

**Universidade Federal de Santa Catarina  
Departamento de Informática e Estatística**

Crystie Allan Rosa

**Ética Computacional: um estudo das violações à ética pelos  
profissionais e estudantes de informática**

**Florianópolis  
2006**

Crystie Allan Rosa

**Ética Computacional: um estudo das violações à ética pelos  
profissionais e estudantes de informática**

Monografia apresentada à Universidade Federal de Santa Catarina para obtenção do título de Bacharel em Sistemas de Informação, sob a orientação do Professor Dr. Jovelino Falqueto.

**Florianópolis  
2006**

Monografia apresentada como requisito necessário para a obtenção do grau de Bacharel, do Curso de Sistemas de Informação, da Universidade Federal de Santa Catarina – UFSC.

BANCA EXAMINADORA

Prof. Dr. Jovelino Falqueto  
**Orientador**

Profa. Dra. Edla Maria Faust Ramos  
**1ª Examinador**

Prof. Dr. José Eduardo De Lucca  
**2ª Examinador**

## **Agradecimentos**

Primeiramente a minha família, pelo apoio incondicional. Também agradeço ao meu orientador nesse trabalho, Jovelino Falqueto, pela ajuda na condução das atividades e aos membros da banca Edla Ramos, com contribuições essenciais em todas as partes da monografia, e, José De Lucca pelo suporte às questões relacionadas ao software livre e pirataria.

Por último e principalmente, agradeço a Michele Pinheiro, meu grande amor e futura esposa, por toda ajuda e apoio em absolutamente todo o processo de elaboração deste trabalho. Sem ela não seria possível sua conclusão – pelo menos não sem ganhar alguns fios brancos de cabelo.

## **Resumo**

Este trabalho visa o estudo das violações éticas cometidas por profissionais e estudantes na área de informática, através da análise dos problemas éticos mais comuns, a destacar: pirataria, hackerismo, invasão de privacidade e Ética na internet. Constitui-se, ainda, na aplicação de um questionário entre os acadêmicos de Sistemas de Informação e o restante da Universidade Federal de Santa Catarina com o intuito de saber a opinião dos acadêmicos em relação à Ética tanto no estudo quanto na profissão, com uma posterior análise descritiva. O questionário é composto de treze perguntas objetivas que avaliam desde a ocupação do acadêmico, passando pela necessidade de haver uma disciplina específica de Ética no currículo, até que, por fim, instigando o acadêmico a relacionar critérios morais aos tipos de situações práticas que enfrentam ou possam vir a enfrentar no cotidiano.

Além de incentivar um estudo mais aprofundado da Ética no curso de Sistemas de Informação, reforça ainda a necessidade da elaboração de um código de Ética na área da Computação, que, por razão da sua constante evolução, torna a tarefa extremamente complicada.

**Palavras-chave:** Ética, moral, informática, violação ética.

## **Lista de Tabelas**

<b>Tabela 1 – Número de acadêmicos por centro da UFSC em 2006/1 .....</b>	<b>58</b>
<b>Tabela 2 – Número de acadêmicos do Centro Tecnológico em 2006/1 .....</b>	<b>59</b>
<b>Tabela 3 – Valores de amostragem por centro .....</b>	<b>60</b>

## **Lista de Ilustrações**

<b>Ilustração 1 – Ocupação dos acadêmicos .....</b>	<b>60</b>
<b>Ilustração 2 - Nível de satisfação em relação ao curso .....</b>	<b>61</b>
<b>Ilustração 3 – Capacidade de preparação ético-cidadã do curso (%) .....</b>	<b>61</b>
<b>Ilustração 4 – Necessidade de uma disciplina de Ética no curso.....</b>	<b>61</b>
<b>Ilustração 5 – Ciência de um código de Ética na área.....</b>	<b>62</b>
<b>Ilustração 6 – Frequência (%) de leitura sobre Ética .....</b>	<b>62</b>
<b>Ilustração 7 - Nível de conhecimento ético oferecido pelo curso pelos defensores da existência de uma disciplina específica no assunto (%) .....</b>	<b>62</b>
<b>Ilustração 8 - Nível de conhecimento ético oferecido pelo curso pelos não defensores da existência de uma disciplina específica no assunto (%) .....</b>	<b>63</b>
<b>Ilustração 9 - Consciência entre práticas que envolvem ou não discussões morais .....</b>	<b>63</b>
<b>Ilustração 10 – Entendimento sobre questões morais (em porcentagem) .....</b>	<b>64</b>
<b>Ilustração 11 – Avaliação de critérios morais (Num Pessoas x Critério) .....</b>	<b>64</b>
<b>Ilustração 12 – Tipos de contravenções mais anti-éticas (número de pessoas).....</b>	<b>65</b>
<b>Ilustração 13 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (%) .....</b>	<b>66</b>
<b>Ilustração 14 – Pessoas que assinalaram que, em se tratando de questões morais, cada um tem seu ponto de vista, e seus critérios que utilizam para julgá-las.....</b>	<b>66</b>
<b>Ilustração 15 - – Pessoas que assinalaram que, em se tratando de questões morais, deve- se discutir e chegar a um ponto comum, e seus critérios que utilizam para julgá-las .....</b>	<b>67</b>
<b>Ilustração 16 - Ocupação dos acadêmicos de Sistemas de Informação .....</b>	<b>68</b>
<b>Ilustração 17 – Nível de satisfação em relação ao curso de Sistemas (%).....</b>	<b>68</b>
<b>Ilustração 18 – Capacidade de preparação ético-cidadã do curso de Sistemas (%) .....</b>	<b>68</b>
<b>Ilustração 19 – Necessidade de uma disciplina de Ética no curso de Sistemas.....</b>	<b>69</b>
<b>Ilustração 20 – Ciência de um código de Ética na área.....</b>	<b>69</b>
<b>Ilustração 21 – Frequência de leitura sobre Ética (%) .....</b>	<b>69</b>
<b>Ilustração 22 – Nível de conhecimento ético em Sistemas de Informação, pelos defensores da existência de uma disciplina específica no assunto (%) .....</b>	<b>70</b>
<b>Ilustração 23 - Nível de conhecimento ético em Sistemas de Informação, pelos não defensores da existência de uma disciplina específica no assunto (%). .....</b>	<b>70</b>
<b>Ilustração 24 – Consciência entre práticas que envolvem ou não discussões morais (Sistemas de Informação).....</b>	<b>70</b>

<b>Ilustração 25– Entendimento sobre questões morais em Sistemas de Informação (%). .</b>	<b>71</b>
<b>Ilustração 26 – Avaliação de critérios morais em Sistemas de Informação (Num. Pessoas x Critério). .....</b>	<b>71</b>
<b>Ilustração 27 – Tipos de contravenções mais anti-éticas para Sistemas de Informação (Num. Pessoas). .....</b>	<b>72</b>
<b>Ilustração 28 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (%) .....</b>	<b>72</b>
<b>Ilustração 29 - Pessoas que assinalaram que, em se tratando de questões morais, cada um tem seu ponto de vista, e seus critérios que utilizam para julgá-las (Sistemas de Informação).....</b>	<b>73</b>
<b>Ilustração 30 – Pessoas que assinalaram que, em se tratando de questões morais, deve-se discutir e chegar a um ponto comum, e seus critérios que utilizam para julgá-las (Sistemas de Informação).....</b>	<b>73</b>



## Sumário

1	Introdução.....	6
1.1	Sobre este trabalho.....	7
2	Desenvolvimento.....	9
2.1	A palavra da moda.....	9
2.2	Os problemas da moral e ética.....	9
2.3	O que é mesmo Ética?.....	11
2.3.1	A Ética e a Grécia Antiga.....	12
2.3.2	Ética classificada.....	14
2.3.2.1	Ética empírica.....	14
2.3.2.1.1	A Ética anarquista.....	14
2.3.2.1.2	A Ética utilitarista.....	15
2.3.2.1.3	A Ética ceticista.....	17
2.3.2.1.4	A Ética subjetivista.....	17
2.3.2.2	Ética dos bens.....	18
2.3.2.2.1	A Ética socrática.....	18
2.3.2.2.2	A Ética platônica.....	19
2.3.2.2.3	A Ética aristotélica.....	19
2.3.2.2.4	A Ética epicurista.....	19
2.3.2.2.5	A Ética estóica.....	20
2.3.2.3	Ética formal.....	20
2.4	Ética na computação.....	21
2.4.1.1	A problemática atual das violações éticas.....	21
2.4.1.1.1	Pirataria de software.....	21
2.4.1.1.1.1	Protegendo a propriedade intelectual.....	24
2.4.1.1.1.2	Software livre para voar.....	27
2.4.1.1.1.3	“Suavizando” o <i>copyright</i> .....	31
2.4.1.1.1.4	Posso ou não copiar softwares?.....	32
2.4.1.1.2	Hackers.....	35
2.4.1.1.2.1	A Ética Hacker.....	40
2.4.1.1.3	Invasão de privacidade.....	42
2.4.1.1.4	Ética na Internet.....	48
2.4.1.2	Códigos de Ética na computação.....	53
3	Pesquisa.....	58
3.1	Procedimentos.....	58
3.2	Resultados Obtidos.....	60
3.2.1	Questionário aplicado na UFSC (sem Sistemas de Informação).....	60
3.2.2	Questionário aplicado no curso de Sistemas de Informação.....	68
4	Considerações Finais.....	74
5	Bibliografia.....	78
6	Anexos.....	80
	Anexo I – Questionário sobre Ética para acadêmicos de Sistemas de Informação.....	80
	Anexo II - Questionário sobre Ética para acadêmicos da UFSC.....	82
	Anexo III - ACM Code of Ethics and Professional Conduct.....	84
	Anexo IV – IEEE-CS/ACM Code of Ethics.....	92
	Anexo V – Artigo.....	100

## 1 Introdução

Os computadores se tornaram uma ferramenta indispensável para todas as pessoas do chamado mundo moderno, e é justamente por esse motivo que eles foram fazendo parte, mesmo que de forma um tanto imperceptível, de nossas vidas. Há diversas atividades que julgávamos independentes de automação computacional e, agora, nos vemos “enganados” nesse pensamento. Hoje, é quase inconcebível entrar numa loja, por exemplo, e fazer compras sem ter a opção de pagá-las eletronicamente – o chamado dinheiro de plástico. Os benefícios proporcionados por essas facilidades são extraordinários, mas também nos colocam numa situação de dependência exagerada em relação aos computadores. Em princípio, isso não deveria ser um problema já que os avanços tecnológicos alcançados pelo homem através de décadas são justamente para facilitar a vida das pessoas; tornar as coisas mais simples.

A informatização dos elementos que nos rodeiam não é, portanto, algo que se deva condenar. Todavia, ela traz novas variáveis no que diz respeito a optar pelo o que é certo ou errado em nossas decisões. Se antes tínhamos que nos preocupar somente com a segurança de papéis sigilosos, citando um exemplo de alguém que trabalhe em um escritório, agora devemos imaginar como manter os arquivos digitais que geraram os documentos fora do alcance de pessoas não autorizadas. A utilização inadequada desses documentos por terceiros poderia trazer conseqüências indesejáveis.

Este pequeno exemplo é apenas um dentre os vários que envolvem decisões práticas, sendo que essas decisões podem ou não ter relação com questões morais. Em caso afirmativo, é primordial que algum background ético seja utilizado como referência na tomada de decisão.

Porém, falar de Ética em Computação é algo realmente complicado. Primeiro que a Ética em si não é uma ciência tida como de conceitos “sólidos e indiscutíveis”, algo que contrasta com a precisão exigida pela Computação. No entanto, essa precisão torna-se maleável no mesmo sentido em que inovações vão sendo constantemente introduzidas na área. Obviamente isso não aplica aos conceitos elementares da Computação, mas às condições a que são submetidos seus usuários em razão de supostas inovações. Segundo, a área computacional, em relação às profissões mais tradicionais como medicina e advocacia, por exemplo, está na sua infância. Praticamente não houve tempo para criar uma regulamentação num ambiente em que novas descobertas alteram constantemente o

paradigma de atuação do profissional e usuários. Já nas profissões tradicionais, essa variável não se observa mais, uma vez que um período secular foi o suficiente para estabelecer aspectos regulamentais. Mas nem por isso a tarefa de propor limitações éticas nas questões relacionadas à Computação deve ser deixada em segundo plano ou mesmo abandonada.

