Responsabilidade Civil por Ato Ilícito na Utilização de Rede Corporativa: a utilização do Captive Portal como ferramenta na autenticação de acessos à Internet
Civil Liability for Unlawful Acts in the Use of Corporate Network: the use of Captive Portal as a tool to authenticate Internet access

Fabrício V. dos Santos
Tribunal Regional Eleitoral de Santa Catarina – (TRE-SC)
R. Barão do Rio Branco, 377, Sala 300 – Centro – 89240-000
São Francisco do Sul – SC – Brasil
fveiga@tre-sc.jus.br

Marcio M. Piffer
Instituto Federal Catarinense – Campus Araquari (IFC)
Rodovia BR 280 - km 27 – Cx. Postal 21 - CEP 89245-000
Araquari – SC – Brasil
marcio.piffer@ifc.edu.br

ABSTRACT

Este trabalho demonstra como tribunais brasileiros tratam a responsabilidade civil do proprietário de uma rede de computadores quando ocorre um ato ilícito na Internet originado desta rede privada. Abordará brevemente a responsabilidade civil, a legislação e o entendimento e jurisprudencial sobre o tema, o rastreamento de endereços IP para os tribunais e a importância do registro e guarda das conexões à Internet originadas de uma rede privada. Apresentaremos proposta de solução em software livre para controlar o acesso à Internet, no intuito de auxiliar e identificar o responsável causador do prejuízo ou dano, fornecendo ao administrador e ao proprietário da rede mecanismos idôneos de prova de autoria do dano verificado.

ABSTRACT

This study demonstrates how the Brazilian courts consider the civil liability of the owner of a computer network when an unlawful act occurs on the Internet originated from their private network. After a brief review of the civil liability institute, legislation and jurisprudence on the subject, addresses tracking to the courts and the importance of registering and saving Internet connections originating from a private network. Besides, it presents a proposed free software solution implemented to control access to the Internet, in order to assist and identify the responsible party that caused the damage, providing the administrator and network owner suitable proof of authorship of the damage verified.

CCS Concepts

•**Applied computing** → *Law;*

Keywords

Responsabilidade civil; rede corporativa; captive portal; controle de acesso
Civil responsability; corporate network; captive portal; access control

1. INTRODUÇÃO

A utilização dos recursos de rede das organizações por seus colaboradores, quando desviados da finalidade a qual é disponibilizada, pode gerar consequências cíveis à corporação, pois é responsabilidade do proprietário a utilização de sua rede. Assim, a fim de se identificar e responsabilizar eventual infração na má utilização da rede corporativa, é importante a utilização de um mecanismo de controle de acesso à rede. Tanto o Marco Civil da Internet, Lei nº 12.965/2014 [5], doravante referenciado apenas como MCI, como o Código Civil, Lei nº 10.406/2002, [1] doravante referenciado apenas como CC, consideram objetiva a responsabilidade civil das organizações no mau uso dos referidos recursos disponibilizados aos seus colaboradores, ou seja, é responsabilidade da corporação arcar e indenizar qualquer dano causado a uma terceira pessoa caso este dano tenha como origem a sua rede de computadores.

O art. 10 da Lei n. 12.965/2014 [5] estabelece critérios mínimos para que se identifique o causador de dano aos provedores de serviço, visando rastrear eventual causador de dano civil. Estes critérios podem ser utilizados, analogicamente, pelo proprietário da rede, para identificar o usuário que utilizou os recursos a ele disponibilizados e que ocasionaram dano ou prejuízo a outra pessoa, para que se possa responsabilizar o efetivo autor do fato. Tem-se por premissa a adoção de um mecanismo eficiente, capaz de guardar os registros das conexões efetuadas a partir de uma estação, com a data e hora do início e término da conexão, a duração, o

endereço IP utilizado e uma informação acerca do usuário que a realizou, baseada em software livre, para, caso exista a necessidade, acionar o responsável judicialmente. Ademais, a guarda das informações referentes a quem está utilizando sua rede, o período de uso, bem como o IP utilizado pelo terminal.

Na solução estruturada, que visa um meio de identificação do usuário e período por meio de software livre, é proposto a utilização de IP (*Internet Protocol*) públicos, como uma solução simples e eficaz no caso de pequenas e médias empresas/corporações, bem como a manutenção e guarda dos registros de log gerados. Assim, busca-se no presente analisar a responsabilidade civil e suas consequências quando há má utilização dos recursos oferecidos a terceiros por uma empresa, instituição ou corporação. Para isto, será feita uma análise doutrinária e jurisprudencial do tema, e sua aplicação prática no cotidiano do administrador de redes, bem como a implementação de um mecanismo de autenticação de acesso à Internet apto a controlar e registrar esses acessos, aliado a guarda dessas informações, com o fim de resguardar o proprietário da rede dos danos causados pelos usuários.

Visando a compreensão do tema será abordado na seção 2 a responsabilidade civil: conceito, origem da responsabilidade civil, seus pressupostos, a responsabilidade civil subjetiva e objetiva e sua aplicação nas redes corporativas. Já na seção 3 será abordado o endereçamento IP e sua aplicação na responsabilidade civil, bem como o entendimento dos tribunais acerca do rastreamento de IP como elemento para se identificar o causador do dano, e a importância de se manter os registros de conexão à rede. Na sequência, é exposto na seção 4 a utilização da ferramenta gratuita Captive Portal, sua configuração, monitoramento de acessos, geração de logs e guarda dessas informações. Portanto, a análise da responsabilidade civil por dano originado em uma rede de computadores e o uso de uma ferramenta eficaz no controle de acesso à rede para a identificação do seu autor será o escopo do presente trabalho.

2. RESPONSABILIDADE CIVIL

O Marco Civil da Internet [Brasil, 2014] veio regulamentar, dentre outras coisas, a responsabilidade civil por ato ilícito na Internet, tornando cada empresa responsável pelo tráfego originado por sua rede, bem como em relação ao conteúdo recebido e transmitido por seus computadores e demais dispositivos. Qualquer atividade que possa causar dano ou prejuízo a uma terceira pessoa gera o dever de reparar e indenizar o prejuízo, por conta do instituto jurídico da responsabilidade civil. Toda atividade causadora de dano ou prejuízo a outra pessoa é passível de indenização ao prejudicado. Nas palavras de Stocco [15]:

> A noção da responsabilidade pode ser haurida da própria origem da palavra, que vem do latim respondere, responder a alguma coisa, ou seja, a necessidade que existe de responsabilizar alguém pelos seus atos danosos. Essa imposição estabelecida pelo meio social regrado, através dos integrantes da sociedade humana, de impor a todos o dever de responder por seus atos, traduz a própria noção de justiça existente no grupo social estratificado. Revela-se, pois, como algo inarredável da natureza humana.

Na legislação brasileira, tanto o ato ilícito civil (quando se viola o direito de alguém ou causa dano) como a responsabilidade de indenizar o terceiro prejudicado pela sua ocorrência é descrita no Código Civil, nos seguintes artigos:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. (...)
>
> Art. 927. Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem [1].

Tratam-se, nesses casos, de responsabilidade civil originada pela prática de ato ilícito civil. Na definição de Tartuce [17]:

> Pois bem, o ato ilícito é o ato praticado em desacordo com a ordem jurídica violando direitos e causando prejuízos a outrem. Diante da sua ocorrência a norma jurídica cria o dever de reparar o dano, o que justifica o fato de ser o ato ilícito fonte do direito obrigacional. O ato ilícito é considerado como fato jurídico em sentido amplo, uma vez que produz efeitos jurídicos que não são desejados pelo agente, mas somente aqueles impostos pela lei, sendo, por isso, chamados de involuntários. Quando alguém comete um ilícito há a infração de um dever e a imputação de um resultado. (...)
>
> Dessa forma, pode-se afirmar que o ato ilícito é a conduta humana que fere direitos subjetivos privados, estando em desacordo com a ordem jurídica e causando danos a alguém.

