (2006, p. 25), a estratégia tem como objetivo enfrentar com sucesso as forças competitivas.

De acordo com essa concepção, a principal função da adoção de uma política de tecnologia de informática deve ter como foco a simplificação dos procedimentos de Gestão Estratégica, concebido integralmente para atender as necessidades dos profissionais que atuam em funções críticas no processo de gerenciamento da inovação. Na visão de Valentim (2010, p. 20):

O tratamento da informação deve contemplar novas metodologias de análise, processamento e disseminação da informação, buscando futuras realidades sociais. A informação é complexa necessitando de equipes multidisciplinares para desenvolver os processos de análise da informação. O profissional da informação deve apreender a trabalhar em equipe, buscando qualidade de resposta às pesquisas solicitadas pelos usuários / clientes.

A gestão do conhecimento exige o uso adequado das informações para favorecer as vantagens estratégicas a partir de sua capacidade de mobilizar conhecimento, experiência e competências tecnológicas para criar novos produtos, processos e serviços.

A gestão da Informatização visa oferecer à empresa os recursos necessários à adoção das melhores práticas na estruturação das funções de Informática, melhor relacionamento com áreas usuárias, as melhores metodologias de desenvolvimento, os melhores planos de desenvolvimento dos projetos, com ou sem a utilização de serviços terceirizados e melhores processos. (VALENTIM, 2010)

A gestão da inovação tecnológica tendo como fio condutor a interação desta com a estratégia competitiva da empresa, seja ela industrial ou de serviços. A capacidade de inovar exige o desenvolvimento sistemático de competências e atividades que estão distribuídas entre distintas funções da organização. O uso de

estratégia permite o desenvolvimento de ações decisórias que favorece a identificação da informação adequada para a função de produção e de aprendizagem.

Este processo tem não só uma dimensão individual, mas também uma dimensão coletiva e interativa que pode designar-se por aprendizagem organizacional. Neste quadro, o papel e a crescente importância do fator humano na vida das organizações, tornam dificilmente dissociáveis, já que as mudanças qualitativas dependem das capacidades individuais e coletivas dos recursos humanos. (VALENTIM, 2010)

A formação passa a ser um componente essencial da gestão dos recursos humanos, no interior da organização. Através de uma estratégia de formação global, participada e interativa, é possível construir uma visão partilhada do futuro da organização, das suas finalidades, dos meios de ação, dos valores que lhe estão subjacentes.

A otimização do potencial formativo dos contextos de trabalho passa, em termos de formação, pela criação de dispositivos que facilitem a transformação das experiências vividas no cotidiano profissional em aprendizagens. Esse processo requer autoformação, marcado pela reflexão e a pesquisa, a nível individual e coletivo. Picchiali; Lopes e Oliveira (2007, p. 2) consideram que:

A gestão do conhecimento é um modelo adotado para promover a disseminação das melhores práticas, desenvolverem as habilidades dos empregados e ajudar as empresas a recrutarem e reterem talentos. Este modelo conta com ferramentas da tecnologia de informação tais como portais corporativos, e-mail, internet, fóruns de discussão entre outros, que visam à constante inovação baseada no capital intelectual.

Todas essas ferramentas que fazem parte integrante do modelo de implementação da gestão do conhecimento se constituem em um processo de articulação entre novos modos de organizar o trabalho e novos modos de organizar a formação (centrada no contexto organizacional) que facilita e torna possível a produção simultânea de mudanças individuais e coletivas.

A geração de conhecimento favorece a disseminação do fluxo de informação que se potencializa associada às experiências garantidas com a colaboração e a troca de informações. As comunidades de prática se articulam nas trocas de experiências como solução para a resolução de problemas. (PICCHIALI; LOPES; OLIVEIRA, 2007)

Ainda Bufrem (2010) analisa que a geração do conhecimento está interligada à tecnologia de informação e as formas de uso das informações. As empresas de um modo geral, principalmente as de maior porte, são depositárias de grande quantidade de informações, as quais alimentam seu processo decisório. No entanto, é comum que as informações se encontrem dispersas pelas diversas áreas que compõe a empresa. Assim, é relevante para a geração de conhecimentos, o compartilhamento das informações, por isso é essencial juntá-las, analisá-las e dar-lhes uma interpretação que contenha um caráter corporativo.

A tecnologia de informação trouxe inúmeras facilidades que estão sendo proporcionadas pelos avanços do conhecimento tanto em relação ao aumento da capacidade de armazenamento e processamento de dados que contém de informações, como em relação ao vertiginoso desenvolvimento das comunicações (Ex: Internet), que estão representando uma força no desenvolvimento dos sistemas de inteligência competitiva.

Nesse aspecto, o uso cada vez mais abrangente de metodologias para monitorar o ambiente de negócios e tomar decisões é cada vez mais complexo e exige ferramentas de apoio.

A gestão estratégica da informação que tem como objetivo permitir que os tomadores de decisão nas organizações se antecipem sobre as tendências dos mercados e a evolução da concorrência, a partir da detecção e avaliação de ameaças e oportunidades que se apresentem no seu ambiente interno e externo depende de dados informacionais. Portanto, o capital intelectual nas organizações depende da tecnologia de informação e comunicações para a definição de ações ofensivas e defensivas mais adaptadas às estratégias de desenvolvimento da empresa. (CARVALHO, 2010)

Desta forma, compreende-se que o processo sistemático de coleta, tratamento, análise e disseminação da informação sobre atividades dos concorrentes, tecnologias e tendências gerais dos negócios, visam principalmente subsidiar a tomada de decisão e atingir as metas estratégicas da empresa, como ferramenta para gestão da inovação tecnológica; como instrumento para tomada de decisão; e ainda como forma de agregar valor à função da informação como geradora de capital intelectual.

Os cientistas sociais, em sua maioria, comemoraram o advento da Internet no palco político como propiciadora de um acesso democrático aos cidadãos

comuns à vida política porque entendiam que seria uma maneira barata de realizarem uma ampla divulgação de sua imagem e ideologia.

A www (World Wide Web) e o e-mail permitiriam a criação de novos mecanismos de relacionamento entre as instituições públicas e os cidadãos, favorecendo a transparência na execução dos orçamentos públicos (acessíveis on-line), facilitando trâmites e reclamações relacionados a serviços, disponibilizando informação e sugerindo novas formas de organização dos serviços públicos. Mas, sobretudo, as novas tecnologias da comunicação abririam a possibilidade de uma nova forma de participação cidadã, horizontal, independente das grandes estruturas políticas e dos organismos de comunicação de massa — afinal, cada indivíduo poderia ter voz ativa na construção de um espaço de opinião pública realmente democrático. A internet seria particularmente relevante para o desenvolvimento da sociedade civil, pois permitiria a criação de redes flexíveis, a rápida mobilização para campanhas ad hoc e a distribuição de informação alternativa e facilitaria a criação de redes nacionais e internacionais de militantes não-filiados às estruturas políticas tradicionais. Negri e Hardt deram forma a uma visão revolucionária do papel da internet, que seria o novo espaço alternativo da multidão (conceito amplo e que se refere a todos os potenciais contestadores do poder do “Império”). (SORJ, 2006, p. 124)

A Internet é tida como uma ampla estrutura de rede democratizadora ramificada em ilimitados nós e interconexões que permite a comunicação sem um “ponto central de controle” [...]. (SORJ, 2006, p. 124) “Este modelo democrático é o que Deleuze e Guattari chamam de rizoma, uma estrutura de rede não-hierárquica e não-centralizada”, complementam os autores.

2.4 UMA ANÁLISE DOS PONTOS POSITIVOS E NEGATIVOS DA INTERNET

Para Sorj (2006), os especialistas da comunicação geralmente associam os efeitos potencialmente negativos da Internet à propagação ou atuação no âmbito do crime organizado ou para o terrorismo, mas é “crescente a preocupação com os esforços dos Estados autoritários de controlar o acesso aos conteúdos da internet, inclusive com o apoio ativo de grandes provedores de sistemas e sites de busca, como Cisco e Google”.

Entre essas nações, podem ser citadas Cuba, China e países com governos de orientação islâmica. Recentemente, a “luta contra o terror” tem levado também governos democráticos a aumentar o controle sobre os conteúdos que trafegam na rede. De forma crescente, começam a surgir trabalhos

questionando o papel potencialmente renovador dos novos meios de comunicação sobre a vida política. (SORJ, 2006, p. 125)

Cunha (2006) também aventa a possibilidade do cerceamento, por parte de governos totalitários e repressores da liberdade em nome de uma maior segurança na Internet por conta de crimes de pedofilia e terrorismo, principalmente; no entanto, o próprio formato da rede mundial impede grandes sanções à liberdade do tráfego de informações sobre os mais variados assuntos. Cabe dizer que o próprio internauta é que vai selecionar o que é bom para ele na Internet, pelo menos em países onde a democracia impera.

Fazendo referência ao paradoxo proporcionado pela comunicação em rede, Castells (2006: 227) afirma que o momento de eclosão das tecnologias de liberdade, em particular da internet, mas também do conjunto de tecnologias informáticas em rede, de telecomunicação de banda larga, comunicação móvel e de computação distribuída, é também, sob pretexto de terrorismo e pornografia, o momento da obsessão pela segurança. Se estabelece uma ameaça à liberdade de expressão, dentro e fora da internet, do controle dos Estados sobre a comunicação. Mas o autor também afirma que a arquitetura da internet foi desenhada deliberadamente para dificultar seu controle, mas não a vigilância da mensagem. Por isso, mesmo sofrendo cada vez mais interferências à livre comunicação, é o meio local-global mais livre que existe, permitindo descentralizar os meios de comunicação de massa. (CUNHA, 2006, p. 145)

Surgem correntes de pensadores que questionam os efeitos benéficos da Internet para a geração de leitores, quando afirmam que ela tende a formar leitores que só leem aquilo com que se identificam. “Uma primeira geração de trabalhos se sustentava numa perspectiva ‘tradicional’ do conceito de elo social, que só poderia se estabelecer efetivamente a partir do encontro físico entre as pessoas”, segundo Sorj (2006).

Para tais autores, a nova sociabilidade virtual desfaz as bases da interação cara a cara, destruindo a formação da ágora, corroendo o fundamento do espaço público e aumentando as possibilidades de controle da população pelo Estado. Na nova geração de trabalhos que procuram analisar os processos sociais em curso, ainda que com dados não-sistemáticos, sobressai o livro Republic.com, de Cass Sunstein. O autor argumenta que a internet poderá criar uma república de solipsistas, de pessoas que só querem acessar informações e argumentos com os quais possuem afinidade, evitando o debate de ideias característico do espaço público. (SORJ, 2006, p. 125)

A expansão dos usuários da Internet é um fenômeno substancialmente novo que irá ocupar o centro de interesse de intelectuais de uma ampla gama de áreas científicas, que englobam as sociológicas, as ligadas à Comunicação segura, às

áreas de comércio eletrônico, de entretenimento, de empresários de amplos setores, tais como o ramo educacional superior que encontrou na Internet um amplo nicho de mercado para chegar às longínquas regiões do país e de qualquer parte do mundo para oferecer os seus cursos EaD.

3 DESENVOLVIMENTO

Este capítulo apresenta dois aspectos principais da privacidade em dispositivos móveis, que são a invasão de privacidade e os aplicativos sociais baseados em localização, fazendo relação com a experiência do usuário dos dispositivos móveis e o impacto no dia a dia.

3.1 INVASÃO DE PRIVACIDADE

Atualmente, o consumidor deixa-se conhecer com mais facilidade e fornece seus perfis e preferências às empresas, mas no caso do rastreamento dos consumidores, são seus próprios comportamentos que fornecem informações às empresas. Os *softwares* instalados nos smartphones (com ou sem o consentimento do usuário) revelam seus interesses por frequentarem e delongarem-se em determinada seção de uma loja de departamentos ou ao frequentarem determinados bares, por exemplo.