### ***1.1 Sobre este trabalho***

Mais do que “alertar” o usuário ou profissional para fazer somente o que é tido como correto, é interessante estabelecer uma normatização consistente e que seja genérica o bastante para se encaixar nas constantes modificações que a área de informática impõe aos que a ela pertencem.

Pelo fato da computação ser tão importante no dia a dia das pessoas, é primordial que os profissionais ajam com correteza no desempenho de suas atividades. É por dar uma ênfase maior e mais completa da disciplina nos cursos de informática que também o presente trabalho se justifica.

Mais do que profissionais competentes e com conhecimento, uma instituição de ensino precisa orientar seus acadêmicos de maneira que utilizem para o bem toda a bagagem de conhecimento adquirida a tanto custo. O intento de fazer essa análise não pára apenas na constatação das irregularidades, mas num serviço de educação para que as condutas anti-éticas sejam pelo menos refletidas antes de serem cometidas e se possível, evitadas. Essa conscientização somente pode ser feita por um trabalho pedagógico que dê conta de, explicitar muitas das possíveis situações que o profissional terá que lidar na sua carreira, os aspectos legais envolvidos bem como punições passíveis de aplicação.

A idéia principal deste trabalho consiste justamente na discussão dos fatores que envolvam computação e princípios éticos em situações como cópia de softwares, hackerismo, invasão de privacidade (virtual) e comportamento e conduta na internet. Seguindo a isso vem a aplicação de um questionário baseado na pesquisa realizada por Alexandre Lazaretti Zanatta e Jaime José Rauber, da Universidade de Passo Fundo, RS. Nessa pesquisa, o foco concentrou-se nos egressos do curso de Ciências da Computação da UPF-RS. Foram distribuídos, via correio, os questionários que serviriam de base para o trabalho para a posterior análise descritiva dos resultados. Algumas modificações foram feitas a partir desse

questionário elaborado por Zanatta e Rauber para que se adequassem aos propósitos deste trabalho. Porém, o foco central permaneceu inalterado.

Na parte da pesquisa, o levantamento de dados será realizado com o foco principal no curso de Sistemas de Informação, onde o contato com computadores é obrigatório. Porém, essa coleta será estendida pelos demais centros da Universidade Federal de Santa Catarina para fins de comparação.

O primeiro capítulo (que envolve os itens 2.1, 2.2 e 2.3) trata de dar um panorama generalista da Ética como teoria, seus principais pensadores e classificação. O segundo capítulo trata exclusivamente das questões éticas referentes ao mundo computacional. Optou-se por dividir este capítulo em duas partes: a primeira tratando das principais violações éticas conhecidas (pirataria, hackers, invasão de privacidade, Ética na internet) e segundo sobre códigos de Ética na computação.

## 2 Desenvolvimento

### 2.1 *A palavra da moda*

Ética. Essa palavra provavelmente tornou-se uma das mais escritas e faladas no Brasil de hoje dado o cenário de corrupção generalizada. Como toda palavra usada exaustivamente, ela vai adquirindo “outras interpretações” até, divergindo um tanto do significado original. Para qualquer coisa errada que um indivíduo cometa, diz-se que “faltou-lhe ética”. Outros colocariam “moral” no lugar de ética. Esse uso meio que indiscriminado confunde a cabeça das pessoas, que acabam por propagar o “erro”. Porém, mesmo os teóricos causam confusão na medida em que escrevem seus textos muitas vezes sem o cuidado de observar o correto significado dessas duas palavras (ética e moral). O conceito mais comumente aceito de ética é o de que ela é o estudo da moral. Mas há quem defenda que as duas possuam o mesmo significado.

Este trabalho não irá referenciar ética e moral como sinônimos. No entanto, para tentar elucidar melhor esse impasse, seria interessante observar as questões envolvidas para cada uma delas, a começar pela classificação dos problemas a que se referem.

### 2.2 *Os problemas da moral e ética*

Não, não há nada de errado com nenhuma das palavras. O que se pretende aqui é diferenciar o que pertence à moral ou à ética. Para começar, poder-se-ia tomar como exemplo as situações do cotidiano de qualquer indivíduo. Quando alguém faz uma promessa para outra pessoa e mais tarde a primeira descobre que se tiver de cumpri-la vai acabar prejudicando a si mesma, o que fazer? Será que é certo deixar de lado o que foi combinado previamente ou deve-se ir até o fim, pois a palavra empenhada é o que vale mais? Se numa guerra é ordenado a um soldado que mate, esse soldado estaria agindo corretamente em detrimento de alguém que faz o mesmo num cenário urbano para conseguir dinheiro para alimentar a si mesmo ou à sua família? Posso mentir se no fim a razão para isso se justifique?

Todos esses problemas citados anteriormente são problemas práticos que se apresentam em situações reais, onde as decisões e ações dos indivíduos são julgadas por eles mesmos.

Segundo Adolfo Sanchez Vazques, são problemas cujas soluções influenciam tanto a pessoa que as pratica ou idealiza quanto a terceiros, que em tese sofreriam as conseqüências também.

Para que pessoas julguem as ações como certas ou erradas é preciso haver um consenso geral na sociedade sobre isso. Dessa forma são criadas normas que relacionam a conduta de seus integrantes e tornam a tomada de certas decisões ou ações compreensível perante todos.

Sobre essas normas poderíamos dizer que são regimentos morais. O indivíduo compara a ação praticada com uma situação previamente pensada e a partir daí delibera sobre sua validade. Esse comportamento de “classificação e julgamento” sempre existiu nos grupos sociais humanos através dos tempos e, com isso, podemos determinar que os elementos morais sofram alterações conforme os padrões sociais vão mudando também.

Assim, os chamados problemas práticos do nosso cotidiano são regidos pelo comportamento considerado moral. Quando o indivíduo começa a refletir sobre a moralidade, sobre o porquê de aquela ação ser considerada moralmente aceita e estabelecer parâmetros gerais baseados ainda em outras ações e decisões, começa-se a cruzar a fronteira entre a Moral e a Ética.

Não é a toa que a Ética tem tanto a ver com a Filosofia. Na tentativa de racionalizar o pensamento, o homem procurou respostas mais precisas para explicar o comportamento em sociedade. A Ética não responde ao indivíduo o que deve ser feito especificamente para cada situação no mundo real. Isso pode ser buscado pelas normas morais.

Aristóteles, na Antiguidade grega, propõe o problema teórico de definir o que é o bom. Sua tarefa é investigar o conteúdo do bom, e não determinar o que cada indivíduo deve fazer em cada caso concreto para que o seu ato possa ser considerado bom. (VAZQUES, 1970)

Apesar desse distanciamento das questões práticas por parte da Ética, é inegável que suas conclusões possam afetar ou mesmo dar uma pista do que deve ser feito numa determinada situação hipotética. Ou seja, quando o indivíduo consegue identificar o princípio ético, torna-se mais fácil decidir como agir. Logo, Moral e Ética estão intimamente relacionadas.

No entanto, definir o que é bom não é exatamente uma tarefa fácil. O conceito do que é bom pode mudar de pessoa para pessoa, tornando ingrata a análise. Vazques ainda adiciona a essa problemática o fator *responsabilidade*.

É possível falar em comportamento moral somente quando o sujeito que assim se comporta é responsável pelos seus atos, mas isto, por sua vez, envolve o pressuposto de que pode fazer o que queira fazer, ou seja, de que pode escolher entre duas ou mais alternativas, e agir de acordo com a decisão tomada. O problema da liberdade da vontade, por isso, é inseparável do da responsabilidade. (VAZQUES, 1970)

### 2.3 *O que é mesmo Ética?*

Sabendo que os problemas éticos diferenciam-se dos morais basicamente pela sua generalidade, vejamos a definição dada por Vazques:

*“A Ética é a teoria ou ciência do comportamento moral dos homens em sociedade. Ou seja, é ciência de uma forma específica de comportamento humano”*

Sendo uma ciência, a Ética deve possuir, por conseqüência, um caráter científico não abrindo mão da rigidez e fundamentação das suas proposições. A moral, como vimos, não possui essa característica.

Apesar dessa clara separação, nem sempre é possível manter o devido distanciamento entre os conceitos da Ética e moral, o que acaba gerando confusão. Mesmo sendo essencialmente teórica a Ética tem certo caráter prático na medida em que pode direcionar as ações que são baseadas nas normas morais, como já argumentado. A contínua subutilização da Ética nesse sentido reduz essa ciência a uma disciplina normativa apenas, quando todo o conceito é muito mais amplo que isso. Dessa maneira abre-se espaço para subjetividades e por vezes conflitos, já que a Ética, encapsulada numa espécie de teoria moralista, estaria sujeita às normas que sofreram transformações pelos tempos.

A Ética não pode estar “à deriva” das mutações dos costumes e comportamentos da sociedade. A função dela é justamente a de explicar a razão pela qual essas mudanças se deram, esclarecendo aos indivíduos os diferentes paradigmas comportamentais em diferentes épocas e o porquê deles estarem sendo utilizados. Segundo Vazques:

A Ética parte do fato da existência da história da moral, isto é, toma como ponto de partida a diversidade de morais no tempo, com seus respectivos valores, princípios e normas. Como teoria, não se identifica com os princípios e normas de nenhuma moral em particular e tampouco pode adotar uma atitude indiferente ou eclética diante delas. (VAZQUES, 1970)

Como vimos, a Ética tem como objeto de estudo a moral. Essa relação tão intrínseca por certo não é demonstrada pela origem etimológica das duas palavras. Ética vem do grego *ethos*, que significa *modo de ser*. Já a palavra moral vem do latim *mores*, que significa *costumes*.

### 2.3.1 A Ética e a Grécia Antiga

Falar de Ética sem mencionar a Grécia Antiga é, no mínimo, uma afronta. O pensamento grego contribuiu e muito com definições e teorias até hoje válidas no campo da Ética e da moral. Citam-se, pelo menos, três nomes de peso nessa área: Sócrates, Platão e Aristóteles.

Sócrates (470-399 a.C.) utilizava o método da *maiêutica* para realizar seus estudos. Este método consistia em interrogar um interlocutor até que este chegasse por si mesmo à verdade, sendo o filósofo uma espécie de “parteiro das idéias”. A maiêutica é, afinal de contas, uma generalização do método de *elenchos* (que significa interrogação, refutação). Nela os interlocutores de Sócrates partiam de conceitos que consideravam como “verdades certas”, mas que após alguns exemplos acabavam virando contradições (ironia socrática). Sócrates aplicou essa técnica para analisar os principais princípios morais de sua época, que eram a piedade, sabedoria, coragem, temperança e justiça. As certezas em relação a esses tópicos viravam incoerências num aspecto conclusivo, a ponto do próprio Sócrates declarar-se um ignorante no assunto. Os questionamentos de Sócrates eram considerados “avançados” demais pelas autoridades, de forma que foi obrigado a beber veneno (cicuta), sob a acusação de estar seduzindo a juventude, não honrando os deuses da cidade e desprezando as leis da polis (cidade-estado).



Platão (427-347 a.C.) era discípulo de Sócrates e deixou sua obra escrita em forma de *Diálogos*. Ele parte da idéia que todos os homens buscam a felicidade, assim como as doutrinas gregas da época também o faziam.

“Mas não se deve pensar, daí, que Platão pregava um egoísmo rasteiro. Pelo contrário, ao pesquisar as noções de prazer, sabedoria prática e virtude, colocava-se sempre a grande questão: onde está o *Sumo Bem*?”

*Sumo Bem* consiste na purificação, onde o homem desprende-se do corpo e de tudo que é material para meditar aquilo que é imutável, eterno. A inversão da hierarquia de bens proposta por Platão naturalmente não era levada a sério na sua época, a ponto de ele ser considerado como louco.

Aristóteles (384-322 a.C) levava a observação empírica mais a sério nos seus trabalhos, fugindo um pouco da linha teórica de Platão. Destacou-se em várias áreas, mas na Ética, especificamente, deixou obras consideradas como referência. São elas: Ética a Eudemo, onde o objetivo da vida humana é o culto e contemplação do divino (VALLS, 1987), a Ética a Nicômaco onde as coisas relativas (e necessárias) são relativas igualmente, como o prazer, a felicidade, a virtude.

### 2.3.2 Ética classificada

A seguinte classificação considera as quatro formas fundamentais de manifestação do pensamento ético-ocidental adotado por Eduardo García Máynez<sup>2</sup> e citado por José Renato Nalini<sup>3</sup>, que seriam a ética empírica, de bens, formal e valorativa.