Face ao exposto, pode-se dizer que quando uma pessoa pratica alguma ação ou omissão que fere a legislação e causa dano ou viola direito de terceiro, comete um ato ilícito civil e deve ser responsabilizado, arcando com as suas consequências e indenizando a vítima na mesma medida do prejuízo que causou. Quando se fala em responsabilidade civil, deve-se entender que ela pode ter duas origens: ela pode ser contratual, ou extracontratual. A responsabilidade civil é contratual quando uma pessoa descumpre uma obrigação contratual previamente estipulada, descumprindo uma ou mais cláusulas desse contrato [14]. Assim, é contratual toda responsabilidade civil cuja origem é a infração de um contrato (acordo) firmado entre duas partes. O contrato é um pacto onde se estabelecem condições para cumprimento de determinadas obrigações, e a violação dessas condições é o que gera o dever de indenizar a parte prejudicada.

A responsabilidade civil extracontratual, também chamada de responsabilidade aquiliana, é aquela responsabilidade derivada de um ato ilícito civil, cujas consequências são as descritas no art. 186 do Código Civil [1]. Esta responsabilidade não tem origem em um contrato anterior, e sim, em

uma ação ou omissão que causa dano ou viola o direito de uma outra pessoa. Não há nenhum vínculo jurídico anterior entre aquele que causa o dano e a vítima, até a ação ou omissão que causou o dano. Vínculo jurídico é o que une as partes envolvidas nesse processo de responsabilização e reparação de dano. No caso da responsabilidade contratual, o vínculo é o contrato: ele que une as partes que se obrigaram a realizar determinada ação ou omissão. Na extracontratual o vínculo surge no momento em que o autor do dano fere a legislação ou direito de outra pessoa, causando prejuízo, seja ele material, moral ou ambos.

Assim, o presente trabalho busca analisar a responsabilidade civil extracontratual, causada por colaborador que, utilizando-se de recursos tecnológicos e de rede corporativa, por exemplo, causa dano a terceiro. Em outras palavras, visa demonstrar a responsabilidade que a corporação tem pelos atos praticados por pessoas que utilizam sua rede de computadores, quando estas causarem prejuízo ou violarem direitos de terceiros.

2.1 Pressupostos da Responsabilidade Civil

A lei define algumas condições para que a responsabilidade civil seja configurada. Estes pressupostos estão descritos no art. 186 do CC. São requisitos para se configurar responsabilidade civil de acordo com a lei Brasileira [1]:

1. Ação ou omissão do agente: Agente é aquele que, por ação ou omissão, viola direito ou causa dano a alguém. Ele pode ser responsabilizado por ato próprio (o próprio causador do dano pratica o ato ilícito, sendo ele responsável pela reparação do dano, por exemplo, João, civilmente capaz, quebra uma janela de vidro de um imóvel, e por este motivo tem o dever de reparar a janela) ou por ato de terceiro (ou seja, a pessoa fica sujeita a reparar o dano por ato de outra pessoa que está sob sua sujeição. Exemplificando, o pai deve reparar o dano causado pelos atos do filho menor que está em sua companhia ou guarda, ou ainda empregador que responde pelos atos dos empregados etc.) [1];

2. Culpa do agente: para existir responsabilidade há necessidade de se analisar se o agente praticou a ação com dolo (vontade livre e consciente do agente em agir para atingir o resultado, tendo plena consciência do mal, ou seja, a intenção deliberada em causar prejuízo ou violação de direito) ou culpa (violação de um dever que o agente podia conhecer e observar, segundo o comportamento padrão médio). Esta culpa consiste em três modalidades. São elas [11]:

   - Imprudência (quando o agente age sem as cautelas necessárias que, se fossem adotadas, poderiam evitar o resultado, como, por exemplo, utilizando equipamentos de proteção);
   - Imperícia (inaptidão técnica ou ausência de conhecimentos para a realização e prática de um ato ou omissão em se adotar as providências necessárias, como o desconhecimento na operação de determinando equipamento) ou;
   - Negligência (falta de atenção e ausência de reflexão onde o agente poderia e deveria ter previsto o resultado, e não o fez, por exemplo, permitir que empregados trabalhem sem equipamentos de proteção individual). A análise do dolo ou culpa deve ser verificada caso a caso, em conformidade com a situação e intenção do causador do dano.

3. Relação ou nexo de causalidade: deve-se provar o vínculo entre a ação ou omissão do agente e o dano causado à vítima. Se o comportamento do agente não foi o causador do dano, não há dever de reparação [14];

4. Dano: por fim, há de se constatar a necessidade de um dano experimentado pela vítima, pois não há presunção de ocorrência de dano quando se existe um ato ilícito civil (existe a possibilidade de ocorrer um ato ilícito civil e não ocorrer dano à vítima). Logo, inexistindo dano, não há que se falar em responsabilidade civil.

Há, atualmente, no Brasil, dois tipos de responsabilidade civil: a) subjetiva, onde se leva em consideração o dolo (vontade livre e consciente na causa do dano a terceiro, violação intencional do dever jurídico) ou culpa (ação ou omissão decorrente de negligência, imperícia ou imprudência, deixando o agente de agir com a prudência necessária para evitar o dano), e; b) objetiva, que, comprovado o dano e o nexo de causalidade, independe de verificação de dolo ou culpa do agente para que ocorra a responsabilização. Na legislação civil, a empresa é responsabilizada de forma objetiva, ou seja, sem verificação de dolo ou culpa por parte de quem cometeu o ato danoso, cabendo a empresa/proprietário o dever de indenizar quem sofreu o dano.

Esse conceito de responsabilidade objetiva baseia-se na Teoria do Risco, que entende que se determinado empresário produz riqueza a partir de sua atividade econômica, deve ter responsabilidade, independente de culpa ou dolo, por qualquer prejuízo que sua atividade econômica venha ocasionar a terceiros. Exemplificando, estando o empregado executando o serviço ou tarefa para a qual ele foi contratado, e vier a causar dano ou violar direito de terceiro, a reparação do dano será responsabilidade do seu empregador, ainda que ele, empregador, não tenha participado de modo algum para que este dano acontecesse. Neste contexto está inclusa a ocorrência de dano a terceiro cujo meio utilizado é a rede de computadores empresarial, sendo passível a responsabilização da empresa para responder pelo dano ocasionado. Este é o entendimento que está consolidado no Código Civil [1]. Os artigos 932 e 933 atribuem como objetiva a responsabilidade das empresas em relação aos danos causados por seus funcionários no ambiente de trabalho.

3. O ENDEREÇAMENTO IP E A RESPONSABILIDADE CIVIL

O Protocolo de Internet (IP) é o principal protocolo utilizado para a comunicações inter-redes na arquitetura TCP/IP. Na versão IPv4 (Protocolo de Internet versão 4), mais utilizada hoje, é composto de um endereço constituído por quatro octetos de oito bits cada, em uma notação decimal separada por ponto. Este endereçamento IP é composto por dois níveis macro: NetId, fornecido pela *Internet Assigned Number Authority* (IANA), que é o órgão gestor da Internet e corresponde ao endereço de rede, atribuído ao primeiro octeto e HostID, sendo este responsabilidade das organizações, servindo estes para a divisão dos demais endereços em sub-redes [9].