Uma tecnologia recente permite às empresas terem acesso aos smartphones dos consumidores por determinadas regiões ou locais para enviar-lhes mensagens publicitárias, normalmente, contendo ofertas promocionais de modo a conduzi-lo à aquisição de algum produto específico. Vejamos um exemplo:

Na Inglaterra, a operadora de telefonia O2 fez uma parceria com a marca de bebidas alcoólicas Bulmers. A empresa instalou radares nas proximidades de mais de 1 000 bares no país, de modo a reconhecer quem passasse nas redondezas portando um smart-phone, e enviou automaticamente uma mensagem com uma oferta para comprar a bebida com desconto. (IKEDA, 2013, p. 3)

Neste caso específico, a iniciativa da Bulmers em parceria com a empresa de telefonia O2 inglesa surtiu bastante eficácia, pois 50% dos consumidores que receberam o anúncio clicaram nele e cerca de 25% adquiriu a bebida em promoção. (IKEDA, 2013)

O Belezuca é um aplicativo Android ou iOS para as pessoas que desejam acessar lojas virtuais ou frequentar lojas presenciais que tenham parceria com o

Belezuca, porque ao entrar em uma loja credenciada, o consumidor é detectado e passa a receber moedas virtuais que a partir do acúmulo de 250 poderão ser trocadas por produtos ou serviços; ao entrar em uma loja credenciada, o usuário já ganha 100 pontos, mas é a loja que detecta-o e oferece os pontos, sem a possibilidade do usuário optar por isso. O aplicativo brasileiro é um similar do Shopkick norte-americano. Um dos parceiros do Belezuca é a rede de lanchonetes Subway. (DARAYA, 2013)

A tabela 3 apresenta o logotipo do Belezuca bem como a explicação de sua aplicabilidade:


	<p>Ao entrar em uma loja parceira, você ganha pontos. Ao escanear o código de barras de um produto destacado no app, também. Ao visualizar catálogos e encontrar bônus que estão escondidos, mais ainda. E, assim, vai acumulando as suas moedas virtuais, as Belezucas, que podem ser trocadas por vales-compra, produtos e serviços.</p> <p>O visual é bonito, a interface é bem intuitiva e os usuários não devem ter problemas para utilizá-lo. No entanto, é importante destacar que, ao entrar em uma loja, não há como dar check-in. É o hardware instalado no estabelecimento que deve identificar a sua presença. Isso incomoda um pouco. Poderia haver uma opção de você marcar onde está.</p>
--	--

Tabela 3 – Belezuca é um aplicativo Android ou iOS
Fonte: Ikeda, 2013

O Shopkick³, que trabalha com as bandeiras Visa e MasterCard, tem os seguintes parceiros: Target, Macy's, Old Navy, Best Buy, American Eagle, Crate & Barrel, Sports Authority, Toys"R"Us, Simon Malls (largest U.S. mall operator), Procter & Gamble, Kraft Foods, Unilever, Coca-Cola, Intel, HP, Disney, General Mills, Colgate, Clorox, Revlon, Levi's.

A Toys "R" Us, empresa multinacional do ramo de brinquedos e eletrônicos criou por meio do roster Shopkick oportunidades para os consumidores arrecadarem cupons móveis, por meio de visitas ao *site* das lojas *online* para desfrutarem de promoções e ofertas em primeira mão. O acúmulo de cupons móveis por meio dos

³ O Shopkick foi fundada em junho de 2009 por Cyriac Roeding, Jeff Sellinger, Aaron Emigh, e é financiado pela Kleiner Perkins iFund, Greylock Partners e Reid Hoffman, fundador do LinkedIn e investidor no Facebook e Zynga, e Ron Conway. (SHOPKICK, 2013)

kicks (chute em português) leva o consumidor a adquirir produtos para acumular descontos correspondentes a 2 kicks por cada dólar gasto. A loja Toys “R” Us argumenta em suas chamadas publicitárias da seguinte maneira:

O crescimento explosivo de dispositivos de detecção de localização (por exemplo, dispositivos de GPS e dispositivos portáteis), juntamente com as comunicações sem fio e bancos de dados móveis resulta em desenvolver aplicativos baseados em localização que fornecem informações específicas para seus usuários com base em suas posições atuais. Alguns exemplos dessas aplicações incluem localizador da loja, relatórios de tráfego baseados em localização e publicidade baseada em localização. Embora os serviços baseados em localização prometam segurança e conveniência, eles ameaçam a privacidade e a segurança dos usuários de tais serviços ao exigir explicitamente que os usuários compartilhem informações de local privado com o serviço. Se um usuário quiser manter sua informação de localização privada, ela tem que desligar seu dispositivo de reconhecimento de local e, temporariamente, cancelar a assinatura do serviço. Estudos recentes mostram que tais preocupações com a privacidade – desde preocupações sobre spionagem de empregadores sobre o paradeiro dos seus trabalhadores a temores de rastreamento por potenciais assediadores – são um sério obstáculo para a adoção mais ampla de serviços baseados em localização. (MOKBEL, 2007)

3.1.1 O RASTREAMENTO E A PRIVACIDADE DAS PESSOAS

As expectativas de privacidade emergem do contexto mais amplo em que as pessoas vivem. É razoável supor que as pessoas soubessem que seus dispositivos móveis também são dispositivos de rastreamento. Os usuários com conhecimento de rede móvel provavelmente fazem tal suposição, mas não está claro se outros consumidores facilmente chegariam a tal conclusão. Na verdade, a resposta às notícias indica uma desconexão entre as expectativas de privacidade e realidade, devido a uma falta de transparência sobre as práticas de coleta de dados. (WHALEN, 2011)

Companhias de telefonia móvel têm interesse em manter seus clientes felizes, e algumas mudanças já foram lançadas para responder às preocupações de

privacidade, como a redução da quantidade de dados de localização armazenados localmente e proteger dados armazenados usando criptografia. É encorajador ver medidas concretas que estão sendo tomadas para melhorar as práticas de manipulação de dados móveis, no entanto, há questões mais amplas a considerar para criar um conjunto mais eficaz de proteção à privacidade do consumidor. Os usuários têm perguntas sobre o consentimento, em particular tendo em conta que os serviços de localização são muitas vezes ativado por padrão. Em um nível prático, há pouca disposição para que os usuários personalizem a quantidade de detalhes que eles fornecem para vários recursos de localização. Dado o valor dos dados de mobilidade para fins de vigilância, é importante considerar seriamente princípios de privacidade e como incorporá-los em dispositivos móveis e serviços baseados em localização. (WHALEN, 2011)

O internauta tem que estar consciente que todos os seus passos ou “cliques” são monitorados constantemente por lojas e anunciantes, pois eles sabem quais páginas são visitadas e as pesquisas são usadas para conhecer o comportamento do usuário para exibir anúncios direcionados e buscar, assim, alavancar vendas. Por exemplo: um internauta que consulte os preços de passagens de avião em algumas companhias aéreas vai passar a receber em sua tela os anúncios e promoções dos destinos que está pesquisando. Dessa forma, será motivado à compra das passagens até mesmo em momentos em que não seja a atividade que esteja realizando no computador. (FÁVERO, 2013)

Nas lojas físicas, o sistema de rastreamento tem a função de levar informações de ofertas e promoções aos portadores de dispositivos móveis com internet. A loja instala um sistema de rastreamento por meio de sensores que detectam e geram dados sobre os interesses dos clientes baseados no tempo que gasta em determinada seção ou em determinada prateleira ou gôndola específica. Dessa forma, o sistema dispara um SMS para o dispositivo móvel do cliente com as promoções referentes a determinado produto.

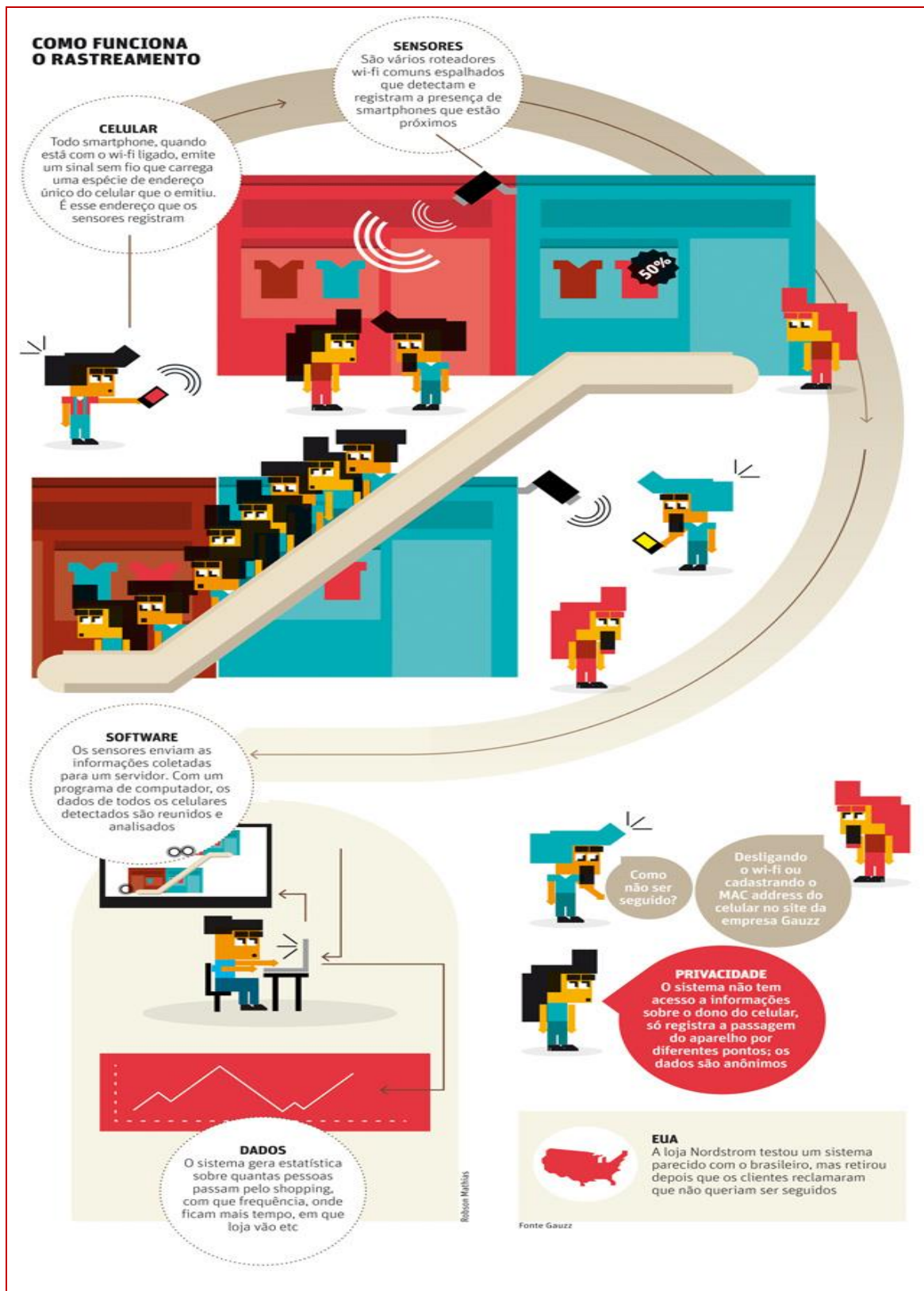
A start-up brasileira Gauzz quer dar o mesmo poder às lojas físicas tradicionais, implementando sensores que rastreiam por onde os clientes andam e o que fazem quando estão comprando.

O sistema usa sensores para registrar a passagem de qualquer smartphone que esteja com o receptor de wi-fi ligado mesmo que ele não esteja conectado a uma rede. (FÁVERO, 2013, p. 2)

Esse rastreamento tem sido objeto de discussão entre autoridades públicas, juristas e associações de consumidores que a veem como uma invasão de privacidade. Nos Estados Unidos, a rede varejista Nordstrom realizou inúmeros testes com um sistema similar que quando veio à tona foi muito criticado como invasão de privacidade. Os defensores do sistema de rastreamento argumentam que todos os dados gerados a partir dos comportamentos dos usuários são anônimos e visam gerar dados estatísticos para oferecer produtos e serviços ao consumidor. Defendem ainda que as informações capturadas referem-se a uma sequência numérica que identifica o aparelho, mas o proprietário do dispositivo móvel não é identificado e também não é essa a intenção dos rastreadores. (FÁVERO, 2013)

No Brasil, há um sistema de rastreamento sendo testado na cidade de Sorocaba/SP em um shopping center pela empresa Gauzz que quer oferecer aos lojistas a oportunidade de rastrear os potenciais consumidores avisando-os da existência desse tipo de rastreadores nas dependências ou cercanias da loja. Dessa forma, o cliente estará ciente da presença do rastreamento e poderá optar em desligar seu smartphone ou mantê-lo ligado para receber as promoções, ofertas e pontos referentes para serem acumulados, segundo Fávero (2013).

