UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

GESTÃO DE IDENTIDADES EM CIDADES DIGITAIS: IDENTIFICAÇÃO E RESPONSABILIZAÇÃO LEGAL DOS USUÁRIOS

TRABALHO DE CONCLUSÃO DE CURSO

Lucas Powaczuk

Santa Maria, RS, Brasil

2013

CTISM/UFSM, RS	POWACZUK, Lucas	Graduado	2013

GESTÃO DE IDENTIDADES EM CIDADES DIGITAIS: IDENTIFICAÇÃO E RESPONSABILIZAÇÃO LEGAL DOS USUÁRIOS

Lucas Powaczuk

Trabalho apresentado ao Curso de Graduação em Tecnologia em
Redes de Computadores, Área de concentração em Segurança da Informação, da
Universidade Federal de Santa Maria (UFSM, RS),
como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores.

Orientador: Prof. Ms. Walter Priesnitz Filho

Santa Maria, RS, Brasil

2013

Universidade Federal de Santa Maria
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores

A Comissão Examinadora, abaixo assinada,
aprova a Monografia

GESTÃO DE IDENTIDADES EM CIDADES DIGITAIS: IDENTIFICAÇÃO E RESPONSABILIZAÇÃO LEGAL DOS USUÁRIOS

elaborada por
Lucas Powaczuk

como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA

Walter Priesnitz Filho, Ms.
(Presidente/Orientador)

Eugênio de Oliveira Simonetto, Dr. (UFSM)

Renato Preigschadt de Azevedo, Ms. (UFSM)

Santa Maria, 18 de julho de 2013

AGRADECIMENTOS

Ao concluir este trabalho, gostaria de agradecer a todos que me acompanharam neste percurso:

Inicialmente a minha esposa Vanessa e ao meu filho Matheus, pela presença de amor, companheirismo e alegria que representam.

A minha mãe Ana Carla e meu pai Fernando pelo amor e dedicação dispensados a mim.

Aos meus irmãos pelo apoio e incentivo que me dedicaram no decorrer desta trajetória.

Ao professor e orientador Walter Priesnitz Filho, pela atenção e amizade desprendida a mim neste percurso e principalmente pela disponibilidade na orientação do decorrer deste estudo.

Enfim, a todos os demais que, de uma forma ou de outra, contribuíram para a realização deste estudo.

RESUMO

Monografia
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

GESTÃO DE IDENTIDADES EM CIDADES DIGITAIS: IDENTIFICAÇÃO E RESPONSABILIZAÇÃO LEGAL DOS USUÁRIOS

AUTOR: LUCAS POWACZUK
ORIENTADOR: WALTER PRIESNITZ FILHO
Data e Local da Defesa: Santa Maria, 18 de julho de 2013

Esta pesquisa trata do sistema de autenticação nas cidades digitais (CDs) do Rio Grande do Sul que disponibilizam acesso à Internet gratuita a população, enfocando o gerenciamento de identidades e a responsabilização legal dos usuários na utilização da rede de computadores. O estudo foi desenvolvido a partir de uma abordagem descritiva analítica. Como ações da pesquisa foram realizadas leituras bibliográficas para maior aprofundamento do assunto, pesquisa em *sites* de consulta pública sobre as cidades digitais de modo a identificar as CDs do RS; consulta na legislação vigente sobre os cibercrimes; elaboração de ações direcionadas a qualificar o gerenciamento de identidades. A partir do estudo realizado averiguou-se que apenas 24% do total de cidades digitais do Rio Grande do Sul apresentam uma rede pública para acesso à Internet de forma livre os cidadãos. No que se refere ao gerenciamento de identidades este é organizado a partir de informações gerais, tais como CPF/CNPJ, RG, Nome, Endereço compondo um cadastro individual do usuário. Entretanto, o processo de validação dos dados não é realizado na grande maioria das cidades que disponibilizam acesso à Internet gratuita a população. Apenas duas cidades do Rio Grande do Sul apresentam ações direcionadas a este quesito. Estas questões ganham destaque tendo em vista que o anonimato na rede vem sendo apontado como um ponto que merece estudo aprofundado, sendo a identificação dos usuários a postura mais adequada para fins de isenção de responsabilidade e identificação do real infrator (SOUTO JUNIOR, 2010). Considera-se que as cidades digitais merecem uma atenção especial tendo em vista que o gerenciamento da rede é feito por um órgão estatal, e no caso de delitos gerados através de uma rede de acesso livre, a responsabilização penal, de acordo com as normativas atuais, recairia sobre o gestor da rede. Assim, destaca-se para ações direcionadas a identificação do usuário final, de modo a configurar uma política de segurança que dê confiabilidade aos usuários.

Palavras-chave: Cidades Digitais; Gerenciamento de Identidades; Autenticação; Cibercrimes;

ABSTRACT

Monography
Superior Course of Technology in Computer Networks
Universidade Federal de Santa Maria

IDENTITY MANAGEMENT IN DIGITAL CITIES: IDENTIFICATION AND LEGAL LIABILITY OF USERS

AUTHOR: LUCAS POWACZUK
ADVISER: WALTER PRIESNITZ FILHO
Defense Place and Date: Santa Maria, July 22th, 2013

This research deals with the authentication system in digital cities (DCs) of Rio Grande do Sul that provide free Internet access to the population, focusing on identity management and legal accountability of users in the use of the computer network. The study was developed from a descriptive analytical approach. As actions of research literature readings were taken for further deepening of the subject, research sites public consultation on digital cities in order to identify the DCs RS; consultation on legislation on cybercrime, developing actions aimed at qualifying the management identities. From the study ascertained that only 24% of digital cities of Rio Grande do Sul have a public Internet with free access of citizens. With regard to identity management that is organized from general information such as CPF / CNPJ, RG, Name, Address composing a register individual user. However, the process of data validation is not performed in most of the cities that provide free Internet access to the population. Only two cities in Rio Grande do Sul present actions directed at this question. These issues are highlighted in view that anonymity on the net is being touted as a point that deserves thorough study, and the identification of the users posture more suitable for the purposes of exemption from liability and identify the actual infringer (SOUTO JUNIOR, 2010). It is considered that digital cities deserve special attention in view of that network management is done by a state agency, and in the case of offenses generated through a network of free access to criminal liability, according to the current standard , would be on the network manager. Thus, there is need for actions directed to identify the end user in order to configure a security policy that gives reliability to users.

Key words: Digital Cities; Identity Management; Autentication; Cybercrimes;

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

O conceito de cidades digitais (CDs) vem se mostrando como uma estratégia de democratização do acesso à informação, bem como a modernização da gestão pública. A inclusão digital e a modernização na prestação de serviços de diferentes áreas são elementos que validam a proposta de implementação de uma cidade digital.

De acordo com Simão (2010), a implementação de um projeto de cidade digital vem sendo estimulada pelo governo federal diante da necessidade de modernização dos estados em acompanhar uma nova ordem mundial sob pena de ficarem à margem do desenvolvimento da nova economia.

É nesse contexto que as cidades digitais estão surgindo no Brasil, fruto de iniciativas de todos os setores da sociedade e com um importante papel sendo desempenhado pelo governo, em todas as suas esferas: municipal, estadual e federal (Souto, et al, 2006).

Nesta direção, o programa Cidades Digitais constitui-se como uma iniciativa do Ministério das Comunicações que tem como objetivo auxiliar as prefeituras na implementação dos projetos de modernização de gestão dos órgãos da rede pública e criação de pontos de acesso à internet públicos (COMUNICAÇÕES, 2012).

Uma cidade digital apresenta um conjunto de benefícios os quais abrangem: (i) prestação de serviços de governo eletrônico, a partir de ferramentas digitais; (ii) a inclusão digital a partir da organização de laboratórios públicos e Internet gratuita á toda a população; (iii) promoção de uma rede de serviços interligados entre os órgãos públicos; (iv) o aumento da transparência dos órgãos públicos.

Muitos municípios já possuem o projeto em funcionamento. Segundo Simão (2010) cidades como Chapadão do Céu, em Goiás; Tapira, em Minas Gerais; Sud Mennucci e Pedregulho, em São Paulo e Santa Cecília do Pavão, no Paraná podem ser chamadas de cidades digitais. Borba (2012) cita cidades do Rio Grande do Sul, como Garibaldi, Alvorada, Ribeirão Preto, Manoel Vitorino, bem como, projetos implantados em cidades norte americanas e do contexto europeu e asiático como Toronto, Londres, Bologna, Singapura dentre outras.

A informação, um dos principais ativos das organizações e, por consequência, o uso adequado das tecnologias da informação e comunicação tem sido tomados como fatores determinantes para o sucesso do gerenciamento da gestão pública.

Entretanto, diversos aspectos vem sendo problematizados diante da complexidade das relações que permeiam a funcionalidade das propostas de cidades digitais. Dentre estas estão as questões relativas a segurança das informações dos usuários; o sistema de autenticação e gerenciamento de identidades de modo a garantir a responsabilização dos usuários sobre possíveis infrações cometidas através da rede (BORBA, 2012; SOUTO JUNIOR, 2010).

De fato estas problemáticas não são exclusivas dos programas de cidades digitais, caracterizam-se como questões pertinentes ao acesso à Internet como um todo. Entretanto, as cidades digitais merecem uma atenção especial tendo em vista que o gerenciamento da rede é feito por um órgão estatal, e no caso de delitos gerados através de uma rede de acesso livre, a responsabilização penal, de acordo com as normativas atuais, recairia sobre o gestor da rede.

Assim, considera-se que esta perspectiva precisa ser acompanhada de um conjunto de ações que permitam a identificação e consequentemente a responsabilização legal dos usuários. A criação de estratégias de segurança configura-se, portanto, como um investimento caracterizando a configuração de uma política de segurança que dê confiabilidade aos usuários.

A Internet, atualmente tem se caracterizado como um espaço propício à pratica de atos ilícitos, devido a ausência de mecanismos de controle e de responsabilização dos usuários. Nesta direção Colli (2010, p.15) posiciona-se ao afirmar que “apesar de a internet facilitar e ampliar a intercomunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a prática e a organização de infrações penais”.

Inellas (2004) corrobora afirmando que é indubitável que a Internet modificou o comportamento humano. Se, por um lado, incentivou a busca de novos conhecimentos e a expansão da cultura, por outro lado, também propiciou o surgimento dos criminosos digitais.

A legislação brasileira possui diversas fragilidades em relação aos delitos cometidos por meio da Internet, os crimes cibernéticos. O anonimato na rede vem sendo apontado como um ponto que merece estudo aprofundado, sendo ainda a identificação dos usuários a postura mais adequada para fins de isenção de responsabilidade e identificação do real infrator (SOUTO JUNIOR, 2010). Assim, um dos problemas a serem enfrentados nos delitos cometidos por meio da Internet, é o da autoria, isto é, da identificação do autor da infração penal.

Diante disso, surgiu a motivação para esta pesquisa que trata do sistema de autenticação nas cidades digitais do Rio Grande do Sul que disponibilizam acesso à Internet de forma gratuita a população, enfocando o gerenciamento de identidades e a

responsabilização legal dos usuários na utilização da rede de computadores.