Forouzan [10] traz uma definição sobre endereços IPv4:

Revista de Sistemas e Computação, Salvador, v. 9, n. 2, p. 375-386, jul./dez. 2019
http://www.revistas.unifacs.br/index.php/rsc

> Um endereço IPv4 é um endereço de 32 bits que define de forma única e universal a conexão de um dispositivo (por exemplo, um computador ou um roteador) à Internet. Um endereço IPv4 tem 32 bits de comprimento. Os endereços IPv4 são exclusivos no sentido de que cada endereço define uma, e somente uma, conexão com a Internet. Dois dispositivos na Internet jamais podem ter o mesmo endereço ao mesmo tempo.

Por ser endereço único, que define uma e somente uma conexão com a Internet, é que a jurisprudência tem adotado o endereço de IP como parâmetro para a responsabilização do causador do dano na Internet. Através do registro deste endereço é possível localizar o ponto de origem da conexão, identificando de onde se originou o dano. Os endereços IP, no seu início, utilizavam uma divisão em cinco classes (A, B, C, D, E), sendo cada classe ocupante de determinado intervalo de endereços, de acordo com a Figura 1. Tanembaum e Wetherall [16] complementam o estudo das classes de endereços IPv4, com o conceito de máscara de sub-rede:

> (...) Como o tamanho do prefixo não pode ser deduzido apenas pelo endereço IP, os protocolos de roteamento devem transportar os prefixos aos roteadores. Às vezes, os prefixos são simplesmente descritos por seu tamanho, como em um '/16' que é pronunciado como 'barra 16'. O tamanho do prefixo corresponde a uma máscara binária de 1s na parte destinada à rede. Quando escrita dessa forma, ela é chamada máscara de sub-rede.

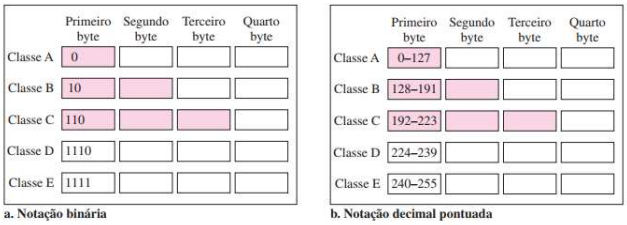

Figure 1: Intervalo de Classes de Endereços IPv4 [10]

A máscara de sub-rede ajuda a encontrar o NetId e o HostId de uma rede. Embora o comprimento do Netid e Hostid (em bits) seja predeterminado no endereçamento com classes, também podemos usar uma máscara (chamada máscara-padrão), um número de 32 bits composto de 1s contíguos seguidos por 0s contíguos [10].

A notação descrita na coluna CIDR (*Classless Interdomain Routing* – roteamento interdomínios sem classes) é utilizada hoje para definir os endereçamentos sem classe, ou seja, neste tipo de endereçamento é fornecido a uma entidade uma faixa de endereços IPv4 que varia de acordo com o tamanho e natureza da entidade, evitando, desse modo, o desperdício de endereços IP. Esses endereços devem ser contíguos, ser uma potência de 2 e também o primeiro endereço deve ser divisível pelo número de endereços, tendo a máscara uma quantidade entre 0 e 32 bits. Nesse tipo de notação, O primeiro endereço no bloco pode ser encontrado configurando-se em 0 os 32 – n bits mais à direita na notação binária do endereço, e o último endereço pode ser encontrado configurando-se em 1 os 32 – n bits mais à direita na notação binária do endereço. Kurose e Ross [12] detalham a atribuição de endereços de IP para organizações mediante o uso de CIDR:

> A estratégia de atribuição de endereços da Internet é conhecida como roteamento interdomínio sem classes (*Classless Interdomain Routing* – CIDR) [...]. O CIDR generaliza a noção de endereçamento de sub-rede. Como acontece com o endereçamento de sub-redes, o endereço IP de 32 bits é dividido em duas partes, e, mais uma vez, tem a forma decimal com pontos de separação a.b.c.d/x, em que x indica o número de bits existentes na primeira parte do endereço. Os x bits mais significativos de um endereço na forma a.b.c.d/x constituem a parcela da rede do endereço IP e normalmente são denominados prefixo (ou prefixo de rede). Uma organização normalmente recebe um bloco de endereços contíguos, isto é, uma faixa de endereços com um prefixo comum [...]. Nesse caso, os endereços IP de equipamentos e dispositivos dentro da organização compartilharão o prefixo comum [...]. Os restantes (32-x) bits de um endereço podem ser considerados como os bits que distinguem os equipamentos e dispositivos dentro da organização e todos eles têm o mesmo prefixo de rede. Esses serão os bits considerados no repasse de pacotes em roteadores dentro da organização. Esses bits de ordem mais baixa podem (ou não) ter uma estrutura adicional de sub-rede tal qual como aquela discutida anteriormente.

Esta distribuição de endereços IP é responsabilidade da IANA, organização mundial que supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autônomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet.

3.1 A Jurisprudência e o rastreamento de endereços IP

O registro do endereço IP já é considerado pela jurisprudência, antes mesmo da entrada em vigor do Marco Civil da Internet, como medida de segurança média esperada pelos provedores de acesso à Internet para viabilizar o rastreamento do autor do dano, o que pode ser aplicado, analogicamente, pelo administrador de redes para eventual responsabilização do art. 934 do Código Civil [1]. Senão vejamos:

> DIREITO CIVIL E DO CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS

PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA.

[...]

7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na Internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet.

8. Recurso especial a que se nega provimento." [Supremo Tribunal de Justiça, 2010] [3].

Em caso semelhante, também anterior ao MCI, o Tribunal de Justiça de São Paulo já entendia que cabe aos provedores de acesso manterem o registro das conexões, por ser atividade própria ao risco do negócio.

> Trata-se de ação de indenização por danos materiais e morais c/c obrigação de fazer ajuizada pela Autora, na ocasião representada por seu genitor, em razão de sua menoridade, em face das Rés, sob o argumento de que utiliza uma das contas de e-mail de seu genitor e que possui endereço eletrônico "tavareskel@uol.com.br".
>
> [...]
>
> A mensagem "hahahaha" foi enviada por meio da Internet para a conta de e-mail de propriedade de seu pai, além de mais 25 pessoas de seu contato social. Anexo à mensagem, foram divulgadas fotografias com 05 imagens de 03 jovens, dentre as quais a Autora e, por cima das imagens foram adicionadas os textos "puta", "idiota", "dona de puteiro", todos de caráter injurioso. A conta "festa-de-bosta@hotmail.com" utiliza o domínio "hotmail.com", registrado nos Estados Unidos em nome da Microsoft Corporation, representada no Brasil pelo Microsoft Informática Ltda., e a mensagem injuriosa foi emitida a partir do endereço IP nº 201.37.170.10, de responsabilidade da Net São Paulo Ltda. Tentam as Ré eximirem-se da obrigação delas reclamada pela Autora, sob o fundamento de que inexiste norma a obrigá-las ao armazenamento de dados de usuários de número "IP". Aqui cabe indicar que provedor de acesso é a pessoa jurídica que possibilita, ao usuário que contrata os seus serviços, o acesso à rede mundial de computadores, por meio de contrato em que consta nome, endereço, CPF, RG etc. Ela atribui, ao usuário, um determinado número de IP, que acompanhará o "internauta" durante todo o tempo que permanecer conectado à "Internet", número este que funcionará como o seu "RG", ou código de identificação, na rede. Nestes termos, a Ré Net São Paulo Ltda. efetivamente presta serviços como provedor de acesso à rede mundial de computadores, tanto que, segundo alega, não pode fornecer os dados solicitados, mas por problemas técnicos, que, no entanto, não foram especificados. [...] Ademais, em que pese não existir lei específica que discipline o cadastro de usuários da Internet pelos provedores de acesso, não menos certo é que a manutenção desses cadastros é atividade inerente ao risco do negócio desenvolvido pela Rés, que no caso a Net São Paulo Ltda., é a proprietária do serviço Net Virtua, enquanto a Microsoft Corporation representada no Brasil pela Microsoft Informática Ltda., administra o serviço de hotmail, serviços que indubitavelmente lhes trazem lucros [Tribunal de Justiça de São Paulo, 2013] [4].

