

Sistemas de Informação

Aula 9

Os Desafios Éticos da Tecnologia da Informação

A Dimensão Ética



- A revolução da informação com sua tecnologia da informação ampliou drasticamente nossa capacidade para adquirir, manipular, armazenar e comunicar informações
- A TI tornou mais fácil se comunicar, trabalhar em cooperação, compartilhar recursos e tomar decisões, tudo eletronicamente
- A tecnologia da informação também tornou possível o engajamento eletrônico em práticas empresariais éticas ou antiéticas em qualquer lugar do mundo

A Dimensão Ética



- As dimensões éticas de controvérsia que o gerente pode ter de encarar incluem:
 - Devemos monitorar eletronicamente as atividades de trabalho e o correio eletrônico de seus funcionários?
 - Devemos deixar os funcionários utilizarem seus computadores de trabalho para atividades particulares ou levarem cópias de softwares para suas casas para uso pessoal?

A Dimensão Ética



- Devemos acessar eletronicamente os registros de pessoal ou as estações de trabalho de seus funcionários?
- Devemos vender para outras empresas informações sobre clientes extraídas dos seus sistemas de processamento de transações?

Fundamentos Éticos



- Existem diversas filosofias éticas que o gerente pode utilizar que ajudam a orientá-lo na tomada de decisões éticas.
- São elas:
 - Egoísmo
 - Lei Natural
 - Utilitarismo
 - Respeito pelas Pessoas

Fundamentos Éticos



- Egoísmo
 - O que é melhor para um determinado indivíduo é o certo
- Lei natural
 - Os homens devem promover sua própria saúde e vida, propagar-se, buscar conhecimento do mundo e de Deus, buscar relações íntimas com outras pessoas e submeter-se à autoridade legítima

Fundamentos Éticos



- Utilitarismo
 - São corretas as ações que produzem o bem maior para o maior número de pessoas
- Respeito pelas pessoas
 - As pessoas devem ser tratadas como fim e não como meio para um fim; e as ações são corretas se todos adotarem a regra moral pressuposta pela ação

Fundamentos Éticos



- Existem modelos éticos de como os seres humanos aplicam sua filosofia ética escolhida às decisões e escolhas que precisam fazer diariamente no trabalho e em outras áreas de sua vida
- Uma teoria se concentra nos processos de tomada de decisão das pessoas e enfatiza como os vários fatores ou as nossas percepções desses fatores afetam nosso processo de tomada de decisão ética

Fundamentos Éticos



- Outra, a teoria do estágio comportamental, afirma que as pessoas passam por diversos estágios de evolução moral antes de se fixarem em um nível de raciocínio ético

Ética Empresarial



- A ética empresarial pode ser subdividida em duas áreas distintas:
 - A primeira diz respeito às práticas ilegais, antiéticas e questionáveis de gerentes ou organizações, suas causas e suas possíveis correções
 - A segunda diz respeito às numerosas questões éticas que os gerentes devem enfrentar como parte de suas decisões empresariais cotidianas

Ética Empresarial



- Os gerentes utilizam diversas alternativas importantes quando confrontados com decisões éticas sobre questões de negócios
- Essas alternativas incluem:
 - Teoria do Acionista: Sustenta que os gerentes são agentes dos acionistas e sua única responsabilidade ética é aumentar os lucros da empresa sem violar a lei ou se envolver em práticas fraudulentas

Ética Empresarial



- Teoria do Contrato Social: Afirma que as empresas possuem responsabilidades éticas para com todos os membros da sociedade, o que permite às empresas existirem com base em um contrato social
- Teoria das partes interessadas: Sustenta que os gerentes possuem uma responsabilidade ética na administração de uma empresa para o benefício de todo o seu público, que são todos os indivíduos e grupos que possuem um interesse ou um direito em uma empresa

Dimensões Éticas e Sociais da TI



- O uso da TI nos negócios possui impactos importantes sobre a sociedade e, com isso, levanta sérias considerações éticas em áreas como:
 - Privacidade
 - Crime
 - Saúde
 - Condições de Trabalho
 - Individualidade
 - Emprego e
 - Busca de soluções sociais por meio da TI