Neste sentido, justifica-se a relevância deste estudo tendo em vista sua possibilidade de identificar como se dá o processo de gerenciamento de identidades nas cidades digitais do Rio Grande do Sul, bem como, fornecer indicativos que corroborem para a qualificação do processo de gestão de identidades que viabilizem a responsabilização legal dos usuários da rede.

Isto posto, apresenta-se no **primeiro capítulo** discussões relativas aos conceitos de cidades digitais a partir dos estudos de Souto (et al, 2006). Destaca-se para o programa de implementação de cidades digitais incentivado pelo governo federal, enfocando o planejamento e os níveis de urbanização de uma cidade digital.

No **segundo capítulo,** denominado autenticação e gerenciamento de identidades apresentam-se os conceitos de autenticação enfocando o gerenciamento de identidades através de sistema de cadastro de usuários.

No **terceiro capítulo** aborda-se questões relativas as regulações do ambiente virtual, a partir dos estudos de Souto Junior (2008), problematizando para a complexidade das relações do mundo virtual e as limitações no que diz respeito a penalização de atos ilícitos.

No **quarto capítulo** o enfoque está sobre os crimes virtuais, explicitando o conceitos de cibercrimes e para os tipos de atos ilícitos mais praticados no ambiente virtual de acordo com Inellas (2004). Aborda-se ainda para o processo de identificação eletrônica dos usuários, bem como, para as provas digitais.

No **quinto capítulo** apresenta-se a metodologia da pesquisa, trazendo os objetivos da investigação realizada, bem como os procedimentos adotados. Posteriormente, no **sexto capítulo** explicitam-se os resultados da pesquisa a partir da análise realizada.

Finaliza-se com as **considerações finais** da pesquisa, na qual retomam-se os objetivos almejados no estudo.

1 DESENHO DA INVESTIGAÇÃO

1.1 Tema

Gestão de identidades em cidades digitais.

1.1.1 Delimitação do Tema

O objeto de análise do estudo é o sistema de autenticação nas cidades digitais do Rio Grande do Sul que disponibilizam acesso à Internet de forma gratuita a população, enfocando o gerenciamento de identidades e a responsabilização legal dos usuários na utilização da rede de computadores.

1.2 Objetivos

1.2.1 Objetivo geral

Identificar o processo de gerenciamento de identidades em cidades digitais do Rio Grande do Sul que disponibilizam acesso à internet de forma gratuita a população, enfocando o gerenciamento de identidades e a responsabilização legal dos usuários na utilização da rede de computadores.

1.2.2 Objetivos específicos

- Investigar quais cidades, no Rio Grande do Sul, são consideradas digitais e disponibilizam o acesso gratuito a Internet á população.
- Averiguar como é feita a identificação dos usuários nas cidades digitais do estado do Rio Grande do Sul.
- Analisar as implicações relativas à utilização do gerenciamento das informações no que se refere a responsabilização legal dos usuários
- Identificar a legislação brasileira relacionada á crimes cibernéticos, destacando as informações necessárias para responsabilização legal e jurídica dos usuários no que se refere aos seus atos na rede.
- Fornecer indicativos para o desenvolvimento de uma proposta de gerenciamento de identidades que viabilize a responsabilização legal dos usuários no que se refere aos seus atos na rede.

1.3 Metodologia

Este trabalho foi desenvolvido a partir de uma abordagem descritiva analítica. Desta forma, o estudo abrange a descrição e a análise do processo de gerenciamento de identidades em cidades digitais do Rio Grande do Sul (RS). Como ações da pesquisa foram realizadas leituras bibliográficas para maior aprofundamento do assunto, pesquisa em *sites* de consulta pública sobre as cidades digitais de modo a identificar as CDs do RS; consulta na legislação vigente sobre crimes virtuais; elaboração de ações direcionadas a qualificar o gerenciamento de identidades; escrita do relatório final.

2. CONCEITOS DE CIDADES DIGITAIS

O conceito de cidades digitais, de acordo com Simão (apud LEMOS, 2010) abrange que existem quatro visões distintas. O primeiro tipo refere-se a um projeto governamental, que tem como objetivo criar uma representação na *Web* de um determinado lugar, como um portal com informações e serviços de uma determinada área urbana.

A segunda visão refere-se a cidades digitais que não representam, necessariamente um

espaço urbano real. Estes projetos se destinam a cidades digitais criadas no ambiente virtual, ou seja, são *sites* que criam comunidades virtuais onde na verdade não existe uma cidade real. Um exemplo famoso deste projeto é o *Second Life*[1].

A terceira visão refere-se a modelagens em três dimensões (3D) para a simulação de espaços urbanos. Esse tipo de projeto é útil para ajudar no planejamento do espaço, servindo como instrumento estratégico do urbanismo contemporâneo. Sistemas de Informação Espacial e Sistemas de Informações Geográfica são exemplos deste tipo de cidade digital.

O quarto conceito está diretamente relacionado à criação de infraestrutura, serviços e acesso público em uma determinada área urbana para o uso das novas tecnologias e redes telemáticas. O objetivo desse tipo de cidade digital é criar interfaces entre o ciberespaço e o espaço físico por meio de uma infraestrutura de telecomunicações, disponibilizados para os cidadãos por meio de telecentros, quiosques multimídia, ou mesmo pelo acesso direto à Internet. Cabe ressaltar que o presente estudo toma como objeto de análise e discussão as cidades digitais caracterizadas neste último conceito de cidade digital.

Assim, define-se como cidade digital aquela que, utilizando os recursos que oferecem as tecnologias de informação e de comunicação, entre eles a Internet, disponibiliza a seus habitantes um conjunto de serviços inteligentes que melhoram o nível de desenvolvimento humano, econômico e cultural da comunidade tanto de forma individual como coletiva (SIMÃO, 2010).

2.1 Cidades digitais: uma proposta governamental de universalização do acesso aos serviços públicos

Atualmente, em tempos de globalização, a rápida expansão e evolução dos meios de comunicação tem provocado grandes transformações sociais, econômicas e políticas. Como elemento definidor deste processo está o advento da Internet, o qual pode ser indicado como o principal responsável pela ampliação do acesso à informação.

A partir destas transformações surge o conceito das tecnologias de comunicação e informação. As Tecnologias de Informação e Comunicação (TICs) surgem com o objetivo de facilitar a comunicação e o acesso a informação. Espíndola (et al, 2011) afirma que os governos de todo o mundo estão investindo fortemente no desenvolvimento de padrões em TIC. Frey (2000) refere-se as tecnologias de informação e comunicação como uma alternativa

[1] O Second Life é um mundo em 3D no qual todas as pessoas que você vê são reais e todos os lugares que você visita são construídos por usuários. Disponível em: http://secondlife.com/whatis/?lang=pt-BR Acesso em: 06/07/2013.

mais democrática e participativa de governança para enfrentar os problemas sociais e econômicos.

As TICs podem ser definidas como um conjunto de recursos tecnológicos que buscam a democratização e a universalização do acesso aos serviços públicos, contribuindo no relacionamento entre o estado e o cidadão. Para Espíndola (et al, 2011) a utilização dessas tecnologias permitem o aumento da eficácia, da eficiência e da transparência governamental.

Entende-se que a utilização da Internet e das TICs em favor dos cidadãos vem contribuindo para melhorar a governabilidade e a administração pública do País. No entanto, Espíndola (et al, 2011) afirma que é fundamental o aprimoramento da administração pública para esta nova realidade, pautada pelo uso de tecnologias aos serviços prestados pelo estado.

Frey (2000) afirma que existem duas abordagens básicas de estratégias de governança eletrônica. A primeira aborda a necessidade de oferecer serviços públicos *online* pela Internet. O seu objetivo é a centralização do governo e tornar disponíveis os serviços públicos a qualquer hora do dia através de PCs e quiosques públicos. A segunda abordagem problematiza a questão da "exclusão digital", pelo fato de que algumas pessoas não seriam beneficiadas por estes serviços *online*, pelo menos enquanto não existir os pontos de acesso público.

O governo iniciou seu processo de governo digital no ano 2000 (ESPÍNDOLA, et al 2011) através de um programa de governo eletrônico, conhecido também como programa e-Gov. Este programa tem como característica a utilização de TICs em diversas áreas, informatizando processos e trazendo facilidades para a sociedade, através dos serviços eletrônicos.

Atualmente existem diversos serviços e-Gov em funcionamento. No Governo Federal, entre as ações ligadas ao tema, pode-se destacar o Programa de Modernização do Estado, o Programa Sociedade da Informação (PSI) e o Programa Governo Eletrônico.

Estes programas são incentivados pelo Governo Federal através da disponibilização dos recursos necessários para a sua viabilização, para municípios e órgãos públicos. É o caso do programa e-Gov Cidades Digitais, que é uma iniciativa do Ministério das Comunicações para auxiliar prefeituras na implementação de seus projetos de modernização de gestão dos órgãos da rede pública e criação de pontos de acesso à Internet públicos, conforme a (COMUNICAÇÕES, 2013)[2].

Os Projetos de cidades digitais tem ocasionado um grande interesse pelos gestores públicos em implantar esse projeto. Simão (2010) relata que as primeiras iniciativas de projetos de cidades digitais surgiram no início da década de 90. O mesmo autor relata que

[2]

para que sejam implantados projetos denominados como cidade digital, com maiores chances de sucesso, é necessário que se tenha uma infraestrutura mínima de informatização dos processos da administração pública.

Este projeto possibilita a modernização da gestão das cidades com a implantação de infraestrutura de conexão de rede entre os órgãos públicos além da implantação de aplicativos, com o objetivo de melhorar a gestão e o acesso da comunidade aos serviços de governo. Podem participar da seleção prefeituras e regiões administrativas do Distrito Federal (DF). (COMUNICAÇÕES, 2013)

As cidades que implementam este projeto recebem softwares para os setores financeiro, tributário, de saúde e educação, e os servidores públicos são capacitados para o uso específico dos aplicativos e da rede, assim como nas Tecnologias de Informação e Comunicação (TICs). Também está prevista a instalação de pontos de acesso à Internet para uso livre e gratuito em espaços de grande circulação em locais definidos a critério das prefeituras. (COMUNICAÇÕES, 2013)

2.2 Planejamento de Cidades Digitais

Para viabilizar a implementação de um projeto digital, Simão (2010, p. 106) afirma que devem-se realizar as seguintes ações: i) realizar análise preliminar sobre a possibilidade de se transformar em cidade digital; ii) definir um Grupo de Trabalho (GT) para estudar o tema; iii) realizar levantamento sobre os níveis de apropriação e uso de TICs na cidade; iv) buscar as melhores práticas de implantação de projetos de cidades digitais; v) definir o escopo do projeto; vi) elaborar um estudo de viabilidade; vii) elaborar um projeto; viii) enviar o projeto para o Legislativo Municipal; ix) elaborar o edital; x) avaliar as propostas; xi) implantar o projeto; xii) solicitar licença de operação na Anatel; xiii) elaborar uma campanha para divulgação do projeto; xiv) realizar estudo de impacto econômico e social do projeto; xv) inaugurar o projeto; xvi) avaliar o projeto; xvii) buscar a sustentabilidade do projeto; e xviii) expandir o projeto.