O mesmo Tribunal de Justiça de São Paulo (TJSP), no Acórdão proferido na Apelação 0019001-91.2012.8.26.0602, traz alguns conceitos sobre IP e o que se espera sobre a sua manutenção:

> O endereço IP é o endereço do Protocolo Internet (IP), dado a cada computador conectado à Internet e necessário para enviar as informações, assim como um endereço ou caixa postal são necessários para receber correspondência via correio regular. Se a conexão for feita por meio de um roteador, todos os computadores daquela rede irão compartilhar um endereço IP (endereço de Protocolo de Internet) similar - embora cada computador na rede tenha um endereço único e exclusivo. Existe o IP32 estático (ou fixo) e o IP dinâmico, o qual, por sua vez, é um número que é dado a um computador quando este se conecta à rede, mas muda toda vez que há conexão. Existem poucos números de IP possíveis, comparado ao imenso número de computadores no mundo, por isso eles são distribuídos pelas organizações competentes, como a IANA e a LACNIC. Cada país pode usar uma determinada faixa de IP, muitos provedores usam endereços IPs específicos para determinadas regiões. Há programas que permitem o rastreamento do endereço IP, permitindo a identificação, tal como uma pesquisa realizada na página do Google com "IP Lookup" ou "IP Geolocation"; há várias orientações de como obter o endereço IP. Se as páginas na Internet fornecem instruções de como conseguir esta informação, a própria Microsoft também poderia fornecê-los, pois o provedor de Internet (ISP, do Inglês "Internet Service Provider") tem a obrigação de manter os dados cadastrais [8].

De acordo com o Tribunal bandeirante, a obrigação de se manter os registros de acesso por parte do ISP que providencia a conexão à Internet é clara, não podendo as organizações (nesse caso, a Microsoft) desconhecer dos procedimentos para a obtenção e o rastreio das informações requeridas. Do mesmo modo, a jurisprudência dominante no Superior Tribunal de Justiça (STJ) entende que "o fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na Internet constitui meio satisfatório de identificação de usuários" [5]. A importância da guarda dos registros por parte dos provedores de acesso à Internet é reconhecida pelos Tribunais, como no julgado a seguir transcrito, do Tribunal de Justiça do Distrito Federal e Territórios [7]:

> CIVIL E PROCESSUAL CIVIL. AGRAVO DE INSTRUMENTO. GOOGLE. CORREIO ELETRÔNICO. FORNECIMENTOS DE DOCUMENTAÇÃO. INFORMAÇÃO DO IP QUE ORIGINOU O E-MAIL. FORNECIMENTO DE DADOS CADASTRAIS. GUARDA DE DADOS. LAPSO TEMPORAL. PERÍODO SUPERIOR AO PREVISTO NA LEI N. 12.965 /2014. DECISÃO PARCIALMENTE REFORMADA. AGRAVO PRO-VIDO. 1. Na qualidade de provedora do correio eletrônico, a Google não tem como indicar o nome, endereço, CPF, RG etc, de seus usuários, no entanto, outra empresa que compõe a teia de interligação da Internet, chamado de provedor de conexão (ou acesso), tem como indicar os dados do usuário relacionados ao IP. 2. Contudo, a partir dos dados por ela fornecidos, em face da decisão judicial, torna-se impossível à agravada obter informações do usuário que criou o e-mail indesejado, pois todos os usuários, quando se conectam à rede mundial de computadores recebem um número de identificação chamado IP, que funciona como se fosse o RG do usuário na Internet e possibilita o seu rastreamento. 3. Merece reforma a parte da decisão que determinou, liminarmente, o cumprimento de obrigação inviável, em razão do prazo legal para a guarda de registros, que é limitado ao período de seis meses, bem como porque o Gmail é um provedor de correio eletrônico gratuito e não de acesso e, por tal razão, não é obrigatório o registro de dados pessoais dos usuários, em face da inexistência de lei nesse sentido. 4. Agravo conhecido e provido [7].

A guarda desses registros torna possível à vítima identificar de qual dispositivo o dano foi causado. Ainda que o meio utilizado (correio eletrônico de responsabilidade da empresa Google, segundo o julgado acima) não possua todas as informações para uma identificação exata, mas indique qual endereço IP foi utilizado para criar e acessar a conta, o ISP responsável por este endereço é capaz de resgatar as informações pertinentes visando a responsabilização do autor do fato. Portanto, a corporação que fornece acesso a seus empregados, alunos e/ou usuários à Internet deve se resguardar sobre a prática de eventuais abusos e atos ilícitos. Vejamos o caso concreto a seguir:

> RESPONSABILIDADE CIVIL. SITE DE ENCONTROS AMOROSOS. CADASTRAMENTO INDEVIDO. COMPUTADOR DE PROPRIEDADE DA UFSC. MENSAGENS OFENSIVAS. RECEBIMENTO. DANO MORAL CARACTERIZADO. INDENIZAÇÃO. VALOR. CRITÉRIOS DE ARBITRAMENTO. 1.- A causalidade entre o dano e os serviços prestados pela UFSC não se discute, uma vez que a mensagem indevida partiu comprovadamente de um dos computadores de sua propriedade. Ao possibilitar a seus alunos a utilização de computadores conectados à Internet em suas instalações, obrigou-se a Universidade a velar pelo bom uso dos equipamentos, respondendo objetivamente por eventual falha na vigilância e a consequente perpetração de ato ilícito.
>
> (...)
>
> Resta incontroverso que a senha utilizada no momento do ilícito pertencia ao réu. Não obstante, a prova testemunhal, de forma segura e coerente, assegurou a prática no Laboratório de Informática Jurídica do uso da senha dos monitores por outros alunos, seja porque não tinham o próprio acesso, seja porque precisavam utilizar programas ou acessar arquivos só existentes nos equipamentos exclusivos dos monitores. Além disso, constatou-se que as senhas, antes dos fatos, não possuíam caráter estritamente sigiloso, já que a listagem das senhas provisórias- normalmente não alteradas pelos usuários- era facilmente visualizada no LINJUR. Outrossim, o estabelecimento de regras para a utilização da senha pessoal, mormente as constantes da fl. 18, foram determinadas após o ilícito *sub examen*.
>
> (...)
>
> A prova coligida, de outro lado, não logrou comprovar o cometimento do ilícito pelo réu, ao contrário, assegurou apenas que o computador foi "logado" com a sua senha, sendo que qualquer aluno da UFSC poderia estar utilizando o equipamento quando do cadastro ilegal.
>
> Também não há falar em culpa por descuido no emprego da senha pessoal, já que está assente nos autos que a utilização da senha dos monitores pelos demais alunos, sem qualquer fiscalização, era prática corriqueira no LINJUR. O estabelecimento de regras quanto às senhas só ocorreu após os fatos, como visto acima [2].

