INVASÃO DE PRIVACIDADE – CONTROLE DE E-MAILS NAS EMPRESAS

Marli Imaculada da Cruz, Luís Augusto Mattos Mendes, Elio Lovisi Filho,
Débora Maria Gomes Messias
Universidade Presidente Antônio Carlos – UNIPAC
Rua Monsenhor José Augusto, 203 - São José - Barbacena - MG
marlicruz@unipac.br

RESUMO: Hoje, a todo o momento, pessoas correm o risco de sofrerem invasões, em seus e-mails. Empresas já adotam métodos de monitoramento para vigiar o acesso dos funcionários a *Internet* e *e-mails* durante o horário de serviço. Os servidores de *e-mails* estão cada vez mais protegidos contra Spams[1].

1- INTRODUÇÃO

As relações de trabalho sofreram grandes modificações com o advento do uso da *Internet* no cotidiano das empresas. De fato, não podemos negar os benefícios e vantagens trazidas por esta fantástica ferramenta, criada na segunda metade do século XX. Porém, não se pode fechar os olhos para o fato de que a expansão do uso e acesso da *Internet* no local de trabalho também trouxe algumas questões nunca antes suscitadas, colocando em ameaça os direitos personalíssimos.

Nesse sentido, discute-se hoje em dia, o cabimento do monitoramento de *e-mails* pelo empregador. Decorre daí a pergunta inevitável: o *e-mail* usado em ambiente profissional é revestido das garantias de sigilo e inviolabilidade, inclusive perante o empregador que fornece e promove o uso e o acesso ao *e-mail*? Em que pese a Carta Magna garantir a inviolabilidade de correspondência e o sigilo de dados, com efeito, o

[1] *Spams*: Lixo eletrônico enviado por e-mail.

Direito brasileiro ainda é escasso para alcançar uma resposta pacífica e certa para esta questão.

2- MONITORAMENTO DE FUNCIONÁRIOS

Pessoas que param de trabalhar durante o dia para se distrair na *Internet*, ficam alguns momentos da hora de trabalho planejando alguma viagem, divertindo-se com *games*, procurando outro emprego, namorando em *chats*, visitando *sites* pornográficos ou fazendo qualquer outra coisa via *Internet* que não fosse trabalhar. Estas pessoas estão entre milhões que podem estar sendo espionadas, rastreadas, advertidas ou demitidas por uso impróprio da *Internet*. Patrões e empregados se justificam acobertados por leis que se anulam na fraqueza de uma legislação atrasada diante do avanço tecnológico.

Com a dinâmica do mercado, tornou-se necessário criar estratégias para acompanhar a agilidade das informações e dos dados que chegam à empresa, em tempo hábil, para assim conseguir otimizar essas informações dentro do processo produtivo. Uma das formas de dinamizar tais processos é a informatização da empresa e utilização do correio eletrônico.

O fornecimento de endereço virtual aos funcionários tem gerado conflitos nas relações de trabalho. Em virtude de falta de legislação específica do confronto de interesses entre empregador e empregado e da desinformação do assunto, as empresas, preocupadas em manter o fator segurança, resolvem, por elas mesmas, criar subsídios para se proteger dos possíveis malefícios criado pela má administração dessa tecnologia.

Assim, grande parte das empresas realiza o monitoramento para verificar o que se passa na *Internet* da organização. O monitoramento eletrônico é feito por meio de programas que registram os *sites* visitados por seus funcionários, com que freqüência e por quanto tempo permanecem no *site* registram e classificam automaticamente cada

palavra que passa pelos *e-mails* que circulam no ambiente organizacional. O que se discute é a legalidade deste monitoramento ante a dificuldade legislativa que ronda à relação empregador-empregado no que se refere ao uso do correio eletrônico. [MARTINS, 2004]

Para os empregadores, o monitoramento eletrônico é necessário para impedir a perda de produtividade do empregado e para que diminua as chances de entrada de vírus imperceptíveis que possam afetar o servidor, o que pode retardar o tempo de resposta do sistema, fazendo a empresa perder rapidez e flexibilidade nos seus processos.

Sendo assim, os patrões alegam ter esse direito, pois são donos dos computadores, da linha telefônica e de toda a estrutura que envolve o empregado. Também possuem a responsabilidade de administrar os riscos de negócios, podendo assim interferir em qualquer coisa que possa, na sua estrutura organizacional, denegrir as atividades e processos que alimentam a organização. Com isso resta ao trabalhador o dever de obediência, colaboração e fidelidade na vigência da relação de emprego.