O conteúdo dos agrupamentos a seguir dispostos não deve ser encarado como mutuamente exclusivo. Não há, muitas das vezes, como distinguir limites entre as classificações. Até mesmo as próprias classificações não são algo fixo e amplamente aceito como a única alternativa para apontar as diferentes correntes da Ética, juntamente com seus idealizadores. A idéia é apenas a exposição dos conceitos de uma forma geral.

#### 2.3.2.1 Ética empírica

É a ética baseada na observação empírica dos fatos? Segundo Kant, os princípios racionais e a experiência são os elementos base para essa linha de pensamento. De acordo com Nalini (NALINI, 2001), os preceitos disciplinadores do comportamento estão implícitos no próprio comportamento. Mas como funciona isso? A conduta do homem não pode ser analisada simplesmente pela sua ação num contexto isolado, mas pelo que ele tem feito naturalmente através de sua existência. É como se fosse um tipo de “arquivo” onde nele estariam as premissas julgadoras para as ações que venham ocorrer. Enfim, determinada ação se justifica para certo indivíduo se aquilo é o que ele tem feito no passado e “ninguém reclamou”. Isso torna essa divisão da Ética extremamente relativista, pois torna os valores morais subjetivos, dependendo de cada indivíduo.

Todo esse relativismo pode levar ao *ceticismo* ou mesmo ao *niilismo*, no sentido de que se uma coisa é boa para um, pode não ser para outro. Os valores morais passam a não ter significado universal, mas particular para cada indivíduo, fortalecendo a visão do *útil*. A seguir, as correntes da Ética que se identificam ou derivam desse pensamento:

##### 2.3.2.1.1 A Ética anarquista

A idéia de anarquia nos leva a pensar em algo sem regras, sem comando certo. Nesse caso não foge muito a isso. Nenhuma norma ou valor são considerados por serem taxados como frutos da ignorância dos homens, nascidos para satisfazer condições pessoais usando-se de métodos baseados na arbitrariedade.

Se não há regras, cada um faz o que quer, certo? É mais ou menos assim. Segundo Nalini, prepondera a vontade humana que varia de indivíduo para indivíduo. Farão prevalecer sua decisão apenas os mais fortes. Aqui se percebe que ao menos há alguma hierarquia, já que não são todos que têm o direito de fazer valer suas vontades, ao mesmo tempo em que há certa contradição considerando ainda a seletividade daqueles que podem impor seus intentos (o que por si só é um tipo de regra). Esse não é um ponto de vista necessariamente aceito pelos anarquistas que consideram como culpado disso o sistema capitalista atual exclusivamente focado ao lucro, egoísta, alienado e exploratório, abominando toda a organização política imposta por ele. Esse tipo de organização seria, seguindo essa linha de pensamento, contra as exigências da natureza, atentando contra o princípio da liberdade dos homens. Entre os anarquistas há ainda aqueles que são individualistas e comunistas. Ambos lutam contra o Estado, porém usando métodos diferentes: o individualista acredita no uso da razão, tolerando as propriedades privadas e o comunista defende o uso da violência se para isso a liberdade estiver em jogo, não reconhecendo as propriedades privadas como algo legítimo.

O anarquismo, em geral, contempla a busca do prazer, evitando ao máximo a dor (hedonismo). Embora essa busca, segundo tal filosofia, não deva propiciar a criação de normas que restrinjam a liberdade das pessoas, um mínimo de organização deve existir para que o convívio em sociedade não se transforme num inferno sem lei. Até mesmo sua facção mais extremista – comunista - ainda que não reconheça isso por ir contra sua ideologia libertária, deve saber que no íntimo isso é verdadeiro.

#### **2.3.2.1.2 A *Ética utilitarista***

O utilitarismo teve sua origem pelas obras de Jeremy Bentham e John Stuart Mill, entre os séculos 18 e 19. Nele, considera-se bom tudo o que é útil, desde que essa utilidade tenha a ver com a obtenção da felicidade. Há dois detalhes a considerar nessa última frase, como veremos a seguir.

O primeiro é que aparentemente não há limites para se determinar o que é útil, ou seja, se o intento é atingir a felicidade, então posso usar de quaisquer métodos para obtê-la. Isso torna válido roubar, matar, ou mesmo fazer outras coisas moralmente inaceitáveis, o que nos leva à conhecida fala *os fins justificam os meios*. Segundo Máynez, esses meios não requerem justificação, sendo apenas meros instrumentos de ação, um intermediário para atingir um objetivo. Quando esses meios deixam de ter utilidade nesse sentido, passam a não ser mais autênticos e, portanto, seu uso seria ilegítimo. Aparentemente uma doutrina egocêntrica, teve essa impressão desfeita quando Francis Hutcheson, filósofo escocês de origem irlandesa, propôs a teoria do *moral sense* (algo como o sentido da moral) a qual dizia que a melhor ação é aquela que busca a maior felicidade para o maior número de pessoas. Hutcheson ainda tentou algo estranho como uma espécie de aritmética moral, em busca da melhor consequência para uma ação – algo realmente mirabolante que não poderia resultar em coisa consistente.

O utilitarismo tem, pode-se dizer, algumas subclassificações que variam conforme o tipo de visão empregada. Por exemplo, há o utilitarismo por ações e por regras. O primeiro analisa o valor das consequências de um determinado ato antes de decidir se este é válido ou não. É que o tem sido basicamente explanado até agora: essa análise se basearia na decisão do que poderia trazer a máxima felicidade para o maior número de indivíduos possível. Nesse contexto existe um exemplo clássico até, que descreve uma situação hipotética em uma sala de emergência de um hospital. Nela estão alguns pacientes, todos com sérios problemas em órgãos diferentes, necessitando de um transplante para poder sobreviver. Chega então à sala um novo paciente, recém operado e fora de perigo, apenas em período de recuperação. Pela teoria utilitarista seria viável o médico retirar os órgãos desse paciente sadio para salvar todos os outros. Estaria, assim, promovendo a felicidade desses pacientes em detrimento de apenas uma morte. Imagine se alguém em sã consciência aceitaria ser atendido num hospital que trabalhasse seguindo esses princípios.

O utilitarismo por regras, o segundo a ser mencionado, mudaria apenas o foco da análise, ou seja, ao invés de basear sua decisão nas consequências das ações, procuraria uma regra de conduta que melhor se adaptasse ao caso. Analisando as consequências dessa regra aí sim tomaria a decisão apropriada. Realmente é um pouco confuso, isso. A tendência de generalizar as coisas parece inevitável nesse tipo de utilitarismo, já que, se considerarmos o exemplo da sala de emergência, onde encontraríamos o capítulo no manual de conduta que rege sobre situações que ocorrem dentro de uma sala de emergência?

O segundo ponto a ser considerado, retornando ao gancho do início desse texto, é a subjetividade do conceito de felicidade. Os fins que justificam os meios podem não ser tão justificáveis assim para todas ou pela maioria das pessoas em determinados casos. O eudemonismo, assim chamada a busca pela felicidade, não tem seguidores em todos os ramos da Ética. Kant era um deles. Ele achava que a felicidade não passava de uma alegria empírica (fosse ela superior (dignidade, honra, etc) ou inferior (comida, sexo, etc)), que não ia além da concretização das vontades de cada um. Sendo assim, seria impossível determinar uma linha de pensamento padrão que apontasse o caminho para a felicidade e, que ainda, estaria desconectada do que seria considerado como fundamento para os princípios morais.

### ***2.3.2.1.3 A Ética ceticista***

Pode-se dizer que o ceticismo é um reflexo do pensamento subjetivista da Ética empírica. Tem como característica a pouca ou nenhuma crença nos dogmas relacionados com os princípios de conduta.

Ao mesmo tempo em que essa corrente se mantém “sóbria” frente aos delírios de teorias novas e espalhafatosas, também é extremamente conservadora no sentido de precisar de “um tempo” para analisar a situação. Esse período, que muitas vezes poderia ser eterno (o que curiosamente é uma característica dogmática e não ceticismo), é um dos motivos de crítica daqueles que acham que esse estilo metódico de duvidar não se traduz necessariamente em conhecimento.

Na verdade, para os cétricos, só o fato de duvidar já induz ao conhecimento mínimo. A famosa frase de Sócrates ilustra bem isso: “Só sei que nada sei”. Em termos práticos, o ceticismo dificilmente seria viável de ser seguido tão e puramente só, já que aquele que duvida de algo pode pôr essa dúvida em dúvida, que por sua vez a coloca em dúvida novamente e assim por diante. Esse ciclo possivelmente não teria fim e a consequência mais comum desse tipo de pensamento é a paralisia frente a uma situação que exija tomada de decisão.

A Ética ceticista funciona muito bem acompanhada de outra, como se fosse um “tempero”, uma ajuda para balancear os momentos de cegueira ideológica.

### ***2.3.2.1.4 A Ética subjetivista***

Se há um tipo notório de identificação com a Ética empírica, essa é a subjetivista. E isso pela razão de pregar que cada indivíduo deva optar pela conduta ética que melhor lhe seja cômodo ou oportuno.

De acordo com Nalini (NALINI, 2001), o precursor desse tipo de pensamento foi Protágoras de Abdera; sua frase famosa “o homem é a medida de todas as coisas”, expressa que o homem é a dimensão do que realmente é válido. Melhor dizendo, tomando a premissa como verdadeira, nada deve ser medido para os homens já que ele próprio é quem deve fazê-lo. Assim, um conjunto de normas ou regras deve ser definido por um conjunto de pessoas, sendo que não necessariamente essas normatizações precisem ser iguais para localidades diferentes. O foco dessa linha ética reside no individualismo do conhecimento das coisas, o que pode levar a um profundo relativismo.

### **2.3.2.2 Ética dos bens**

Saindo do campo do relativismo, a Ética dos bens nos diz que sempre deve existir o valor fundamental que é chamado de bem supremo. Segundo Nalini, “a criatura humana é capaz de se propor fins, eleger meios e colocar em prática os últimos, para alcançar os primeiros”. Parecido com o Utilitarismo? A grande diferença é que para a Ética dos bens os meios são importantes e junto com a finalidade, formam o bem supremo para obtenção de outro fim, ao contrário do Utilitarismo, que considera a forma como se obteve acesso ao fim um instrumento descartável.

#### **2.3.2.2.1 A Ética socrática**

Sócrates, o filósofo ateniense, tem duas frases que marcaram a sua visão sobre a Ética: “só sei que nada sei” e “conhece-te a ti mesmo”. A sabedoria para Sócrates era a pedra chave para o alcance da felicidade. Se esta não era fosse obtida, era porque resultou da ausência de conhecimentos. Como bem explica Nalini:

A bondade é resultado do saber. Para alguém ser feliz é necessário ser bom e para ser bom é preciso ser sábio. Aquele que encontrou a verdade oculta em sua alma sente-se obrigado a ajustar com ela sua conduta. Assim, o conhecimento do bem determina a prática da virtude. Não

existem pessoas más, senão extraviadas. A maldade é produto da ignorância. (NALINI, 2001).

#### **2.3.2.2.2 A Ética platônica**

Para Platão, outro filósofo ateniense, a teoria da conduta só poderia ser válida se fosse baseada numa plataforma inflexível. As nuances trazidas pela subjetividade não teriam a força para fazê-lo. Assim, os elementos resultantes das inúmeras possibilidades geradas pela diversidade de pensamentos seriam todos classificados através de uma abstração, de um revestimento, ou seja, a *idéia*. Dessa forma, a percepção, através dos sentidos, de qualquer consistência do chamado mundo real tem sua imagem no espectro das idéias.

O conhecimento aqui também é extremamente importante, mas a alma de cada indivíduo é tomada como matéria prima para obtenção do todo dessa sabedoria.

Cada uma das partes da alma tem função especial e virtude própria. À inteligência corresponde a sabedoria; à vontade, o valor; aos apetites, a temperança. São virtudes que atuam em coordenação e cuja harmonia constitui a justiça. A justiça é, para Platão, a harmonização das atividades da alma e suas respectivas virtudes. (NALINI 2001).

#### **2.3.2.2.3 A Ética aristotélica**

A busca nesse tipo de pensamento é restrita ao bem absoluto referente à felicidade. Para Aristóteles, o sucesso nessa empreitada é diretamente relacionado à prática constante das virtudes. Ele ressalta que práticas eventuais nesse sentido não são relevantes. É preciso adquirir uma persistência, um hábito em agir dessa forma. O excesso ou falta da prática constituem uma fuga ao que ele chama de meio termo. O meio termo seria a “quantidade” ideal de exercício da virtude, que, segundo Nalini, não está exatamente equidistante dos extremos viciosos.