Como se pode observar, a Universidade Federal de Santa Catarina foi responsabilizada por não gerenciar, de modo efetivo, os acessos de seus alunos e colaboradores. Quem fornece acesso a outras pessoas deve estar preparado para identificar, caso seja necessário, o usuário que agiu em desacordo com as normas legas e ocasionou dano ou violação de um direito.

3.2 Registros de conexão na rede

Por motivos de segurança, é indicado que o proprietário de uma rede com vários dispositivos conectados e vários usuários adote um registro dos acessos e usuários autenticados em sua rede, de modo semelhante ao exigido no Marco Civil da Internet (MCI) para os provedores de acesso. Isso tornará possível, caso processado e condenado por má utilização da rede, localizar o usuário responsável e cobrá-lo judicialmente dos prejuízos que a empresa/instituição sofreu com sua conduta. Analisando-se o art. 10 do MCI, ele estabelece que deverão ser guardados os dados de registro de conexão e de acesso de aplicações de Internet, estabelecendo no §1º, a saber, "outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial". Além, o inciso VI do art. 5º do MCI [5] define:

> Art. 5º Para os efeitos desta Lei, considera-se:
>
> (...)
>
> VI - Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados [5].

Apesar desta regra prevista no MCI não ser obrigatória às redes internas, sua aplicação é altamente recomendada visando buscar uma segurança para o proprietário da rede de computadores e para seu administrador. Como o exemplo da UFSC [2], em que não existia esse controle e guarda de acesso por parte da administração da rede, a impossibilidade de se verificar o efetivo causador do dano não possibilita à instituição reaver o prejuízo que sofreu ao indenizar terceiro lesado por ato ilícito que partiu de seu parque computacional.

Portanto, a adoção de um mecanismo eficiente, capaz de guardar os registros das conexões efetuadas a partir de uma estação, com a data e hora do início e término da conexão, a duração, o endereço IP utilizado e uma informação acerca do usuário que a realizou possibilitará a identificação pretendida, caso exista a necessidade de se acionar o responsável judicialmente.

3.3 A utilização de NAT e Proxy e o registro de conexões à rede

Há de se considerar que, com a quantidade de dispositivos conectados hoje na rede mundial de computadores e a escassez de endereços IPv4 públicos a serem disponibilizados a todos, apenas esta informação não é suficiente para que se possa identificar a autoria de eventual ato ilícito, posto que atrás de um único endereço IPv4 público poderão estar vinculados milhares de outros endereços IPv4 privados, utilizando um *proxy* ou um NAT (*Network Address Translation*). Esses dois mecanismos possibilitam uma grande quantidade de dispositivos de uma rede interna, dotados de IPv4 privados, acessem à Internet por meio de um único endereço ou uma quantidade pequena de IPv4 públicos. Assim, 500 dispositivos de uma rede interna, por exemplo, podem ter acesso à rede mundial de computadores utilizando um endereço IPv4 público, ou um pequeno rol de endereços públicos.

Contudo, essas soluções dificultam a identificação de qual dispositivo ocasionou um dano a terceiro, já que o rastreamento de IP levará ao endereço público de origem, e não à estação específica atrás desse endereço. Contextualizando, *proxy* ou servidor *proxy* é um "servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet" [13]. Age como um intermediário entre os clientes de uma rede e a Internet. Serve, inclusive, para compartilhar o acesso à Internet quando apenas há um endereço público disponível para a rede, sendo o único computador ligado à Internet e os demais computadores acessam a rede mundial por este computador.

Por sua vez, o NAT é um recurso que também permite a transformação de endereços internos em endereços públicos, roteáveis na Internet. É muito semelhante ao *proxy*, porém as conexões via NAT são quase totalmente transparentes ao usuário. Esta foi uma solução emergencial adotada ao se verificar a escassez de endereços IPv4 disponíveis para conectar todos os dispositivos à Internet.

Tanembaum e Wetherall [16] trazem as circunstâncias em que o recurso foi adotado:

> O problema de esgotar os endereços IP não é um problema teórico que poderia ocorrer em algum momento no futuro distante. Ele está acontecendo aqui e agora. A solução a longo prazo é a Internet inteira migrar para o IPv6, que tem endereços de 128 bits. Essa transição está ocorrendo com lentidão e a conclusão do processo demorará muitos anos. Para contornar a situação nesse interstício, foi necessário fazer uma rápida correção. Essa correção veio sob a forma da NAT (*Network Address Translation*), descrita na RFC 3022 [...].

3.4 Da solução adotada

Após essa breve análise das tecnologias de *proxy* e NAT, podemos dizer que sua utilização é prejudicial à possibilidade de identificação dos usuários que utilizaram uma rede de computadores no âmbito interno da corporação, pois todas as conexões terão como endereço de IP público registrado aquele utilizado pelo servidor *proxy* ou na NAT, o que levará o rastreio dessas informações até a borda da rede monitorada, mas sem maiores informações sobre a utilização dos recursos. Por conta dessas tecnologias, querendo o administrador de redes ou proprietário da instituição se resguardar quando o assunto é a utilização dos seus recursos de informática, propõe-se, ao menos, a guarda das informações referentes a quem está utilizando sua rede, o período de uso, bem como o IP utilizado pelo terminal.

Na solução estruturada, que visa um meio de identificação do usuário e período por meio de software livre, é proposto a utilização de IP públicos, como uma solução simples e eficaz no caso de pequenas e médias empresas/corporações. A manutenção e guarda dos registros de acesso acima citados também é de suma importância para resguardar civilmente a empresa/instituição, dentro do prazo prescricional de eventual ação de danos morais e materiais (três anos, conforme disposto no art. 206, §3º, V do Código Civil) [1], sendo importante a implementação de backup para os logs de acesso gerados pela rede. Busca-se desse modo guardar as informações mínimas e necessárias para a eventual identificação do causador do dano (como, por exemplo, o número de seu CPF ou matrícula, data de acesso, hora de início e fim da sessão, estação utilizada e número de IP da estação).

Não se trata de realizar fiscalização prévia ou posterior sobre o conteúdo acessado pelo colaborador ou usuário do dispositivo a partir da rede corporativa, pois, inclusive, é bastante controverso na doutrina e jurisprudência a possibilidade ou não do proprietário efetuar esse controle. Propõe-se apenas fornecer meios para que a organização identifique o causador do dano e tome as providências cabíveis. Na solução que será proposta, o conteúdo não será monitorado ou vistoriado. No presente trabalho, será analisada uma possível solução para que o proprietário ou administrador de da rede identifiquem eventual causador de dano: uma rede constituída de endereços em IPv4, com terminais utilizando endereços públicos, utilizando-se o software pfSense (software livre) e sua ferramenta Captive Portal.

4. DA FERRAMENTA ADOTADA

Em uma rede de computadores corporativa, podem existir diversos tipos de equipamentos e dispositivos interconectados, entre eles servidores, computadores portáteis, celulares, estações de trabalho, comutadores, roteadores, entre outros, como se pode extrair da Figura 2, na sequência. No exemplo exposto na figura, há dispositivos portáteis (*laptops* e *smartphones*, por exemplo), estações de trabalho (desktops), utilizados pelos colaboradores para a execução de suas ta-

refas, servidores que disponibilizam os diversos tipos de serviços aos usuários e à corporação (como servidores de arquivos, correio eletrônico, impressão, banco de dados, entre outros). Todos esses dispositivos estão conectados por um comutador (*switch*), responsável pelo encaminhamento dos pacotes ao dispositivo correto, bem como por um ponto de acesso sem fio, que possibilita que dispositivos se conectem à rede sem a utilização de cabos. Todos estes dispositivos estão interagindo entre si e acessando a Internet, cujo acesso é gerenciado pelo dispositivo situado na borda da rede (*firewall*). Ele também é responsável pelo filtro de pacotes que entram e saem da rede, visando conferir à rede segurança contra ataques externos. Para atender as mais diversas topologias de redes, visando a guarda das informações que são o escopo do presente trabalho, há algumas ferramentas no mercado à disposição do administrador de redes, podendo-se citar como exemplo o uso de Windows Server com Active Directory, uma solução proprietária oferecida pela empresa Microsoft bastante utilizada nas redes corporativas.

