

# **E-mail Empregados x Empresas <sup>1</sup>**

**Ly Freitas Filho <sup>2</sup>**

**Cynthia Mayra Mascarenhas, Frederico Segall Terra, Káryta Moura  
Alabarce Bove, Samanta Silveira dos Anjos.**

## **Resumo**

Atualmente, é grande o número de empresas que disponibilizam aos seus empregados o acesso à internet, de modo que eles possam utilizar essa importante ferramenta para realização de suas tarefas. Ocorre que, uma vez tomada essa iniciativa pelas empresas, os empregados passam a ter a sensação de que tudo é grátis e não tem limites, proporcionando conflitos de interesses e direitos. Os empregados passam a ter acesso a todo tipo de informação disponível na internet, inclusive a conteúdo estranho às atividades profissionais, como, por exemplo, sites esportivos, de bate-papo, de compras, pornográficos, entre outros. Conflitos de interesses e direitos, são gerados, como o que hoje se vê entre as empresas, que pretendem garantir seus negócios e se sentem lesadas por empregados que usam suas máquinas, endereços e tempo de serviço para mandar e receber mensagens de conteúdo incompatíveis com as atividades profissionais dos seus empregados e estes, que pensam estarem sendo vítimas de ataques aos seus direitos e garantias individuais de liberdade e privacidade.

## **Palavras-chave**

Monitoramento; Segurança; Privacidade.

## ***E-mail Employees X Companies***

### ***Summary***

*Actually, it is big the number of companies that they make available their employees the access to the internet, so that they can use that important tool for accomplishment of their tasks. It happens that, once taken that initiative companies, the employees start to have the sensation that everything is free and they doesn't have limits, providing conflicts of interests and rights. The employees start to have access the every type of available information in the internet, besides to strange content to the professional activities, as, for instance, sporting sites, of chat, of purchases, pornographic, among others. Conflicts of interests and rights, they are generated, as what today sees her among the companies, that intend to guarantee their businesses and if they are harmed by employees that use their machines, addresses and time of service to order and to receive incompatible content messages with their employees' professional activities and theses, that they think be being victims of attacks to their rights and individual warranties of freedom and privacy.*

### ***Keywords***

*Monitoramento; Safety; Privacy.*

---

<sup>1</sup> Trabalho desenvolvido no curso de pós-graduação MBA – Gestão de Sistema de Informação da UCB

<sup>2</sup> Professor da disciplina Segurança da Informação do MBA – Gestão de Sistema de Informação da UCB

# 1. Introdução

O e-mail é uma correspondência eletrônica, é um dos mais utilizados recursos proporcionados pela Net, pois é através dele que os usuários poderão se comunicar, enviando e recebendo mensagens. É a forma básica de interação entre pessoas na Internet.

O mundo evolui, todos nós evoluímos. Com a tecnologia, em tempos de globalização, não é diferente, pelo contrário, as mudanças e os avanços são constantes, rápidos e substanciais, As empresas preocupadas com a segurança vêm monitorando os e-mails e, por outro lado, os trabalhadores estão exigindo o direito de privacidade.

O fator segurança deve ter preocupação redobrada nas empresas que se conectam a Internet, principalmente quando fornecem endereço eletrônico a seus empregados. Realmente "... o mundo digital não é exatamente o melhor lugar para pessoas inocentes". A questão não está apenas relacionada à relação de emprego, trata-se da questão de informações. A segurança versus privacidade entre EMPREGADOS X EMPRESAS vem se acirrando e a questão ainda não é consensual, havendo muita discussão e desencontros pela falta de legislação específica.

Nas empresas deve existir uma política de proteção contra os danos que podem advir do mundo virtual. E que essa política, em nome do bom senso, tem de ser conhecida por ambas às partes, o que não ocorre atualmente. Desenvolver uma política de privacidade para proteger as informações de seus clientes é apenas o início de uma mudança profunda. O que, taxativamente, não pode ocorrer é a empresa, monitorando, descobrir situação pessoal do empregado que em nada influa no bom andamento do negócio - preferência sexual, por exemplo - e, por causa dela, aplicar-lhe a sanção. Nesse caso ele poderá - e a todos é garantido o direito à petição - acionar a corporação por discriminação, o que pode trazer à empresa graves conseqüências.