#### **2.3.2.2.4 A Ética epicurista**

Baseada nos trabalhos do filósofo grego Epicuro de Samos, a Ética epicurista dá relevância ao prazer como significado do alcance da felicidade. Prazer, deixando claro, não exclusivamente carnal, luxurioso, mas espiritual.

Há uma forte inclinação ao individualismo nessa corrente de pensamento ético, já que a busca do prazer é tida como algo pessoal, até egocêntrico. Pouco interessa se o semelhante atingiu a busca da felicidade se a sua própria foi alcançada.

Nalini aponta que de reflexões epicurista o conceito da justiça tenha emergido:

“E há nela um certo utilitarismo. Os homens viviam como feras, à margem da lei e decidiram um dia unir-se para pôr um paradeiro naquele estado de beligerância. Surgiu assim a justiça, conceito negativo de não prejudicar os semelhantes, em troca do dever recíproco e idêntico deles.” (NALINI, 2001).

#### **2.3.2.2.5 A Ética estóica**

O prazer, aqui, é “amaldiçoado” por estabelecer vínculos afetivos, o que escravizaria o homem. Este deve desligar-se das coisas do chamado mundo exterior.

O enfoque é total na busca da virtude e, “viver virtuosamente é viver de acordo com a natureza”. Natureza esta representada pela razão e não pelo fator biológico.

#### **2.3.2.3 Ética formal**

Segundo Nalini (NALINI, 2001) a Ética formal, ao contrário da Ética empírica, que se atém basicamente ao que ocorre de fato, e da Ética dos bens, que se preocupa com “a relação estabelecida entre o proceder individual e o supremo fim da existência humana”, foca sua atenção na pureza da vontade e retidão de propósitos. Uma das principais manifestações dessa corrente são os famosos imperativos categóricos, a citar: “Age só segundo uma máxima tal que possas querer ao mesmo tempo que se torne lei universal”.



## 2.4 *Ética na computação*

### 2.4.1.1 **A problemática atual das violações éticas**

A constante atualização dos meios de comunicação nos trouxe dilemas que até então eram inimagináveis. No assombro do que se efetivamente *pode* fazer, esqueceu-se do que se *deve* fazer. A Ética fornece elementos que podem servir de base para apontar (ou pelo menos tentar fazê-lo), nesse trabalho, os princípios básicos de conduta para as situações que ocorrem tanto no nosso cotidiano como fora dele. A seguir serão abordados alguns tópicos pertinentes à Ética no campo da computação. Esta lista de forma alguma pretende apresentar uma abordagem definitiva sobre o assunto, que de tão vasto e inexplorado impossibilita conclusões absolutas.

#### 2.4.1.1.1 *Pirataria de software*

Pode-se dizer que o software é uma das principais “peças” de um computador. Sem ele não há sentido em se ter todo um maquinário à disposição, pois, afinal, o que iria se executar se não existissem programas? Em outros tempos, nos primórdios dos microcomputadores, o hardware (a parte física do computador, assim dizendo) tinha alto custo. Porém, atualmente isso não mais se observa, o que destaca cada vez mais a importância do software no conjunto total.

Sendo assim, as grandes fabricantes de software valorizam bem seus produtos, o que acaba não sendo muito interessante para aqueles que não se dispõem a pagar altas quantias por programas. Pronto, dá-se aí o primeiro impasse: há a motivação de se obter algo de graça (ou a baixo custo) que em tese por vias legais custe muito mais.

Nesse ambiente de pirataria há diversos atores. Há aqueles que ganham dinheiro descobrindo códigos de registro de programas, fazendo engenharia reversa para “lançar” executáveis que desabilitem as funções restritivas dos softwares em versão de experimentação (são softwares que após certo tempo deixam de funcionar, obrigando ao usuário comprar uma licença), e também há aqueles que simplesmente são consumidores desses “lançamentos”, assim como há aqueles que ficam numa posição intermediária, ou seja, apenas repassam os produtos para os consumidores (e cobrando para isso, é claro).

Entre aqueles que são os mentores intelectuais há muitos que apenas fazem tal coisa pelo prazer de desafiar as grandes corporações. Porém, essas pessoas, muitas das vezes, não estão preocupadas em afrontar diretamente uma empresa X, apenas querem sempre por à prova suas habilidades. Toma-se um caso recente na mídia<sup>1</sup>: Jon Lech Johansen, ou mais popularmente conhecido, *DVD Jon*<sup>2</sup>.

Ele criou o programa DeCSS<sup>3</sup>, que é uma espécie de driver de DVD (Digital Vídeo Disk). Esse programa decripta e reformata o conteúdo do DVD, fazendo com que seja possível executá-lo em drives de diferentes regiões<sup>4</sup>.

Johansen foi processado pela MPAA<sup>5</sup> (Motion Pictures Association of America) por cometer crime econômico e por outros muitos que consideraram a atitude dele ilegal.

No entanto, há controvérsias sobre o fato de Johansen infringir a lei de direitos autorais, pois o que o programa dele faz é na verdade decriptar, ou seja, traduzir. Em princípio tal elemento por si só não é suficiente para duplicar um disco de DVD. Porém, é inegável que o programa serve de ferramenta para aqueles que têm o intuito de fazê-lo. Ao que parece a intenção de Johansen talvez tenha sido apenas propiciar aos usuários de sistemas operacionais de código aberto (como o *Linux*) a facilidade de poder ler as mídias de DVD. Isso aliado ao fato de que o DeCSS apenas traduz, talvez seja a razão que o esteja salvando nos tribunais, atualmente.

É claro que esse é um caso à parte. Há muitas pessoas que têm realmente o intuito de lesar a propriedade intelectual alheia. A pirataria é um dos maiores problemas do mundo moderno e é uma verdadeira indústria aliada ao mercado negro. A produção está localizada centralmente na Ásia com desdobramentos na América Latina e no resto do mundo. A situação está claramente fora do controle e por mais que se adotem medidas é uma batalha quase que perdida, semelhante ao combate do tráfico de drogas e armas.

A problemática atual com os direitos autorais não é novidade na nossa civilização. Segundo Forrester e Morrison, isso vem desde a Idade Média, e mesmo nessa época as autoridades enfrentavam adversidades no sentido de preservar a propriedade intelectual. Vê-se que, nesse sentido, o homem pouco valoriza o aspecto ético do esforço alheio em produzir. Se é que há uma classificação na área Ética para isso, um *Utilitarismo* meio que deturpado é

---

<sup>1</sup> [http://www.theregister.co.uk/2003/01/07/dvd\\_jon\\_is\\_free\\_official/](http://www.theregister.co.uk/2003/01/07/dvd_jon_is_free_official/)

<sup>2</sup> <http://nanocrew.net/>

<sup>3</sup> <http://www.lemuria.org/decss/>

<sup>4</sup> Regiões – são zonas pré-definidas que limitam a execução dos DVDs. É um tipo de bloqueio econômico que força, em tese, o consumidor a adquirir somente produtos destinados para sua zona. O Brasil pertence à zona 4 e o EUA, 1.

<sup>5</sup> <http://www.mpa.org/>

sempre aplicado, ou seja, se for para causar algum bem para outra pessoa ou a si mesmo, justifica-se o ato de piratear.

Ainda segundo Forrester e Morrison, de acordo com a United Nations' Patent Office<sup>6</sup> (algo como a Firma de Patentes das Nações Unidas) e WIPO<sup>7</sup> (World Intellectual Property Organization), a propriedade intelectual é definida como os direitos, entre outras coisas, aos resultados da atividade intelectual nos campos industrial, científico, literário ou artístico. A lei de direitos autorais tem tradicionalmente protegido as produções literárias, da lei de patentes às invenções mecânicas.

No entanto, como ficam os softwares? Eles são quase como sendo a parte “abstrata” das produções. É possível duplicar um arquivo instantaneamente ao toque de algumas teclas do teclado (ou ainda mais fácil, a cliques de mouse) sem que se tenha a exata noção do que se está realmente manipulando. É claro que um software complexo não é manipulável tão facilmente como um arquivo de música ou texto, por exemplo, mas por certo que há uma dose de replicação proporcionalmente comparável com os arquivos de mídia, distantes “anos-luz” de qualquer outro tipo de produção intelectual convencional (como livros impressos, por exemplo).

Some isso ao fato de que os meios de transmissão de informações sofreram profundas transformações, o que tornou a comunicação entre pessoas de quaisquer partes do mundo uma coisa simples e instantânea e temos uma situação incontrolável. As redes Peer to Peer (P2P) foram o empurrão que faltava para a cópia indiscriminada de qualquer material, seja ele protegido por direitos autorais ou não. O esquema de disponibilização descentralizada que esse sistema permite foi a grande sacada para o problema do congestionamento dos servidores no fornecimento de arquivos grandes. Ao invés de todos os computadores clientes estarem conectados a um servidor, todos são servidores e clientes ao mesmo tempo. Assim, basta que um dos vários computadores esteja on line e “disposto” a fornecer dados para que seja possível a transferência. Cita-se ainda o protocolo BitTorrent<sup>8</sup>, desenvolvido por Bram Cohen. Em princípio o BitTorrent era usado pelos desenvolvedores do sistema operacional Linux para distribuir suas versões mais facilmente, mas logo descobriu-se o potencial dessa ferramenta e hoje ela é amplamente usada na troca de quaisquer tipos de arquivos.

O detalhe dessa troca de arquivos pelas redes P2P é que não há limites para a propagação de material. Na internet há uma só lei e ela prega exatamente que não há lei. Tudo

---

<sup>6</sup> <http://www.patent.gov.uk/>

<sup>7</sup> <http://www.wipo.int>

<sup>8</sup> <http://www.bittorrent.com/>

é possível e válido, basta alguém estar disposto a disponibilizar. É possível entrar contato com filmes que sequer ainda tenham estreado no cinema. São casos em que as grandes produtoras distribuem uma cópia secreta para certas pessoas de influência num período anterior à veiculação comercial do produto para assim obter um *feedback* antecipado do que esperar do público. Nesse caso, alguém aproveitou-se da condição privilegiada da pessoa que recebeu o material em primeira mão e tomou “emprestado” por alguns minutos. Esse tempo é mais do que suficiente para se fazer uma cópia digital do conteúdo de um DVD, por exemplo. Depois basta escolher como colocar na rede.

#### **2.4.1.1.1 Protegendo a propriedade intelectual**

Um sujeito resolve desenvolver um software para realizar determinada tarefa. Quando finalmente a conclui, imagina qual o melhor jeito de proteger o seu esforço para chegar ao produto final e ainda conseguir lucrar com isso. Para muitas pessoas, o que vem imediatamente à cabeça (quando não, unicamente) é a palavra *copyright*.

Por esse sistema, os direitos de reprodução, distribuição, exposição pública e derivação do trabalho são únicos e exclusivos daquele que o criou, devendo este ser “compensado” financeiramente toda vez que o seu produto for requisitado de alguma forma por terceiros, se assim este preferir. Com esses predicados, segundo Masiero (MASIERO, 2000), o *copyright* “estimula a invenção de novos dispositivos, o desenvolvimento de novos processos e a criação de novas obras artísticas que possam melhorar o cotidiano da sociedade”. Do contrário, ainda segundo Masiero, “se o produto do trabalho de uns pudesse ser facilmente copiado e reproduzido por outros, o estímulo pra investir seria bastante diminuído e, a longo prazo, toda a sociedade perderia.

O sentido literal de *copyright* é *direito de cópia*, e como já mencionado, seu propósito é restringi-la (a cópia, em princípio) somente aos mentores intelectuais. Antigamente havia a necessidade de registrar o trabalho para obter o reconhecimento pelo que foi desenvolvido, mas hoje isso não é mais necessário. Basta que ele seja criado para que automaticamente esteja protegido o direito do autor sobre a obra. Dessa forma, no caso de um livro, basta haver uma cópia deste, no caso de uma idéia, basta que haja algo que demonstre a sua existência (nem que seja um manuscrito num guardanapo). Aliás, no caso de haver justamente a existência da idéia, sem concretização de nada, é algo que pode se tornar um tanto aberrativo. De acordo com Arthur Kuflik, em seu artigo “*Moral Foundations Of Intellectual Property*

*Rights*”<sup>9</sup>, só o fato de ter uma concepção útil de alguma coisa não é suficiente para suportar um pedido de patente. Ele cita um diálogo imaginário entre duas pessoas onde uma diz ter tido uma idéia baseada na observação de um fenômeno natural. No caso, ele percebeu que a neve derretia em diferentes proporções dependendo do tipo de superfície em que estivesse depositada. Ele então imaginou a possibilidade de uma substância que acelerasse esse processo em qualquer superfície. Indagado pelo seu interlocutor sobre qual substância ele se referia, ele respondeu que não sabia, mas que iria patentear-la assim mesmo. Dessa forma, se no futuro alguém pusesse em prática sua idéia, teria de pagar a ele os *royalties*. Essa situação hipotética pode acontecer na vida real, pois o chamado *segredo do negócio* não faz distinção entre a criação imaginária de alguma coisa e a eventual concretização desta.