A TI e o Emprego



- O impacto da TI sobre o emprego é uma preocupação ética importante e está diretamente relacionada ao uso de computadores para alcançar a automação
- O uso da TI gerou novos empregos e aumentou a produtividade. Entretanto, ela ainda tem provocado uma redução significativa em alguns tipos de oportunidades de trabalho



A TI e a Individualidade

- Uma crítica freqüente à tecnologia da informação diz respeito ao seu efeito negativo sobre a individualidade das pessoas. Os sistemas são criticados como:
 - Sistemas impessoais que desumanizam e despersonalizam as atividades, já que eliminam as relações humanas presentes nos sistemas sem computadores. As pessoas sentem uma perda de identidade
 - Sistemas em que as pessoas sentem uma perda de individualidade já que alguns exigem a arregimentação do indivíduo e exigem adesão estrita a procedimentos detalhados



A TI e a Individualidade

- Os sistemas baseados em computador podem ser ergonomicamente projetados para acomodar fatores humanos que:
 - Minimizem a despersonalização e a arregimentação
 - Projetem softwares que sejam personalizados [people-oriented] e “amigáveis ao usuário”

A TI e Condições de Trabalho



- A TI eliminou algumas tarefas monótonas ou perversas no escritório e na fábrica que anteriormente tinham de ser executadas por pessoas. Dessa forma, pode-se dizer que a TI eleva a qualidade do trabalho
- Entretanto, muitas operações automatizadas são também criticadas por relegarem as pessoas a um papel de apoio de “não fazer coisa alguma”

Monitoração pelo Computador



- Uma das questões éticas mais explosivas referentes à qualidade do trabalho é a monitoração pelo computador, os quais são utilizados para monitorar a produtividade e o comportamento de milhões de funcionários em seu trabalho
- Segundo se supõe, a monitoração por computador é feita para que os empregadores possam coletar dados de produtividade sobre seus funcionários para aumentar a eficiência e qualidade do serviço

Monitoração pelo Computador



- A monitoração por computador tem sido criticada como antiética porque:
 - É utilizada para monitorar indivíduos, não apenas o trabalho, e essa monitoração é realizada continuamente, violando assim a privacidade e liberdade pessoal dos trabalhadores.
 - É considerada uma invasão da privacidade dos funcionários porque, em muitos casos, eles não sabem que estão sendo monitorados ou não sabem como a informação está sendo utilizada

Monitoração pelo Computador



- O direito legal do funcionário de mover processo pode ser prejudicado pelo uso impróprio dos dados coletados para tomar decisões pessoais.
- Ela aumenta a tensão sobre os funcionários que devem trabalhar sob constante vigilância eletrônica.
- Ela tem sido responsabilizada por problemas de saúde entre os trabalhadores monitorados.
- Ela tem sido responsabilizada por roubar os trabalhadores da dignidade de seu trabalho.

Questões de Privacidade



- O poder da TI de armazenar e recuperar informações pode ter um efeito negativo no direito à privacidade de cada indivíduo. Algumas importantes questões de privacidade que estão sendo debatidas nas empresas e no governo incluem as seguintes:

Questões de Privacidade



- Acessar trocas de correspondência e registros de computador privativos de indivíduos e coletar e compartilhar informações sobre indivíduos obtidas a partir de suas visitas a sites e grupos de notícias da Internet (violação da privacidade)
- “Saber” sempre onde uma pessoa está, principalmente quando os serviços de telefonia celular e paging se tornam mais estreitamente associados com as pessoas do que com os lugares (monitoração por computador)

Questões de Privacidade



- Utilizar informações de clientes para comercializar serviços adicionais (cruzamento de informação por computador)
- Coletar números telefônicos e outras informações pessoais para montar perfis de cada cliente (arquivos pessoais não autorizados)
- Utilizar equipamento automatizado seja para gerar chamadas ou para colher informações do usuário (identificação de chamadas)