Figura 2 – Ilustração sobre o funcionamento do sistema de rastreamento



Fonte: Fávero, 2013

A legislação referente à segurança nos ambientes virtuais ainda está sendo construída no Brasil devido a ser um fenômeno recente e crescente. Quanto ao rastreamento realizado pelas lojas em busca de consumidores não há regulamentação legal, mas qualquer lesão aos direitos do consumidor encontra tutela no CDC (Código de Defesa do Consumidor), que, no entanto, encontra-se defasado por não abordar as novas tecnologias devido à sua elaboração ter sido em 1990.

Está em elaboração um Anteprojeto de Lei sobre Dados Pessoais (ALPDP) para regulamentar o setor das novas tecnologias e uso da Internet de modo a respeitar as boas práticas e punir as más. No entanto, sua redação ainda está sendo realizada sem previsão de finalização. Tal dispositivo é fruto de um trabalho conjunto entre da FGV (Fundação Getúlio Vargas) e do MJ (Ministério da Justiça), que se inspiraram em leis diversas de âmbito internacional (Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense, as quais são analisadas na sequência deste trabalho. (LIMA; MONTEIRO, 2013)

O Título I “Da Tutela dos Dados Pessoais”, em seu Capítulo I do Anteprojeto de Lei estabelece *in verbis*:

Art. 1º Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.

Art. 2º Toda pessoa tem direito à proteção de seus dados pessoais.

Art. 3º A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional por pessoa física ou jurídica de direito público ou privado, ainda que o banco de dados seja localizado no exterior. (BRASIL, 2013)

A intenção do legislador é demonstrar que os dados pessoais de uma pessoa são tutelados pelo princípio da Dignidade da Pessoa Humana já especificado no Art 5º da Constituição Federal de 1988. Neste sentido, os direitos do usuários são resguardados de forma que a invasão de sua privacidade incorreria em crime e passível de sanção.

A respeito do texto do anteprojeto citado, Lima e Monteiro (2013, p. 61) argumentam:

A proliferação de novas tecnologias e, principalmente, da Internet no país pressiona para a existência de marcos legais. Considerando-se que o objetivo do texto do Anteprojeto não é somente a proteção dos dados

personais, mas também o estabelecimento de um paradigma jurídico - que possa servir de sustentáculo para investimentos econômicos e desenvolvimento tecnológico - o dispositivo também poderia contemplar as proteções de ordem econômica e das relações de consumo que envolvem o cidadão.

Cuthbert e Wilkinson (2013)⁴ afirmam que a privacidade dos usuários é invadida por meio de seus próprios dispositivos móveis, de tal forma, que o rastreamento possibilitado pelos celulares é semelhante ao que o Governo pratica para localizar chamadas suspeitas ou pertencentes a suspeitos. As empresas de comunicação têm obrigação legal de entregar todos os dados das chamadas requisitadas pelo Poder Público. Neste sentido, a privacidade de todos é invadida de forma semelhante ao romance de George Orwell "1984" onde o Grande Irmão vê a todos e conhece seus pensamentos.

Gomes; Costa; Duarte (2009) apresentam algumas medidas de precaução para a utilização das redes sociais digitais sem correr riscos quanto aos ataques da engenharia social que não poupa nem organizações nem cidadãos comuns para aliciar informações sigilosas que podem ser aproveitadas para atividades criminosas contra o patrimônio de particulares e de organizações.

- Avaliar que informações podem ser públicas sem causar danos. Informar o endereço e a rotina não é uma atitude coerente, uma vez que pode deixar o usuário vulnerável a ataques.
- Verificar as opções de privacidade disponibilizadas pela rede, restringindo o acesso aos seus dados a determinadas pessoas ou grupos.
- Desconfiar de pessoas estranhas uma vez que nestas redes é relativamente fácil usar uma identidade falsa.
- Usar senhas que não sejam descobertas facilmente.
- Tomar conhecimento da política de privacidade do site. É importante saber se a rede disponibiliza suas informações a terceiros, como no caso da propaganda e dos aplicativos, falados anteriormente.

⁴ O projeto Snoopy foi criado para explorar exatamente isso e talvez seja um aviso de que não devemos somente com o maior/mais óbvio adversário da privacidade. O Snoopy é uma estrutura de rastreamento distribuído, interceptação de dados e geração de perfil. Ele foi criado com um orçamento apertado e tem sido concedido gratuitamente.

O Snoopy tem um modelo de cliente/servidor, com inúmeros "drones" implantados no campo coletando dados sobre os sinais de Wi-Fi emitidos pelos dispositivos nos seus bolsos. Todos esses dados são carregados em um servidor central para processamento. Um drone pode ser qualquer dispositivo baseado em Linux com um adaptador IEEE 802.11 compatível com injeção de pacote e alguma forma de conectividade com a Internet. Exemplos de dispositivos drones incluem o Nokia N900, o SheevaPlug e o RaspberryPi. (CUTHBERT; WILKINSON, 2013)

3.1.2 INVASÃO DA PRIVACIDADE VIA DISPOSITIVOS MÓVEIS

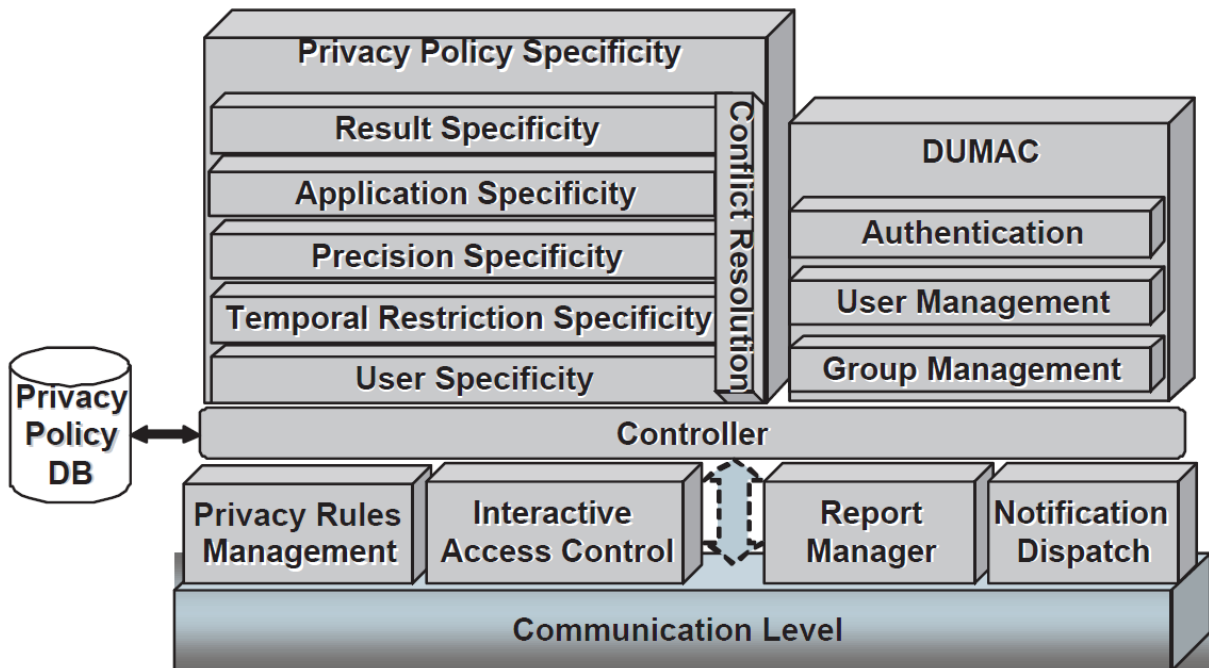
Em 2003, já temia-se a invasão de privacidade por meio de dispositivos móveis devido ao rápido desenvolvimento de tecnologias de posicionamento, que após cerca de duas décadas de campanha publicitária conseguiram fundir as tecnologias de computação às tecnologias de comunicação. Dessa fusão, surgiram telefones celulares habilitados para Java com a capacidade de executar uma série de poderosas aplicações, incluindo acesso à Internet móvel, ao passo que os notebooks passaram a se conectar com alta velocidade, utilizando banda larga *wireless* como recurso padrão. (SCHILIT; HONG; GRUTESER, 2003)

A questão ética ronda as operadoras de celular e outras empresas com relação à forma como iriam utilizar o recurso de localização dos usuários, pois a Lei de Proteção de Privacidade sem fio de 2003 propôs a alteração da Lei de Comunicações de 1934 com o intuito de exigir o consentimento do cliente para a prestação de informações sobre a localização de chamadas sem fio. (SCHILIT; HONG; GRUTESER, 2003)

3.1.3 MODELOS CONCEITUAIS E APLICATIVOS PARA ASSEGURAR PRIVACIDADE

Sacramento-Rodrigues (2006) desenvolveu um modelo conceitual para embasar o desenvolvimento do serviço de privacidade voltado a uma comunidade de usuários, discutindo determinados requisitos necessários a um projeto de tal envergadura. A maior parte dos requisitos delinearam o projeto e implementação do Context Privacy Service (CoPS). (Figura 3)

Figura 3 – Arquitetura geral do CoPS



Fonte: Sacramento-Rodrigues, 2006

A estrutura das regras de privacidade no CoPS é complexa e formada por distintos campos que se fazem presentes nos momentos de requisição de acesso ao contexto. “Toda regra de privacidade está associada a uma política de acesso padrão (e.g., Reservado, Liberal ou Sob-Demanda). Tal associação é feita pelo *Policy Maker* e determinará o funcionamento do algoritmo básico de avaliação para cada requisição”, segundo Sacramento-Rodrigues (2006, p. 61).

A Tabela 4 apresenta os campos das regras de privacidade no CoPS e respectivos:

{ <i>Policy Maker</i> : Usuário que define/configura a regra de privacidade (pode ou não ser o próprio <i>Subject</i>);
{ <i>Subject</i> : Usuário ou entidade cuja informação de contexto (e.g., localização) é controlada pela regra de privacidade;
{ <i>Requester</i> : Usuário ou componente de software que requisita acesso à informação de contexto do <i>Subject</i> ;
{ <i>Context Variable</i> : Informação de contexto requisitada pelo <i>Requester</i> (e.g., localização do <i>Subject</i>);
{ <i>Application</i> : Lista de nomes das aplicações que podem ser utilizadas pelo <i>Requester</i> para acessar a variável de contexto. O símbolo “coringa” “*” representa qualquer aplicação;
{ <i>Precision</i> : Especifica a precisão, ou granularidade, do valor da variável de contexto a ser divulgada (e.g., para informação de localização, este atributo poderia ter valores Prédio, Andar, Sala, etc.);
{ <i>Temporal Restriction</i> : Restrições de hora e data para divulgar a informação de contexto (e.g., dias da semana, das 9:00 às 14:00);

{ <i>Freshness</i> : Especifica quão recente deve ser a informação de contexto a ser divulgada para um dado Requester (e.g., revelar somente a localização inferida há 15 minutos atrás, ou revelar a localização corrente);
{ <i>Timestamp</i> : Registra o horário em que a regra de privacidade foi criada ou atualizada. Este campo é usado para resolver possíveis conflitos entre as regras com resultados contraditórios;
{ <i>AccessPolicy</i> : Representa a política de acesso (Reservado, Liberal ou Sob-Demanda) com a qual a regra de privacidade está associada;
{ <i>Policy Level</i> : Nível da hierarquia da regra de privacidade. O CoPS provê suporte às seguintes hierarquias: "Organization", "Individual" ou "Default" (com este grau de precedência);
{ <i>Result</i> : Resultado a ser aplicado à requisição de acesso à informação de contexto. Os possíveis valores são: "Not Available", "Ask Me", "Grant" e "Deny";
{ <i>Notify Me</i> : Tipo de notificação a ser enviada para o <i>Subject</i> quando uma requisição é avaliada pela regra. Por exemplo, "NoNotification", "E-Mail", "MSN" ou "SMS".