A sanha pelo recebimento de *royalties* pode emperrar ou até barrar definitivamente projetos, já que as penalidades costumam ser severas no caso de infringimento das cláusulas de *copyright*, patentes, etc.

Alguém que esteja com uma idéia para ser desenvolvida precisa consultar um batalhão de advogados para descobrir se não há problemas nesse sentido ou ainda descobrir quais são as reais intenções do autor relativas à distribuição ou modificação da obra original.

Vale lembrar que o *copyright* não é a mesma coisa que *patente*, ou *trademarks*. *Copyright* protege obras literárias<sup>10</sup> (livros, panfletos, poemas e outros trabalhos cujo núcleo são textos), trabalhos dramáticos (filmes, vídeos, peças, scripts, etc), trabalhos musicais (composições (compostas por apenas palavras e música ou somente música)), trabalhos artísticos (pinturas, desenhos, mapas, fotografias, esculturas e trabalhos arquitetônicos)<sup>11</sup>.

Há ainda outros elementos menos palpáveis que o *copyright* pode proteger como a performance de um dançarino, por exemplo. No caso da patente, diferentemente do *copyright*, há a exigência do registro da obra. É aplicada mais comumente a novos equipamentos, técnicas e processos. No entanto, há casos de registros de software ou mesmo elementos relacionados à computação. Quem não se lembra do registro de patente da Microsoft sobre o clique duplo do mouse, ou mesmo sobre os *emoticons*<sup>12</sup>?

Os *trademarks* também devem ser registrados e são aplicados em slogans, nomes e formas de produtos, distintivos, etc.

---

<sup>9</sup> Artigo integrante do livro *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum, editora Prentice Hall, 1995.

<sup>10</sup> Softwares são considerados como obras literárias pelos registros de *copyright*.

<sup>11</sup> U.S. Copyright Office (<http://www.copyright.gov/>).

<sup>12</sup> Simbologia através de caracteres para se expressar emoções.

Não há um real consenso sobre qual categoria os softwares estariam encaixados. Muito embora a idéia mais comum seja a de que o *copyright* represente a melhor escolha, há quem defenda a patente como opção, ou ainda algo como um “meio termo” entre esses dois.

Nos Estados Unidos, conforme ainda o website *U.S. Copyright Office*, todas as obras criadas em ou depois de 1 de Janeiro de 1978 (quando a regra de *copyright* foi alterada para os padrões atuais) são automaticamente protegidas desde o momento da sua criação perdurando por toda a vida do criador mais um adicional de setenta anos após sua morte. Se houver mais de um autor, essa regra se aplica ao último sobrevivente.

No caso ainda da obra ser um trabalho contratado, ou seja, a criação final não foi idealizada pelo seu executor, ou ainda do autor ser anônimo ou referenciado por pseudônimo (isso se não for revelada a verdadeira identidade nos registros de *copyright*), a duração do *copyright* passa a ser de noventa e cinco anos a partir da publicação da obra e de cento e vinte anos para a criação. Nesse caso, vale o que for mais curto.

No Brasil, segundo Masiero, a lei 9609/98 (direcionada para os softwares) protege a obra por cinquenta anos sob o domínio do autor.

No contexto moderno de distribuição de mídia, destaca-se um “reforço” resultante do *esforço* dos principais detentores de direitos autorais (música, vídeo, software) para o cumprimento das cláusulas do *copyright*: DRM. *Digital Rights Management* (ou Gestão de Direitos Digitais) tem o propósito de “assegurar” que as limitações impostas para a mídia em questão sejam respeitadas e que não sejam burladas. Exemplificando, se uma gravadora de determinado cd diz que a cópia digital do conteúdo não é autorizada sem a devida permissão, então esse dispositivo (o DRM) trataria de fazer cumpri-la.

Na verdade, o DRM é um ampliador das restrições já existentes do *copyright*, na medida em que viabiliza diferentes tipos de condições antes não imaginadas, como a quantidade de cópias de uma determinada mídia permitidas antes do bloqueio definitivo (no caso do cd de áudio).

Mas, voltando ao caso do início desse capítulo, do sujeito que desenvolveu o software, ele poderia ter optado por um outro tipo de licença de direito autoral. Ao invés de restringir o direito de cópia e manipulação, que tal se os liberasse? “– Ah, mas agora enlouqueceste de vez!”, diria o incrédulo. Não é bem assim. Há um homem que pensou (e ainda pensa) desse jeito: Richard Matthew Stallman.

#### 2.4.1.1.2 Software livre para voar

Houve uma época que softwares e seus códigos-fonte eram disponibilizados sem ônus de nenhum tipo aos desenvolvedores interessados. Bem, na verdade isso datava das décadas de 50 e 60 e os computadores pessoais eram coisas que estavam por vir, implicando no fato do hardware ser mais importante que o software. Não que fosse independente dele, não é esse o ponto, mas com computadores que ocupavam uma sala toda, o custo dessas máquinas era exorbitante a ponto de fazer os programas que rodavam nelas (bem sumários, diga-se de passagem) ser apenas um detalhe.

A situação se inverteu quando o computador pessoal se popularizou, diminuindo extremamente o valor do hardware. Os softwares foram ficando mais complexos e deu-se a mágica: passaram a ficar “fechados”, ou seja, o código-fonte passou a ser segredo, e quem quisesse ter acesso ao programa em si (executável) teria de desembolsar algum dinheiro. Surge a Microsoft, e a partir daí o enredo da história é mais ou menos conhecido, desembocando nos padrões atuais de comercialização de programas.

Porém em 1983, eis que Richard Stallman, até então trabalhando como programador no MIT (Massachusetts Institute of Technology), observa com desgosto um trabalho acadêmico seu ter o código fechado pela própria MIT. Stallman desliga-se da instituição e resolve fundar a *Free Software Foundation*<sup>13</sup>. Essa fundação seria baseada nos princípios que ele acreditava ser corretos para o desenvolvimento e disponibilização do software. Nasce, então, o projeto GNU<sup>14</sup>, calcado nessa filosofia. GNU é um acrônimo recursivo (típico de hackers) que significa “*GNU is not Unix*”.

A idéia do software livre é justamente essa que o nome sugere (ainda bem que não há a ambigüidade do inglês): é a libertação do software. Não há mais “algemas” prendendo o desenvolvimento dos projetos. Para ser livre, todo programa deve ter disponibilizado seu código-fonte (juntamente com o executável) e é permitido modificar o código original como se quiser, desde que o resultado dessa modificação seja também disponibilizado da mesma forma como o foi no original.

Isso pode parecer loucura para alguns. Como iriam permitir que o trabalho de anos no desenvolvimento de um projeto fosse entregue “de graça” para todos copiarem e replicarem? É normal que pensemos assim num primeiro momento. Porém, há uma linha de raciocínio que merece ser visitada. Nas décadas de 50 e 60 não havia caixa-preta para os programas. Tudo

---

<sup>13</sup> <http://www.fsf.org/>

<sup>14</sup> <http://www.gnu.org/>

era disponibilizado abertamente também em nome da evolução. Com a ajuda mútua entre diversos programadores chegar-se-ia ao bem comum que era o produto final, o software funcionando para a finalidade a que tinha sido proposta inicialmente. Descontando-se as diferenças tecnológicas entre as épocas, a idéia é a mesma para os dias de hoje. Com uma comunidade empenhada a melhorar programas disponíveis publicamente, o aparecimento de programas cada vez mais elaborados e com novas funções poderia facilitar a vida de todos.

Sabe-se que a coisa não é tão simples assim. Sempre haverá aquele que tentará se apropriar do código para então “patenteá-lo” e monopolizar os ganhos. Justamente para isso que Stallman foi irredutível no sentido de obrigar a manter a licença livre para todas as modificações feitas com base num código considerado também livre. Na verdade, aí está a grande diferença do software livre para o chamado software de código aberto. Nesse último é possível estabelecer algumas restrições no produto modificado, o que poderia descaracterizar toda a filosofia de liberdade.

Até mesmo no sistema operacional Linux é possível notar essa distinção. A alma do Linux é um software chamado kernel. Desenvolvido pelo finlandês Linus Torvalds, o kernel foi pela primeira vez disponibilizado na internet em 17 de setembro de 1991, sob a licença GPL<sup>15</sup>, que é a licença com valor jurídico do projeto GNU (GNU Public License). Dessa forma todos podiam contribuir para melhorar mais e mais o sistema. Inicialmente não havia interface gráfica, o que não colaborou muito para a popularização entre os menos iniciados na arte de “escovar bytes”. Mas isso mudou com a chegada dos ambientes gráficos KDE<sup>16</sup> e Gnome, desenvolvidos pela comunidade de programadores. Com as possibilidades múltiplas de crescimento, o Linux passou a ter diversas versões diferentes criadas por pessoas ao redor do mundo. Essas versões se chamam *distribuições*.

---

<sup>15</sup> <http://www.gnu.org/copyleft/gpl.html>

<sup>16</sup> O ambientes KDE e Gnome foram alvo de uma discussão acirrada em 1998 na comunidade Linux, pois o KDE usava partes de código fechado na sua constituição (bibliotecas fornecidas pela empresa Troll Technology). Essas bibliotecas proprietárias possuíam um código com desempenho mais estável, ao contrário da do Gnome, que era livre, mas não totalmente confiável em robustez (porém, preferiu continuar livre). Na época, a Troll Technology havia se recusado a aderir à licença GPL, optando pelo código proprietário, o que causou uma ruptura na comunidade Linux. Porém, com a chegada da licença de código aberto, a Troll Technology pôde alcançar um meio termo, não perdendo o controle sobre seu código proprietário e acalmando um pouco os ânimos da comunidade Linux.



É bom deixar claro que softwares livres ou de código aberto não são exclusividade do sistema operacional Linux. Esses são elementos universais que podem ser aplicados em qualquer sistema operacional. Citando o sistema operacional Windows, não é por ser pago que não existam partes do seu código que sejam livres, assim como os programas que rodam sob essa plataforma.

A generalização do conceito do software livre, de forma que possa ser aplicado a outras áreas chama-se *copyleft*. Mas, o *copyleft* pode dar dinheiro? Há correntes contra e a favor dessa questão. Para alguns, é inegável que o benefício trazido pelo copyright é mais óbvio e rápido. No entanto, em termos de software, a prestação de serviços seria uma das bandeiras levantadas pelos defensores do software livre como o responsável pelo ganha-pão.

Stallman uma vez disse que, se por acaso fôssemos Beethoven e desejássemos escrever uma sinfonia, teríamos mais dificuldades em concluir essa tarefa de forma satisfatória do que em evitar infringir patentes já existentes.

O que implicitamente isso quer dizer é que o processo criativo passa necessariamente pelo “reuso” de outros elementos que previamente já existiam. Tudo bem, o uso da palavra “necessariamente” pode ter sido um pouco pesado demais, mas só se tornaria inválido em casos raros, onde a genialidade estivesse presente em níveis diferentes dos padrões normais. E isso pode ser muito bem aplicado ao campo da computação.

Quando as leis de *copyright* são levadas ao extremo por meios jurídicos, o que acontece na verdade é um congelamento da capacidade de inovar das pessoas. Segundo Lawrence Lessig (LESSIG, 2003), professor de Direito na Stanford Law School e fundador do projeto *Center for Internet and Society*, essas leis somente contribuem para a criatividade comercial. Melhor dizendo, o mercado é o único destino e a única possibilidade de tornar viável o incentivo aos artistas para criar coisas. Ninguém está pregando que a visão do lucro é coisa do demônio, mas quando as relações se estreitam de tal forma que impedem a propagação e desenvolvimento de idéias baseadas nas que já existem, há uma “concentração de criatividade”, se é que existe esse termo. Isso, em médio e longo prazo pode levar a um cenário bizarro de monopolização da cultura. Imagine, por exemplo, só poder existir filmes de uma cadeia de produtoras. Esse cenário também é perfeitamente aplicável ao campo da computação.