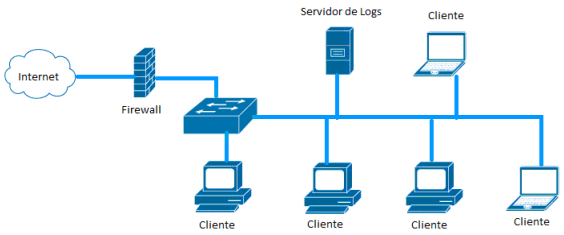

Figure 2: Ambiente de testes proposto

A ferramenta oferecida pela Microsoft é, sem dúvida, bastante completa e oferece ao administrador da rede as funcionalidades necessárias para registro, manutenção e guarda dos logs de acesso dos usuários da rede. Contudo, como sendo uma ferramenta proprietária, há custos para a aquisição da licença (variável dependendo da versão) e, que deverão ser adquiridas para a utilização legal do referido sistema operacional e suas funcionalidades.

A solução para quem não deseja ou não tem recursos para arcar com os custos de licenças é a adoção de uma solução em software livre, que cumpra com os objetivos e atenda a todos os requisitos identificados pelo administrador da rede. Portanto, a adoção de software livre traz economia de recursos a quem o utiliza, que podem ser destinados para outros fins e realizam tarefas de modo satisfatório, sendo uma alternativa viável ao uso de ferramentas pagas, ou ainda outros softwares como Kiwi, Nagios (versões com licenças pagas), AUGE etc.

A escolha na utilização do pfSense e do Captive Portal foi pautada em três fatores: a facilidade na utilização, configuração e gerenciamento das ferramentas, a eficácia no registro e controle dos acessos efetuados e serem ferramentas baseadas em software livre. Ademais, o uso do sistema pfSense também é compatível com o sistema operacional Windows, podendo gerenciar autenticações de estações que utilizem este sistema operacional, e opera em uma rede composta exclusivamente de clientes Windows, mistas, ou exclusivamente com clientes baseados em software livre. Como exemplo, poderão coexistir na mesma rede clientes Linux, Windows, Android e IOS, todas tendo seu acesso à Internet autenticado pelo Captive Portal e suas conexões registradas nos logs.

Visando possibilitar ao empreendedor uma solução baseada em software livre para gerenciamento e guarda dos logs dos acessos à Internet realizados a partir da rede corporativa, a solução escolhida e adotada para os testes de laboratório foi o Captive Portal, disponível de modo nativo no pfSense. O Captive Portal atende a todas as necessidades descritas no presente trabalho para o gerenciamento dos acessos, geração e guarda de logs. A estrutura a seguir descrita necessita de uma quantidade de endereços de IPv4 públicos disponíveis para que cada cliente receba um endereço fixo, vinculando, assim, máquina ao endereço IP destinado. Para o ambiente de testes foi estruturada uma rede onde os endereços IP dos clientes são privados, apenas para demonstrar a eficácia da ferramenta apresentada. Novamente, frisa-se, para se conseguir o resultado desejado, os endereços IPv4 das estações envolvidas deverão ser públicos. A solução proposta é composta de:

a) Uma máquina na borda da rede interna, funcionando como Firewall e com o software pfSense versão 2.4.1, instalado, que será responsável por autenticar as conexões com a Internet, gerar logs das autenticações, além de servir como gateway da rede. Esta máquina, no presente experimento, receberá como IP da interface interna o endereço 10.10.10.254 /24 e receberá o IP da interface externa por DHCP, do provedor de Internet;

b) Um servidor de logs, funcionando com sistema operacional Debian 7 - Wheezy, que será responsável por receber os logs enviados da estação pfSense para guarda e manutenção dos arquivos de log, cujo endereço IP designado é 10.10.10.252/24;

c) Estações clientes com sistema operacional Ubuntu instalado, para teste de geração de logs, acessos à Internet e gerenciamento Web do pfSense e Captive Portal. Configurações propostas para o servidor pfSense: instalação da ferramenta pfSense versão 2.4.1 no servidor, configuração de IP Fixo (10.10.10.254/24), DNS, Captive Portal, autenticação de usuários (aluno1, aluno2, aluno3, fabricio), configuração de LAN (*Local Area Network*) e WAN (*Wide Area Network*) e envio de logs a servidor remoto;

Configurações propostas para a estação Servidor de Logs (Instalação de Debian 7):

- Wheezy, configuração de IP fixo (10.10.10.252/24), habilitação do serviço de Rsyslog (rsyslog.conf) para receber e gravar os logs de acesso gerados pelo Captive Portal do pfSense ou, alternativamente, habilitação do serviço Syslog-ng.

Configurações propostas para as estações Cliente:

- Sistema operacional Ubuntu Desktop 14.04.LTS, com IP fixo.

Para a rede anteriormente descrita foi designada como máscara de rede 255.255.255.0, com endereço de rede 10.10.10.0/24, *broadcast* 10.10.10.255/24 e 254 endereços de host. Todas as interfaces de rede dos clientes e servidores operarão em rede interna, salvo uma interface do servidor pfSense, que operará com uma interface interna e outra externa. Utilizamos o software de virtualização VirtualBox versão 5.1.30 para simular a estrutura proposta. Em cumprimento ao art. 10 do MCI (A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade,

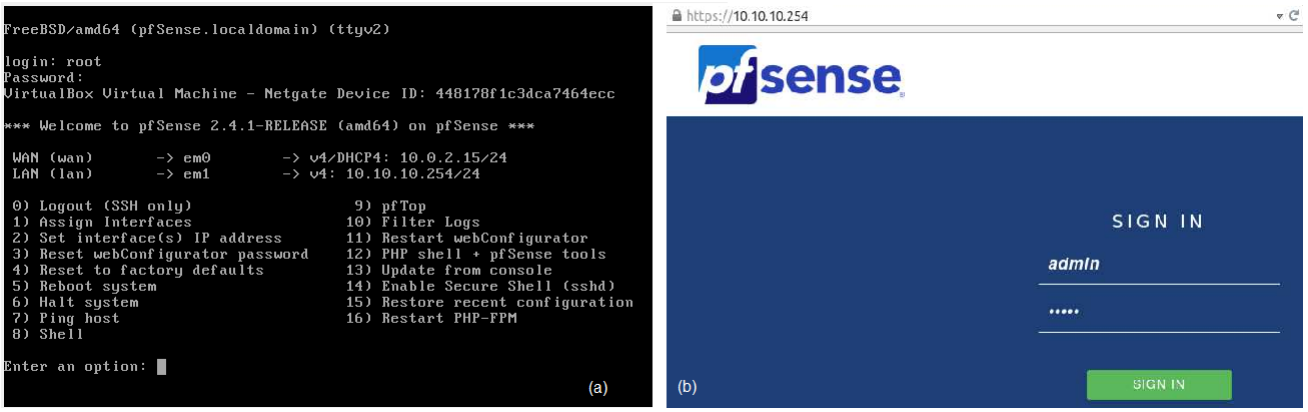

Figure 3: (a) Tela inicial do Servidor com a ferramenta pfSense e (b) Acesso ao servidor pfSense utilizando-se um web browser

da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas), apenas o registro da data/hora, IP da estação e nome do usuário são registrados pelo sistema. Não há registro dos endereços ou conteúdos acessados pelo usuário, e sim apenas os dados que possam contribuir para sua identificação, deixando o registro do conteúdo dessas informações sob responsabilidade daqueles que o oferecem. A adoção desta política também preserva o disposto no art. 11 do MCI [6], uma vez que o cumprimento das leis brasileiras quanto aos direitos de personalidade estão sendo cumpridos, não existindo, ainda que exista corrente que entenda ser plenamente legal o monitoramento de conteúdo por parte do administrador de redes, qualquer ingerência sobre o conteúdo que é acessado pelo usuário (corroborando, inclusive, com o disposto no art. 14 - Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet).