Já Souto (et al, 2006) define que para a implantação de cidades digitais, do nível de urbanização existente em cada localidade até seu nível máximo (cidade digital plena), pode ser aplicada a metodologia de planejamento apresentada na figura 1, composta de quatro fases

inter-relacionadas, descritas a seguir:

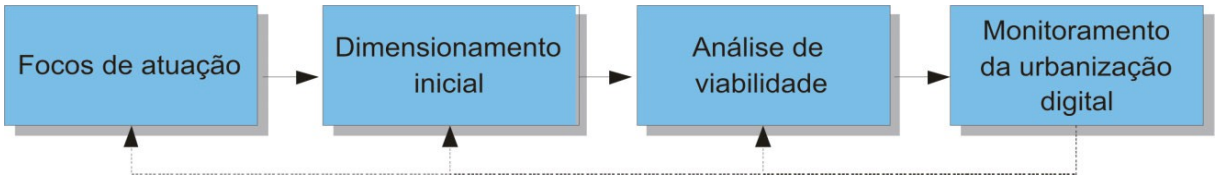

Figura 1 – Metodologia de planejamento de cidades digitais

Fonte: Souto (et al, 2006, p. 112).

A primeira fase refere-se à identificação do nível de urbanização digital da cidade analisada. A partir disso, devem ser definidos os focos de atuação necessários para a evolução gradual dos níveis de urbanização, para um nível superior, onde devem abranger pelo menos quatro áreas: disponibilidade e cobertura de serviços de telecomunicações e de acesso à Internet, perfis da população a ser atendida, serviços públicos e privados a serem oferecidos, além de níveis de integração de serviços e de recursos.

Na segunda fase é preciso fazer um levantamento sobre as demandas de cada uma das ações nas quatro áreas da primeira fase. O objetivo deste levantamento é mapear os interesses da população por serviços eletrônicos públicos e privados. Este levantamento pode ser feito por meio de entrevista, buscando identificar a quantidade de indivíduos interessados em cada serviço, o tempo estimado de utilização, a frequência de utilização e o preço que se está disposto a pagar.

Na terceira fase é preciso estudar a viabilidade técnica e econômica para escolher as melhores soluções para a evolução. Este estudo deve ser baseado em métodos quantitativos através de recursos computacionais de simulação. Essas análises devem dimensionar, em cenários de longo prazo, os investimentos anuais para cada ator envolvido, à obtenção de outros tipos de recursos, tais como incentivos fiscais, fundos setoriais e de universalização, e à ação de empresas e de organizações não-governamentais.

A quarta fase refere-se à monitoração da evolução tecnológica. Isso em razão da velocidade de surgimento e transformação das tecnologias envolvidas em assunto tão recente

e complexo como as cidades digitais. O tempo de monitoração recomendada não deve ser superior a 12 meses, o que deve permitir uma avaliação consistente quanto às opções tecnológicas nacionais e internacionais e às expectativas, validade e qualidade dos serviços prestados à população.

2.3 Níveis de urbanização das cidades digitais:

Souto (et al, 2006) afirma que similarmente às cidades reais, as cidades digitais apresentam diferentes níveis de "urbanização":

> Assim como as cidades tradicionais se diferenciam quanto às características físicas e em termos do desenvolvimento que apresentam – ou seja, o alcance e a qualidade da infraestrutura de água e esgoto, a oferta de serviços públicos, a eficiência do sistema de transporte, a segurança pública, a quantidade e a qualidade de áreas de lazer, a existência de planejamento urbano, a extensão e a densidade populacional, etc. –, as cidades digitais também podem ser classificadas em termos do quanto se encontram integradas ao ciberespaço. (Souto et al, 2006, p-70).

O mesmo autor classifica as cidades digitais em seis níveis, em que são considerados tanto os aspectos tecnológicos quanto os de natureza social, como usabilidade, acessibilidade e inteligibilidade. Segundo o autor as cidades consideradas digitais possuem variados níveis de infraestrutura de redes de telecomunicações, de acesso as TICs e de oferta de serviços eletrônicos públicos e privados. A seguir são descritos os seis níveis de cidades:

Figura 2 – Nível de urbanização dos municípios brasileiros.

Fonte: http://wirelessmundi.inf.br/indice-edicao-n-9/903-capa. Acesso em 03/06/2013.

- O primeiro nível é classificado como o patamar mínimo que uma cidade pode apresentar, no que se refere a informatização. Trata-se de cidades com acesso básico, ou seja, dispõem de infraestrutura e serviços de telecomunicações porém com algumas limitações. Em geral, as cidades que são classificadas neste nível de digitalização não possuem provedor local de acesso à internet (ISP). Então conclui-se que a conexão é de baixa velocidade e qualidade insuficiente.

- O segundo nível representa as cidades que disponibilizam telecentros para o acesso público à internet. Neste nível de digitalização, a cidade já possui ISPs locais, porém ainda existem restrições de conexão com a Internet, como limite de banda de transmissão, e recursos mínimos referentes a acessibilidade e usabilidade;

- O terceiro nível referencia as cidades que possuem serviços eletrônicos em funcionamento. Neste nível, as cidades já possuem cobertura total de acesso público à Internet, através de telecentros públicos e a população, através do acesso as TICs, podem usufruir de alguns serviços públicos e privados virtualmente. Cabe destacar que os recursos de acessibilidade e usabilidade são mais presentes;

- O quarto nível é classificado como cidades pré-integradas. Neste nível, a cidade já é considerada como digital. Os serviços públicos encontram-se integrados é a cidade possui cobertura total e sem limitação de banda para o acesso público. Os telecentros e serviços públicos dispõem de diversos recursos de acessibilidade, usabilidade e inteligibilidade. Este nível possui alguns serviços privados em ambiente virtual;

- O quinto nível representa as cidades digitais com serviços integrados. Este nível é caracterizado pelo alto grau de digitalização da cidade, com cobertura total para o acesso público e para o acesso individual a Internet. Os serviços são integrados e existem uma grande quantidade de recursos de acessibilidade, usabilidade e inteligibilidade;

- O sexto nível é referente as cidades digitais plenas, onde os serviços públicos e privados são totalmente integrados, criando um espaço virtual similar à cidade real. As TICs passam a fazer parte da urbanização da cidade;

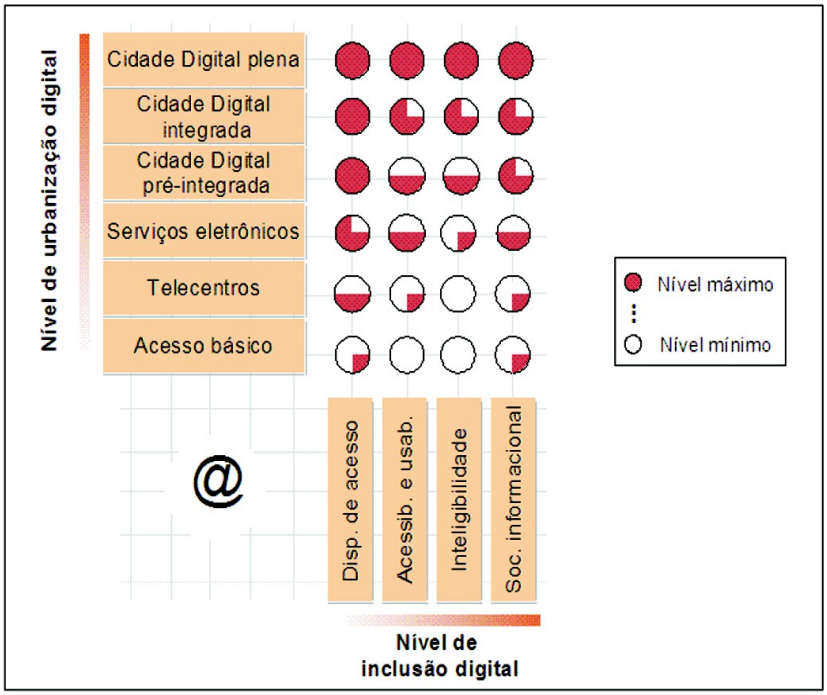

Figura 3 – Cidades digitais e inclusão na sociedade informacional.

Fonte: Souto (et al, 2006 p. 79).

3 AUTENTICAÇÃO E GERENCIAMENTO DE IDENTIDADES

Autenticação é um tema bastante conhecido e utilizado em diversos segmentos da rede. O conceito pode ser explicado como uma maneira de validar a identidade de uma pessoa. Tanenbaum (2003) descreve como a técnica através da qual um processo confirma que seu parceiro na comunicação é quem deve ser e não um impostor. De acordo com este autor as pessoas autenticam outras pessoas ao reconhecer seus rostos, vozes e caligrafia (assinatura no papel). Define-se então que a autenticação é responsável pela confirmação de identificação de alguém. Porém, sabe-se que nenhuma destas opções estão disponíveis eletronicamente, desafiando para elaboração de propostas que enfrentem esta problemática.

Autenticação é um tema amplo, com uma ampla diversidade de aplicações e utilizações. Pode-se citar alguns exemplos como o método de autenticação através de controles de acesso a arquivos pessoais ou redes, assinaturas eletrônicas de documentos e pessoas, certificados digitais e muitos outros. Borba (apud MALLICK, 2012) diz que o método mais simples de autenticação é a combinação de usuário e senha em um controle de acesso a uma determinada aplicação.

A implementação de técnicas de segurança, como sistemas de autenticação e ferramentas para o controle da rede, acarretam obstáculos para operacionalidade e para a acessibilidade para o usuário. Entretanto, há de se destacar que a disponibilização de redes de comunicação sem mecanismos de segurança pode favorecer a prática de atos ilícitos. Borba corrobora com a seguinte afirmação:

> Se o acesso público for concedido sem quaisquer dispositivos de segurança e gerenciamento, todo o contexto da cidade digital também estará comprometido tornando o ambiente propício para a prática de crimes digitais, além da ocorrência dos mais diversos tipos de incidentes que podem colocar em risco a sustentabilidade e consequentemente, a continuidade deste tipo de projeto – o de acesso gratuito à internet. (BORBA, 2012, p. 19)

Assim, a autenticação constitui-se como um requisito fundamental em segurança de redes de computadores. Processo que nos remete ao gerenciamento de identidades, pois a autenticação implica a disponibilidade de dados que permita a confirmação da veracidade das informações.

Considera-se que o gerenciamento de identidades proporciona um controle de acesso

na rede, através do cadastro das informações dos usuários que utilizam a rede. Com ele é possível compor um banco de dados, trazendo vantagens como a identificação dos usuários, o controle de acesso a rede e, consequentemente, o incremento do nível de segurança da rede.

Borba (2012) em seus estudos sobre cidades digitais propõe para a utilização de bancos de dados existentes e de acesso público para a autenticação dos usuários na rede pública. Segundo este autor, seria uma solução viável pela possibilidade de aplicação em todo território nacional:

> A solução proposta utiliza recursos adicionais que fazem parte da realidade de órgãos públicos municipais, estes recursos são banco de dados existentes em todas as prefeituras do Brasil, característica que permite a sua aplicabilidade em 100% dos municípios brasileiros sem alterações significativas na solução a ser proposta. (BORBA, 2012, p. 43)

Este modelo consiste na utilização das informações existentes no sistema de cadastro de imóveis do município, o IPTU (Imposto Predial e Territorial Urbano) e no sistema de cadastro de usuários do SUS, Sistema Único de Saúde. Segundo Borba (2012, p.43) atualmente é comum esta prática pelo país, "o governo federal mantém vários serviços que utilizam banco de dados nacionais como fonte de alimentação".