Toda essa discussão de direitos autorais entre copyright e copyleft, do ponto de vista da Ética, até seria irrelevante se considerarmos que independente do conceito, os parâmetros (de conduta) a serem seguidos devem ser sempre os mesmos. Porém, ponderando que essa é a situação ideal e não a real, tal discussão passa a ser válida.

Por mais polêmicas que sejam as duas filosofias, numa coisa elas concordam: conhecimento do produto é a questão chave do processo. Em termos de software, antes de criar uma boa reputação, o produto precisa passar pelo crivo dos seus usuários e, para isso, nada melhor do que ter em mãos uma versão de testes do programa (o chamado *shareware*). Essa é a parte legal, digamos, desse pensamento. A outra, ilegal, seria o que certas pessoas fazem com essas versões *sharewares* (que muitas vezes são versões completas apenas limitadas por uma trava programada). Usando técnicas de engenharia reversa, por exemplo, encontram e desabilitam essas travas, fazendo o programa trabalhar com todas as suas funcionalidades disponíveis, sem pagar nada, ou ainda que não sejam completas (as versões *shareware*), alteram o executável principal (o famoso *patch*) de forma que quando instalado com o pacote original passe a atuar sem limites. Esses programas são “lançados” na internet (alguns não sem um “acompanhamento” extra (um *trojan*, por exemplo)) e são distribuídos amplamente. Se for um software de qualidade ou que pelo menos resolva satisfatoriamente o problema para que foi desenvolvido, por certo estará bem no mercado, inclusive no legal. Isso mesmo, no mercado legal, também. Quando as empresas publicam o faturamento de um determinado produto e reclamam que as vendas não foram melhores por causa da pirataria, há um paradoxo. Justamente a pirataria fez o marketing necessário para que mais e mais pessoas tomassem conhecimento do produto e optassem por comprá-lo por meios legais. Isso não é aplicável para todas as cópias vendidas, obviamente (afinal de contas, para quê serve o departamento de marketing de uma empresa?).

Segundo o coletivo Wu Ming, em *O Copyleft explicado às crianças* (MING, 2003), uma cópia pirata não é igual a uma cópia não-vendida. Na sua obra é usado o exemplo da Microsoft, com o sistema operacional Windows. Ele diz que o sistema não seria tão difundido se a pirataria não tivesse feito o seu “trabalho”. Para completar, chega a afirmar, de uma forma até um pouco exagerada, que uma cópia pirateada é igual a uma cópia vendida. Talvez nem seja tanto assim, mas por certo a pirataria “dá uma mãozinha” nesses casos.

É bom deixar claro que nem sempre a pirataria é tão benéfica assim. Por diversas vezes o software pode vir ser adulterado de forma a conter código nocivo. Em termos de vendas, e dependendo do programa, também, as pessoas podem simplesmente ignorar o fabricante e jamais comprar o produto original. Como havia alertado anteriormente, é um paradoxo.

### 2.4.1.1.1.3 “Suavizando” o *copyright*

Sabe-se que extremismo algum é bem sucedido de forma plena e por isso uma solução que representasse um meio termo seria o ideal nessa situação. A idéia não seria abominar nenhum dos lados. A decisão pela utilização tanto do *copyleft* quanto do *copyright* deveria ser deixada na mão daquele que estivesse a disponibilizar o trabalho intelectual, sem o peso de julgamentos de terceiros. Os adeptos do *copyleft* pregam a seu favor com o argumento de que a disseminação do conhecimento traria o bem comum, na medida em que o coletivo trabalharia pelo mesmo fim. Mas vá dizer isso para uma empresa que investe milhões em pesquisa para aperfeiçoamento de seus produtos continuamente para manter-se no topo do mercado. Possivelmente essa empresa não compactuaria com tal regime cooperativo. No entanto há aquelas empresas que, na sanha descontrolada para obter lucro, desejam estipular limites cada vez mais invasivos aos consumidores. Isso pôde ser constatado no caso da Sony, com seu DRM limitador de cópias de cd de áudio (também apelidado pela mídia de *rootkit*). Desenvolvido pela empresa *First4Internet*<sup>17</sup>, o programa era instalado sem o conhecimento do usuário e assim fazia valer certas restrições. Ora, o que temos aqui? Um caso explícito de desrespeito à conduta ética. Para piorar, ao lançar um patch para dar a opção do usuário de retirar o *rootkit*, o tal software tinha problemas e deixava o computador do usuário aberto a ataques de *hackers* maliciosos. O caso ganhou repercussão mundial e a Sony foi obrigada a se retratar frente aos seus consumidores, recuando na utilização do *rootkit*.

Atualmente está sendo discutida a formulação da terceira versão do GPL (na verdade já há uma versão rascunho desde janeiro de 2006 disponível) e nela há uma forte repreensão ao uso do DRM. Mas nem com essas restrições mais avançadas impediu-se a propagação indiscriminada de conteúdo “protegido” pela internet. Enfim, quanto mais se discute a respeito, mais se chega à conclusão de que há muito que fazer e que ainda não existe solução ideal.

Embora essa solução não esteja disponível, há uma idéia bem interessante desenvolvida por Laurence Lessig: *Creative Commons*<sup>18</sup>.

Segundo ele próprio, o *Creative Commons* (representado pela sigla cc) funciona como uma camada sobre o *copyright*. O autor da obra estaria apto a explicitar o que pode ser feito exatamente com a criação ao invés da famosa frase “todos os direitos reservados”, se assim desejar, claro. Dessa forma uma das grandes barreiras para o desenvolvimento de novas idéias

---

<sup>17</sup> <http://www.first4internet.co.uk/>

<sup>18</sup> <http://creativecommons.org/>

baseadas nas já existentes poderia ser mais facilmente quebrada se o autor da idéia original estivesse disposto a ceder. Geralmente é preciso todo um “ritual” jurídico para se ter certeza que determinados conteúdos possam ser utilizados sem que o autor original apareça um dia com uma ação judicial de direitos autorais batendo à porta. Obviamente de nada adiantaria o *Creative Commons* se a cessão de direitos não fosse concedida.

Tido como alguns como um suavizador do *copyright*, o *Creative Commons* tem se difundido relativamente bem pela internet. No entanto há correntes, dentro da comunidade do software livre que não vêem o CC com bons olhos, pois o consideram como mera extensão do sistema abusivo de *copyright*. De fato, o CC apenas repete as restrições de *copyright* se o detentor da obra não desejar ceder em nenhum dos aspectos. No entanto, nos casos em que isso não se aplica, pode ser uma boa idéia.

#### **2.4.1.1.1.4 Posso ou não copiar softwares?**

Diante de tudo o que foi explanado até agora, será que seria possível arriscar a questionar sobre a validade ou não da cópia de um programa? A resposta para muitos possivelmente seria “não”. O que há de ser considerado é que existe uma diferença bem clara entre um programa que é cedido a terceiros por alguém que o adquiriu legalmente e aquele que adquire (ou não) e depois o disponibiliza pela internet, por exemplo. Se o fabricante do software deixa explícito que nenhuma cópia é autorizada, qual das situações seria moralmente aceitável, se é que há alguma?

De acordo com Helen Nissenbaum, no seu artigo “*Should I Copy My Neighbor’s Software?*” a segunda opção definitivamente tem como resposta, “não”. No entanto, no caso da primeira opção, a resposta é “em alguns casos, sim”. Nissenbaum expõe seu ponto de vista diante de argumentos dos produtores de software sob dois aspectos éticos: o consequencialismo e o deontologismo, para depois rebatê-los.

Sob o ponto de vista consequencialista, fazer cópias sem autorização seria moralmente inaceitável pois traria conseqüências negativas. Segundo Nissenbaum, apesar da cópia trazer benefícios a curto prazo, a longo traria problemas tanto para consumidores quanto produtores. Primeiro pela razão de desencorajar o desenvolvimento de novos programas (como já foi citado anteriormente) e segundo pelo fato de hipervalorizar o preço do produto. Mas será que essas objeções são realmente válidas? O cenário mais comumente associado com a situação de pessoas copiando softwares é o de que ninguém mais pagaria para tê-los causando

desestímulo nos desenvolvedores. Descontando-se os fatos extremos, não é bem assim que acontece. A pirataria, como já comentado, é maléfica realmente e deve ser combatida. Usada muitas vezes pelas grandes corporações para justificar perdas é incentivada “pelos bastidores” até como instrumento de monopolização de mercado. Mas tem seu efeito “positivo”, se é que se pode afirmar desse jeito. É o efeito similar ao do chamado *uso justo*. Fazendo uma comparação bem rotineira, seria o caso de uma pessoa que compre um cd de áudio e que, para fins de adequação a outros tipos de equipamento (como um mp3 player, por exemplo), precisa transformar o conteúdo do cd adquirido legalmente. Para a indústria fonográfica e associações que lutam pelo cumprimento de direitos autorais essa prática é terminantemente condenável. Esses órgãos dizem que a pessoa estaria cometendo pirataria ao fazer o justo uso de seus direitos de consumidor que adquiriu o produto, ao passo que, na verdade, além de simplesmente usufruí-lo, poderia divulgá-lo (não confundir com “distribuir”) de forma mais ampla e sem ônus extra para o fornecedor do conteúdo. No caso dos softwares, na ocorrência de alguém que tenha adquirido um programa legalmente e que se encontre na situação de, por exemplo, ter um amigo em dificuldades financeiras precisando do tal programa para conseguir tocar seu negócio, seria imoral emprestar o software para esse cidadão até que ele pudesse enfim se recuperar? Sob o ponto de vista de Nissenbaum, essa seria uma situação válida. O segundo argumento, o de hipervalorizar o preço dos softwares, refere-se ao “seguro pirataria”. Melhor dizendo, algumas produtoras incluem uma porcentagem adicional ao preço que praticariam prevendo futuras perdas com a cópia indiscriminada do programa. Na verdade, o contra argumento para isso estaria implícito no fato da pirataria não ser o fator principal da queda de vendas. Aquele que não compra um programa ou o obtém de forma ilícita possivelmente não o faria nunca por vias normais. Então, dando a “oportunidade” desses experimentarem serviria como uma espécie de canal de propaganda, fato esse já comentado conforme os escritos do coletivo Wu Ming.

Sob o ponto de vista deontologista, os céticos defendem que copiar software seria imoral pela razão disso se constituir numa violação moral e desrespeito aos produtores do programa copiado.

Diante dessa questão, surge outra que é de difícil resolução. Até onde vai o direito dos produtores? Será que eles podem ter total controle e autorização sobre o que criaram mesmo depois de comercializados? De acordo com Nissenbaum, o fato de se ter direitos de propriedade sobre alguma coisa não constitui no direito de restringir totalmente o seu uso privado, dando espaço para novamente o uso justo entrar em cena (o que novamente justifica o uso do termo “em alguns casos, sim”, ao questionar sobre a validade ou não da cópia de

software). Na verdade, com o usuário se tornando um meio de propaganda para outros clientes, este pode acabar seduzindo outros por vantagens extras da compra legítima (como serviços especiais, por exemplo), que por sua vez eventualmente acabam desembolsando o dinheiro necessário. Fecha-se então, um círculo vicioso. Por essa linha de pensamento, será que ceder um software adquirido legalmente a terceiros é realmente tão anti ético como é comumente visto? Mais: quais os reais direitos de quem adquire um software e que, por conveniência baseada em princípios morais válidos, precisa emprestá-lo a quem quer que seja? A questão fica em aberto já que o limite do que pertence ao produtor e ao cliente ainda é impreciso, por mais que o senso comum dê todos os créditos para quem fornece (embora Nissenbaum acredite que nesse caso, a cópia não seria imoral).

#### 2.4.1.1.2 Hackers

Quando se pronuncia a palavra *hacker*, a primeira coisa que geralmente vem à cabeça é de que alguma coisa ilegal foi feita ou comentada sobre. Não raro temos acesso aos jornais impressos, televisivos ou digitais sobre casos em que alguém teve sua conta bancária limpa por algum criminoso ou seus dados vasculhados de forma a disponibilizar informação sigilosa, etc. O que talvez poucos saibam é que o nome correto para quem pratica esse tipo de ação é *cracker*, e não *hacker*.