Tabela 4 – Regras de privacidade e seus significados – CoPS

Fonte: Sacramento-Rodrigues (2006, p. 61)

Mediante a crescente difusão de redes *wireless* IEEE 802.11 e mediante o avanço das técnicas de posicionamento baseadas na força de sinal de rádio frequência (RF) o desenvolvimento de aplicações e serviços sensíveis ao contexto e à localização (*Location Based Services*) se faz cada vez mais necessário. Com vistas à segurança quanto à privacidade do usuário, principalmente quanto à sua localização, pode-se explicar, da seguinte maneira, o projeto de Sacramento-Rodrigues (2006, p. 5):

Para auxiliar o desenvolvimento de aplicações sensíveis ao contexto, projetamos e implementamos alguns serviços que constituem o núcleo de uma arquitetura de provisão de contexto, chamada MoCA (*Mobile Collaboration Architecture*). Esses serviços implementam a coleta, o processamento e a difusão da informação de contexto através de interfaces de comunicação síncronas e baseadas em eventos. A MoCA serviu de base para o desenvolvimento da nossa pesquisa sobre privacidade na qual projetamos um serviço que auxilia o usuário no controle de privacidade das suas informações de contexto, em especial, da sua informação de localização.

Fiorini (2006) argumenta que as tecnologias de redes sem fio e os dispositivos móveis vêm se desenvolvendo, trazendo a roça o uso da Computação Móvel na área de negócios e pessoal. A mobilidade possibilita o acesso à informação rapidamente em qualquer lugar e a qualquer hora denominada "comunicação pervasiva". No entanto, a variabilidade dos protocolos exigidos pelas aplicações para a Computação Móvel dificulta a ampla comunicação. Assim, a

autora propôs uma arquitetura genérica de *software* para a disponibilização de uma aplicação web para dispositivos móveis, que pode ser assim entendida:

Essa arquitetura possibilita a uma aplicação web, do lado servidor, ser disponibilizada para a Computação Móvel, de forma a ser acessada por um cliente independente do tipo de dispositivo móvel, do sistema operacional (tanto dos servidores como dos dispositivos móveis), do protocolo de comunicação e da arquitetura de rede sem fio utilizada.

O principal componente dessa arquitetura é o Processador da Camada de Apresentação, que disponibiliza a informação de acordo com o dispositivo que a solicitou. Ele é baseado em XSLT (*Extensible Stylesheet Language Transformation*), que é a parte mais importante dos padrões XSL (*Extensible Stylesheet Language*) do W3C.

Com XSLT é possível transformar arquivos XML para qualquer linguagem de apresentação desejada, como HTML, WML, cHTML e XHTML. Isso é feito com a criação de *templates* específicos para cada linguagem de apresentação e para o tipo de dispositivo desejado, com a vantagem de que, além da transformação, é possível escolher quais são os elementos relevantes de serem visualizados de acordo com o tipo de dispositivo móvel e da aplicação em questão, basta que estes sejam especificados nos *templates*. (FIORINI, 2006, p. 6)

As tecnologias e serviços baseados em localização, ou seja, LBT (*Location-Based Technologies*) e LBS (*Localization Based Services*), respectivamente, surgiram em decorrência de pesquisas militares que foram desenvolvidas com o fito de conhecer a localização, exercer o controle, monitoramento e vigilância de pessoas, locais e objetos. (LEMOS, 2009)

Alguns autores vêm se preocupando com os perigos que convencionaram chamar de “internet das coisas”⁵ (KUITENBROUWER, 2006; Van KRANENBURG, 2008 *apud* LEMOS, 2009), porque há formas simplificadas de armazenar (em *databases*) e/ou disseminar informações pessoais, gerando vulnerabilidade e insegurança à privacidade por meio de câmeras de vigilância, redes *Bluetooth*, telefones celulares, *smartphones* e uso de etiquetas RFID (*radio frequency identification* – identificação por radiofrequência).

A computação ubíqua invade lugares transformando tudo e todos em fontes de dados. *Digital footprints* emanam de forma invisível, oferecendo informações desse *sujeito inseguro* como a forma mais sutil de vigilância na sociedade do controle. Os *pervasive environments* criam territórios informacionais e demandam *digital bubble* ou *virtual wall* para a proteção da

⁵ Internet das Coisas, um termo cunhado por Kevin Ashton, co-fundador do Centro de Auto-ID do MIT, quando ele e sua equipe criaram o sistema padrão de RFID e outros sensores. A Cisco Systems tem re-denominado esse movimento para Internet of Everything (Internet de Tudo), pois acredita que, eventualmente, tudo será conectado. Na verdade, a Cisco diz que já há mais coisas ligadas à Internet, hoje, do que pessoas no mundo. "Coisas que eram silenciosas agora têm uma voz [vontade]", acrescenta Dave Evans, "futurista-chefe da Cisco. (SIQUEIRA, 2011)

privacidade. Artistas e ativistas têm tensionado essas questões a partir do uso crítico das LBT e LBS. O termo *locative media* foi por eles criado para se diferenciarem de projetos comerciais. (LEMOS, 2009, p. 621)

Lemos (2009, p. 622) define mídias locativas “como a conjunção de LBS e LBT, como dispositivos, sensores e redes digitais (e os serviços a eles associados) que reagem ao contexto local”. A expressão⁶ “mídias locativas” foi criada por um grupo de artistas com o intuito de se diferenciarem dos projetos comerciais e para expor as ambiguidades implícitas nos conceitos de mobilidade, localização, espaço público, vigilância.

As mídias locativas e a internet das coisas colocam em risco a privacidade das pessoas por meio dos dispositivos móveis que dão acesso à localização e aos seus dados pessoais. (LEMOS, 2009)

Vigiando (controlando e monitorando) as mídias locativas ameaçam a vida privada e o anonimato. A privacidade pode ser definida como o controle e a posse de informações pessoais, bem como o uso que se faz posteriormente delas. Anonimato, por sua vez, implica na ausência de informação sobre um indivíduo e também ao controle sobre a coleta de informações pessoais. (LEMOS, 2009, p. 623)

A mídia digital, por outro lado, capacita as pessoas para controlar informações sobre si mesmas, protege as pessoas contra perturbações indesejáveis, ou o direito de estar sozinho; está relacionada com dignidade nas obrigações recíprocas de divulgação entre as partes; é também um agente regulador no sentido de que pode ser usada para equilibrar e verificar o poder daqueles capazes de recolher dados, segundo Lemos (2009).

Santos (2010) desenvolveu um modelo para o gerenciamento de confiança em dispositivos móveis por entender que a confiança é complexa e subjetiva, dificultando o estabelecimento de um padrão de confiança. Ao observar uma relação entre dois usuários, nota-se que o grau de confiança entre eles pode, comumente, não estar no mesmo nível, porque o usuário “A” pode ter mais ou menos confiança do que o usuário “B” tem nele. Os níveis de confiança influenciam na decisão de começar uma interação com determinado usuário; além do nível de confiança, o estabelecimento de interação entre as partes depende do contexto e do risco

⁶ A expressão foi proposta em 2003 por Karlis Kalnins e vários autores têm aderido à essa terminologia. Um dos pioneiros foi Russel (1999) propondo um manifesto em que dizia que, de agora em diante, o ciberespaço estaria “pingando” nas coisas: “*the internet has already started leaking into the real world*”. (LEMOS, 2009, p. 622)

envolvido. O modelo para o gerenciamento de confiança em dispositivos móveis de Santos (2010) possui as seguintes características:

Este modelo de confiança tem uma abordagem dinâmica, o que possibilita decrementar ou incrementar o grau de confiança de um agente em relação a outro, sem realizar consultas ao mesmo. Neste modelo existem dois tipos de contextos, o social e o transacional. Este modelo é autoajustável e para isso utiliza a troca de informações de confiança sobre agentes que estão presentes na população de uma rede composta de usuários, esta rede é chamada de contexto social. O contexto transacional é a rede composta por produtores e consumidores que têm a necessidade de interagir através de serviços. O contexto transacional utiliza as informações de confiança do contexto social para formar, disseminar e evoluir a confiança de agentes da rede. (SANTOS, 2010, p. 4)

O modelo de confiança elaborado por Santos (2010) prevê a criptografia de chave pública como forma de autenticar as informações de confiança de um agente (usuário), pois cada usuário possuiria um par de chaves pública e privada. O modelo foi composto sobre três componentes centrais: a disseminação da confiança, a formação da confiança e a evolução da confiança, como explica o idealizador:

Neste modelo um agente *A* é chamado de *trustor* se ele é quem irá dar o voto de confiança a um outro agente *B*, o qual recebe o nome de *trustee*. A obtenção de informações de confiança por agentes pode ser feita de duas maneiras, por experiências diretas ou por recomendações.

As experiências diretas ocorrem quando há uma interação entre os agentes interessados em colaborar, durante essa interação o modelo (framework) coleta o histórico de interações entre os agentes. As recomendações são indicações feitas por agentes que já tiveram uma interação com o agente o qual se deseja interagir. Essas recomendações são fornecidas por agentes que pertencem ao contexto social e dessa forma o componente de disseminação de confiança do modelo publica-as com o propósito de difundir a confiança deste agente no contexto social. A partir de então a informação de confiança é utilizada pelo componente de formação de confiança que irá predizer a credibilidade do agente *trustee*. Assumindo que ocorra uma interação entre um agente *A* e um agente *B* é necessário que *A* obtenha um feedback para assim inferir a credibilidade de *B* percebida por *A*. Isso será utilizado como um dado de entrada para o componente de evolução de confiança, que por sua vez, terá como objetivo atualizar as informações de confiança armazenadas no ambiente local do agente *A*. (SANTOS, 2010, p. 4)

Segundo Minch (2004), a busca consciente da localização é a capacidade de determinar a posição geográfica e corresponde a uma tecnologia emergente com benefícios significativos e implicações de privacidade importantes para usuários de dispositivos móveis, como telefones celulares e PDA. A localização é determinada internamente por um dispositivo ou externamente por sistemas e redes com as quais

o dispositivo interage, e as informações de localização resultante pode ser armazenada, usada e divulgada sob várias condições.

As informações sobre o local estão se tornando parte integrante de diferentes dispositivos móveis. Os serviços móveis atuais podem ser melhorados com características location-aware (busca consciente da localização), proporcionando ao usuário uma transição suave para os serviços sensíveis ao contexto. Os campos de aplicação potenciais podem ser encontrados em áreas como informações sobre viagens, compras, entretenimento, informações de eventos e diferentes profissões nômades ou móveis. (KAASINEN, 2003)

A adição de recursos de localização de sensibilização para a computação e dispositivos de comunicação certamente terá profundos impactos sociais e no âmbito dos negócios. A fim de colher corretamente os muitos benefícios possíveis, será necessário considerar cuidadosamente as implicações de privacidade da tecnologia e proporcionar as salvaguardas necessárias para proteger tanto os direitos das pessoas quanto facilitar a evolução ordenada de produtos e serviços habilitados para a privacidade. Minch (2004) sugere que as pesquisas necessárias em muitas áreas deveriam incluir:

- (1) Teorias de informações baseadas em localização e privacidade baseado em localização;
- (2) A capacidade técnica da própria location-awareness;
- (3) Aplicações no mercado comercial, setor governamental, e em outros lugares;
- (4) Os direitos normativos ou prescritivos de consumidores/utilizadores e responsabilidades;
- (5) A pesquisa empírica em consumo/attitudes de usuários, preocupações e preferências. (MINCH, 2004)

Um estudo realizado por Kaasinen (2003) concluiu por meio de entrevistas com usuários potenciais e das avaliações de usuários de alguns dos primeiros serviços de busca consciente da localização que as expectativas do usuário são altas; os usuários finlandeses, no momento das avaliações, confiavam nos atuais prestadores de serviços e nas políticas de mercado para as questões relacionadas com a proteção da privacidade. Isto constitui um bom ponto de partida para os serviços de busca consciente da localização.