No que se refere ao cadastro utilizando dados do IPTU (Imposto Predial e Territorial Urbano), Borba (2012) afirma que através deste poderia ser criado um código de ativação do serviço, gerado exclusivamente para o responsável pelo imóvel. Já o Sistema Único de Saúde é um banco de dados que está disponível á toda população brasileira, onde cada cidadão possui um número de identificação única. Borba (2012) acrescenta que "este sistema não possui quaisquer restrições de idade ou condições sociais, portanto pode ser emitido para pessoas de quaisquer idades e classes sociais abrangendo 100% da população.

É importante ressaltar que para o funcionamento desta proposta os usuários precisam possuir cadastro em no mínimo um destes dois sistemas. Para o registro no banco de dados do IPTU é obrigatório possuir ao menos um imóvel no nome. Para o cadastramento no sistema do SUS, é necessário uma visita presencial até o local destinado ao credenciamento, geralmente são hospitais, clínicas, postos de saúde, ou locais definidos pela secretaria de saúde do município.

Considera-se que a proposta de Borba (2012) é válida por trazer a viabilidade de utilizar bancos de dados nacionais para a autenticação em cidades digitais. No entanto considera-se que as informações de cadastro municipal de imóveis é limitado, pois não atinge

a totalidade da população. Apenas as pessoas que possuem (propriedades) imóveis seriam cadastradas no sistema. No que tange ao sistema de cadastro do SUS sua limitação está também relacionado à sua abrangência, pois apesar deste serviço público ser disponibilizado a população, não necessariamente todos os moradores de uma cidade fazem uso deste.

4 REGULAMENTAÇÃO DO MEIO VIRTUAL

A problemática referente aos dispositivos de segurança, nos quais se enquadram o processo de autenticação e validação de identidade constituem-se em um importante aspecto da sustentabilidade e continuidade do projeto de cidades digitais.

Souto Junior (2010) explica que esta necessidade se dá em razão da realização de diversas atividades tais como comércio eletrônico, transações financeiras, compra e venda de produtos, implicando preceitos legais e jurídicos nas relações estabelecidas.

A Internet é um ambiente de fácil acesso que atinge grande parte da população mundial e possibilita o contato e a troca de informações de maneira instantânea, mas também tem se constituído em um ambiente favorável para a prática de crimes. Esta realidade do mundo virtual é um desafio a ser enfrentado. Sabe-se que para a elaboração de uma determinada lei é necessário que o crime já exista. Souto Junior (2010) afirma que é normal que a lei surja após a existência do fato, ou seja, a tecnologia está sempre um passo a frente da elaboração jurídica. Conclui-se que o fato surge para o Estado regulamentar. Inellas (2004) corrobora que infelizmente os criminosos são mais rápidos que os legisladores e que isso é no mundo inteiro.

A questão de regulamentação da Internet é ampla e complexa. Sabe-se que o mundo virtual não possui fronteiras e donos, por essas e outras questões torna-se bastante difícil para qualquer país regulamentar o ciberespaço com suas próprias leis. Inellas (2004) afirma, através do artigo 70 do Código de Processo Penal, que a competência será determinada pelo lugar em que se consumar a infração. A lei penal vigora dentro dos limites que o Estado exerce sua soberania.

Diante destas problematizações de legalidade na Internet, cabe colocar em destaque discussões relativas às concepções de regulação da rede. Dentre elas estão: a teoria libertária; a teoria da arquitetura da rede; a teoria internacional e a teoria tradicionalista.

4.1 Teoria Libertária

A corrente libertária é contrária a qualquer forma de regulação da rede, advogando que esta se daria a partir do autogestionamento da rede. O principal defensor desta abordagem, segundo Souto Junior (2010), refere-se a John Perry Barlow. Este autor defende a independência do espaço virtual, com ausência da interferência Estatal. Não havendo fronteiras, o ciberespaço seria um mundo que está em todos os lugares e em lugar algum. Um lugar ausente de preconceitos, livre a todos, sem privilégios, onde a liberdade de expressão teria plena validade, independentemente de regras locais. É um ambiente sem existência física, afastado então o poder de coerção do Estado, sendo que a ética dos agentes da rede é que governariam o ambiente (BARLOW apud SOUTO JUNIOR, 2010).

Desta forma, o ciberespaço seria um local democrático naturalmente regulado, não havendo preconceito de raça ou cultura, privilégios, poder econômico ou força militar. Esta abordagem analisa a eficácia do sistema informático existente como viável e suficiente para regular as relações inseridas no ambiente virtual. Importa destacar que Barlow (apud SOUTO JUNIOR, 2010) considera *download* de arquivos, filmes e músicas com finalidade de utilização pessoal ou compartilhamento entre usuários, sem fins comerciais como uma atividade legal e prevista nas relações do mundo virtual.

A justificativa principal na qual se assenta a teoria libertária está na ausência de territorialidade do ciberespaço. Transações, contratos, dentre outras relações, são formalizadas instantaneamente em diversos lugares do mundo, sem fronteiras e domínios estatais.

Souto Junior (2010) argumenta que transferir o controle da rede aos usuários caracteriza-se como uma medida arriscada e irresponsável, não garantindo a segurança e confidencialidade das transações ocorridas no mundo virtual. Questiona como seriam solucionados os impasses e atos ilícitos em uma rede governada por todos e para todos. Um ambiente libertário, segundo este mesmo autor, não auxiliaria na solução de questões direcionadas à responsabilidade civil. Desta forma considera que a legislação vigente ou futura é basilar para direcionar normas de conduta, que sejam norteadoras de cumprimento e reparação de atos eletrônicos, apresentando, inclusive, aspectos de coação aos violadores, tornando fundamental a participação Estatal.

4.2 Teoria da Arquitetura da Rede

A teoria da arquitetura da rede considera necessário o Estado determinar a natureza tecnológica do espaço virtual para que se possa regulamentar, por meio do direito, o mundo *on-line* (LESSIG apud SOUTO JUNIOR, 2010). Souto Junior (2010) afirma que esta corrente tem como principal expoente Lawrence Lessig.

A aliança entre governo e comércio é a proposta central desta teoria. A arquitetura da rede seria delineada pelos próprios agentes da rede, com intervenção do Estado para determinar os rumos a serem seguidos por esse ambiente. Desta forma, seria possível evitar que alguém do mercado determine um controle maior sobre a rede pelo tipo de programação, de forma alheia à vontade do Estado (SOUTO JUNIOR, 2010 p. 31).

Note-se, como exemplo, a divulgação de fotos e vídeos eróticos na rede. Em vez de proibir na totalidade a exposição deste material, que é legal a maiores de idade, o sistema judicial poderia exigir meios tecnológicos que evitem o acesso de menores de idade a esses conteúdos. Alguns provedores de correio eletrônico, por exemplo impedem automaticamente o envio de milhares de mensagens idênticas para destinatários múltiplos simultaneamente, presumindo que o conteúdo de tais mensagens é não-solicitado; Outro exemplo são os *web sites* que exploram o comércio eletrônico apenas autorizando determinada transação se utilizada criptografia para proteger os dados do consumidor.

Então ao regular a arquitetura da conduta do usuário, regula-se a conduta de forma indireta. Isso é a arquitetura. As normas são pautadas pelos programadores e usuários da rede, nem sempre através do legislador. Alguns provedores já possuem normas de conduta que formam a arquitetura da rede nos padrões por eles estabelecidos.

A solução proposta pela arquitetura seria mista, pois não ignora o valor legislativo nos atos praticados no ambiente virtual e acrescenta que normas de conduta têm o poder de suprir lacunas legislativas.

Alguns doutrinadores não concordam com Lessig, dentre eles Patrícia Peck, que propõe a criação de uma infinidade de leis próprias. Tal legislação seria limitada no tempo (vigência) e no espaço (territorialidade), dois conceitos que ganham outra dimensão em uma sociedade convergente (SOUTO JUNIOR, 2010, p. 33-34).

A tecnologia se desenvolve em velocidade bastante superior à legislativa, motivo que

demanda adaptação do direito às inovações trazidas pela tecnologia. Normas de conduta utilizadas pelos usuários para arquitetar o funcionamento da rede são relevantes em um local ainda ausente de legislação adequada, porém não suficientes.

Com isso, para essa teoria, o sistema jurídico tradicional é insuficiente para regular a conduta dos usuários da rede. A legislação e o mercado devem habitar o sistema concomitantemente.

4.3 Teoria do direito Internacional

A corrente internacional define o espaço virtual como um ambiente sem fronteiras e, por tal motivo, há o mundo eletrônico, desconsiderando países e suas fronteiras geográficas.

A Internet não possui dono e legislação única. Ela simplesmente existe e permite a circulação de milhões de arquivos diariamente e em diversos países. Condutas tidas como ilegais em alguns países não são ilícitas em outros, como os jogos de azar em *sites* virtuais.

A efetividade desta teoria está calcada em encarar o ambiente virtual como um local internacional pela falta de territorialidade. Transmite a ideia de cooperação legislativa entre os entes globais. As relações entre os países ocorreriam através de tratados e costumes internacionais.

Na visão de Carlos Alberto Rohrmann (ROHRMANN apud SOUTO JUNIOR, 2010):

> Os tratados internacionais têm sido utilizados pelo direito para normatizar situações que poderiam ocorrer em local em que o direito ainda seria, aparentemente, de difícil aplicação por falta do elemento territorialidade. Ou, de uma forma mais específica, por se tratarem de locais que não pertencem a nenhum Estado. (ROHRMANN, 2005, p. 28).

Neste contexto internacional não haveria soberania de Estado algum sobre o ambiente virtual. Por essa teoria, o internauta estaria sujeito à sua jurisdição de residência ou Estado no qual navega na rede, sendo, de acordo com Souto Junior (2010), mais um empecilho para solucionar divergências.

Dentre os maiores defensores dessa teoria, segundo este mesmo autor, é o professor norte-americano Stuart Biegel, que preconiza a utilização de modelos internacionais de cooperação (BIEGEL apud SOUTO JUNIOR, 2010). Biegel discute o problema da

regulamentação de uma área que não é limitada ao físico. Uma possível solução seria na elaboração legislativa com força executória em todo o mundo. O próprio autor entende a dificuldade dessa corrente, já que a legislação exige uma extensa análise dos costumes e do direito internacional.

4.4 Teoria Tradicionalista

A corrente tradicionalista defende a aplicação do direito doméstico nas relações ocorridas na rede mundial de computadores.

A Internet não possui barreiras, limites. Ela está no Brasil e no mundo, sem localização geográfica. A partir do momento que determinado material é disponibilizado no ciberespaço, todos podem acessá-lo. Aqui, reside o obstáculo inicial ao direito tradicional, pois ele se orienta pelo foro, seja domicílio de eleição, local de trabalho, do crime, etc (SOUTO JUNIOR, 2010).