A denominação *hacker* pouco ou nada tem a ver, em princípio, com delitos computacionais e sua origem é antiga, não estando necessariamente relacionada com computadores. Para ser mais exato, essa palavra já existia mesmo antes de alguém pensar em computação. Os antigos artesãos tinham como principal utensílio de trabalho o machado, e, justamente o ato de talhar, ou ainda de cortar lenha era a denominação original de *hacker*. A associação desse termo com a computação se deu por uma analogia feita com programadores que mergulhavam fundo nas suas atividades, buscando cada detalhe para tornar um programa sempre melhor. Essa dedicação além do nível normal acabou por cunhar o termo *hacker* no sentido computacional. Então podemos observar que ser *hacker* é apenas ser “fuçador”, extremamente ligado ao trabalho que se executa. Segundo Pekka Himanem, filósofo finlandês, autor da obra *A Ética dos Hackers e o espírito da era da informação* (HIMANEM, 2001), o *hacker* é um apaixonado pelo trabalho. Buscar sempre caminhos que levem à solução mais inteligente dos problemas é mais do que cumprir com a obrigação e ser recompensado por superiores ou clientes. É um prazer. Esse deleite torna-se ainda maior quando o *hacker* tem conhecimento de que o seu trabalho ajuda outras pessoas a executar suas tarefas mais facilmente. Não se trata de um ato altruísta, deixa-se bem claro. Na verdade, é exatamente o contrário. É um ato egoísta, solitário, apenas para massagear seu ego e provar que o *hacker* é capaz de dominar a engenhosidade do problema. O fato de disponibilizar o resultado para outras pessoas, os leigos, serve apenas como parte desse reconhecimento, mas extremamente importante dada a condição de seres sociais que somos, e pela busca incessante de nos introduzirmos num contexto também social, mesmo que isso seja feito virtualmente, ou ainda anonimamente.

Considerando que Himanem afirma que ser *hacker* é ser “amante do trabalho”, temos que qualquer pessoa que desempenhe uma atividade qualquer com extremo afinco pode ser chamada também de *hacker*. O padeiro da esquina que se aprofunda nos detalhes de produção

buscando aperfeiçoar o resultado da sua atividade, segundo essa definição, também pode ser chamado de *hacker*.

Se ser hacker é ser no máximo um trabalhador esforçado, como atualmente este termo adquiriu sentido de invasor, malfeitor, criminoso em termos computacionais? É complicado estabelecer limites precisos, mas a idéia remonta algo parecido com o surgimento do conceito do software livre. A partir do momento que algo tido como benéfico para as pessoas tornou-se um pacote fechado, obrigatoriamente acessível por meios financeiros, deu-se aí o incentivo para que pessoas com habilidades específicas na área de tecnologia empenhassem seus talentos para burlar tais barreiras. Nesse caso a figura do *hacker* sai de cena para a entrada do *cracker*. Crackers são aqueles que usam seu conhecimento para perpetrar ações danosas em sistemas. Essa seria, em tese, a única diferença entre esses dois atores do mundo da computação. Porém, ambos lidam com manipulação de softwares, sistemas, invasões, etc. A palavra *hacker* assumiu, com o passar dos anos, uma variação não inocente do termo “fuçar” e vem sendo repetida e amplificada, com a explosão de possibilidades que a tecnologia vem permitindo, pela mídia não especializada e especializada. Qualquer jornal, seja em que meio for, refere-se àqueles que cometem crimes virtuais como *hackers*. E isso talvez por ignorância ou mesmo comodidade, já que o público imediatamente entende por esse caminho o conteúdo que está se tentando passar.

Embora teoricamente *hackers* não causem prejuízos a outras pessoas, suas ações são discutíveis do ponto de vista ético. Afinal de contas, eles usam de meios teoricamente ilegais, explorando brechas de sistemas para invadir e vasculhar dados. Há uma visível violação de privacidade nas suas ações e isso possivelmente não tem sido bem visto pela sociedade. Já os *crackers* utilizam-se dos mesmos meios (às vezes até piores, já que não existe a preocupação prévia de não causar dano àquele que está sendo invadido) e, além disso, ainda destroem algo. Existem até empresas que contratam serviços de *hackers* para constantemente pôr em prova seus produtos ou criam feiras, ou espécies de concursos onde os inscritos podem colocar em prática suas habilidades e de quebra dar um feedback para a empresa desenvolvedora do produto que serve de alvo para seus participantes. Ou seja, ao mesmo tempo em que a ação de *hackers* é condenada, também é considerada como uma possibilidade plausível dependendo do contexto analisado. Em outras situações mais obscuras, há casos de empresas que se utilizam de *hackers* para efetuar espionagem industrial. Aqui, a ação do *hacker* seria danosa, já que informação é essencial para determinar linhas de planejamento empresarial.

Parece que é possível identificar duas linhas de atuação entre *hackers* e *crackers*. A primeira é o ato de propriamente invadir um sistema (ou ainda vasculhar as linhas de código



de um programa por meio de engenharia reversa, por exemplo) e o segundo o que fazer depois que essa invasão for bem sucedida. Do ponto de vista ético, essa última (se executado alguma ação maléfica em seguida) aparentemente não provoca maiores discussões relacionadas com sua identificação. Afinal de contas, trata-se de um ato danoso contra terceiros. Mas e quanto à invasão? Seria eticamente correto uma pessoa aproveitar-se de falhas em sistemas ou programas e ter acesso à informação que em tese deveria ser confidencial? Não é uma questão tão fácil de ser resolvida. Obviamente ninguém gostaria que um desconhecido de repente soubesse de segredos comerciais, por exemplo, que pudessem ter sido fruto de pesquisa sendo eles relevantes ou não. Forrester e Morrison afirmam em *Computer Ethics* (FORRESTER, MORRISON, 1993) que isso pode ser relativo dependendo da cultura local. No Canadá, por exemplo, se um estranho entrar na sua residência olhar e sair sem fazer nada, ele não estará cometendo crime algum. Por que isso não poderia ser aplicado no mundo virtual igualmente? Nos Estados Unidos é comum vermos, principalmente em filmes, as residências sem nenhum tipo de demarcação física que obstrua a passagem de pessoas entre uma propriedade e outra. Já no Brasil, por exemplo, isso é bem raro. Geralmente se constata exatamente o contrário: verdadeiras fortalezas com muros altos, grades e cadeados. Obviamente isso reflete todo um contexto baseado principalmente no nível de violência de cada localidade, mas mesmo assim poderia servir de parâmetro de diferenciação da forma de avaliação da gravidade de “espionar”, mesmo que sem interferir, entre duas culturas diferentes.

Então se chega à conclusão de que invadir a privacidade das pessoas pode ser eticamente aceitável dependendo da cultura local em questão? Não é bem assim. Deve-se tomar cuidado com as analogias feitas entre o mundo virtual e o real visto que as duas têm características bem distintas. No entanto, podemos destacar um desses aspectos, mais pertinente nesse caso, que na verdade é um grande incentivador dos *hackers* e *crackers* a “entrarem num local sem ser convidados”: o aparente anonimato.

Diferente de quando alguém invade um local pessoalmente, a invasão virtual pode ser feita comodamente de qualquer lugar. Esse elemento por si só já produz um efeito de segurança ao invasor, mesmo que falso. No mundo real há uma série de fatores que podem desencorajar a conclusão do ato, como por exemplo: o que fazer se alguém aparecer? É preciso tomar cuidado para não ser visto por vizinhos ou qualquer outro quando entrar. E se houver algum animal protegendo a residência? E se houver câmeras por dentro dela? Todos esses fatores, que na verdade soam como empecilhos, simplesmente desaparecem no mundo virtual. A isso se soma a característica introspectiva quase que inerente às pessoas que geralmente são mentoras desse tipo de ação. Há inúmeros estudos relacionados a isso e é

comum termos associado à figura do *hacker* ao sujeito geralmente do sexo masculino, jovem, socialmente retraído e rejeitado. No Brasil, observamos em contraste nos noticiários e jornais, jovens com perfil bem diferente do citado acima sendo presos por crimes virtuais. Apesar de não ser possível generalizar o perfil dos invasores, podemos dizer que isso nos leva a outra subcategoria de *crackers*: os *script kiddies*. Nela estão aqueles que não possuem conhecimento suficiente para elaborar ferramentas de invasão ou de realizá-las usando técnicas suas ou desenvolvidas com estudo. Eles apenas são usuários do que *hackers* e *crackers* disponibilizam na rede. Na verdade, a modalidade de invasão que atualmente se aplica com mais frequência por essa categoria é a mais simples de todas: a do *cavala de tróia* (explicada mais a seguir).

Retornando à linha de pensamento, o fato de não haver necessidade de confronto face a face torna a invasão virtual bem atrativa para qualquer perfil de invasor. Esse mundo virtual é o que chamamos de *ciberespaço*. O ciberespaço não precisa ser essencialmente ligado à computação, bastando que haja certa abstração para caracterizá-lo. A abstração é algo tão poderoso que pode nos livrar praticamente de todos os compromissos éticos que temos na vida real. O exemplo mais recentemente atribuído a isso é o do vídeo game. Nele o sujeito senta em frente à televisão e começa a lidar com coisas tipicamente vistas no mundo verdadeiro, só que com uma diferença: não é verdade. Então se pode matar, roubar, destruir sabendo que ao reiniciar o jogo tudo estará pronto para ser novamente morto, roubado, destruído. A questão não é discutir se é eticamente correto haver jogos que incitem esse tipo de comportamento no cotidiano verdadeiro, mas uma coisa é inegável: há uma relação entre isso e aqueles que usam meios virtuais para alterar coisas na vida real. É a sensação que ao “reiniciar o jogo” da vida real tudo estará bem novamente traduzida pelo aparente anonimato das ações virtuais.

Um exemplo de abstração não exatamente relacionado com computadores em primeiro plano é o da telefonia. Quando não havia meios tecnológicos disponíveis para interação virtual, o telefone era o que de mais comum se usava para se abstrair do mundo real. Nos primórdios das ações *hackers*, havia quem tentasse burlar o sistema de cobrança por fichas de telefones públicos. Os *phreakers*, assim chamados, foram primeiramente notados nos Estados Unidos e descobriram essa possibilidade com um pequeno apito que vinha de brinde junto com uma caixa de cereais. John T. Draper (ou melhor diria, Capitão “Crunch” (o nome do cereal)) percebeu que o som do apito era idêntico ao emitido pelos telefones públicos para efetuar a discagem. Ele então desenvolveu um aparelho chamado mais tarde de “bluebox” (caixa azul), baseado nessa característica de emitir sons idênticos aos dos telefones reais.

Dessa forma era possível discar para qualquer lugar do planeta sem gastar um mísero centavo. Não é preciso dizer que ele foi descoberto e preso, assim como muitos que tentaram usar a descoberta do “Capitão Crunch”.

Mesmo hoje, com o advento da internet, o telefone continua sendo usado como método bem eficiente para *hackers*, maliciosos ou não, obterem informações: é uma das técnicas da chamada *engenharia social*. Segundo Kevin Mitnick (famoso hacker e hoje especialista em segurança computacional, fundador da empresa de consultoria *Defensive Thinking*), autor do livro *A Arte de Enganar*, a engenharia social é extremamente poderosa. Ele cita Albert Einstein, dizendo: “Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro para o primeiro”. O que isso exatamente quer dizer? Não adianta um sistema estar repleto de elementos de segurança, sejam eles os mais rígidos possíveis, esse sistema sempre estará vulnerável, pois é operado por humanos. Qual o principal alvo daqueles que roubam dinheiro eletronicamente de contas bancárias: os bancos ou os usuários? Obviamente é a segunda alternativa. Os bancos estão muito bem protegidos e a não ser que o intento seja “provar a capacidade de invasão” a uma instituição financeira, o caminho mais fácil para conseguir seus objetivos é atacar justamente o elo mais fraco de todo esse sistema: os usuários. No caso da engenharia social esse ataque é feito sem usar de nenhuma ferramenta computacional. Simplesmente um telefone e uma boa dose de esperteza. Mas esses sujeitos podem ser considerados *hackers* (ou talvez *crackers*)? Sem dúvida através da abstração do ciberespaço proporcionada pelo telefone eles conseguem “hackear” sistemas simplesmente obtendo senhas que dão acesso a eles. Mas como, em sã consciência, alguém daria seus dados confidenciais para um estranho por telefone? Aí que reside a grande sacada da engenharia social. É um trabalho de paciência, ou seja, não é feito somente com uma tentativa. O primeiro passo é geralmente obter informações básicas, despreziosas até, de forma que nas outras abordagens a “vítima” tenha a impressão de estar falando com alguém que esteja por dentro do assunto. É preciso ser gentil e educado nas primeiras tentativas, já que muito pouco se tem de concreto em mãos. Dessa forma, obtendo um limiar de confiança, ainda que ínfimo, torna-se mais fácil obter o desejado. Nas abordagens seguintes as perguntas vão sendo encaixadas dentro de um contexto de rotina, e, mais para frente, o tom geralmente empregado é o de “o chefe para seu subordinado”. O funcionário, vendo que o interlocutor está de posse de tantas informações a priori sigilosas, acaba não questionando a autenticidade da sua autoridade e libera o conteúdo sem maiores problemas. E isso sem usar sequer uma ferramenta de invasão, ou mesmo nos casos mais severos, uma arma. Apenas a lábia e um

aparelho telefônico. Estaria a estupidez humana referida por Einstein alçando vôos rumo ao infinito?