Hoje já se pode encontrar programas capazes de gerar relatórios sobre como os empregados utilizam seus *e-mails* corporativos, estes programas são ferramentas de gerenciamento do envio/recebimento de mensagens eletrônicas da empresa.

Além da possibilidade de gerenciar *e-mails* que não tratam de assuntos profissionais e melhorar a produtividade dos empregados, o programa lista os usuários que mais utilizam tal serviço, o assunto das mensagens e o tipo de arquivos que estão circulando, tudo isso sem que o administrador do sistema ou o gerente precise ler o conteúdo da mensagem do empregado na íntegra. Trata-se, então, de uma ferramenta estratégica de controle e segurança que atende de maneira ética a decisão promulgada pelo TST (Tribunal Superior do Trabalho).

Uma organização que entende quais são as tendências e padrões na comunicação via *e-mail* pode tomar melhores decisões corporativas, gerenciar mais efetivamente a produtividade de seus funcionários e aplicar políticas. A implementação de um produto como esse hoje em dia trás vantagens táticas e preciosas para a organização.

3- MONITORAMENTO DE E-MAILS: SEGURANÇA OU INVASÃO

O monitoramento de *e-mails* dos empregados tem causado uma incerteza não somente no meio jurídico, mas também no meio empresarial. Recentemente a 3ª Turma do Tribunal Regional do Trabalho da 10ª Região determinou que o HSBC Seguros do Brasil não havia violado a privacidade do empregado acusado de enviar fotos pornográficas pela *Internet* utilizando o provedor da empresa e reconheceu a justa causa na sua demissão, revertendo, portanto, a decisão da primeira instância.

Multinacionais como a General Motors, Ford, entre outros, demitiram nos últimos meses alguns funcionários pelo mau uso do *e-mail* durante o horário de trabalho. Este assunto é ainda mais alarmante quando uma pesquisa realizada pela *Personal Today*, uma empresa americana de recursos humanos, e *Websense*, uma empresa que monitora o uso da *World Wide Web*, demonstrou que cerca de 25% das empresas americanas já demitiram funcionários por conta do mau uso da *Internet* durante o horário de trabalho. A pesquisa aponta que 69% das demissões estão relacionadas à pornografia. Outras causas da perda de emprego referem-se a participar de salas de *chat* (10%), acessar *sites* de *webmail* (9%), *sites* de racismo (5%) ou fazer *download* de música (4%). Segundo o relatório, 40% das companhias já receberam denúncias de empregados sobre colegas que estariam "perdendo tempo" na *Internet*. [PERSONAL TODAY, 2005]

Em razão do acima exposto, surgiram inúmeras questões acerca deste assunto, tais como a proteção da privacidade das comunicações por *e-mail*, a possibilidade do monitoramento dos *e-mails* dos empregados pelo empregador, a expectativa do empregado em gozar de um mínimo de privacidade no local de trabalho, e, se as regras de inviolabilidade de correspondência postal ou epistolar constitucionalmente garantidas aplicam-se aos *e-mails*. [MARTINS, 2004].

O monitoramento de *e-mails* no ambiente, o qual está vinculado à questão do equilíbrio da privacidade do empregado com a necessidade do empregador em continuar seus negócios, está atualmente em pauta. O empregado tem uma expectativa legítima que encontrará privacidade no seu ambiente de trabalho. Entretanto, essa expectativa precisa ser equilibrada com os interesses do empregador em continuar seus negócios de maneira eficiente e de se proteger contra quaisquer danos que possam ser causados pelo empregado. Nesta árdua tarefa de atingir um equilíbrio, inúmeros princípios precisam ser levados em consideração, principalmente os da proporcionalidade e da finalidade. Ainda que o monitoramento de *e-mails* do empregado pelo empregador no ambiente de trabalho possa servir aos interesses do empregado, isso o justifica. Para tanto, as seguintes perguntas devem ser analisadas pelo empregador: (1) o monitoramento é realizado de forma transparente aos empregados? ; (2) é necessário? O empregador poderia obter o mesmo resultado por meio de métodos tradicionais de supervisão? ; e (3) a restrição da privacidade do empregado é proporcional ao resultado que o empregador pretende obter?[OLIVEIRA, 2004]

No tocante ao desenvolvimento desta questão no exterior, a União Européia publicou em Maio deste ano um relatório que visa analisar a questão do monitoramento de comunicação eletrônica no ambiente de trabalho nos países da comunidade européia

à luz da Diretiva de Proteção de Dados (95/46/EC) e das recentes decisões da Corte Européia de Direitos Humanos. De acordo com o relatório o monitoramento de *e-mails* deve ser realizado somente nos casos em que os métodos de supervisão tradicionais forem ineficientes e sempre com um certo grau de transparência.