As diferenças entre as correntes anteriormente citadas são extensas. Enquanto a libertária defende a completa ausência estatal da rede, sendo os internautas os detentores do controle, a teoria da arquitetura visa o controle através dos programas de computador, mas com sustentáculo estatal. Já a teoria internacional se sustenta na cooperação entre os Estados para elaboração de tratados e costumes internacionais. A tradicionalista utiliza do ordenamento jurídico doméstico para solucionar os impasses no ambiente virtual. Por essa corrente, os casos judiciais serão analisados através das normas vigentes, entendimento jurisprudencial e/ou tratados aos quais o Brasil é adepto.

De acordo com Carlos Alberto Rohrmann (ROHRMANN apud SOUTO JUNIOR, 2010), essa é a tendência a ser seguida pelo ambiente virtual: “A tendência pela regulamentação local, com a aplicação do direito doméstico vem demonstrando a viabilidade da regulamentação jurídica dos atos jurídicos praticados no ambiente eletrônico”.

5 CRIMES VIRTUAIS

As infrações e crimes no ambiente digital tem se constituído como uma problemática em destaque na atualidade. Inellas (apud NIGRI, 2004) que afirma que “o crime informático, caracteriza-se, principalmente, por constituir um ato lesivo cometido através de um computador ou de um periférico com a intenção de se obter uma vantagem indevida.”

Já o autor Souza (et al, 2012) afirma que crimes virtuais ou cibernéticos são atos praticados ilicitamente com o intuito de roubar, ofender, denegrir, prejudicar, abusar psicológica ou fisicamente outro indivíduo. Estes atos podem ser realizados contra uma pessoa ou contra bens materiais e imateriais, sendo que este último pode ser direcionado a bens governamentais, como bancos, ou pode ser realizado contra bens de um indivíduo.

Inellas (apud NIGRI, 2004) revela que os crimes informáticos mais comuns, são o furto, a fraude, o estelionato, a falsificação, o furto de tempo de rede de sistema de computador, a violação de sistemas de processamento de dados, a implantação de vírus, a criação de sites de pedofilia, de pornografia infantil, de incitação ao racismo, de violação de marcas através de registros de domínio, de pirataria digital, de violação de direitos autorais, de sabotagem e o terrorismo.

Apesar do crescimento dos tipos de crimes cometidos via Internet, não houve tais progressos por parte das leis que regularizam o meio virtual. Os atos praticados na rede surgiram antecipadamente a qualquer previsão legal tendo em vista as características favoráveis do mundo virtual. De acordo com Vianna (2000), os crimes digitais são um fenômeno mundial e se alastram rapidamente. Não obstante a isso, o direito penal parece não conseguir acompanhar o ritmo da tecnologia deixando muitas vezes os criminosos digitais impunes.

Nesta mesma direção Barbosa (et al apud NISHIJIMA, 2012) posiciona-se ao afirmar que a legislação acompanha a sociedade com certo atraso, por consequência disso, condutas sem previsão legal não são consideradas criminosas, mas também não são protegidas por nenhuma lei. Souto Junior (2010) acredita que por ser um meio de comunicação considerado recente, com maior desenvolvimento neste século, legislação, doutrina e posicionamentos jurisprudenciais ainda não são comuns no direito brasileiro.

Estas discussões sobre legislação e responsabilidades relacionadas aos cibercrimes

ocorrem em diversos países, não sendo uma problemática somente brasileira.

5.1 Identificação digital:

No mundo virtual, os usuários não possuem identificações como documentos e assinaturas. Cada pessoa recebe um identificador referente ao computador que a pessoa está utilizando. É através deste identificador que é possível se comunicar pela rede.

Este identificador é chamado de endereço IP e pertence ao protocolo de Internet (IP), cuja função é realizar a comunicação entre dois ou mais computadores pela rede. Atualmente o protocolo IP na versão quatro é o mais utilizado na grande maioria das redes (BRAGHETTO et al, 2003). Kurose e Ross (2010) afirmam que o protocolo IP é um dos principais protocolos da Internet.

Cabe destacar que o identificador do protocolo de internet, o endereço IPv4, possui um comprimento de 32 *bits*, resultando em cerca de 4 bilhões de combinações de endereços possíveis. Estes identificadores são descritos em notação decimal onde cada *byte* é dividido por um ponto.

Os endereços IPv4 são segmentados, através de classes de IPs. As classes são intervalos de tamanho fixo de endereços IP. As classes do IPv4 são segmentadas em: A, B, C, D, E. Além destas, existem classes especiais, onde ficam os IPs que não são endereçáveis, ou seja, que são reservados e que não podem ser atribuídos para equipamentos ou para redes.

O protocolo IP define intervalos de endereços reservados para redes privadas e para redes públicas. Para explicar o conceito de redes públicas e redes privadas é necessário saber a diferença de um endereço IP público e privado. Segundo Marcos (2013) os endereços IP públicos, são visíveis e acessíveis por qualquer computador conectado a Internet, ou seja, são globalmente conhecidos na Internet. Já os endereços IP privados, que podem ser acessíveis apenas por computadores que fazem parte daquela rede local, privada, de computadores, independente deles estarem conectados à Internet. Através destes conceitos definimos que redes privadas são redes que não podem se comunicar diretamente com as redes públicas, em razão de utilizarem IPs privados.

Em relação as redes privadas, todos os computadores possuem um endereço IP privado, no entanto um mesmo IP público quando conectados na Internet. Um exemplo deste

tipo de rede são as *Lan Houses*, onde vários computadores, cada um com um endereço IP privado, compartilham uma única conexão com a Internet (rede pública), através de um único endereço de IP público.

Os IPs públicos são de propriedade de provedores de acesso, grandes empresas ou instituições. Uma pessoa física não pode efetuar a compra de um endereço IP, no entanto é possível alugar um IP público de um provedor.

O protocolo IP possui um método de endereçamento parecido com os números de telefone. Assim como qualquer telefone no mundo é único, cada computador ligado na Internet possui um número único, chamado de endereço IP (público). Esse número serve para identificar o computador na Internet. Para se comunicar pela Internet, é necessário mandar mensagens endereçadas ao endereço IP do computador de destino.

5.2 Provas digitais:

Pode-se dizer que as atividades que utilizam como meio a Internet para comunicação, sempre são registradas e documentadas. Computadores, celulares e qualquer dispositivo eletrônico, sempre que conectado na Internet geram registro sobre as atividades realizadas.

Estas informações podem ser e são utilizadas como provas virtuais. Entretanto, sua vinculação está relacionada ao computador de procedência da ação. Isto se dá pois a identificação eletrônica de um equipamento conectado na Internet é através de seu endereço IP. Através dele, é possível determinar a localização geográfica do equipamento. No entanto, sabe-se que o endereço IP como prova virtual para cibercrimes não é suficiente para a identificação do equipamento, e consequentemente para a identificação do usuário infrator. Isso se dá em razão que o protocolo de acesso á Internet possui funcionalidades de disfarce do endereço IP. Algumas destas técnicas são:

I. IP-Spoofing: É uma técnica do protocolo IPv4 para personificar o endereço IP, onde um computador consegue se passar por outro, ou seja, onde um usuário consegue executar tarefas se passando por outro. Um exemplo prático desta técnica são os ataques de negação de serviços (*DoS - Denial of Service*).

Este tipo de ataque busca a sobrecarga do servidor alvo, através de requisições do

serviço disponibilizado pelo servidor atacado. Para que este tipo de ataque seja "bem-sucedido" é necessário um grande número de requisições para que o servidor não consiga "dar conta" e então sobrecarregue. Para isso, é necessário uma grande quantia de computadores. Geralmente estes ataques são feitos através de máquinas zumbi, ou seja, computadores infectados por códigos maliciosos, vírus que permitem o controle remoto do computador, sem que o dono do computador saiba disso.

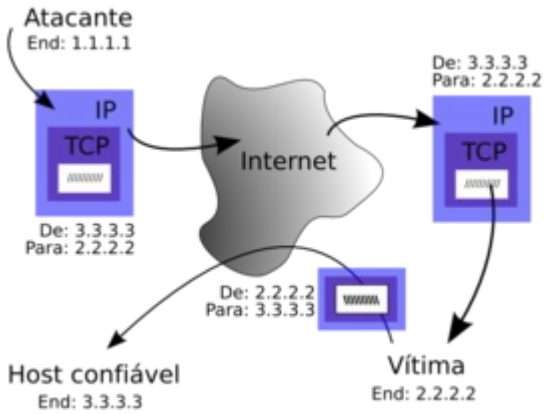

Figura 4 – Técnica de IP *Spoofing*.

Fonte: http://www.ebah.com.br/content/ABAAAemHMAF/introducao-ao-firewall?part=4

II. Mascaramento NAT: Esta funcionalidade possibilita a comunicação de uma rede privada, com diversos computadores, com a rede pública, através da utilização de apenas um IP público. Esta técnica foi criada para solucionar um sério problema do protocolo IPv4, a escassez de IPs públicos. Um exemplo bastante conhecido são as *Lan-Houses* e as redes públicas de acesso à Internet, onde geralmente possuem apenas um IP público para uma rede privada de computadores.

Marcos (2013) afirma que no caso da Internet predial, o mesmo endereço IP é sabidamente compartilhado por dezenas (por vezes centenas) de computadores, sendo virtualmente impossível se determinar o agente através da famosa sequencia de números.

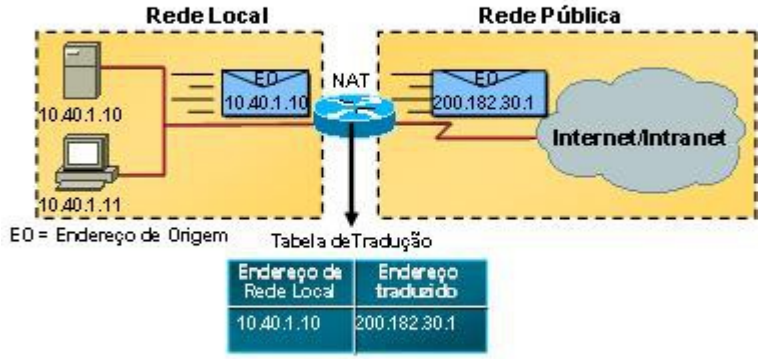

Figura 5 – Mascaramento *NAT.*

Fonte: http://www.gta.ufrj.br/grad/01_2/nat/

III. Proxy: É um servidor que centraliza todas as conexões de uma rede, onde recebe as requisições dos clientes ,executa e depois retorna aos remetentes. Os servidores *proxy* possuem diversas funcionalidades, como o controle de acesso *web,* através de filtros de conteúdos, e o acesso anônimo a Internet pelos clientes.

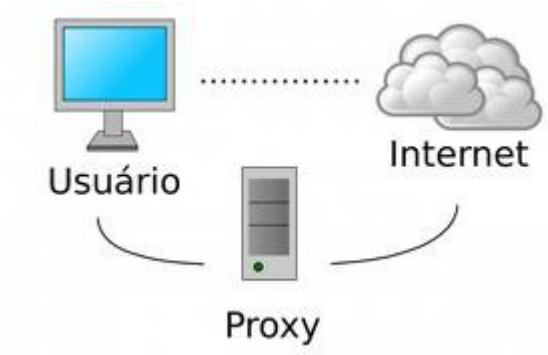

Figura 6 – Servidor *Proxy*.