Não ocorreu à maioria dos usuários de que eles poderiam ser localizados ao usar serviços de busca consciente de localização. Tal fato reveste de responsabilidade adicional os prestadores de serviços e os decisores políticos.

Os resultados do estudo de Kaasinen (2003) destacam a necessidade de serviços globais, em termos de cobertura geográfica, amplitude (número de serviços incluídos) e profundidade (informações suficientes sobre cada serviço individual). A seleção de conteúdos e opções devem cobrir as diferentes necessidades de usuários individuais e ao usuário deveria ser dada uma descrição realista da cobertura do serviço. A necessidade de informação atualizada é alta, pois os usuários podem obter informações estáticas de qualquer lugar antes de começar a sua jornada.

As necessidades do utilizador podem estar relacionadas com o passado, com o presente, ou local planejado e cada usuário pode ter preferências pessoais sobre o que ele precisa nas diferentes situações de uso. Os usuários precisam de cadeias de serviços sem ruptura que os assistam em todas suas atividades móveis, por exemplo, planejamento, busca de serviços, encontrar a rota, bem como visitar e armazenamento de informações.

Os resultados da avaliação apontam para a necessidade de utilização espontânea e ocasional. Os serviços devem ser fáceis de encontrar, e também facilitar a obtenção de uma visão geral sobre os serviços disponíveis, bem como a sua cobertura. (KAASINEN, 2003)

A disposição do usuário em estar participar ativamente não pode ser subestimada. Apesar dos usuários se beneficiarem de um serviço personalizado, que pode não estar pronto para definir um perfil separado para cada serviço e cada contexto de uso, os usuários podem querer participar da criação de conteúdo, ao invés de ser consumidores passivos de informação. (KAASINEN, 2003)

Em 2001, a maioria das transações de comércio eletrônico eram realizadas por usuários em locais fixos, utilizando estações de trabalho e computadores pessoais. No entanto, Ghosh; Swaminatha (2001) previam que em breve, uma parcela significativa do e-commerce seria realizada via dispositivos sem fio habilitados para a Internet, tais como telefones celulares e assistentes pessoais digitais. É essa a realidade que presenciamos atualmente.

Os dispositivos sem fio oferecem aos usuários mobilidade para pesquisar, comunicar e adquirir bens e serviços de qualquer lugar a qualquer momento, sem estar amarrado a determinada localização. Uma das principais aplicações sem fio é o acesso Web para recuperação de informações em tempo real, como previsão do

tempo, resultados esportivos, informação e reserva de voos, mapas de navegação e cotações de ações. (GHOSH; SWAMINATHA, 2001)

Embora muitos dos riscos da área de trabalho do comércio baseado na Internet permeiam o m-commerce, o m-commerce apresenta novos riscos. A natureza do meio exige um grau de confiança e cooperação entre os nós membros das redes que podem ser explorados por entidades maliciosas para negar o serviço, bem como recolher informações confidenciais e divulgar informações falsas. Além disso, as plataformas e linguagens sendo desenvolvidas para dispositivos sem fio não conseguiram adotar conceitos fundamentais de segurança empregados na atual geração de máquinas desktop. Os protocolos de comunicação criptografados são necessários para garantir a confidencialidade, integridade e serviços de autenticação para aplicações de m-commerce. Talvez o maior risco de links de comunicação criptografados, porém, seja a falsa sensação de segurança que eles fornecem aos usuários e fornecedores de m-commerce sem fio. Provavelmente, o risco mais significativo para os sistemas de m-commerce será mesmo o código malicioso que no início do século XXI penetrou nas redes sem fio. O código malicioso tem a capacidade de prejudicar outras tecnologias de segurança, como assinatura, autenticação e criptografia porque reside no dispositivo com todos os privilégios do proprietário. (GHOSH; SWAMINATHA, 2001)

Os riscos apresentados por scripts maliciosos móveis para dispositivos sem fio são significativos. Os fabricantes de dispositivos sem fio e desenvolvedores de linguagem têm ignorado lições aprendidas no que diz respeito aos riscos de segurança e privacidade do código móvel. O objetivo do estudo de Ghosh; Swaminatha (2001) foi destacar os principais riscos de segurança e de privacidade já aparentes nesses dispositivos e suas plataformas de linguagem a fim de influenciar fabricantes o dispositivo e a plataforma para construir sistemas mais robustos e seguros. (GHOSH; SWAMINATHA, 2001)

A melhor estratégia para lidar com os riscos de conteúdo baseado na Internet de segurança e privacidade é a construção de segurança na plataforma e aplicativos próprios, ao invés de tentar introduzir os patches de segurança mais tarde. Os fabricantes de dispositivos e desenvolvedores de linguagem para aplicações sem fio devem alavancar as décadas de progresso em modelos de sistemas operacionais seguros e proteger modelos de computação antes de ir para a frente com aplicações sem fio relacionadas com a privacidade de negócios

críticos. Caso contrário, estamos condenados a repetir os erros do passado, e, potencialmente, dar dois passos para trás à medida que avançamos um passo em frente. (GHOSH; SWAMINATHA, 2001)

3.1.3.1 O LOCSERV – SERVIÇO DE MIDDLEWARE

Um primeiro passo importante na proteção local da privacidade dos usuários é notificá-los dos pedidos de informações. Por exemplo, um sistema pode pedir aos usuários para autorizar liberação de suas informações de localização clicando em “OK” em uma caixa de diálogo para cada novo pedido. Tal sistema estaria em desacordo com a visão de Mark Weiser da *calm technology*. Weiser argumenta que para a tecnologia se tornar verdadeiramente onipresente, deve fundir-se de tal forma que ela se torne uma parte da vida cotidiana. Assim, o objetivo é minimizar a intromissão da tecnologia e as exigências dos utilizadores. (MYLES; FRIDAY; DAVIES, 2003)

Myles; Friday; Davies (2003) desenvolveram o LocServ para apoiar as diversas aplicações baseadas em localização desenvolvidas nos laboratórios da *University of Arizona* e da *Lancaster University*. O LocServ é um serviço de middleware, que se situa entre os aplicativos baseados em localização e as tecnologias de rastreamento de localização. Por tecnologias locationtracking unificadores, o LocServ permite que aplicativos baseados em localização usem vários sistemas de posicionamento.

Em essência, os usuários LocServ podem especificar uma consulta local, utilizando qualquer um dos modelos de localização simbólicos ou geométricos que o LocServ entende e o serviço pode resolver as consultas usando qualquer número de tecnologias subjacentes. Assim, o LocServ permite que aplicativos sejam escritos de uma forma que é totalmente independente da tecnologia de localização subjacente que eles usam. Tal serviço requer mecanismos para controlar o acesso a informações sobre a localização dos usuários sem a intervenção repetida do usuário. (MYLES; FRIDAY; DAVIES, 2003)

3.1.3.2 O SECURITY-ENHANCED LINUX (SELINUX) PARA SEGURANÇA NOS SMARTPHONES

Segundo Shabtai; Fledel; Elovici (2010), o Framework Android da Google incorpora uma grande parte do sistema operacional e do software para dispositivos móveis. Usar um sistema operacional de propósito geral, como o Linux em dispositivos móveis tem vantagens, mas também riscos de segurança. O Security-Enhanced Linux (SELinux) pode ajudar a reduzir os danos potenciais de um ataque bem-sucedido.

Os *smartphones*, em geral, foram projetados como abertos, como dispositivos de rede programáveis que podem fornecer diversos serviços do tipo PC, tais como mensagens, e-mail e navegação na web. Como tal, eles são vulneráveis a ataques que podem comprometer a confidencialidade, integridade e disponibilidade de dados e serviços. Vetores de ataque de propagação de *malwares* em smartphones incluem redes de celular, Bluetooth, Internet (via Wi-Fi, General Packet Radio Service Enhanced taxas de dados para GSM Evolution, ou de acesso à rede 3G), USB e outros periféricos. Mecanismos de segurança para telefones móveis, tais como *antimalware* e *antispam software*, ferramentas de detecção de intrusão baseados em *host*, e firewalls estão disponíveis, embora a maioria dos proprietários de telefone celular não consideram *smartphones* como computadores regulares e raramente executam qualquer uma destas soluções de segurança. (SHABTAI; FLEDEL; ELOVICI, 2010)

3.1.3.3 SEGURANÇA NO ANDROID

O Linux fornece vários mecanismos de controle de acesso. O elemento básico desses mecanismos são os usuários (ou seja, entidades). Usuários (representado por um número inteiro ou ID de usuário) objetos próprios (um processo, um arquivo ou diretório). Os usuários são ainda atribuídos a grupos.

No mecanismo de permissões de arquivos Linux, cada arquivo é associado a um usuário proprietário e IDs de grupo e três tuplas⁷: ler, gravar e executar permissões (rwx). O kernel impõe a primeira tupla sobre o proprietário, o segundo em usuários que pertencem ao grupo, e o terceiro sobre os restantes utilizadores. Os arquivos no Android (ambos os arquivos de sistema e aplicação) estão sujeitos ao mecanismo de permissão Linux. Geralmente, os arquivos de sistema no Android são de propriedade do sistema ou usuário root, e arquivos do aplicativo são de propriedade de um usuário específico do aplicativo. Os usuários separados para cada aplicação e para os arquivos de sistema e permissões adequadas fornecem a segurança necessária para o acesso ao arquivo. Os arquivos criados por um aplicativo não serão acessíveis a outros aplicativos (a menos que explicitamente especificados). (SHABTAI; FLEDEL; ELOVICI, 2010)

3.1.3.4 USANDO SELINUX NO ANDROID

Shabtai; Fledel; Elovici (2010) apresentaram vários cenários que demonstram a utilidade do SELinux no Android; nesses cenários, assume-se uma vulnerabilidade existente no Android e demonstra como o SELinux reduziria os danos que poderiam causar quando fosse explorado, prolongando assim o período de tempo disponível para corrigir adequadamente a vulnerabilidade.

3.2 APLICATIVOS SOCIAIS BASEADOS EM LOCALIZAÇÃO (LBSAS)

Os aplicativos sociais baseados em localização (LBSAs) contam com as coordenadas de localização dos usuários para fornecer serviços. Hoje, *smartphones* usando essas aplicações agem como simples clientes e enviam localizações de usuários para servidores de terceiros não confiáveis. Esses servidores têm a lógica

⁷ Em matemática, uma tupla é uma lista ordenada de elementos, como por exemplo: (100,200,300,400). Porém, em teoria de banco de dados, essa definição é mais abrangente. Em banco de dados, significa uma função que mapeia nomes a valores respectivos, portanto os elementos podem vir em qualquer ordem, já que eles têm um nome associado a eles. Exemplo: (instrumento: "guitarra", cordas: 6)

do aplicativo para fornecer o serviço e para coletar grandes quantidades de informação de localização do usuário ao longo do tempo. Puttaswamy; Zhao (2010) defendem que as LBSAs devem adaptar-se a uma abordagem em que os servidores de terceiros não confiáveis sejam tratados simplesmente como armazenamentos de dados criptografados, e a funcionalidade do aplicativo ser movida para os dispositivos do cliente.

As coordenadas de localização são criptografadas, quando compartilhadas, e podem ser decifrada apenas pelos usuários ao quais os dados são destinados. Esta abordagem melhora significativamente a privacidade da localização do usuário. Argumenta-se que essa abordagem não só melhora a privacidade, mas também é flexível o suficiente para suportar uma ampla variedade de aplicativos baseados em localização usados hoje. Puttaswamy; Zhao (2010) realizaram um estudo para identificar os blocos de construção essenciais necessários para construir as aplicações em determinada abordagem; os autores exemplificam e ilustram como usar os blocos de construção através da construção de várias aplicações e delineiam as propriedades de privacidade fornecidos por esta abordagem. Assim, é apresentada uma abordagem que oferece um *design* alternativo prático para LBSAs que pode ser implantado com os seguintes objetivos:

- (a) O projeto deve preservar a localização e a privacidade dos usuários, enquanto os usuários usam as aplicações. Para preservar a privacidade, todos os dados compartilhados no projeto são criptografados, e somente os amigos do usuário serão capazes de descriptografar os dados de um usuário (localização);
- (b) O projeto deve ser flexível para suportar uma variedade de aplicativos sociais baseados em localização. A flexibilidade é demonstrada através do projeto proposto para esboçar a implementação de vários tipos diferentes de aplicativos baseados em localização.
- (c) O principal objetivo é manter o *design* simples e prático para estimular a sua adaptação. A criptografia simétrica foi amplamente utilizada para manter a sobrecarga sobre os celulares de baixa, e expor as interfaces *hashtable-like* simples usando o sistema fácil para programadores;
- (d) O projeto deve ter baixa implantação de sobrecarga e ser destacável hoje. Para facilitar a implantação, o projeto deve ser mantido de

acordo com os serviços de armazenamento e computação fornecidos por instalações de computação em nuvem já existentes de forma a aproveitar esses serviços em nuvem para construir LBSAs escaláveis rapidamente.