Privacidade na Internet



- A Internet é famosa por dar a seus usuários uma sensação de anonimato quando, na realidade, eles são altamente visíveis e estão abertos a violações de sua privacidade
- Grande parte da Internet e de sua Rede Mundial de Computadores e grupos de notícias ainda constitui uma fronteira eletrônica escancarada e insegura sem quaisquer regras rígidas sobre quais informações são pessoais e privativas

Privacidade no E-Mail



- As empresas possuem diferentes políticas de privacidade, principalmente quando estas se aplicam ao e-mail
- Algumas empresas, por exemplo, nunca monitoram as mensagens de e-mail de seus funcionários, ao passo que outras afirmam que se reservam o direito de fazê-lo
- Algumas empresas monitoram constantemente e-mails, enquanto outras o fazem apenas se percebem que há uma razão para suspeitar que um funcionário o esteja utilizando para uma atividade ilegal ou não autorizada

Cotejo de Computadores



- O cotejo de computadores é o uso de computadores para exibir e equiparar dados sobre características pessoais fornecidos por uma diversidade de sistemas de informação baseados em computador e bancos de dados com o objetivo de identificar indivíduos para fins empresariais, governamentais e outros
- O uso não autorizado ou equívocos no cotejo de computadores de dados pessoais podem ser uma ameaça à privacidade

Legislação sobre Privacidade



- Nos Estados Unidos, a Lei Federal de Privacidade regulamenta rigidamente a coleta e uso de dados pessoais por agências governamentais
- A lei especifica que os indivíduos têm o direito de inspecionar seus registros pessoais, fazer cópias e corrigir ou eliminar informações errôneas ou confusas

Legislação sobre Privacidade



- A Lei Federal de Privacidade especifica que as agências federais:
 - Devem anualmente divulgar os tipos de arquivos de dados pessoais que elas mantêm.
 - Não podem revelar informações pessoais sobre um indivíduo a nenhum outro indivíduo ou agência exceto sob certas condições estritas.

Legislação sobre Privacidade



- Devem informar os indivíduos sobre as razões para estarem lhes solicitando informações pessoais.
- Devem reter registros de dados pessoais apenas se estes forem “relevantes e necessários para realizar” um propósito legal da agência.
- Devem estabelecer salvaguardas administrativas, técnicas e físicas apropriadas para garantir a segurança e confidencialidade de registros.

Legislação sobre Privacidade



- O Congresso dos Estados Unidos aprovou a Lei de Privacidade nas Comunicações Eletrônicas e a Lei sobre Fraude e Abuso do Computador em 1986
- Essas leis de privacidade federais são uma das tentativas principais de aplicar a privacidade de arquivos e comunicações baseados em computador

Legislação sobre Privacidade



- Essas leis proíbem a interceptação de mensagens de comunicações de dados, roubo ou destruição de dados ou invasão dos sistemas de computadores relacionados ao governo federal

Difamação e Censura por Computador



- O lado oposto do debate da privacidade é o direito das pessoas de saberem sobre assuntos que outras podem desejar manter reservados (liberdade de informação), o direito das pessoas de expressarem suas opiniões sobre esses assuntos (liberdade de discurso) e o direito das pessoas de publicarem essas opiniões (liberdade de imprensa)

Difamação e Censura por Computador



- Alguns dos maiores campos de batalha no debate são os bulletin boards, caixas de e-mail e arquivos on-line da Internet e redes públicas de informação como a Prodigy, CompuServe e America Online. As armas que estão sendo utilizadas nesta batalha incluem o flame mail, leis sobre difamação e censura

Difamação e Censura por Computador



- Spamming – é o envio indiscriminado de e-mail não solicitado para muitos usuários da Internet. O spamming é a tática favorita dos remetentes de massas de propagandas não solicitadas ou junk e-mail.