Fonte: http://canaltech.com.br/o-que-e/software/Conheca-todos-os-formatos-de-audio/

Inellas (2004) afirma que alguns criminosos, camuflam seu endereço IP, para impedir ou dificultar sua identificação, através das técnicas de IP *Spoofing* e os *Proxies*. Assim o IP de origem é trocado, dificultando sua identificação.

Nesta perspectiva, as características do protocolo IP, no que se refere a identificação, são deficientes para a responsabilização dos crimes virtuais. Isto posto, por serem funcionalidades implementadas no protocolo de acesso à Internet, não há atualmente uma solução viável destas problemáticas dentro da prerrogativa do protocolo IP. Para isso, é necessário buscar soluções que consigam combater estas problemáticas, considerando as funcionalidades do protocolo.

Marcos (2013) afirma que, mesmo que se consiga identificar efetivamente um ou alguns dos endereços IP que originaram o ataque, eles não necessariamente apontam para o real autor do crime ou ato delituoso. Os proprietários destes computadores infectados, que foram usados para cometer delitos, em quase sua totalidade, não tiveram participação direta, conhecida e proposital. Na verdade, sequer imaginavam que pudessem ser vítimas de tal prática.

Marcos (apud SCUDERE, 2013) afirma que o IP ou IPs identificados como "evidências legítimas e sólidas" de participação do(s) ataque(s) podem pertencer – de fato – a terceiros, podendo levar a endereços físicos falsos, ou ainda nos induzir a erro, indicando uma origem por demais óbvia à vítima através de eventos anteriores ou julgamentos precipitados.

Marcos (apud SEVAGE, 2013) afirma que:

> O atual design da internet garante virtualmente o anonimato dos usuários. Mas hoje esse anonimato é o desafio mais incômodo para as autoridades. Um agressor na internet pode rotear uma conexão através de muitos países para ocultar a sua localização, que pode ser atrávés de uma conta em uma Lan-House adquirida com um cartão de crédito roubado. Logo, mesmo com a proposta de se apontar uma direção, uma tendência para os casos acima, as respostas certas no Direito Digital ainda são raras.

6 ANÁLISE DOS DADOS

O Rio Grande do Sul é um dos estados brasileiros que apresenta um número expressivo de iniciativas de Cidades Digitais. Segundo informações do site

RedeCidadeDigital[3] existem, aproximadamente, 21 cidades que desenvolveram ou estão em processo de criação de programas e serviços de inclusão digital, dentre eles: sinal de Internet gratuita, governo eletrônico (e-gov), telecentros, centrais de monitoramento e portais de comunicação.

Do total de cidades digitais do Rio grande do Sul, apenas cinco (5) atendem os requisitos de análise do presente estudo, os quais dizem respeito a disponibilização de acesso público a Internet. Esta relação está expressa no quadro 1 a seguir:

Disponibilizam acesso gratuito à Internet	**Não disponibilizam acesso gratuito à Internet**		
Alvorada	Canoas	Jari	São Leopoldo
Campo Bom	Caxias do Sul	Lajeado	São Miguel das Missões
Garibaldi	Candelária	Não-me-toque	Tapejara
Novo Hamburgo	Dois Irmãos	Nova Bassano	Venâncio Aires
Porto Alegre	Entre-Ijuís	Piratini	
	Estrela	Santo Ângelo	

Quadro 1 – Cidades Digitais do Rio Grande do Sul.

6.1 Cidades Digitais do Rio Grande do Sul que disponibilizam acesso gratuito á Internet[4]

6.1.1 Alvorada

Cidade localizada a 16 km da capital Porto Alegre, Alvorada possui o programa Internet Social, implementado sob o projeto Alvorada Cidade Digital, que disponibiliza pontos de Internet gratuita a toda a população. O acesso é concedido através de uma rede composta por vinte e cinco pontos de acesso, localizados em escolas, unidades de saúde e locais públicos, permitindo que o máximo de pessoas tenham acesso à Internet Social. Aos

[3] Disponível em <http://www.redecidadedigital.com.br/mapa_rs.php>

[4] Todas as informações foram obtidas nos sites das cidades digitais investigadas.

locais com distância maior que 200 metros do ponto de acesso, é necessário a utilização de antenas. (ALVORADA, 2013)

Figura 7 – Projeto Alvorada cidade digital.
Fonte: Alvorada (2013).

O programa Internet Social possui um sistema de autenticação onde oferece uma conta de acesso para cada cidadão, pessoa física com CPF, jurídica com CNPJ e visitantes, sendo estes maiores de 18 anos. Este acesso se dá através de um cadastro disponível no site do programa. O método de autenticação de Alvorada não valida as informações dos usuários e o acesso é permitido apenas para maiores de 18 anos. Após o preenchimento do formulário de cadastro, em até 24 horas a conexão é liberada, através do seu CPF/CNPJ como login e a senha cadastrada. O município disponibiliza a velocidade de acesso de 300Kbps para cada usuário conectado.

6.1.2 Campo Bom

A cidade Campo Bom, localizada a 57 quilômetros de Porto Alegre, implementou um projeto de cidade digital no ano de 2009, sendo uma das cidades digitais pioneiras no Rio Grande do Sul. O município possui um programa chamado de W-Campo Bom, onde disponibiliza Internet gratuita para toda a sua população, através de 21 antenas de transmissão.

Figura 8 – Programa W-Campo Bom.
Fonte: Campo Bom (2013).

De acordo com Fabiano Boff, coordenador de TI do município, “é um projeto que possibilitou a ampliação da inclusão digital dentro do nosso município, dando àqueles que não tinham condições de pagar por um serviço privado, acesso não apenas à web, mas a educação, cultura e conhecimento” afirma Boff. (CAMPO BOM, 2013)

O programa W-Campo Bom conta com um sistema de autenticação dos usuários com validação das informações, onde que para utilizar a rede pública, é necessário que o usuário faça um cadastro na prefeitura, pessoalmente. Após concluída esta etapa, o cidadão recebe uma senha pessoal e então é autorizado o acesso a rede.

Além da Internet pública, o município disponibiliza outros serviços eletrônicos como o Portal do Cidadão, para disponibilização de serviços aos contribuintes e contabilistas; Nota Fiscal Eletrônica; e, implantação de telefonia VOIP.

6.1.3 Garibaldi

Cidade localizada na serra gaúcha, Garibaldi foi um dos primeiros municípios a implementar o programa de cidade digital do Rio Grande do Sul. Segundo Garibaldi (2013) seu projeto iniciou em setembro de 2011, através da construção de onze quilômetros de fibra óptica pela cidade, com o objetivo de interligar os setores públicos, como postos de saúde, escolas, bibliotecas e a prefeitura. Posteriormente o município criou o programa Internet para todos, onde foi implementada uma infraestrutura de rede *Wireless*, disponibilizando acesso

gratuito a população.

Figura 9 – Programa Internet para todos de Garibaldi.

Fonte: Garibaldi (2013).

Existem nove áreas na cidade que possuem cobertura do sinal *Wi-Fi*, e para as áreas que não possuem abrangência, é possível utilizar antenas para a recepção do sinal, possibilitando aos cidadãos a utilização da Internet em suas casas. (GARIBALDI, 2013)

Garibaldi possui um sistema de autenticação de usuário no qual é necessário um cadastro prévio, onde é solicitado o preenchimento de um formulário com diversas informações pessoais.

Figura 10 – Informações de pré-cadastro de Garibaldi.

Fonte: Garibaldi (2013).

Após, é feita uma análise de viabilidade técnica, e então o usuário é chamado para efetuar a validação do cadastro presencialmente.

6.1.4 Novo Hamburgo

Município localizado a 40 km de Porto Alegre, Novo Hamburgo começou a se tornar uma cidade digital no ano de 2013, a partir da disponibilização de Internet gratuita em uma praça da cidade como início da implementação do projeto digital. Neste projeto serão instalados 28 quilômetros de fibra óptica pela cidade, além da disponibilização de serviços eletrônicos a população.

A rede *wireless* de acesso público não possui sistema de autenticação. Para ter acesso, os usuários deverão aceitar os termos e as políticas de uso da rede. Após a concordância, o acesso é liberado. Não existe nenhum tipo de identificação dos usuários conectados na rede.

6.1.5 Porto Alegre

A cidade de Porto Alegre, capital do estado, é a primeira capital brasileira a disponibilizar uma rede pública gratuita de Internet sem fio (Procempa, 2013). O município iniciou a implementação do projeto de cidade digital no ano de 2006, onde inicialmente o objetivo era prover acesso à Internet gratuita à população.

Hoje, a Prefeitura de Porto Alegre possui108 pontos de acesso gratuito a Internet espalhados pela cidade e também possui dois outros projetos em funcionamento, chamados de *Wireless* Educacional e *Wireless* Saúde.

O projeto educacional disponibiliza acesso à Internet de alta velocidade da Procempa as escolas municipais, trazendo benefícios como rematrículas online. O projeto de saúde,

busca a integração de informações para o atendimento ao usuário. Este projeto visa criar o prontuário eletrônico do paciente, implementando o conceito de assistência continuada.

Segundo informações da Procempa (2013), a população pode acessar livremente a rede pública sem nenhum tipo de autenticação, ou seja, para conectar na rede é necessário apenas um equipamento portátil com dispositivo *Wireless*.

6.2 Discussão dos Dados

O estudo realizado permitiu identificar que das cinco cidades digitais que disponibilizam acesso gratuito de Internet à população, duas não fazem uso de nenhuma forma de autenticação dos usuários ficando sem nenhum tipo de controle e gerência dos usuários da rede. Deste modo, fica clara a dificuldade de repassar a responsabilidade de um crime, caso tenha partido de um usuário específico utilizando a rede. As outras três cidades analisadas utilizam mecanismos de cadastro e autenticação dos usuários.

Cidades Digitais sem autenticação	**Cidades Digitais com autenticação**
Novo Hamburgo	Alvorada
Porto Alegre	Campo Bom
	Garibaldi

Quadro 2 – Relação das cidades digitais com e sem modelos de autenticação.

O processo de gerenciamento de identidades nas cidades de Alvorada, Campo Bom e Garibaldi fazem uso de um conjunto de informações pessoais do usuário como CPF/CNPJ, RG, Endereço. Entretanto dentre as três cidades apenas uma realiza a validação das informações fornecidas pelos usuários.

Cabe destacar que a identificação do usuário precisa ser acompanhada da comprovação dos dados, de forma a verificar a veracidade das informações disponibilizadas. Como se sabe atualmente a possibilidade de ter acesso a dados pessoais de outras pessoas é

uma realidade no mundo virtual, viabilizando a utilização de informações falsas.

Garibaldi é a única cidade digital do Rio Grande do Sul, segundo informações do site RedeCidadeDigital[5], que realiza a validação dos dados que os cidadãos preenchem no formulário de cadastro para acesso à Internet pública. Isso se dá através de uma convocação presencial no local de credenciamento da rede, buscando a confirmação das informações disponibilizadas no pré-cadastro.