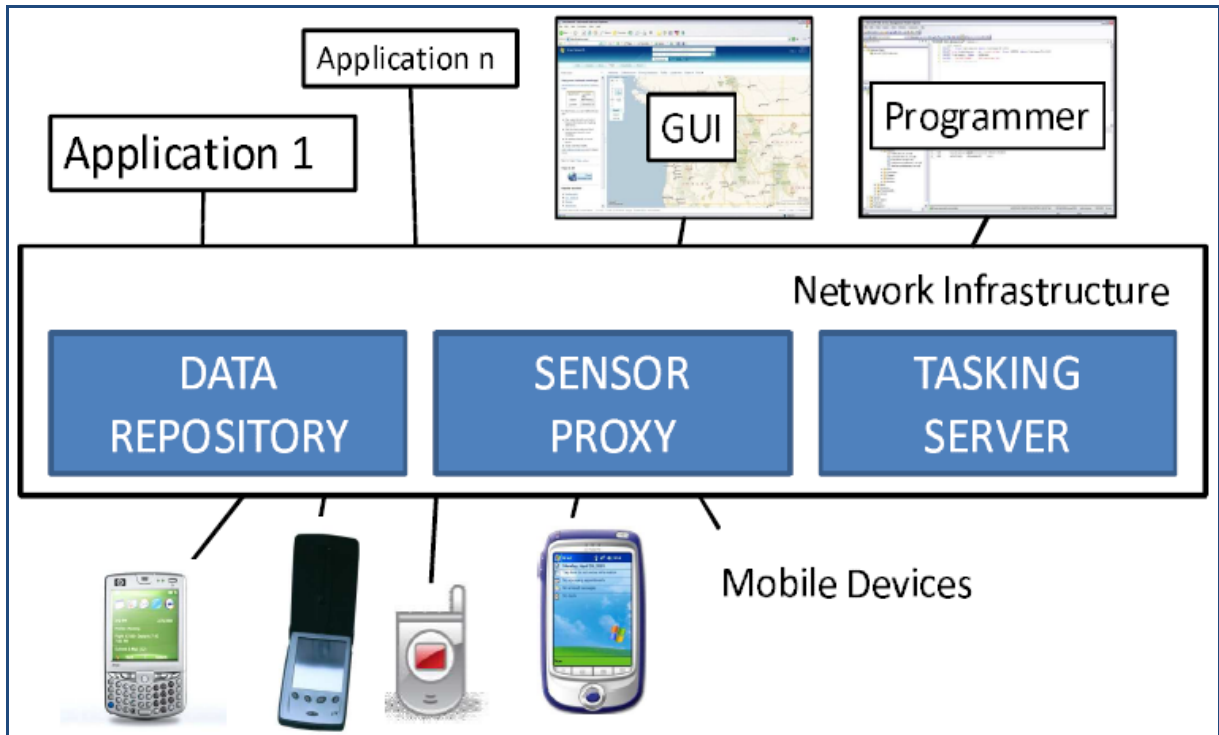
Os telefones móveis têm dois sensores: uma câmera e um microfone. A natureza generalizada e onipresente⁸ de telefones celulares em todo o mundo torna atraente para construir uma rede de sensores em larga escala, utilizando os telefones como os seus nós sensores. (KANSAL; GORACZKO; ZHAO, 2007)

O sistema apresentado na Figura 4 é composto pelas seguintes entidades-chave:

1. Sensores: dispositivos móveis que detectam o mundo físico;
2. Infraestrutura de rede: este sistema inclui um repositório de dados que armazena todos os dados de sensores fornecidos pelos dispositivos móveis;
3. Usuários: os aplicativos que acessam essa rede de sensores compartilhada ou usuários humanos que acessam os dados do sensor através de uma interface gráfica do usuário.

⁸ Computação Ubíqua ou Pervasiva refere-se a ambientes saturados de dispositivos computacionais e redes de comunicação sem fio, que se integram naturalmente à atividade humana. (AUGUSTIN; FERREIRA; YAMIN, 2008)

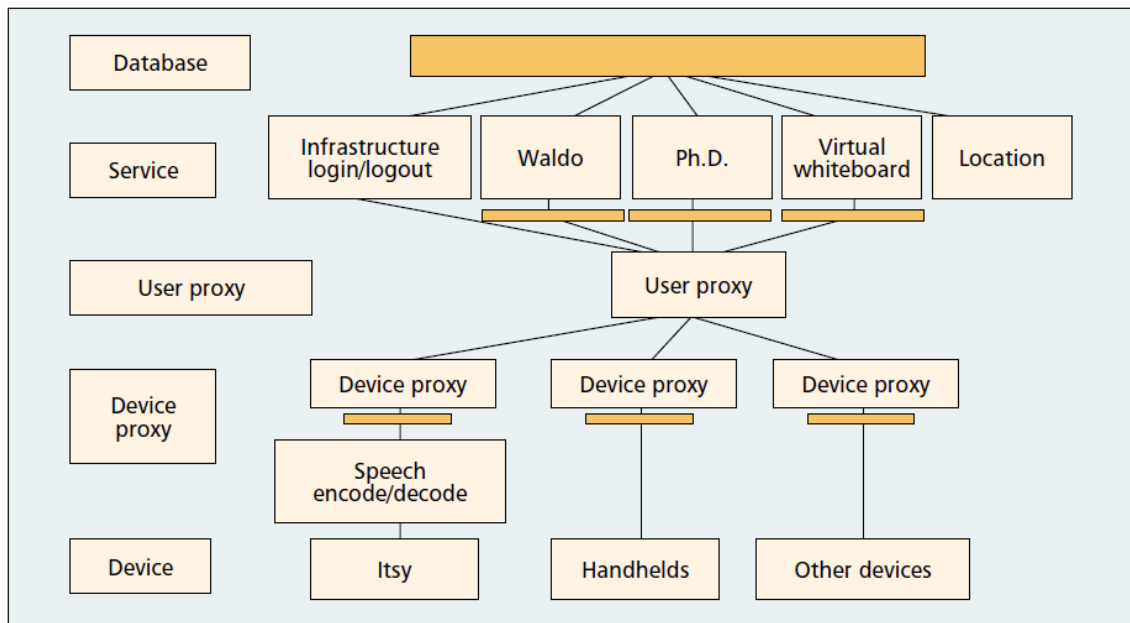
Figura 4 – Rede de sensores compartilhada de telefones celulares



Fonte: Kansal; Goraczko; Zhao (2007, p. 547)

Apresentamos uma primeira tentativa no sentido de compreender e perceber uma rede de sensores programável que usa a grande base implantada de dispositivos móveis como sua infraestrutura de detecção. (Figura 4) Vários desafios precisam ser abordados na construção de um sistema deste tipo. O protótipo demonstra escolhas iniciais do projeto na solução de alguns desses desafios e ajuda a revelar problemas relacionados. (KANSAL; GORACZKO; ZHAO, 2007)

Figura 5 – Handy Andy arquitetura de computação pervasiva



Fonte: Smailagic; Kogan (2002, p. 11)

A maioria dos aplicativos para posição de rastreamento interno lida com direções como aplicável a pessoas a pé. Isso significa que vários metros de erro são aceitáveis. (SMAILAGIC; KOGAN, 2002)

Com a proliferação e ampla adoção da telefonia móvel e de dados, os provedores de serviços estão ansiosos para explorar as informações dos clientes que adquiriram ao longo do tempo. A localização do usuário tem sido tradicionalmente difícil de identificar e utilizar devido ao seu dinamismo e imprevisibilidade inerente a localização do cliente no espaço físico. Com pressões regulatórias e implementação de novas tecnologias integradas em dispositivos móveis leves e terminais, apontar o local está rapidamente se tornando uma ciência exata. As operadoras estão sendo forçadas pelos reguladores para posicionar precisamente chamadas de emergência sem fio, por meio do nº 911 nos EUA, e do nº 112 na União Europeia. (RAO; MINAKAKIS, 2003)

3.2.1 SISTEMA ECALL PARA A UNIÃO EUROPEIA

Os serviços baseados em localização emergiram no princípio do século XXI prometendo ser a próxima killer APP (aplicação arrasadora) em dispositivos sem fio

peçoais, mas com eles surgiram as dificuldades de garantir privacidade quanto à localização. Neste sentido, pesaram mais os argumentos por uma melhor segurança pública em detrimento da privacidade quanto à localização dos usuários que ficaram expostos aos maus usuários desses aplicativos, que visam atividades criminosas e/ou antiéticas. (SCHILIT; HONG; GRUTESER, 2003)

Hoje, quando uma pessoa relata uma situação de emergência discando 911 nos Estados Unidos ou 112 na Europa, o sistema exibe o número de telefone do chamador e endereço para o despachante. A *Federal Communications Commission* dos EUA determinou que até Dezembro de 2005, todas as operadoras de celular seriam capazes de identificar a localização das chamadas de emergência para dentro de 50 a 100 metros por meio da plataforma “www.fcc.gov/911/enhanced”. Em julho de 2003, a Comissão Europeia recomendou a implementação rápida de uma capacidade de localização semelhante ao serviço 112. (SCHILIT; HONG; GRUTESER, 2003)

Os países da União Europeia têm grandes problemas de trânsito nas rodovias, apesar de ter qualidade na pavimentação, chegando na época das férias, principalmente, a um grande número de acidentes de trânsito. A média anual de mortes no trânsito chega a 30 mil e a 1,5 milhões de feridos. Dessa forma, são muitas as propostas de aproveitamento de novas tecnologias para assegurar maior qualidade no trânsito com maior segurança para os condutores. (CIENTISTAS, 2012)

Em 2012, foi desenvolvido um sistema de acionamento automático de unidades de socorro para agilizar o atendimento de vítimas de acidentes de trânsito no sentido de diminuir o tempo de resposta a um chamado de socorro ao Corpo de Bombeiros, Polícia e outras instituições que cuidam da segurança e do atendimento aos acidentados, que consiste no sistema eCall, no qual os carros são equipados com o sistema que permite uma chamada manual ou automática à central 112 (Emergência) em todos os países da União Europeia. Um aparelho é colocado no interior dos automóveis para que o motorista que presencie um acidente, acione por um simples toque de botão à central de emergência e, enquanto sua chamada é atendida, o sistema faz a localização exata da ocorrência por GPS e aciona automaticamente as equipes de socorro mais próximas, reduzindo em até metade do tempo de resposta aos atendimentos.

O Automóvel Clube Croata dá assistência técnica e informação de trânsito aos condutores. O sistema deve ser capaz de prever engarrafamentos e passar por cima das barreiras linguísticas, sobretudo em países como a Croácia, visitada por muitos turistas que não falam a língua.

Os engenheiros estão trabalhar num sistema pan-europeu, que vai permitir realizar as chamadas, independentemente do país. Os fabricantes de automóveis vão poder integrar este sistema de forma a acionar a chamada de emergência ao mesmo tempo que os airbags, em caso de acidente. (CIENTISTAS, 2012, p. 2)

A previsão é que em 2015 toda a União Europeia seja dotada de um sistema desses de forma integrada de modo que todas as barreiras linguísticas sejam ultrapassadas e toda a UE esteja integrada em um sistema eficiente de atendimento rápido às vítimas de acidentes de trânsito e espera-se que o uso do equipamento seja obrigatório, tendo para isso que os automóveis saiam de fábrica com o equipamento instalado.