Difamação e Censura por Computador



- Flaming – é a prática de enviar mensagens de e-mail extremamente críticas, detrativas e muitas vezes vulgares (flame mail), ou mensagens por BBSs para outros usuários na Internet ou serviços on-line. O flaming é principalmente dominante em alguns dos BBSs de grupos de discussão de interesses especiais na Internet. A Internet está muito vulnerável a abusos uma vez que perde atualmente o policiamento formal e apresenta falta de segurança

Crimes com o uso do computador



- O crime com o uso do computador é a ameaça causada pelas ações criminosas ou irresponsáveis de usuários de computadores que estão tirando proveito do uso generalizado das redes de computadores em nossa sociedade. Por isso, ele constitui uma ameaça maior ao uso ético da TI

Crimes com o uso do computador



- O crime informatizado apresenta sérias ameaças à integridade, segurança e qualidade da maioria dos sistemas de informação das empresas e, com isso, faz do desenvolvimento de métodos eficazes de segurança uma prioridade máxima

Legislação sobre Crimes com o uso do computador



- A Lei sobre Fraude e Abuso de Computadores dos Estados Unidos de 1986 define o crime informatizado como uma das atividades envolvendo acesso a computadores de “interesse federal” ou operando no comércio interestadual ou exterior:
 - Com o intuito de fraudar
 - Resultando em uma perda de mais de 1.000 dólares
 - Para obter acesso a certos sistemas de computação médica
 - Traficar senhas de acesso a computadores também é proibido

Legislação sobre Crimes com o uso do computador



- As penalidades para violações da Lei sobre Fraude e Abuso de Computadores dos Estados Unidos incluem:
 - Um a cinco anos de prisão para um primeiro delito
 - Dez anos para um segundo delito
 - Vinte anos para três ou mais delitos
 - As multas podem chegar a 250.000 dólares ou duas vezes o valor dos dados roubados

Legislação sobre Crimes com o uso do computador



- A Associação dos Profissionais de Tecnologia da Informação (Association of Information Technology Professionals, ou AITP) define o crime informatizado como:
 - O uso, acesso, modificação e destruição não autorizados de recursos de hardware, software, dados ou rede.
 - A divulgação não autorizada de informações.
 - A cópia não autorizada de softwares

Legislação sobre Crimes com o uso do computador



- A negação de acesso a um usuário final aos seus próprios recursos de hardware, software, dados ou rede
- O uso ou conspiração para uso de recursos de computação para obter ilegalmente informações ou propriedade tangível

Exemplos de Crime com o uso do computador



- O crime com o uso do computador envolve atividades criminosas utilizando computadores. Isto normalmente inclui:
 - Roubo de dinheiro, serviços, softwares e dados
 - Destruição de dados e softwares, principalmente por vírus de computador
 - Acesso malicioso ou hacking na Internet ou outras redes de computadores
 - Violação da privacidade
 - Violação da lei anti-truste ou internacional

Crime pela Internet



- Os hackers conseguem monitorar e-mail, acesso a servidores da Web ou transferências de arquivo para extraírem senhas ou roubarem arquivos da rede ou inserirem dados que podem fazer com que um sistema dê acesso a intrusos
- Um hacker também pode utilizar serviços remotos que permitem que um computador em uma rede execute programas em outro computador para obter acesso privilegiado dentro de uma rede

Crime pela Internet



- A Telnet, uma ferramenta para uso interativo de computadores remotos, pode ajudar um hacker a descobrir informações para planejar outros ataques
- Os hackers têm utilizado a Telnet para acessar porta de e-mail de um computador, por exemplo, para monitorar mensagens de e-mail em busca de senhas e outras informações sobre contas de usuários e recursos de rede privilegiados

Roubo de Dinheiro



- Muitos crimes com o uso do computador envolvem o roubo de dinheiro
- Eles quase sempre envolvem a alteração fraudulenta de arquivos do computador para encobrir os rastros dos ladrões ou para usufruir do dinheiro de outros com base em registros falsificados

Roubo de Serviços



- O uso não autorizado de um sistema de computador é chamado de roubo de serviços
- Um exemplo comum é o uso não autorizado de redes de computadores da empresa por funcionários
- Isto pode ir da realização de consultas privadas ou finanças pessoais, ou jogo de vídeo games, até o uso não autorizado da Internet pelas redes da empresa