De fato estes encaminhamentos de confirmação são ações que corroboram para uma identificação mais efetiva dos usuários, para além da identificação do IP. Assim o gerenciamento de identidade teria como dados além de informações sobre as máquinas, informações relativas ao usuário. Considera-se que esta iniciativa pode ser indicada como um avanço em relação a ausência total de autenticação dos usuários.

Pondera-se ainda que a utilização de bancos de dados públicos para a autenticação, como sendo uma ação que permitiria a composição de um conjunto de informações sobre o usuário final que viabilizaria uma validação da identificação mais apurada.

Nesta direção, destaca-se para a possibilidade da adoção do sistema do Cadastro de Pessoa Física (CPF), que apesar de não ser um documento obrigatório a toda população, seu nível de abrangência é considerável.

6.2.1 CPF

As informações relativas ao Cadastro de Pessoa Física (CPF) são possibilidades viáveis e funcionais de utilização de cadastramento, tendo em vista que são informações que possuem gerenciamento estatal acerca dos dados, viabilizando a composição de um banco com informações variadas sobre os usuários. Através do número do CPF é possível obter diversas informações, conforme figura 5.

[5] Disponível em <http://www.redecidadedigital.com.br/mapa_rs.php>

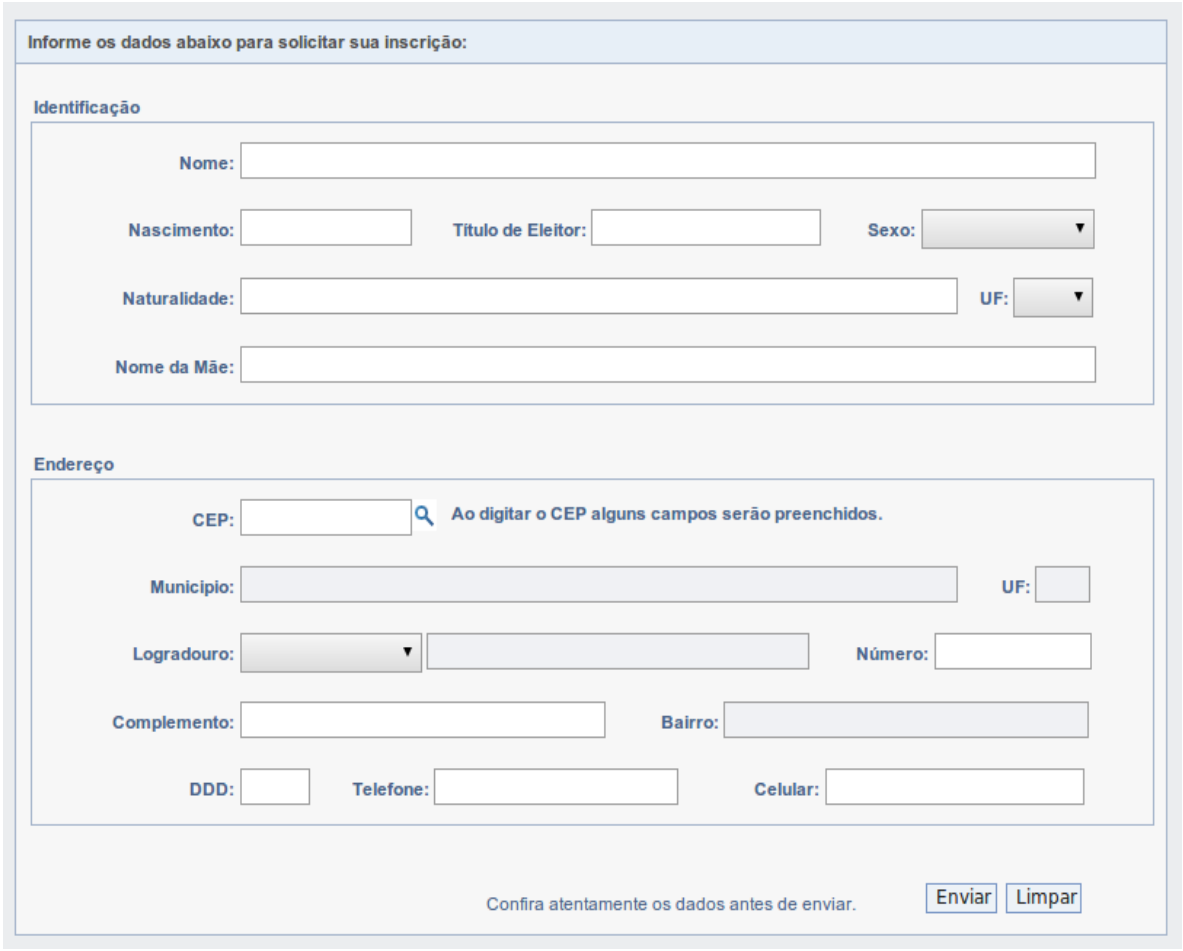

Figura 11 – Informações do Cadastro de Pessoa Física.

Apesar deste documento não ser de uso obrigatório, atinge grande parte da população, devido a sua gama de utilização, independente da idade. Diversas atividades exigem o CPF como documento obrigatório, tais como: abrir conta em banco, declarar imposto de renda, operações imobiliárias, operações bancárias, solicitar a Carteira de Trabalho e Previdência Social (CTPS), etc.

Como suporte complementar a estes dados considera-se que as informações relativas ao título eleitoral poderiam ser incorporadas tendo em vista que se refere a um documento obrigatório a partir dos 18 anos de idade.

6.2.2 TITULO ELEITORAL

A emissão do título pode ser feita a partir dos 16 anos, porém é facultativo até completar 18 anos. O Título de eleitor é o documento que comprova que um determinado cidadão está inscrito na Justiça Eleitoral do País e se encontra apto a participar das eleições, tanto como candidato como votante no âmbito municipal, estadual e federal. É condição fundamental para este documento a nacionalidade brasileira.

Como informações deste banco de cadastro, está o nome do eleitor, a data de nascimento, a unidade da federação, o município, seção eleitoral onde o cidadão vota, o número da inscrição eleitoral, a data de emissão, a assinatura do juiz eleitoral, a assinatura do eleitor ou a impressão digital de seu polegar (caso se trate de um analfabeto).

Atualmente está ocorrendo o recadastramento de toda a população brasileira a partir do programa de identificação biométrica da justiça eleitoral. Este processo iniciou em 2012 e tem previsão de finalizar até 2014. Conforme informações disponíveis no site do tribunal superior eleitoral, a biometria refere-se a um método automático de reconhecimento individual baseado em medidas biológicas (anatômicas e fisiológicas). Tem como principal objetivo reconhecer, verificar ou identificar uma pessoa que foi previamente cadastrada. Para o reconhecimento individual são coletados dados biométricos por meio de sensores que os colocam em formato digital. No caso do cadastramento que será efetuado pela Justiça Eleitoral, os dados serão coletados por um *scanner*. Com esta iniciativa o Brasil poderá criar o maior banco de dados de imagens de impressão digital existente no mundo, de acordo com informações obtidas no site do tribunal superior eleitoral.

De acordo ainda com este tribunal, a identificação biométrica dos eleitores brasileiros também servirá para outros fins. Conforme nota no site oficial:

> A corte firmou acordo com o Ministério da Justiça para colaborar com o fornecimento do Cadastro da Justiça Eleitoral, que compreende mais de 140 milhões de eleitores. O sistema auxiliará na implantação do Registro de Identificação Civil (RIC), o número único que identificará cada brasileiro para identidade, carteira de motorista, passaporte e outros documentos. Disponível em (TSE, 2013) <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/biometria-1>

Considera-se que as ações indicadas de utilização do CPF e título eleitoral são viáveis e operacionais, permitindo a identificação de uma autoria para além do endereço do computador na rede. No caso do Cadastro de Pessoa Física pelo fato de abranger uma diversidade de informações sobre o usuário e pelo fato de constituir-se em um banco de dados nacional. Da mesma forma, o Título eleitoral, o qual agrega ainda a sua obrigatoriedade, abrangendo a totalidade da população maior de dezoito anos, bem como pela possibilidade

que se abre pela adoção da biometria e a viabilidade deste documento ser utilizado para outros fins.

Entretanto, sua confirmação como estratégia que permita a responsabilização legal do usuário não é possível de ser feita, tendo em vista a natureza das relações estabelecidas na Internet e a falta de uma legislação específica a este ambiente operacional. Destaca-se que esta questão de autoria tem sido feita a partir posicionamentos jurisprudenciais não existindo uma legislação clara sobre os dados relativos a responsabilização legal do usuário. Logo, as considerações destacadas caracterizam-se como indicativos operacionalizáveis de identificação do usuário e de mecanismos de validação de informações.

O estudo realizado acerca do processo de gerenciamento de identidades permitiu ainda a identificação de uma proposta desenvolvida fora do âmbito nacional que atende os quesitos de segurança da rede almejados para a identificação e responsabilização penal do usuário. Esta proposta se encontra em funcionamento em alguns estados-membros da União Europeia e denomina-se Cartão Inteligente de Identificação Eletrônica.

6.2.2 Cartão Inteligente

Atualmente este projeto está implementado em alguns países do continente europeu. Rossler (2008) afirma que diversos estados-membros da UE estão buscando a identificação eletrônica aos seus cidadãos. Segundo ele, a Finlândia foi a pioneira a implementar o projeto de identificação, em dezembro de 1999. A Itália começou a utilizar em março de 2001. A Bélgica e a Estônia também implementaram as identidades eletrônicas para seus cidadãos em 2004. A Áustria, Suécia e a Espanha também já estão utilizam esta tecnologia.

O modelo traz uma solução de autenticação eletrônica central que fornece autenticação genérica e serviços de assinatura eletrônica que permite a identificação segura do usuário do sistema[6] para a utilização de serviços eletrônicos prestados pelo governo (e-Gov), onde cada cidadão passa a ter uma identidade eletrônica. Este método de identificação se dá através da utilização de cartões inteligentes (*Smart Cards*) de identidade eletrônica com base em infraestrutura de chaves públicas (ICP).

Este modelo de autenticação tem o objetivo de proporcionar confiança e segurança

[6] Dutch Government to set up e-authentication service. Disponível em <http://istrg.som.surrey.ac.uk/projects/guide/files/>. Acesso em 09/07/2013.

para todos os tipos de transações em toda a Europa (ROSSLER, 2008, p.2). Para se tornar possível a utilização dos cartões e-ID como prova de identificação e assinatura eletrônica, foi necessário adequar um conjunto de normas de regulamentações, dos países que a implementaram, sobre os requisitos técnicos, tais como os requisitos mínimos para dispositivos de criação de assinatura eletrônica, requisitos organizacionais para prestadores de serviços de certificação, formatos para assinaturas eletrônicas e certificados digitais, e se necessário modificações nas leis para viabilizar este processo. Segundo Euclid (2003), na Estônia, foi criada uma lei específica para regulamentar os documentos de identidade e de assinatura eletrônica. Na Finlândia existe uma lei referente aos cartões de identificação e sobre os serviços eletrônicos, criadas em 1999.

6.2.1 Cartão de Identificação Eletrônica

Inicialmente, para a viabilização do projeto, foi necessário criar um método para autenticar e identificar os cidadãos eletronicamente. Precisava-se criar uma forma que combatesse o não-repúdio por parte do usuário e que fosse válido, como um documento real (físico) para a identificação do usuário pela rede, por parte da legislação. A solução criada foi o Cartão de Identificação Eletrônica (cartão e-ID).