O Reino Unido e os Estados Unidos da América já possuem legislações especificas com relação à privacidade na *Internet*. No Reino Unido, nos termos do "*The Telecomunication (Lawful Business Practice) (Interception Communications) Regulations* 2000", de 23 de outubro de 2000, o empregador pode monitorar *e-mails* de seus empregados desde que os mesmos sejam comunicados sobre tal fato, não sendo necessária a obtenção de consentimento prévio. Nos EUA, após o ataque de 11 de setembro de 2001, foi promulgada o *USA PATRIOT ACT*, que restringiu a privacidade dos Americanos. Muitos consideram que essa lei americana foi um retrocesso.

No Brasil, não há legislação específica, nem linha jurisprudencial clara com relação a este assunto. O inciso XII do art. 5º, da Constituição Federal, dispõe ser "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal processual penal". A forma estabelecida pela lei para quebra do sigilo das comunicações telefônicas está prevista na Lei nº. 9.269, de 24 de julho de 1996, que limita a quebra do sigilo das comunicações telefônicas às hipóteses de investigação criminal ou instrução penal. A questão se a transmissão de *e-mail*, ou seja, de dados eletrônicos, pode ser enquadrada nesta disposição legal constitucionalmente garantida é controversa. O que verificamos é que em razão da Lei nº. 9.269, a inviolabilidade não é absoluta.

Dessa forma, podemos entender que mesmo que a privacidade do funcionário não possa ser derrogada por contrato, a mesma não é absoluta. A caixa de correios eletrônicos utilizada pelos empregados não deve ser considerada privativa, pois a utilização adequada da mesma seria para receber e enviar *e-mails* cujos assuntos deveriam ser relacionados exclusivamente ao trabalho desenvolvido pelo respectivo empregado na empresa. Caso o empregado saísse de férias, o empregador poderia redirecionar seus *e-mails* para qualquer outra pessoa que ficasse responsável pelas funções do empregado que está de férias, extinguindo, portanto, o caráter privativo da caixa de correios eletrônicos do funcionário. Este entendimento é claramente refletido pelo precedente norte-americano, pelo qual os tribunais determinaram que a Constituição Americana protege pessoas e não lugares. Segundo tais tribunais, a privacidade somente será preservada quando há uma expectativa que o local é privado, o que não ocorre no ambiente de trabalho. Ainda assim, entendemos que seria adequado que para o monitoramento e/ou leitura do conteúdo dos *e-mails* do empregado, houvesse a anuência prévia por escrito deste último.

A proteção da privacidade no meio eletrônico encontra fundamento na Medida Provisória No. 2.200-2, de 24.10.2001, que versa sobre a certificação de documentos digitais e em projetos de lei atualmente em trâmite no Congresso Nacional (PL No. 4.906/2001 e outros projetos de lei que versam sobre *spam* e *cookies*[2]*)* . A questão de monitoramento de mensagens eletrônicas em ambiente de trabalho ainda não foi analisada por nossos legisladores.

Considerando o acima exposto, o empregador precisa tomar inúmeras decisões para obter o equilíbrio da garantia da privacidade do empregado e da garantia da

[2] *Coockies*: Arquivos locais que guardam informações a respeito da navegação.

proteção de seu negócio. Como podemos contrabalançar essas duas situações? Considerando que a empresa decida monitorar os *e-mails* dos empregados, como deveria esta sempre proceder? Quais as medidas preventivas que o empregador deve tomar no Brasil à luz de todas as certezas doutrinárias, legislativas e jurisprudenciais? Além da utilização de certificação digital e implementação de medidas de segurança eficazes, a melhor medida a ser tomada é informar ao empregado as diretivas da empresa sobre a utilização do *e-mail* informando, entre outras coisas, que o *e-mail* é para ser usado para fins de trabalho e que o seu uso pessoal é um privilégio. Ressalta-se, no entanto, que o empregador deve procurar outras formas de supervisionar o trabalho do empregado utilizando-se de formas mais tradicionais antes de recorrer ao monitoramento. Adicionalmente, as diretivas devem incluir que o empregador possa fiscalizar e monitorar as informações dos *e-mails*, além de todas as proibições e sanções pelo uso indevido do *e-mail*. Como mencionado acima, a fiscalização e o monitoramento dos *e-mails* somente poderão ser feitos mediante a prévia anuência dos empregados, por escrito, que deverá ser entregue pelo mesmo no momento de sua contratação ou da implantação de um sistema de *e-mails*. Essas diretivas devem estar acessíveis aos empregados e serem adotadas como política interna do local de trabalho.