Roubo de Serviços



- Softwares de monitoração de redes, conhecidos como sniffers (farejadores), são freqüentemente utilizados para monitorar o tráfego da rede para avaliar a capacidade da rede, além de revelar evidência de uso impróprio

Roubo de Software



- Programas de computador são propriedade valiosa e por isso estão sujeitos a roubo dos sistemas de computador
- A reprodução não autorizada de software, ou pirataria de software, é uma forma importante de roubo de software porque o software é propriedade intelectual protegida por lei de direitos autorais e contratos de licença com o usuário

Alteração ou Roubo de Dados



- Fazer alterações ilegais ou roubar dados é outra forma de crime informatizado

Acesso Indevido



- Hacking é o uso obsessivo de computadores ou o acesso e uso não autorizados de sistemas de computação em rede
- Hackers ilegais (também conhecidos como crackers) podem roubar ou danificar dados e programas

Vírus de Computador



- Um dos mais destrutivos exemplos de crime informatizado envolve a criação de vírus de computador ou vermes de computador
- Esses vírus normalmente entram em um sistema de computação por meio de cópias de software ilegais ou emprestadas ou por meio de links de rede para outros sistemas de computador

Vírus de Computador



- Um vírus normalmente copia a si mesmo nos programas do sistema operacional do computador e de lá para o disco rígido e em quaisquer discos flexíveis inseridos
- Programas de vacina e programas de prevenção e detecção de vírus são disponíveis, mas podem não funcionar para novos tipos de vírus

Vírus de Computador



- Vírus – é um código de programa que não pode funcionar sem ser inserido em outro programa.
- Verme – é um programa distinto que pode rodar sem assistência.

Questões de Saúde



- O uso da TI no local de trabalho levanta uma série de questões de saúde
- O uso intenso de computadores é tido como causador de problemas de saúde como:
 - Estresse no trabalho
 - Lesões em músculos do braço e pescoço
 - Tensão ocular
 - Exposição a radiação
 - Morte por acidentes provocados por computador

Questões de Saúde



- As soluções para alguns problemas de saúde são baseadas na ciência da ergonomia, às vezes chamada de engenharia de fatores humanos
- A meta da ergonomia é projetar ambientes de trabalho saudáveis que sejam seguros, confortáveis e agradáveis para as pessoas trabalharem, aumentando assim o moral e a produtividade do funcionário

Questões de Saúde



- A ergonomia enfatiza a concepção saudável do local de trabalho, estações de trabalho, computadores e outras máquinas e até de pacotes de software
- Outras questões de saúde podem exigir soluções ergonômicas que enfatizem mais o desenho do cargo do que o desenho do local de trabalho

Soluções Sociais



- A tecnologia da informação pode produzir muitos efeitos benéficos na sociedade
- A TI pode ser utilizada para solucionar problemas humanos e sociais por meio de soluções sociais como:
 - Diagnóstico médico
 - Instrução auxiliada por computador
 - Planejamento de programas governamentais
 - Controle da qualidade ambiental
 - Aplicação das leis

Você e a Responsabilidade Ética



- Como usuário final empresarial, você tem a responsabilidade de fazer algo com relação a alguns abusos da tecnologia da informação no local de trabalho
- Essas responsabilidades incluem desempenhar adequadamente seu papel como um recurso humano vital nos sistemas de informação baseados em computador que você ajuda a desenvolver e utiliza em suas organizações

Você e a Responsabilidade Ética



- O código da AITP fornece diretrizes para conduta ética no desenvolvimento e uso da tecnologia da informação
- Os usuários finais e os profissionais de SI viveriam de acordo com suas responsabilidades éticas se adotassem voluntariamente essas diretrizes

Você e a Responsabilidade Ética



- Você pode ser, por exemplo, um usuário final responsável:
 - Atuando com integridade
 - Melhorando sua competência profissional
 - Estabelecendo padrões elevados de desempenho pessoal
 - Assumindo responsabilidade por seu trabalho
 - Aprimorando a saúde, privacidade e bem-estar geral do público

Bibliografia



- Sistemas de Informação e as Decisões Gerenciais na Era da Internet - James A. O'Brien - Editora: Saraiva