4.1 O cenário em produção

Após a instalação e configuração do servidor pfSense na máquina que será responsável pelo acesso dos clientes à Internet, o servidor apresentará a tela de configuração demonstrada na Figura 3a. Todas as demais configurações e gerenciamentos do pfSense são realizados por meio de uma interface web, que poderá ser acessada de qualquer computador ligado à rede interna. Esse acesso confere ao administrador mobilidade dentro de sua rede, podendo realizar as configurações e acessar as informações que se deseja de qualquer estação, por meio de um navegador. De qualquer estação cliente, tem-se o acesso a ferramenta pfSense para a realização das configurações e busca das informações desejadas digitando-se o endereço IP do servidor na barra de endereços, por meio de tela inicial de acesso, conforme Figura 3b. Após informados os dados para a realização do acesso, o sistema permite o acesso a uma tela inicial com o resumo de várias informações pertinentes na função "Status". Essa interface foi omitida aqui, pois é somente uma tela informativa das configurações do serviço. Nesta tela inicial o operador também terá acesso a diversas informações e configurações pertinentes ao sistema operacional, como sistema, serviços, interface, *firewall*, VPN entre outras. Dentre as configurações possíveis, pode-se escolher que as informações sejam apresentadas no idioma português. Esta interface dá acesso ao serviço Captive Portal, que será responsável por autorizar e registrar os acessos efetuados à Internet. Para que isso ocorra, primeiro deve-se criar uma zona para atuação do serviço.

Esta funcionalidade será responsável pelo modo de autenticação na rede. Para esta proposta, adotou-se a possibilidade de autenticação para usuários previamente cadastrados, ou por meio de vouchers (autorizações temporárias de acesso). Esta medida vincula um usuário a um endereço IP em determinado período de tempo, e elimina, inclusive, um inconveniente em uma rede cujo acesso *wireless* seja possível. A navegação externa só será possível mediante autenticação por intermédio de usuário e senha, e recebimento de um IP público da rede, por DHCP, mantendo assim a prerrogativa de manutenção de usuário, endereço IP e data/hora de acesso. A Figura 4 traz exemplos de usuários autorizados a acessar a solução implementada (visualizados na aba: `System/ User Manager/ Users`).

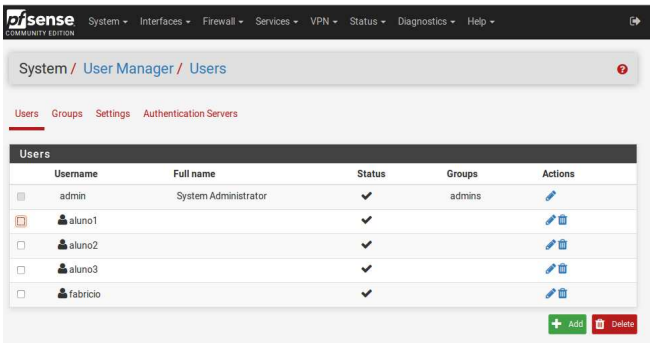

Figure 4: Usuários autorizados a realizar acesso à Internet

Apenas os usuários aluno1, aluno2, aluno3 e fabricio, neste cenário, possuem autorização para acessar a Internet a partir de qualquer dispositivo conectado à rede. A ferramenta possibilita a inclusão e exclusão de usuários de acordo com a necessidade de cada corporação. Qualquer outro usuário que tentar se conectar a um endereço na Internet não conseguirá acesso, uma vez que o Captive Portal só permitirá o tráfego das informações após a autenticação. Essa autenticação é solicitada pela ferramenta assim que o endereço externo é digitado na barra de navegação de um *web browser*. Abre-se

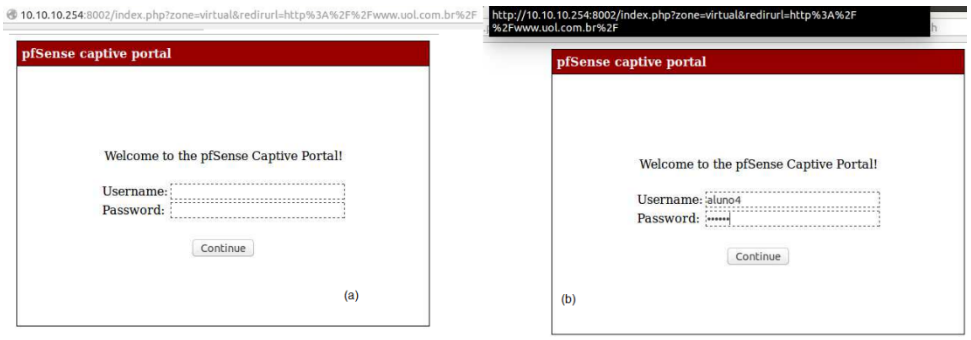

Figure 5: (a)Tela de Autenticação e (b) Acesso à Internet via web browser

uma tela de acesso onde as informações de acesso são solicitadas, de acordo com a Figura 5 (a) e (b) na sequência.

A aplicação não permite que usuários não cadastrados ou com senha incorreta continuem a navegação, autorizando apenas aqueles previamente cadastrados a realizar acesso. Toda tentativa de acesso, inclusive, é registrada e mantida nos logs do Captive Portal, conforme demonstrado pelas Figura 6(a), Figura 6(b) e, a Figura 7.

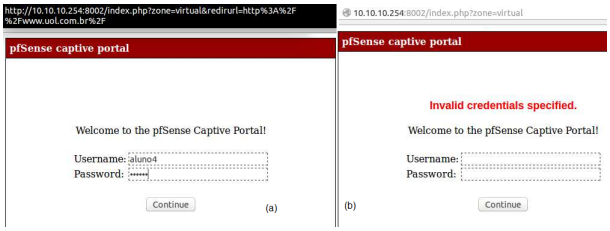

Figure 6: (a) Entrada com dados inválidos e (b) Rejeição do acesso não autorizado

O registro de uma tentativa de acesso é demonstrado na Figura 7.

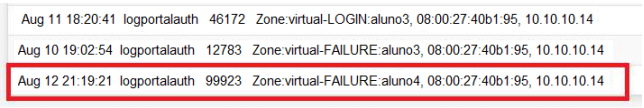

Figure 7: Registro da tentativa de acesso

De forma semelhante, quando é fornecido um nome de usuário e senha já cadastrado anteriormente, o Captive Portal libera o acesso à Internet para aquele usuário e máquina, bem como registra a data, hora, número do processo (PID - *Process Identifier*), a zona, a atividade, o usuário cadastrado, endereço MAC do dispositivo e endereço IP utilizado para a conexão. As imagens a seguir demonstram o processo quando o acesso é realizado por usuário autorizado (Figuras 8, 9 e 10). Como se pode verificar, a aplicação registra e vincula as informações que são necessárias para a correta identificação de um eventual dano causado por alguém utilizando uma rede corporativa.