Figura 12 – Carteira de Identificação Eletrônica da Bélgica.

O livro Euclid (2003 p. 11, tradução nossa), define o conceito do cartão de

Identificação Eletrônica como “um token baseado em cartão inteligente, que contém as chaves privadas e os certificados de chaves públicas correspondentes. Opcionalmente, o cartão pode também incorporar um documento de identificação visual”. Rossler (2008) diz que o cartão e-ID não necessariamente deva ser um cartão inteligente, mas poderia ser um dispositivo móvel, token usb etc, desde que atenda aos requisitos de assinatura eletrônica avançada, como definida na Diretiva de Assinaturas Eletrônicas da UE.

Rossler (2008) afirma que:

> O conceito de e-ID pretende construir um símbolo de identificação eletrônica universalmente reconhecida para a identificação dos cidadãos em vários cenários de uso. (…) Com o e-ID, será possível passar a identidade, uma vez emitida a partir de uma entidade jurídica em outras infra-estruturas existentes de aplicativos, tanto no setor público como no setor privado. (ROSSLER, 2008, p. 52-53, tradução nossa)

O cartão e-ID é composto por um microchip, onde nele são armazenadas informações pessoais do cidadão, sob uma infraestrutura de criptografia de chaves públicas. O chip é composto de um certificado digital remoto que permite a autenticação do titular do cartão na execução dos serviços eletrônicos, garantindo uma forma segura de acesso as aplicações eletrônicas. O cartão possui a assinatura eletrônica do cidadão, podendo ser utilizada na autenticação de documentos e serviços eletrônicos[7].

O cidadão pode usar o cartão para diversas atividades. Rossler (2008, p. 1, tradução nossa) acredita que o cidadão pode utilizar o cartão e-ID para “a identificação, autenticação e assinatura eletrônica, e também poderá desfrutar dos serviços eletrônicos prestados por seu governo e do setor privado.

Este projeto está associado a utilização de serviços de governo eletrônico de forma a garantir a segurança e a certeza da identidade dos usuários a partir do *smart-card*. Conclui-se que o conceito de e-ID levará a um tratamento de dados dos cidadãos automaticamente.

7 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo central investigar o sistema de autenticação das cidades digitais do Rio Grande do Sul que disponibilizam acesso à Internet de forma gratuita a

[7] Dutch Government to set up e- authentication service . Disponível em <http://istrg.som.surrey.ac.uk/projects/guide/files/>. Acesso em 09/07/2013.

população. Nesta direção, a pesquisa evidenciou que apenas 24% do total de cidades digitais implementadas apresenta uma rede pública de Internet com acesso livre aos cidadãos.

No que se refere ao gerenciamento de identidades dos usuários, as cidades investigadas fazem uso de informações gerais, tais como CPF/CNPJ, RG, Nome, Endereço compondo um cadastro individual. A partir deste cadastro é fornecido ao usuário um login e uma senha de acesso a rede. Entretanto, o processo de validação dos dados dos usuários é efetivado apenas em uma das cidades investigadas. Considera-se que esta iniciativa pode ser indicada como um avanço quando comparada a ausência total de autenticação dos usuários, evitando que informações falsas sejam utilizadas. No entanto, a bibliografia consultada sobre os cibercrimes não permitem afirmar que este procedimento garante a identificação eletrônica do usuário.

Importa destacar que a legislação vigente não possui instrumentos suficientes para compor uma prova de um crime virtual dentro dos parâmetros de funcionalidade da Internet. Isso se dá em razão do modo de funcionamento do protocolo de acesso à Internet, que corrobora com o anonimato do usuário. Entende-se que uma alteração nesta versão do protocolo não é viável, visto que demandaria a transformação total do modo de operacionalização da Rede Mundial de Computadores.

Logo a alternativa está em pensar propostas que permitam a identificação do usuário dentro das limitações que o protocolo impõe. Assim, considera-se como indicativos de gerenciamento de identidades nas cidades digitais:

•Ações que garantam a veracidade dos dados cadastrais dos usuários, o que seria obtido a partir da utilização de bancos de informações de acesso da administração pública, tais como o CPF e o cadastro do título eleitoral.

•Confirmação dos dados, acima citados, de modo a tornar operacional o gerenciamento de identidades. Considera-se que a utilização dos dados cadastrais vinculados ao CPF e Título eleitoral possuem um alto grau de funcionalidade, tendo em vista sua abrangência na população municipal.

Os indicativos citados compõem parâmetros para uma solução viável e operacional no contexto brasileiro. Representam o delineamento da identificação de uma autoria para além do endereço do computador na rede. Entretanto, sua validação como estratégia que permita a responsabilização legal do usuário ainda é um tema que merece maiores aprofundamentos.

Já a proposta de cartões inteligentes utilizados em alguns estados-membros da União Europeia evidencia indicativos efetivos de identificação eletrônica dos usuários. Entretanto a

sua operacionalização no Brasil exigiria implementações de hardware e software que viabilizassem a criação do cartão de identificação, bem como, a adequação da legislação de forma a reconhecer a legalidade deste procedimento.

Considera-se, ainda, que ações desta natureza são fundamentais para a consolidação de uma política de segurança da rede que dê confiabilidade as relações estabelecidas no ambiente virtual e consequentemente o incremento dos projetos de cidades digitais com disponibilidade gratuita de Internet a população.

Nesta direção ressalta-se para o caráter exploratório do presente estudo sobre o gerenciamento de identidades nas cidades digitais do Rio Grande do Sul, expressando para a necessidade de novos estudos que venham a corroborar para a revisão, ampliação ou consolidação das considerações aqui levantadas.

REFERÊNCIAS

ALVORADA, P. M. de. **Internet Social**. Disponível em: <http://www.alvorada.rs.gov.br/>. Acesso em 18 de abril de 2013.

BARBOSA, D. P.; NISHIJIMA, M.; COAN, A. L.; NOVAIS, T. M. **Implicações de externalidades negativas da internet sobre a legislação brasileira de crimes no ciberespaço:** O caso de ataques de negação de serviço. Fundação Instituto de Pesquisas Econômicas, v., p. 29-36, 2012.

BORBA, Marcelo de. **Acesso gratuito a internet:** Uma proposta de cadastro e autenticação para o acesso à internet em locais públicos. 2012. 51 f. Monografia (Graduação em Segurança da Informação) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2012.

BRAGHETTO, L, F, B; SILVA, S. C. da; BARBOSA, L. A. M. **IPSec Segurança de Redes** – INF542. 2003. Disponível em: <http://www.braghetto.eti.br/files/IPSec%20-%20Versao%20Final.pdf>. Acesso em 24 de abril de 2013.

CAMPO BOM, P. M. de. **A Internet Grátis de Campo Bom.** Disponível em: <http://www.campobom.rs.gov.br/>. Acesso em 18 de abril de 2013.

COLLI, Maciel. **Cibercrimes:** Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos. Curitiba: Juruá Editora, 2010.

COMUNICAÇÕES, B. M. das. **Edital de Chamada Pública no 01/2012**. Disponível em: <http://www.mc.gov.br/imagens/inclusao-digital/editais/edital-de-chamada-publica-n-001-2012-mc.odt>. Acesso em: 03 de abril de 2013.

ESPÍNDOLA, C. E; OLIVEIRA, J. B. F. de; FORMIGA, M. M. **A Tecnologia da Informação Como Meio para Facilitar o Acesso do Cidadão aos Serviços Públicos.** 2011. Disponível em <http://www.sgc.goias.gov.br/upload/arquivos/2011-06/painel_42-148_149_150.pdf>. Acesso em: 12 de maio de 2013.

EUCLID. **Electronic identity white paper**. Smart Cards / Trailblazer1. 2003 :Public Identity, V 1.0.; European initiative for a Citizen digital ID solution. Disponível em: <http://www.electronic-identity.org/> Acesso em 18 de maio de 2013.

FREY, Klaus. **Governança Eletrônica:** experiências de cidades européias e algumas lições para países em desenvolvimento. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf> Acesso em 13 de março de 2013.

GARIBALDI, P. M. de. **Internet Para Todos**. Disponível em: <http://internetparatodos.garibaldi.rs.gov.br>. Acesso em 12 de abril de 2013.

Guia das Cidades Digitais: Plano nacional de banda larga. v. 3, n. 3, 1-24, 2011. Disponível em: <http://www.networkeventos.com.br/GCD3.pdf> Acesso em 12 de abril de 2013.

INELLAS, G. C. Z de. **Crimes na Internet.** São Paulo: Editora Juarez de Oliveira, 2004.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet:** Uma abordagem Top-down. 5. ed. São Paulo: Addison Wesley, 2010.

MARCOS, S. E. de. **A Fragilidade do Endereço IP como Prova Virtual.** Disponível em: <http://www.trezentos.blog.br/wp-content/uploads/tcc_a-fragilidade-do-endereco-ip-como-prova-virtual.pdf >. Acesso em 04 de junho de 2013.

PROCEMPA. Procempa Livre e Gratuita. Disponível em: <http://www.procempa.com.br/default.php?p_secao=76>. Acesso em 22 de abril de 2013.

SIMÃO, J. B. **A concepção de um modelo de cidade digital baseado nas necessidades informacionais do cidadão:** o caso dos municípios brasileiros de pequeno porte. 2010. 134 p. Tese (Doutorado em Ciência da Computação) — Programa de Pós-Graduação em Ciência da Informação - PPGCINF, UnB, Brasília, 2010.

SOUTO, A. A.; DALL'ANTONIA, J. C.; HOLANDA, G. M. d. **As cidades digitais no mapa do Brasil:** uma rota para a inclusão digital. In: 2006, Brasília, DF. Ministério das Comunicações, 2006. Disponível em: <http://www.cpqd.com.br/component/docman/doc_download/146-as-cidades-digitais-no-mapado-brasil.html>. Acesso em: 12 março 2013.

SOUTO JUNIOR, J. H. **A responsabilidade civil dos provedores de hospedagem frente aos atos praticados pelos seus usuários e terceiros.** 2010. 119 f. Dissertação (Graduação em Direito) – Faculdade de Direito Milton Campos, Nova Lima, 2010.

SOUZA, J. L. R de; MENESES, T. G; SOUZA, V. S. dos S; CABRAL, V. B. da S. Crimes virtuais, punições legais. 2012. Salvador, Bahia. Disponível em: <http://www.slideshare.net/VictorSaid/artigo-crimes-virtuais-punies-reais>. Acesso em 22 de junho de 2013

TANENBAUM, Andrew S. Redes de Computadores. 4. ed. Rio de Janeiro: Elsevier, 2003.

ROSSLER. T. Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. 2008. Disponível em: <http://computerscience.nl/docs/vakken/cry/Projects/OostenrijkseEid.doc.> Acesso em 04 de maio de 2013.

VIANNA, T. L. **Dos Crimes pela Internet.** UFMG, Belo Horizonte, 2000. Disponível em: <http://www.alfa-redi.org/sites/default/files/articles/files/vianna.pdf>. Acesso em 22 de junho de 2013.