Os novos modelos de veículos ligeiros e comerciais vendidos na UE terão de estar equipados com o sistema eCall a partir de 31 de março de 2018, estipula um regulamento hoje aprovado pelo Parlamento Europeu. A implantação deste sistema a bordo de veículos com base no número 112 visa reduzir a mortalidade nas estradas europeias e garantir uma melhor assistência às vítimas de acidentes rodoviários. (ECALL, 2015)

Em 2015, o Parlamento Europeu aprovou a implantação do sistema eCall em todo seu território, obrigando as fábricas/montadoras a soltarem todos os carros novos já equipados com o eCall a partir do ano de 2018.

3.2.2 O CRESCIMENTO DE LBS (SERVIÇOS BASEADOS EM LOCALIZAÇÃO)

As tecnologias ágeis como GPS, técnicas de identificação de telefone celular móvel, e triangulação de rede permitem que as operadoras possam ampliar ainda mais a atividade do cliente em um local físico estritamente definido. Estes serviços baseados em localização (doravante referidas como LBS) têm, portanto, surgido como um importante componente da estratégia m-commerce. A base de assinantes LBS era de cerca de 680 milhões de clientes a nível mundial em 2006, gerando mais de US \$ 32 bilhões na Europa. As inúmeras empresas já surgiram para aproveitar esta oportunidade de crescimento. A LBS pode ser uma nova fonte de oportunidade de receita para vários intervenientes na cadeia de valor móvel. A vantagem

competitiva reverterá a favor aos fornecedores de LBS que se concentram em experiências de clientes superiores, distintos, seguros e serviços de alta qualidade, e marca. (WEE, 2011)

3.2.3 WAZE

Waze é uma aplicação para smartphones ou dispositivos móveis similares baseada na navegação por satélite que disponibiliza informações em tempo real sobre usuários e detalhes sobre rotas, dependendo da localização do dispositivo portátil na rede e a interação de seus usuário com o serviço.

Corroborando o sucesso e o crescimento dos LBS o Waze ganhou o prêmio de melhor aplicativo portátil de 2013 no Congresso Mundial de Portáteis.

O Waze foge do conceito de navegador GPS tradicional pois é uma aplicativo-comunidade de direção que fornece dados complementares do mapa e outras informações de tráfego dos usuários. Como outro software de GPS, ele aprende conforme os usuários dirigem para fornecer rotas e atualizações de tráfego em tempo real. As pessoas podem relatar acidentes, congestionamentos, velocidade armadilhas policiais, e podem atualizar rodovias, pontos de referência, números de casas, etc.

Através do aplicativo, o usuário passa a colaborar involuntariamente com o sistema, transmitindo informações à sua velocidade de deslocamento, que em conjunto compõem as informações sobre o trânsito que são disponibilizadas a todos os usuários. Além disso, a colaboração ativa dos usuários, governo e outras entidades, permite que sejam disponibilizadas informações de bloqueios, acidentes, patrulhamento, etc. Diante das condições das vias, o sistema oferece automaticamente rotas em melhores condições. (ANÁLISE, 2015, p. 6)

O próprio slogan do aplicativo: “WAZE. DERROTANDO O TRÂNSITO, JUNTOS.” seduz o usuário para que ele utilize o serviço e não se preocupe com a disponibilização de suas informações em prol de um bem maior, utilizando o senso comum de que o trânsito é um dos vilões da vida moderna. Isso não é um problema apenas tira o foco do usuário em entender que suas informações e localização serão utilizadas e que com isso existe, ainda que mínimo, a possibilidade de ser utilizada para outras finalidades caso interceptada, divulgada ou ainda disponibilizada aos parceiros do aplicativos.

Alguns defensores da segurança nas estradas relataram o conceito da expectativa de mais motoristas usando o Waze, cujos falas de seu potencial de distrai-los com uma agitação de ícones e notificações e os põe em grande risco de um acidente. Uma tentativa de hackeamento foi feita com êxito por estudantes israelenses do Instituto de Tecnologia de Israel para falsificar um congestionamento mostrando que existe vulnerabilidade e brechas que podem ser utilizadas por pessoas mal intencionadas.

4 CONSIDERAÇÕES FINAIS

As operadoras brasileiras adotaram a Terceira Geração de Tecnologias – 3G, tanto para a Telefonia Móvel quanto para Banda Larga e estão caminhando para o pleno funcionamento da 4G, tecnologias essas que permitiram a popularização e a ampla utilização da Internet nos lares brasileiros e em equipamentos móveis como *notebooks*, *tablets*, telefones celulares.

A disseminação de tecnologias da comunicação tem possibilitado o aumento da utilização de dispositivos móveis para uso pessoal ou empresarial. O m-commerce já é uma realidade presente na sociedade brasileira e a segurança surge como elemento essencial para o maior uso dessas plataformas.

Neste trabalho, apresentamos alguns questionamentos sobre a invasão de privacidade por meio dos dispositivos móveis que podem gerar grandes prejuízos financeiros e morais aos usuários, que muitas vezes sequer sabem que seus equipamentos móveis podem ser localizados facilmente por meio de sistemas de busca consciente de localização ou não buscam saber pelo simples fato das condições de utilização dos aplicativos estarem nos famosos termos de utilização em sua maioria extensos e que são ignorados pelas usuários.

Essa questão é bastante polêmica porque todas as chamadas de emergência para o 911 nos EUA e para o 112 na Europa são rapidamente localizadas pelas autoridades da saúde e segurança pública. O cidadão pode ter sua privacidade invadida por meio de sua localização ou acesso aos seus dados pessoais armazenados na memória dos equipamentos, ainda que esse acesso seja para usar as informações para um rápido atendimento de emergências.

Mesmo seus hábitos e gostos podem ser rastreados por lojas que lhes enviam publicidade dirigida muitas vezes com o aval do usuário porém sem o seu real consentimento, principalmente evidenciando que cada vez menos as pessoas tem disponibilidade de ler longos termos de aceitação disponibilizados pelos aplicativos, no momento da instalação o usuário quer logo utilizar o serviço e concorda sem ler tais termos.

Conforme apresentamos as informações podem ser repassadas inconscientemente pelos aplicativos que seduzem os usuários com uma excelente propaganda sobre seus serviços disponibilizados.

Os números referentes aos utilizadores de aparelhos celulares ativos no Brasil dão conta de que são superiores à população brasileira. Tal fenômeno é semelhante ao que vem ocorrendo pelo mundo.

Como objetivo geral deste estudo tínhamos como proposta analisar a privacidade na internet via dispositivos móveis e a possível invasão dessa privacidade. Nos objetivos específicos a principal vertente foi investigar sobre o uso da localização via dispositivos móveis e sua implicação na privacidade.

Como resultados dos objetivos indentificamos que a utilização da internet via dispositivos móveis é uma realidade e a tendência é que o usuário resolva tudo via esses dispositivos, apenas fica a dúvida:

O usuário está consciente que pode sofrer a violação de sua privacidade mesmo que velada, uma vez que pode aceitar políticas de privacidade sem a leitura adequada devido a correria do dia a dia?

Como proposta para trabalhos futuros podemos realizar uma pesquisa com usuários de dispositivos móveis para identificar qual o percentual desses usuários realiza a leitura das políticas de privacidade antes de instalar aplicativos para os seus dispositivos móveis.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVARENGA, Rúbia Zanotelli de. Direitos da Personalidade do Trabalhador e Correio Eletrônico. **Correio Eletrônico**. Revista Eletrônica. Junho de 2013. Disponível em: <https://juslaboris.tst.jus.br/bitstream/handle/1939/95926/2013_alvarenga_rubia_direitos_personalidade.pdf?sequence=1>. Acesso em: 28 Out. 2017.

ALVES, Cássio Bastos. **Segurança da Informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima**. Brasília: UDF, 2010. 63p.

ANÁLISE da interação do Waze nas condições do trânsito na cidade de São Paulo. 10/11/2015. Disponível em: <<https://singep.org.br/4singep/resultado/246.pdf/>> Acesso em: 03 Out. 2017.

ANDRADE, Danubia; CUNHA, Jane de Souza. **Engenharia Social e a Vulnerabilidade Humana**. Trabalho de Conclusão (Graduação em Redes de Computadores). Goiânia/GO: Faculdade Estácio de Sá de Goiás, 2008. 56p.

ANDRADE, Maria Margarida de. **Introdução à metodologia do trabalho científico**. 7. ed. São Paulo: Atlas, 2011.

AUGUSTIN, Iara; FERREIRA, Giuliano Pereira; YAMIN, Adenauer. Grade Computacional como Infra-Estrutura para a Computação Pervasiva/Ubíqua. **ERAD 2008** — Santa Cruz do Sul, 11 a 14 de março de 2008. pp. 77-118.

BRASIL. **AnteProjeto de Lei sobre Dados Pessoais (ALPDP)**. 2013. Disponível em: <<http://www.acessoainformacao.gov.br/central-de-conteudo/infograficos/arquivos/recursos-passo-a-passo/anteprojeto-lei-protecao-dados-pessoais.pdf/view>>. Acesso em: 1 Jun. 2017.

BUFREM, Leilah Santiago. Levantando significações para significantes: Da gestão do conhecimento a organização do saber. **Enc. Bibli: R. Eletr. Bibliotecon. Ci. Inf.** Florianópolis, nº 01, 1º Semestre de 2010.

BURMANN, Marcia Sanz. **A concretização da privacidade do empregado no ambiente de trabalho**. 2011. Dissertação (Mestrado em Direito do Trabalho) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. doi:10.11606/D.2.2011.tde-03092012-144208. Acesso em: 2017-11-28.

CÂMARA, Paulo Ricardo Matos. **Segurança dos dados nas empresas: problemas e soluções**. Dissertação (Especialização em Redes de Computadores). Vila Velha/ES: ESAB, 2010. 65p.

CANONGIA, Claudia; MANDARINO, Raphael. **Segurança cibernética: o desafio da nova Sociedade da Informação**. Parc. Estrat. Brasília-DF. v. 14. n. 29. p. 21-46. jul-dez. 2009.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. Dissertação de Mestrado em Engenharia de Sistemas e Computação. Rio de Janeiro: COPPE/UFRJ, 2010. 239p.

CAVALCANTI JR., Reinaldo Leopoldino. **Engenharia Social nas Redes Sociais**. Monografia (Especialização em Desenvolvimento de Sistemas para Web). Maringá-PR: Universidade Estadual de Maringá. 2011. 48p.

CIENTISTAS tornam estrada mais segura. 26/07/12. Disponível em: <<http://pt.euronews.com/2012/07/26/cientistas-tornam-estrada-mais-segura/>>. Acesso em: 18 Jun. 2017.

CUNHA, M.R. Campanhas políticas e tecnologias digitais. pp. 143-156. In FIGUEIRAS, R. Lobbying e marketing político. **Comunicação & Cultura**. número 2 | outono-inverno. Lisboa: Universidade Católica Portuguesa. 2006. 231p.

CUTHBERT, Daniel; WILKINSON, Glenn. As máquinas que traíram seus mestres. (Palestra). 2013. [vídeo online]. Disponível em: <https://www.youtube.com/watch?v=Vsn7_4qUdwk>. Acesso em: 1 Jun. 2017.

DARAYA, Vanessa. App dá moedas virtuais para clientes de lojas físicas. **Exame**. 28 de novembro de 2013. Disponível em: <<https://exame.abril.com.br/tecnologia/app-da-moedas-virtuais-para-clientes-de-lojas-fisicas/>>. Acesso em: 6 Out. 2017.

DINIZ, Maria Helena. **Dicionário jurídico universitário**. São Paulo, Saraiva, 2010. 610 p.

ECALL eCall: Parlamento Europeu aprova sistema que ajuda a salvar vidas nas estradas. Sessão plenária Comunicado de imprensa. 28-04-2015. Disponível em: <<http://www.europarl.europa.eu/news/pt/news-room/20150424IPR45714/ecall-parlamento-europeu-aprova-sistema-que-ajuda-a-salvar-vidas-nas-estradas>>. Acesso em: 10 Jun. 2017.