O que se discute, é a legalidade ou não deste monitoramento, com a dificuldade de que inexistente legislação específica acerca da matéria em nosso país. O tempo dos empregados, o necessário foco, atenção e concentração no serviço que devem prestar, não podem e não devem ser influenciada pela troca de correspondência na Internet, a não ser naquilo que seja útil e necessário à empresa.

Embora o fator segurança seja de vital importância na utilização da Internet/e-mails, não se pode ignorar o princípio constitucional da privacidade. A Constituição Federal de 05/10/1988 dispõe no art. 5º, incs, X e XII, que a privacidade é direito fundamental de nossos cidadãos. Com a falta de regulamentação específica sobre privacidade na Internet/e-mail deixa o ciberespaço livre para a utilização de tecnologias que tornam vulnerável a vida das empresas colocando-as em uma vitrine, onde suas atividades e informações são registradas e observadas.

A ética é um princípio sem fim, a segurança da informação é um processo que não termina nunca. Mas ela não existe por si só. Ela existe para possibilitar que o negócio da empresa aconteça de forma protegida no que diz respeito aos dados. A segurança da informação é uma decisão empresarial. A empresa deve sempre proteger a informação.

O empregado deve se conscientizar que os equipamentos de informática são propriedade do empregador, sendo o seu uso restrito aos assuntos da empresa. Todavia,

a subordinação do empregado e o poder de comando do empregador não podem servir de amparo para ações que desrespeitem o direito à privacidade e o sigilo das comunicações.

## 2. Crimes de Informática e seus Aspectos Processuais

O Crime de informática é todo aquele praticado contra os sistemas de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os executados através do computador. Inclui-se neste conceito os delitos praticados através do correio eletrônico. Os crimes de informática são classificados como próprios ou impróprios, onde os crimes próprios são aqueles praticados através do computador, e os impróprios praticados de qualquer forma, mas utiliza eventualmente recursos de informática.

No Brasil, como em todo o mundo, os crimes de informática têm crescido consideravelmente e algumas iniciativas estão sendo tomadas, como a criação de leis específicas de informática e a criação de grupos de controle de tudo que está relacionado com a informática, e principalmente à Internet.

Aqui no Brasil ainda não possuímos uma lei ou norma específica para a informática, mas foi criado a partir da necessidade de coordenar e integrar todas as iniciativas de serviços Internet no país e com o objetivo de assegurar qualidade e eficiência dos serviços ofertados, assegurar justa e livre competição entre provedores e garantir a manutenção de adequados padrões de conduta de usuários e provedores, o Comitê Gestor da Internet, que tem como principais atribuições:

- Fomentar o desenvolvimento de serviços Internet no Brasil;
- Recomendar padrões e procedimentos técnicos e operacionais para a Internet no Brasil;
- Coordenar a atribuição de endereços Internet, o registro de nomes de domínios, e a interconexão de espinhas dorsais;
- Coletar, organizar e disseminar informações sobre os serviços Internet.

Na tabela I, estão exemplificados alguns crimes de informática, com sua respectiva classificação e a pena que pode atribuída em caso de condenação.

**Tabela I – Crimes e Condenações**

Crimes	Classificação	Pena
Ameaça	Impróprio	1 a 6 meses/multa
Interceptação de e-mail / Comercial	Próprio	6 meses/multa
Furto	Próprio	1 a 8 anos/multa
Envio de Vírus e Similares	Próprio	1 a 6 meses/multa
Violação de Direito Autoral	Impróprio	3 a 12 meses/multa
Favorecimento de Prostituição	Impróprio	2 a 5 anos
Ato Obsceno	Impróprio	3 a 12 meses/multa
Adultério	Impróprio	15 a 180 dias
Pedofilia	Impróprio	1 a 4 anos

Uma das questões de maior debate diz respeito à possibilidade de interceptação do correio eletrônico do empregado pelo empregador quando haja desconfiança sobre sua utilização ou simplesmente como uma espécie de extensão de seu poder diretivo de fiscalização. De acordo com as normas nacionais e internacionais a correspondência, seja ela eletrônica ou não, é considerada inviolável, mas as formas de utilização e os

recursos utilizados para o envio da correspondência podem gerar discussões e brechas nas interpretações destas normas ou leis.