Ao se ter o endereço de IP utilizado, nome de usuário, data e hora da utilização da rede já há mecanismo eficaz para a identificação.

O Endereço MAC auxilia, inclusive, na identificação do dispositivo caso os endereços IP sejam distribuídos de modo

Figure 8: Registro da tentativa de acesso

Figure 9: Navegação na Internet

dinâmico, por servidor DHCP (*Dynamic Host Configuration Protocol*), dentro da rede (por exemplo, a dispositivos *wireless* que integrem de modo provisório a rede).

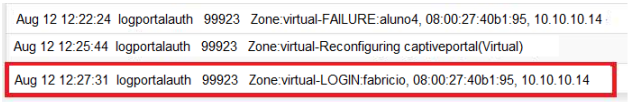

Figure 10: Registro de acesso

No caso de computadores e dispositivos visitantes, que necessitem utilizar a rede para alguma finalidade, é possibilitado a geração e fornecimento de *vouchers* (que disponibilizam acessos de curta duração), sendo recomendado que para cada voucher criado e fornecido, seja realizado um pequeno cadastro sobre seu beneficiário (exatamente para se

manter a rastreabilidade dos usuários, endereços IP e lapso temporal do acesso).

Após o registro das informações desejadas (data e hora do acesso e da desconexão, nome de usuário, endereço IP e endereço MAC), já possibilitam ao proprietário da rede corporativa verificar quem causou o dano, analisando-se esse histórico de logs gerados pelo Captive Portal. Porém a referida ferramenta só guarda os últimos 50 (cinquenta) eventos de log em seus registros, e não gera um documento com os logs desejados, o que não é eficiente para a presente proposta. Por isso se faz necessário que os logs gerados pelo Captive Portal sejam recuperados e guardados em um servidor de logs, à escolha do administrador de redes.

5. CONCLUSÃO

A legislação e a jurisprudência brasileira, no que tange a responsabilização por danos causados a terceiros por meio de uma rede privada de computadores, responsabiliza seu proprietário de forma objetiva a indenizar qualquer dano ou prejuízo que por ventura nela tenha origem. Assim, pode o proprietário tentar buscar soluções que possibilitem identificar o causador do dano, para posteriormente cobra-lo judicialmente de todos os prejuízos que ele, proprietário da rede, foi obrigado a assumir por conta de um ato ilícito cometido pelo colaborador/usuário identificado.

A jurisprudência tem entendido antes mesmo da entrada em vigor do Marco Civil da Internet que o rastreamento do endereço de IP até a máquina ou rede de onde se originou o ato danoso é o suficiente para que seja constatada a autoria do ato ilícito. E este posicionamento se confirmou com a promulgação do MCI, cuja responsabilidade na guarda das informações de acesso passou a ser exigida legalmente aos provedores de acesso à Internet (ISP). Cabe aos ISP informar à autoridade competente e autorizada a requisitar informações os dados cadastrados para a conexão identificada, possibilitando a responsabilização da pessoa/empresa detentora daquele registro no momento do dano.

Por isso é importante aos administradores de redes conhecerem e implementarem um mecanismo de identificação de quem está utilizando a rede, bem como qual endereço IP utiliza e o horário da utilização. Estas são informações importantes que auxiliam a identificar dentro da corporação o verdadeiro agente causador do prejuízo. Por meio da autenticação dos usuários que buscam acessar a Internet é possível realizar essa vinculação entre usuário, endereço IP, horário de utilização e estação, de forma eficiente sem, contudo, fazer uma análise de conteúdo acessado pelo colaborador, já que a possibilidade dessa análise é controversa na doutrina e jurisprudência pátria.

A utilização do pfSense, aliado ao Captive Portal, suas ferramentas de log, Debian Server e Ubuntu, todos softwares gratuitos disponíveis para a comunidade, cumprem os objetivos propostos nesta, e podem ser implementados em uma rede sem custo com licenças, pois são softwares livres. Além disso, sua instalação e configuração são simples, e atendem à necessidade proposta no cenário deste trabalho, inclusive funcionando com conexões wireless, o que é bastante atrativo no cenário atual, considerando-se a tendência BYOD (*Bring Your Own Device* – Traga o seu próprio dispositivo). Essa possibilidade de expansão para realizar autenticação de acesso a dispositivos sem fio com registro e guarda dos logs torna a ferramenta extremamente atraente, verificado seu correto funcionamento e atualização dos registros em tempo real. A implementação do cenário proposto é viável, comprovado nos testes de laboratório, onde se demonstrou a possibilidade de identificação e guarda das informações, em analogia ao que é determinado aos ISP pelo Marco Civil da Internet, identificando o responsável pela conexão, o endereço IP utilizado, o tempo da conexão e o endereço MAC da estação utilizada.

6. REFERENCES

[1] Brasil. Lei n. 10.406 de 10 de janeiro de 2002. institui o código civil. In $http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm$, 2002.

[2] Brasil. Tribunal regional federal da 4ª região. apelreex n. 2003.72.00.012340-3. rel dês. maria lúcia luz leiria. publicado em d.e, 05.03.2009., 2009.

[3] Brasil. Superior tribunal de justiça. recurso especial n 1193764/sp, rel. ministra nancy andrighi, terceira turma, julgado em 14/12/2010, dje 08/08/2011), 2010.

[4] Brasil. Tribunal de justiça de são paulo. apelação 9108382-22.2009.8.26.0000. relator: João pazine neto. data de julgamento: 05/03/2013, 3ª câmara de direito privado. data de publicação: 05/03/2013, 2013.

[5] Brasil. Lei n. 12.965 de 23 de abril de 2014. estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. In $http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm$, 2014($a$).

[6] Brasil. Superior tribunal de justiça. agravo regimental no recurso especial 1402104/rj, rel. ministro raul araújo quarta turma, julgado em 27/05/2014, diário de justiça eletrônico - dje 18/06/2014)., 2014(b).

[7] Brasil. Tribunal de justiça de são paulo. apelação 0019001-91.2012.8.26.0602, relator: Fortes barbosa, data de julgamento: 26/11/2015, 6ª câmara de direito privado, data de publicação: 02/12/2015, 2015(a).

[8] Brasil. Tribunal de justiça do distrito federal e territórios. agravo de instrumento n. 20150020012285. relator: Des. carlos rodrigues. data de julgamento: 22/04/2015. publicado no dje: 15/05/2015. pág.: 147, 2015(b).

[9] M. Dantas. *Tecnologias de redes de comunicação e computadores*. Axcel Books, first edition, 2002.

[10] B. A. Forouzan. *Comunicação de dados e redes de computadores*. AMGH Editora Ltda, fourth edition, 2008.

[11] C. R. Gonçalves. *Responsabilidade Civil*. Saraiva, twelfth edition, 2010.

[12] K. W. Kurose, J. F. e Ross. *Redes de computadores e a Internet: uma abordagem top-down*. Pearson Education do Brasil, fifth edition, 2010.

[13] P. P. Pinheiro. *Direito Digital*. Saraiva, fifth edition, 2013.

[14] S. Rodrigues. *Direito Civil. Responsabilidade Civil*, volume 4. Saraiva, twentieth edition, 2008.

[15] R. Stocco. *Tratado de responsabilidade civil: doutrina e jurisprudência*. Revista dos Tribunais, seventh edition, 2007.

[16] D. Tanembaum, A. S. e Wetherall. *Redes de Computadores*. Pearson Prentice Hall, fifth edition, 2011.

[17] F. Tartuce. *Direito Civil 2. Direito das Obrigações e*

Responsabilidade Civil. Editora Método, tenth edition, 2015.