FÁVERO, Bruno. Rastreamento de clientes pelo celular chega a lojas do Brasil. 25/11/2013. <<http://www1.folha.uol.com.br/tec/2013/11/1375267-rastreamento-de>>

clientes-pelo-celular-chega-a-lojas-do-brasil.shtml>
Acesso em: 10 Jun. 2017.

FIORINI, Melissa. **Uma arquitetura genérica de software para disponibilização de uma aplicação WEB para dispositivos móveis**. Dissertação (Mestre em Engenharia Elétrica). Florianópolis/SC: UFSC, Ab 2006. 108p.

GARCIA, Enéas Costa. **Responsabilidade civil dos meios de comunicação**. São Paulo: Juarez de Oliveira, 2002.

GHOSH, Anup K.; SWAMINATHA, Tara M. Software security and privacy risks in mobile e-commerce. **Communications of the ACM** February 2001/Vol. 44, No. 2. pp. 51-27.

GOMES, Otto; COSTA, Luís Henrique; DUARTE, Talita Lopes. **Redes de Computadores II**. GTA/UFRJ, 2009. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/talita/index.html>. Acesso em: 2 Jun. 2017.

GUIA do Celular. **História do telefone celular no Brasil**. 2011. Disponível em: <<http://www.guiadocelular.com/2011/10/historia-do-telefone-celular-no-brasil.html>>. Acesso em: 5 Jun. 2017.

IKEDA, Patrícia. As empresas ficam na cola do consumidor com smartphones. **Revista Exame**. 24/08/2013. Disponível em: <<http://exame.abril.com.br/revista-exame/edicoes/1047/noticias/na-cola-do-consumidor?page=3>>. Acesso em: 2 Jun. 2017.

IPUC – Instituto dos Profissionais Unificados do Ceará. **Número de usuários de internet no mundo alcança os 2 bilhões**. Disponível em: <<http://ipuc-ce.blogspot.com/2011/01/numero-de-usuarios-de-internet-no-mundo.html#!/2011/01/numero-de-usuarios-de-internet-no-mundo.html>>. Acesso em: 22 Jun. 2017.

ISONI, Miguel Maurício; VIDOTTI, Silvana Aparecida Borsetti. Gregorio. **E - crime em ambientes digitais informacionais da Internet**. DataGramZero - Revista de Ciência da Informação - v.8 n.2 abr/07. Disponível em: <<http://basessibi.c3sl.ufpr.br/brapci/index.php/article/view/0000004380/88c63de853da bba281053a6fdf3ea959>>. Acesso em: 5 Jun. 2017.

KAASINEN, Eija. User needs for location-aware mobile services. **Pers Ubiquit Comput** (2003) 7: 70–79.

KANSAL, Aman; GORACZKO, Michel; ZHAO, Feng. Building a Sensor Network of Mobile Phones. **IPSN'07**, April 25-27, 2007, pp. 547-548.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. 01/06/2005. 137p. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 4 Jun. 2017.

LEMOS, André. **A comunicação das coisas**: teoria ator-rede e cibercultura. São Paulo: Anna Blume, 2013. 310p.

LEMOS, André. Mídias locativas e vigilância: sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. **Surveillance in Latin America**. Vigilância, Segurança e Controle Social. PUCPR. Curitiba. Brasil. 4-6 de março de 2009. pp. 621-648.

LIMA, Caio Cesar Carvalho; MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. ATOZ – Novas Práticas em Informação e Conhecimento. Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <<http://revistas.ufpr.br/atoz/article/view/41320/25260>>. Acesso em: 09 Out. 2017.

LIMA, Lucas Loureiro de Barros; SOUZA, Carla Patricia da Silva. A Motivação dos *Prosumers*: Entendendo o Comportamento do Consumidor-Produtor na Web. **ENAMPAD 2010**. Rio de Janeiro/RJ – 25 a 29 de setembro de 2010.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**, Brasília, v. 30, n. 1, p. 71-81, jan./abr. 2010.

MARTINS, Daniel Mourão. Uma Estratégia para Sistemas de Detecção e Prevenção de Intrusão Baseada em Software Livre. Dissertação (Mestrado em Ciência da Computação). Fortaleza/CE: UFCE, 2012. 100p.

MELO, Emílio Honório de. Análise de Tráfego de Redes 3G/HSPA. Monografia (Especialização em Ciência da Computação). Recife: UFPE/Centro de Informática, 2010. 93p.

MINCH, Robert P. **Privacy Issues in Location-Aware Mobile Devices**. Proceedings of the 37th Hawaii International Conference on System Sciences – 2004. pp. 1-10.

MOKBEL, Mohamed F. Privacy in Location-based Services: State-of-the-art and Research Directions. **IEEE**. 2007. pp. 227-228.

MONTEIRO, Elis. *Nativos digitais já estão dominando o mundo e transformando a forma como o ser humano se comunica*. O Globo de 18/05/2009. Disponível em: <<http://oglobo.globo.com/tecnologia/mat/2009/05/18/nativos-digitais-ja-estao->

dominando-mundo-transformando-forma-como-ser-humano-se-comunica-755911408.asp>. Acesso em: 10 Jun. 2017.

MYLES, Ginger; FRIDAY, Adrian; DAVIES, Nigel. Preserving Privacy in Environments with Location-Based Applications. *Pervasivecomputing*. **Security & Privacy**. January–March 2003. pp. 57-64.

PAIVA, Mário Antônio Lobato de. O monitoramento do correio eletrônico no ambiente de trabalho. **Egov**. 2002. Disponível em: <<http://www.egov.ufsc.br/portal/sites/default/files/anexos/4213-4207-1-PB.pdf>>. Acesso em: 28 Out. 2017.

PICCHIAI, Djair; LOPES, Meire dos Santos; OLIVEIRA, Paulo Sérgio Gonçalves de. Gestão do conhecimento e as comunidades de prática. **Gestão & Regionalidade** - Vol. 23 - N° 68 - set-dez/2007. Disponível em: <http://gvpesquisa.fgv.br/sites/gvpesquisa.fgv.br/files/arquivos/picchiai_-_gestao_do_conhecimento_e_as_comunidades_de_pratica.pdf>. Acesso em: 28 Out. 2017.

PUTTASWAMY, Krishna P. N.; ZHAO, Ben Y. Preserving Privacy in Location-based Mobile Social Applications. **HotMobile'10**, February 22–23, 2010.

RAO, Bharat; MINAKAKIS, Louis. Evolution of Mobile Location-based Services. **Communications of the ACM**. December 2003/Vol. 46, N° 12. pp. 61-65.

REGO, Bruno Motta. **Segurança no Desenvolvimento de Sistemas com Metodologia Ágil SCRUM**. São Paulo: Universidade Presbiteriana Mackenzie, 2011. 54p.

REIS, Allande Souza; PEREIRA, Felipe Rafael Cardoso; SOUZA, Sergia Luiza de. **Estudo de caso de segurança em redes Wifi em uma instituição de Ensino – Pitágoras de Belo Horizonte**. Belo Horizonte/MG: Pitágoras, 2010. Disponível em: <<http://www.slideshare.net/AllanReis1/segurana-em-redes-wifi-estudo-de-caso-em-uma-instituio-de-educacao-superiora>>. Acesso em: 13 Jun. 2017.

SACRAMENTO-RODRIGUES, Vagner. **Gerência de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis**. Tese (Doutorado em Informática). Rio de Janeiro, PUCRJ, 2006. 135p.

SANTAELLA, Lucia; LEMOS, Renata. **Redes sociais digitais: a cognição conectiva do Twitter**. São Paulo: Paulus, 2010.

SANTOS, Alessandro Huber dos *et al.* **Evolução das Tecnologias de Telefonia Celular**. 2014. Disponível em: <<http://www2.cefetrs.tche.br/sistel/trabalhoe.doc>>.

Acesso em: 25 Jun. 2017.

SANTOS, Carlos Roberto. **Fatores de Influência para Adoção da Inovação em Gestão de Projetos: Uma Aplicação em Tecnologia da Informação**. Dissertação (Mestrado em Administração de Empresas), Universidade Presbiteriana Mackenzie, 2006.

SANTOS, Guilherme Nascimento Pate. **Um Modelo para o Gerenciamento de Confiança em Dispositivos Móveis**. Rio de Janeiro: Pontifícia Universidade Católica do Rio de Janeiro, 2010.p. 1-23.

SARTORI, Rodrigo Vinícius. **Technology Transfer in Buzz Marketing**. Revista Gestão Industrial. Ponta Grossa: UFTPR. 2011. p. 70-88.

SCHILIT, Bill; HONG, Jason; GRUTESER, Marco. Wireless Location Privacy Protection. Invisible Computing. **Computer**. p. 135-137. December 2003.

SEVERINO, Antonio Joaquim. **Metodologia do trabalho científico**. São Paulo: Cortez, 2012.

SHABTAI, Asaf; FLEDEL, Yuval; ELOVICI, Yuval. Securing Android-Powered Mobile Devices Using SELinux. **IEEE Security & Privacy**. pp. 36-44. May/June 2010.

SHOPKICK. 2013. Disponível em: < <https://www.shopkick.com/>>. Acesso em: 2 Jun. 2017.

SILVA JUNIOR, Alcides Leopoldo e. **A pessoa pública e o seu direito de imagem: políticos, artistas, modelos, personagens históricos**. São Paulo: Juarez de Oliveira, 2012.

SILVA Lorena Magalhães Freire da. **Valores Comportamentais na Preferência de Uso das Redes Sociais**. Dissertação (Mestrado em Administração de Empresas). Belém/PA: Universidade da Amazônia. 2012. 80p.

SIQUEIRA, Ethevaldo. Nuvem, internet das coisas e internet semântica. **O Estado de S.Paulo**. 13 de março de 2011. Disponível em: <<http://www.estadao.com.br/noticias/impresso,nuvem-internet-das-coisas-e-internet-semantica,691200,0.htm>>. Acesso em: 5 Jun. 2017.

SMAILAGIC, Asim; KOGAN, David. Location sensing and privacy in a context-aware computing environment. **IEEE Wireless Communications**. October 2002. pp. 9-17.

SORJ, B. Internet, espaço público e marketing político: entre a promoção da comunicação e o solipsismo moralista. **Novos estud. – CEBRAP**. Novembro 2006, n. 76, pp. 123-136.

STIVANIN, Taíssa. Mundo já tem 5 bilhões de telefones celulares. **Agência Reuters**. 16 de Julho de 2010. Disponível em: <<http://www.portugues.rfi.fr/mundo/20100716-mundo-ja-tem-5-bilhoes-de-telefones-celulares>>. Acesso em: 25 Jun. 2017.

TARCITANO, J.S.C.; GUIMARÃES, C.D. (2004). **Assédio moral no ambiente de trabalho**. Juiz de Fora: Centro de Educação Tecnológica Estácio de Sá. 51p.

TOMAÉL, Maria Inês; ALCARÁ, Adriana Rosecler; DI CHIARA, Ivone Guerreiro. Das redes sociais à inovação. **Ci. Inf.**, Brasília, v. 34, n. 2, p. 93-104, maio/ago. 2005.

VALENTIM, Marta Lúcia Pomim. **O moderno profissional da informação: Formação e perspectiva profissional**. Enc. Bibli: R. Eletr. Bibliotecon, Ci. Inf. Florianópolis, Brasil, Nº 9, p. 16-28, 2010.

VIEIRA, Vinícius. Atenção: encontradas novas vulnerabilidades no Facebook! 22/04/2013. Disponível em: <<http://sejalivre.org/atencao-encontradas-novas-vulnerabilidades-no-facebook/>>. Acesso em: 28 Jun. 2017.

WEE, Willis. LBS and E-Commerce Together: Is it too early in China? **China Mobile Developers Conference**. 4 de Novembro de 2011. Disponível em: <<http://www.techinasia.com/lbs-and-e-commerce-together-is-it-too-early-in-china/>>. Acesso em: 28 Jun. 2017.

WHALEN, Tara. Mobile Devices and Location Privacy. **IEEE Security & Privacy**. November/December 2011. pp. 61-62.

XAVIER, Sergio de Souza. **Comunidades Virtuais**: A importância da interação no aspecto da relação de consumo no ciberespaço. Dissertação (Mestrado em Administração). Rio de Janeiro: UNIGRANRIO, 2012. 124p.