Como referência, abaixo são citados alguns países e o tratamento de que cada um deles à interceptação de correio eletrônico e as respectivas leis para este tratamento:

- Na **Gran Bretaña** a *Regulation of Investigatory Powers Act 2.000*, vigente desde 24 de outubro permite o acesso do correio eletrônico do empregado utilizado de forma indevida (uso não autorizado) pelo empregador.
- Na **França** no caso *Tareg Al Baho, Ministere Public / Francoise V, Merc F et Hans H o Tribunal Correccional* de Paris condenou os demandados (Diretores da Escola Superior de Física e Química Industrial de Paris) por violação do segredo de correspondência do demandante, porque suspeitaram que o mesmo estava sendo usado para fins pessoais, pois que a Justiça Francesa entende que as contas de correio eletrônico estão amparadas pelo segredo de correspondência.
- Na **Bélgica** o Tribunal do Trabalho de *Bruxelas* proferiu sentença em 02 de maio de 2000, baseado no artigo 8º do Convênio Europeu de Direito Humanos, entendendo que o envio de correio eletrônico pessoal enviado da empresa pertence à vida privada do trabalhador, considerando que o mero atestado do número de correios, seu tamanho e seu caráter privado são dados suficientes para proceder a sansão sem necessidade de intervir no conteúdo do mesmo.
- Na **Holanda** a lei de proteção de dados pessoais de 2001, permite o monitoramento das atividades eletrônicas dos trabalhadores desde que haja a participação do sindicato ou representante dos trabalhadores para acompanhar ou elaborar o sistema de controle. Assim mesmo obriga a empresa a fazer publicas suas metas de controle aos trabalhadores.
- No **Japão** em agosto do ano de 2000 entrou em vigência a lei de interceptação das comunicações, pela qual permite o acesso dos correios eletrônicos no curso da investigação de crimes sérios, como o assassinato, dentre outros.
- Os **Estados Unidos da América** conta com leis de proteção como: *The Federal Wiretapping Act y Electronic Communications Privacy Act* de 1986 que proíbe a interceptação de comunicações eletrônicas, porém permite exceções como a dada através do consentimento do afetado. Muitos Estados tem adotado leis similares a esta lei federal como o Estado de *Maryland* e o da Flórida, que requerem o consentimento de ambas as partes antes que o empregador possa vigiar o correio eletrônico. Assim a jurisprudência americana tem resolvido na maioria dos casos a favor do monitoramento do correio eletrônico pelas empresas.

Desta forma, fica claro que a questão de interceptação do correio eletrônico é vista de formas diferentes entre as diversas culturas em todo o mundo e a aplicação das leis sobre este tema está a cada dia se tornando mais específica.

Casos de condenações de empresas, pela interceptação não autorizada do correio eletrônico, e de empregados, pela má utilização de um recurso que é disponibilizado pela empresa são constantemente apresentados em artigos e matérias de direito e de informática.

Alguns exemplos de casos famosos são apresentados abaixo e mostram a complexidade que o tema interceptação de e-mail causa;

**1º Caso** - Em maio de 2001, a *General Motors* do Brasil demitiu 11 empregados e advertiu 81 sobre o mau uso do correio eletrônico. Isso porque os empregados trocaram mensagens com conteúdo pornográfico. O problema explodiu quando os e-mails chegaram para uma funcionária da GM dos Estados Unidos. Ela contou para a chefia e detonou uma investigação que chegou no nome de empregados da filial brasileira de São Caetano do Sul, no ABC paulista. Conseqüência: demissão por justa causa.

**2º Caso** - Empresas como a americana *Dow Chemical*, *Xerox* e *Pricewaterhouse Coopers* também já dispensaram alguns profissionais pelo uso indevido dos e-mails.