É importante ressaltar que mesmo que sejam adotadas todas estas medidas pelo empregador e que as mesmas tenham concordância do empregado, elas não representam garantias absolutas frente às inúmeras possibilidades que podem surgir no contexto prático de cada caso.

4.Servidores de E-mail

Os servidores de e-mail são programas especializados na transmissão e recepção

de correspondências eletrônicas que pode ainda funcionar como um filtro na rede da empresa descartando assim mensagens que contenham determinado assunto, emitente, anexos executáveis ou ainda, que contenham palavras específicas no corpo do texto como sexo e pornografia.

Os servidores de e-mail, que podem ser de uso interno ou externo, podendo receber e-mails apenas oriundos da empresa no primeiro caso ou oriundos de qualquer endereço da *Internet* como no segundo caso. Dentre as vantagens possibilitadas pelo uso do e-mail corporativo podemos citar:

- Envio de mensagens sem limitação de tamanho imposta pelo provedor, sendo que o tamanho máximo poderá ser determinado e alterado pelo próprio cliente.

- O envio de mala direta para os seus clientes sem as limitações impostas pelos provedores.

- A possibilidade de verificar no *log* (registro de ocorrências) do servidor a entrega do *e-mail* ao servidor do destinatário.

- A manutenção das mensagens no próprio servidor, permitindo um backup de todas as mensagens dos usuários evitando as limitações impostas pelos provedores.

Nos itens 4.1 e 4.2 serão apresentadas duas ferramentas que são comumente utilizadas pelas empresas que possuem um servidor de e-mail.

4.1 SENDMAIL

*Sendmai*l é um agente de transferência de correio (MTA na sigla em inglês) de código aberto: um programa para o roteamento e a entrega de correio eletrônico. Seus autores liberaram a atual versão, *Sendmail* 8.13.4 em 27 de março de 2005.

O *Sendmail* é o servidor de *e-mails* (MTA) mais usado em toda *Internet*, porém

também um dos mais complexos e "difíceis" de serem configurados. A complexidade atribuída a este servidor refere-se a dificuldade encontrada em editar um arquivo de configuração criptográfico e dos difíceis comandos encontrados no *sendmail.cf.*

O *Sendmail+IDA* é diferente do *Sendmail,* pois elimina a necessidade de editar sempre *sendmail.cf* o que permite ao administrador definir roteamentos específicos para sites determinados e configurações de endereçamento através de arquivos de suporte mais legíveis chamados tabelas, comparado com outros agentes de transportes de mensagens, provavelmente não há nada mais rápido e simples que o *sendmail+IDA*. Tarefas típicas que são necessárias para administrar o UUCP[3] ou um site *Internet* podem se tornar bastante simples. Configurações que normalmente são extremamente difíceis tornam-se simples de serem configuradas e mantidas.

Muitos administradores de sistemas não desejam preocupar-se com o trabalho necessário para garantir que o sistema local seja capaz de atingir todas as redes (e por conseqüência os sistemas) do mundo. Dessa forma, é preferível retransmitir todas as mensagens para outro sistema tido “inteligente”. Definir sistema inteligente em nota de rodapé

4.2 POSTFIX

Postfix foi criado primeiramente para substituir o *Sendmail,* um programa que fosse rápido, fácil de administrar e seguro. Trata-se de um projeto *Open Source* bancado pela IBM, criado e mantido por *Wietse Venema*.

[3] *UUCP:* Possibilita transferência de arquivos, execução de comandos e correio eletrônico.

Uma instalação padrão do *Postfix* pode substituir facilmente o *Sendmail* sem alterações significativas no sistema, e transparentemente para o usuário final. As bases de usuários e bases de correio por default são as mesmas.

Os arquivos de configuração são simples e objetivos, preparados para que as variáveis e opções de configurações sejam bastante intuitivas e fáceis de entender.

A arquitetura interna do sistema funciona sem um conceito muito rígido sobre processos "pai-filho", mas com a idéia de processos cooperativos. Basicamente, as tarefas que o *Postfix* roda são independentes, e provêem serviços umas as outras (por exemplo, há uma tarefa que prove reescrita/tradução de endereços para todos os outros processos do *Postfix*).