**3º Caso** - *Chevron* pagou uma indenização de U\$ 2,2 milhões para interromper um processo no qual funcionárias da empresa acusavam-na de permitir que o sistema interno de e-mail fosse usado para transmitir mensagens sexualmente ofensivas. Uma das mensagens usada como evidência era uma lista das “25 razões porque uma cerveja é melhor que uma mulher”.

**4º Caso** - No Brasil, uma multinacional do ramo alimentício que está respondendo a processo em virtude de um funcionário ter enviado um e-mail contendo uma piada de cunho racista para um grupo de destinatários. Uma pessoa negra, que recebeu uma cópia deste e-mail, vinda de outras pessoas, resolveu processar não as pessoas intermediárias ou mesmo o missivista, mas sim a empresa, com base nesta provisão da CLT.

Apesar destas diversidades de aplicação das leis e suas condenações, segundo a Associação Americana de Administração o número de empresas que vigiam seus empregados pulou de 14,9% em 1994, para 38,2% em 2000, ou seja, a cada as empresas investem mais em controle e os empregados reclamam cada vez mais deste controle excessivo.

## 2. Ética

Encontramos no art 2º, da CLT, a seguinte lei: “Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação de serviço”. Com isso, por assumir os riscos, o empregador acaba ganhando o direito diretivo sobre o empregado. Mas será que esse direito não tem limite?

Se o empregador pode normatizar o uso, pelos seus empregados, dos veículos que possui, pode regular o uso do telefone e dos demais equipamentos, como não poderia fazê-lo sobre o tráfego na rede ou de seus e-mails?

O correio eletrônico é uma ferramenta de trabalho dada pelo empregador ao empregado para realização do trabalho, portanto sobre ele incide o poder de direção do empregador e conseqüentemente o direito do mesmo fiscalizar seu uso pelo empregado. Os endereços eletrônicos gratuitos e ou particulares, desde que acessados no local de trabalho, enquadram-se, em tese, no mesmo caso.

Neste sentido, precisamos hoje encontrar um denominador comum que atenda aos direitos e expectativas de ambas as partes sem, entretanto, contrariar as leis de nosso ordenamento jurídico.

Tudo começa pela instituição de regras claras sobre como devem ser usados os recursos da internet colocados ao dispor dos empregados. Ao empregador, que tem o poder hierárquico para dirigir a prestação de serviços por seus empregados, cabe regulamentar como se utilizarão os recursos da empresa no trabalho, através de um documento interno que defina com clareza e precisão não só os procedimentos de rotina como também os direitos e deveres de cada um. Esta seria a melhor maneira de evitar problemas que eventualmente acabam transformando-se em casos judiciais.

Nas grandes empresas o poder da organização se manifesta através da imposição unilateral de um conjunto de normas estruturais chamado Regulamento Interno de Trabalho, cujo teor obriga tanto a comunidade de trabalho como o empregador. O regulamento Interno de trabalho (RIT) deve definir com clareza e precisão não só os procedimentos de rotina como também os direitos e deveres de cada um, a fim de eliminar, de antemão, possíveis causas de conflitos, bem como possibilitar a convergência das ações individuais para o desenvolvimento produtivo do grupo.

Dentre as recomendações para o conteúdo dos documentos que expõe essas regras, sejam eles regulamentos ou normas, destacam-se:

- Deixar claro que os arquivos e mensagens dos empregados podem ser revisados a qualquer momento, sem aviso prévio;
- Que os empregados não devem esperar que qualquer conteúdo que eles criem, armazenem, enviem ou recebam em seus computadores (na empresa) sejam privados;
- Deixar claro que os computadores que os empregados usam pertencem à empresa e só devem ser usados para propósitos profissionais;
- Que as mensagens eletrônicas devem ser escritas e enviadas com o mesmo cuidado que qualquer outra forma de comunicação comercial.

Além disso, os empregados devem estar cientes e ler, assinar e datar o documento, informando que se responsabilizam pelas possíveis violações e pelas ações que elas acarretarão.

É importante que as empresas que disponibilizam e-mails corporativos deixem claro para seus empregados qual a política de privacidade a ser adotada em relação ao seu uso: o funcionário deve saber se suas mensagens estão ou não sujeitas à monitoração.

O que não pode acontecer – e aí está o perigo – são os excessos, por parte das empresas, os quais, sob a alegação de proteção, impliquem a verdadeira invasão na vida pessoal do funcionário. A exposição inicial das regras ao empregado, quando de sua contratação, cientificando-o da existência do monitoramento (alerte-se para o fato de que tal prática jamais pode ser secreta), bem como que ele só poderá utilizar o nome da empresa para o seu trabalho tem surtido bons efeitos na prevenção de litígios.

De fato, pois, uma vez devidamente alertado o funcionário, se for detectado pela empresa que mensagens suas apresentam conteúdo nocivo à imagem da corporação, ou revelam segredos profissionais, poderá haver aplicação de eventual sanção, variável de acordo com a gravidade dos conteúdos.

## 4. Conclusão

A Internet, em especial, como maior rede mundial de conexão para a comunicação entre usuários, transmitindo dados a qualquer lugar do mundo e permitindo acesso de informações pelos *links* em hipertexto, na *Web* e em espaços que vão sendo desenvolvidos, vem ocasionando uma verdadeira revolução.

O avanço tecnológico veio agravar o problema da vida privada, de tal maneira que já não é possível resguardar da curiosidade pública a nossa privacidade.

O fornecimento de endereços virtuais (correio eletrônico) aos empregados tem gerado conflitos nas relações de emprego. As empresas preocupadas com a segurança vêm monitorando os e-mails e, por outro lado, os trabalhadores estão exigindo o direito de privacidade.

As empresas de hoje em dia não querem saber de perda de tempo, e se preparam para controlar o uso da comunicação eletrônica. Junto com as informações, o e-mail pode trazer destruição para o computador, já que os arquivos anexados são um excelente caminho, uma boa estrada, para propagação de vírus ou *scripts* maliciosos e também outros fatores levam as empresas a justificarem a monitoração dos e-mails de seus empregados, além do monitoramento da atividade de navegação na *Web*.

Deve-se analisar com bastante cuidado a conveniência de acesso à Internet pelos empregados no local de trabalho e, enquanto não há legislação específica, é bom que se adote regulamentação interna, ou ainda, que seja regida a questão em contrato e ou norma coletiva. Os perigos à sua espreita vão de vírus a bugs, de crackers a fofoqueiros profissionais, de ladrões online a homens de negócios sem escrúpulo. Nesta virada de milênio, um turbilhão de ameaças paira sobre a segurança e a privacidade de todo mundo.

A falta de cuidados ao endereçar uma mensagem eletrônica poderá expor a EMPRESA e/ou os Usuários a ações judiciais e demais procedimentos pertinentes à falta eventualmente cometida. Cabe aos Usuários diligenciar com prudência o endereçamento de mensagens eletrônicas.

A Internet é uma rede pública, o que significa que ela está aberta a ataques e que é, sim, potencialmente muito perigosa quando não há proteção e isso deve ser levado à sério. O necessário é ter discernimento, é saber até onde e como se pode ir, observando-se os limites de cada um e suas interligações e ramificações, diretas e ou indiretas.

## 5. Referências

[MASIERO, 2000] MASIERO, P.C. “Ética em Computação”, EdUSP, 2000, p.20, 168-171

[PECK, 2002] PECK, P. “Direito Digital”, Saraiva, 2002, p.67-68

[CASTRO&CASTANHEIRA, 2004] CASTRO, G. & CASTANHEIRA, P. Home Page: “Aspectos Trabalhistas Relacionados ao Acesso à Rede”, <http://www.direitonaweb.com.br>, consulta em 23/06/04

[CASTRO, 2003] CASTRO, C.R. “Crimes de Informática e seus Aspectos Processuais”, Lumen Juris, 2ª edição, revista ampliada e atualizada, p.21-24