Há um processo principal (o "máster"), que não faz nada a não ser administrar os outros *daemons* do *Postfix*: carregar o "smtp" quando há necessidade de atender a porta SMTP, manter o "*trivial-rewrite*" rodando para fazer a manipulação dos endereços de correio, chamar o "qmgr" para gerenciar a fila de *e-mails* ainda não entregues, chamar o "*pick-up*" que pega novas mensagens e as joga na fila para entrega, etc.

O "*máster*" também se encarrega de manter uma espécie de *cache* dos *daemons* que já foram iniciados, reutilizando processos ou removendo-os depois de um tempo especifico em ociosidade. O que diminui o tempo e o esforço despendido na maneira tradicional garantindo que não haja desperdício de recursos.

É possível forçar alguns roteamentos de mensagens dentro das filas do *Postfix.* Quando se especifica um caminho diferente do que o sistema usaria normalmente, estamos criando um mapeamento de transporte. Um transporte não se refere apenas ao

destinatário final da mensagem, a ser entregue via smtp; podemos criar mapeamentos de transporte para dentro de outros sub-processos do *Postfix*.

O *Postfix* conta com diversas regras e macros para ajudar no combate a *SPAM*. Essas restrições e macros têm se mostrado bastante efetivas. Dentre as restrições podemos utilizar filtragem de cabeçalho e corpo da mensagem.

Esse tipo de filtragem permite que se barre mensagens na sessão SMTP, antes mesmo da mensagem passar para a fila. Embora isso possa ser vantajoso no sentido de não ser necessário enviar uma mensagem de *bounce* ou retorno quando a mensagem não é aceita, pode trazer problemas sérios de performance para o servidor, uma vez que a mensagem toda tem que ser analisada e filtrada antes de se dar o "*OK*" na sessão SMTP.

Os provedores brasileiros utilizam em sua maioria o *Postfix* devido a sua facilidade e disponibilidade de regras e macros no que tange o combate a *SPAM*.

5- CONCLUSÃO

A ética profissional é fundamental para todas as profissões: ela estabelece os princípios que regulamentam o relacionamento entre o profissional, seus companheiros de trabalho e seus clientes. Praticamente todas as empresas, pequenas ou grandes, utilizam a *Internet*, mas têm sido cada vez mais comuns notícias de uso indevido da *Internet* pelos funcionários dentro de empresas. Devido ao mau uso da *Internet* torna-se possível à invasão, roubo de informação sigilosa e até mesmo a infecção por vírus da rede da empresa. A infecção do servidor na maioria das vezes é causada por e-mails com anexos executáveis, *spywares* que são instalados na visita a sites o que torna vulnerável a confidencialidade da empresa.

Em um país onde não existem leis especificas para lidar com esse tipo de crime é cada vez mais comum encontrar *spywares* nos computadores seja em casa ou nas empresas. Providências devem ser tomadas, pois apesar dos programas de bloqueio funcionarem, a cada dia, novos invasores são criados, sendo assim difícil ter certeza se esta infectado ou não.

Os servidores de e-mails estão cada vez mais se adequando as novas medidas necessárias para lidar com *softwares* de invasão, além de possuírem recursos variados para monitoramento de *e-mails* nas empresas. Portanto, com os servidores de *e-mails* as empresas podem aprimorar suas técnicas de monitoramento, garantindo assim, o bem estar da empresa e dos funcionários.

BIBLIOGRAFIA

ARAUJO, Victor (2004) *Segurança em Redes de Computadores para Servidores Windows em Intranets.* Monografia – UNIPAC - Barbacena: Campus Magnus.

CANO, Ignácio. *Cidadio Deve Ser Protegido Contra Invasão de Privacidade*. Disponível em:<http://www.listaderiscos.com.br/lr/news/notícia.asp?idNoticis=5468>. Acesso em: 26 de agosto de 2005.

DUARTE, Márcio Archanjo Ferreira. *Monitoramento de e-mails* / Disponível em: <www.cbeji.com.br.> Acesso em: 15 de novembro de 2005

MARTINS, Henrique. *E-mail de Funcionários pode ser violado?* Disponível em: <http://www.cbeji.com.br/artigos/artviolacaodeemails.htm> *Acesso em: 19 de novembro de 2005*

TODAY, Personal. *25% das empresas já demitiram por mau uso da web nos EUA. Disponível em:*

http://www1.folha.uol.com.br/folha/reuters/ult112u18409.shl. Acesso em: *19 de novembro de 2005.*

OLIVEIRA, Alex dos Santos *monitoramento*: www.curricular.com.br/alexoliveira - 22k. Acesso em 19 de novembro de 2005.