#### 2.4.1.1.2.1 A Ética Hacker

Independente de o invasor ser classificado como *hacker* ou *cracker*, ambos têm raízes em comum, ou pelo menos concordância em alguns itens pré-estabelecidos, mesmo que informalmente. Segundo Eugene Spafford, autor do artigo “*Are Computers Hackers Break-ins Ethical?*”, os *hackers* usam alguns argumentos para justificar suas ações. O primeiro e mais “famoso” deles é o de que toda informação deve ser livre. É impossível não ligar esse argumento a Richard Stallman e ao conceito de software livre. Porém, temos aqui um diferencial um tanto considerável que é o significado dessa informação por si mesma. Imagine ter seus dados confidenciais disponíveis para qualquer pessoa acessar em nome da liberdade de informação. É bem diferente de permitir que seu trabalho (um programa de computador, por exemplo) seja melhorado e distribuído sem custos para toda uma comunidade virtual.

O argumento da liberdade de informação clamado pelos *hackers* conta, principalmente, com a prerrogativa de que as pessoas conectadas à rede são usuários “ideais”, ou seja, jamais fariam algo de errado com a informação de outrem. Ora, sabemos que isso não corresponde ao real perfil de todos aqueles que vasculham a rede. Mesmo sendo verdadeiro para os *hackers* – afinal de contas a definição do termo hacker implica em não fazer mau uso da informação obtida – não há como garantir que desvios de conduta não ocorram dependendo do “troféu” em mãos. Segundo Spafford, nossa sociedade atualmente está fortemente baseada no controle da informação, e que, por essa razão, deve ser o máximo possível precisa. O princípio da liberdade de informação, tomado assim incondicionalmente, terminaria por causar conflitos éticos em outros níveis. Por exemplo, como um banco poderia certificar a acurácia de suas operações se os elementos com que lida podem ser manipulados por qualquer pessoa? Como o governo de um país poderia administrar os recursos obtidos sejam por impostos ou outros tipos de investimentos se não houvesse um rígido controle da informação?

Longe de significar que toda a informação deva ser trancada a sete chaves, o contra-argumento ao principal fator alegado pelos *hackers* para justamente vasculhar esbarra num outro princípio importantíssimo em tempos modernos: o direito à privacidade. Embora um fator positivo da livre distribuição de informação fosse a possibilidade do aumento do conhecimento sem fronteiras, não há como deixar de ser conservador no aspecto de que deve

haver limite para não transformarmos o mundo atual, conectado e sem fronteiras, num barril de pólvora regido pela anarquia.

O segundo argumento, de acordo com Spafford, refere-se à exploração de falhas em sistemas. Anteriormente discutiram-se as motivações que levam os *hackers* a tentar invadir. Aqui a visão torna-se um tanto mais pragmática. Procurando brechas em sistemas o *hacker* estaria apto, a priori, a avisar sobre possíveis vulnerabilidades e assim ajudar a melhorá-lo. Dessa forma muitos deles pensariam fazer um favor, principalmente para as empresas, e então, talvez, receberiam uma recompensa extra além do reconhecimento de suas habilidades. Obviamente essa linha de pensamento é equivocada. Ninguém se sente seguro sabendo que um desconhecido possa vasculhar seus dados na surdina, ainda mais ignorando as suas reais intenções. Mais uma vez a privacidade seria então ameaçada. No entanto é comum ver empresas (principalmente nos Estados Unidos) agindo de modo dúbio ao contratar, como já citado anteriormente, *hackers* para testar a segurança do próprio sistema. Segundo Spafford, muitas delas remuneram essas pessoas com quantias semelhantes às exigidas em processos judiciais contra aqueles que fizeram (ou tentaram fazer) invasões não autorizadas. Poderia esse comportamento ser considerado anti ético?

Outro argumento usado por *hackers* para justificar invasões é o dos sistemas ociosos. Estando ocioso, o computador estaria “habilitado” a ser usado por eles, seja para ser invadido ou usado como meio para propagar pragas (isso no caso de uma ação maléfica, claro). Esse também é um argumento extremamente discutível. Ninguém adquire um bem pensando em cedê-lo a estranhos quando não o estiver usando.

Spafford ainda cita como justificativas dos *hackers* o processo de aprendizagem que iniciantes passam (precisando, para adquirir experiência e conhecimento, invadir) ou ainda o papel de protetor social que eles poderiam fazer no ato de descobrir falhas e alertá-las aos proprietários de sistemas.

Como se pode perceber, todos esses argumentos citados são questionáveis. É mais simples explicar o porquê de eles invadirem do que a finalidade propriamente dita. Nunca será justificada a invasão do ponto de vista do “paciente”, pois sempre se esbarrará no aspecto primordial que é o direito de privacidade. É interessante lembrar que o conceito de *hacker* no sentido computacional não implica necessariamente em invasores de sistemas, como citado no início desse capítulo. Isso resulta na impossibilidade de generalizar a atitude *hacker* como anti ética, embora não isente os invasores (mesmo apenas os “observadores”).

### 2.4.1.1.3 *Invasão de privacidade*

É comum se dizer que o direito à privacidade é uma das benesses trazidas a tiracolo pela democracia. Em períodos históricos onde a tirania imperava talvez essa fosse uma preocupação até secundária, já que sequer eram respeitados os direitos humanos básicos. Em tempos modernos, teoricamente, o direito a esse item de maneira geral é assegurado por lei na maioria das sociedades. No entanto, com o advento da computação a visão em torno dessa questão passou a mudar significativamente, considerando que praticamente tudo está guardado em bancos de dados, sejam nossos dados pessoais, contas no comércio, etc. Aparentemente não há regras definidas para o manuseio desses bancos de dados, apenas políticas de privacidade que variam de acordo com a empresa que as manipula. Diante dessa variável, como delimitar o acesso e exploração dessas informações (se é que se deve fazer isso) no intuito de preservar a privacidade das pessoas?

Segundo *Ruth Gavison*, autora do artigo *Privacy and the Limits of Law*<sup>19</sup>, a palavra *privacidade* pode ser usada em diferentes contextos. No caso mais sugestivo define-se que privacidade, em termos gerais, é a limitação do acesso de outros a um determinado indivíduo. Gavison ainda aponta que quando uma pessoa goza de perfeita privacidade significa que esta pessoa está completamente inacessível às outras. Ou seja, ninguém tem informação alguma sobre ela, ninguém “presta atenção” nela e ninguém tem qualquer contato físico com essa pessoa. Então a privacidade perfeita é, em termos práticos, impossível de se alcançar em qualquer tipo de sociedade, como salienta Gavison. Ele ainda completa: “a posse ou gozo da privacidade não é um conceito absoluto, ou seja, assim como não há privacidade perfeita também não há perda total dela”.

Embora impraticável no convívio social real, o argumento da privacidade perfeita poderia ser aplicável no mundo virtual? A conta bancária de um indivíduo, por exemplo, deveria ter elementos que a caracterizassem como de privacidade perfeita? É possível que a primeira resposta que viesse à nossa cabeça seja “sim”; afinal de contas, quem gostaria de ter dados da sua conta distribuídos livremente para quem tivesse interesse em verificá-los? Mas e se houvesse outras informações não vitais que o dono da tal conta não se importasse em tornarem públicas? E se uma segunda pessoa achasse exatamente o contrário? Entramos, então, num campo mais subjetivo do que vem a ser privacidade. Essa subjetividade se acentua

---

<sup>19</sup> Artigo integrante do livro *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum, editora Prentice Hall, 1995.

muito mais diante do pouco esclarecimento a respeito disso até agora no que se refere ao mundo computacional. Por exemplo, há empresas que não hesitam em vasculhar a comunicação eletrônica dos seus funcionários em busca de qualquer informação valiosa. Embora o ambiente de trabalho e maquinário sejam proporcionados pela empresa, quem os opera são os funcionários, que em tese deveriam ter a privacidade respeitada. Estes possivelmente não sabem quando (e em alguns casos, nem se) seus superiores praticam esse ato, digamos, “voyeur”. Não seria muito diferente de ter seus dados observados a partir do computador caseiro, por pessoas estranhas.

Há ainda um outro elemento em que não se configura essa relação empregador-empregado, mas fornecedor-cliente. Imagine que por algum motivo alguém contrate os serviços de uma empresa que tenha espaço virtual exigindo os famosos cadastros. O cliente, ávido em obter o serviço, preenche tal cadastro com seus dados pessoais. Tempos mais tarde essa empresa decide, sem consultar seus clientes, vender todo o banco de dados para uma outra empresa que passa então a enviar maciçamente propaganda de forma direcionada para cada contato específico. A confiança inicialmente depositada pelo cliente na primeira empresa foi totalmente dilacerada já que esta agiu de forma não ética. O problema é que em muitas ocasiões não é possível para o cliente identificar quem “vendeu” seus dados. É o que torna a prática bem rentável em diferentes sentidos.

Mas nem tudo é negativo nesse prisma. Através dessa possibilidade de procurar registros em bancos de dados poder-se-ia facilitar a localização de um criminoso, por exemplo. Um dos grandes males da humanidade alavancados pela internet é a pedofilia e, indivíduos que procuram esse tipo de material geralmente lançam mão de ferramentas de busca como Google, Yahoo, etc. E se de repente essas empresas de busca facilitassem a procura pelos órgãos dos governos nos registros dos usuários, identificando assim, ou pelo menos tendo pistas, de quem usa a internet para acessar ou propagar material desse tipo?

O propósito de ter acesso aos registros de mecanismos de busca é tentador, mas ao mesmo tempo representa um rompimento, uma abertura de possibilidades relacionadas com a privacidade *on line* dos usuários que até então se escondia no obscurantismo. De repente o usuário que transferia seus arquivos confidenciais para contas de email com alta capacidade de armazenamento passa a questionar se esses dados estão mesmo seguros e fora do alcance de outras pessoas. Estando cada computador por trás de um número IP, é perfeitamente viável a identificação do usuário (ou pelo menos de alguém responsável), embora essa técnica possa levar a distorções. Essas distorções puderam ser acompanhadas pela mídia internacional, por exemplo, nos famosos casos dos processos impetrados contra endereços de IP pela Recording

Industry Association of America<sup>20</sup> (RIIA). Pessoas que sequer tinham contato com computadores foram acusadas de “baixar” conteúdo protegido por direitos autorais de forma ilícita. Para evitar que o caso fosse levado à corte, a entidade propunha um acordo financeiro de alguns mil dólares. Os usuários, temendo por complicações judiciais, aceitavam o “pedido de resgate”, com exceções raras. Nesse caso, temos aqui uma entidade que, no intuito de atingir seu objetivo (descobrir quem distribui ou baixa conteúdo protegido pela internet) se despe de qualquer princípio ético e usa de todas as ferramentas disponíveis para identificar usuários conectados. Nesses momentos, será mesmo que a afirmação de Ruth Gavison sobre a impossibilidade prática da total perda de privacidade é verdadeira? Claro que são contextos diferentes, mas considerando que o grau máximo de “proteção” de uma pessoa *on line* é a identificação de seus passos pela internet, poderíamos considerar aí uma total perda de privacidade, portanto.

O poder da informação é algo que pode “mover montanhas”. Alguém que planeje investir em determinado setor do mercado, em uma localidade específica, precisa estar a par de como seus serviços seriam recepcionados pelos clientes. Caso contrário todo investimento realizado (seja em maquinário ou mão de obra) corre risco de naufragar junto com a idéia inicial de montar o negócio. Então seria primordial um prévio conhecimento sobre a população alvo para então atacar em determinado nicho e, para isso, nada melhor do que ter um “mapa” sobre as preferências de clientes em potencial. O mapa, que na verdade se constitui num quebra-cabeças sem fim, é resultado da combinação de informações colhidas em determinado espaço de tempo. (esse parágrafo está um tanto perdido – não consegui entender a conexão dele com os seus vizinhos)

Larry Hunter, em seu artigo *Public Image*<sup>21</sup>, aborda bem essa questão da informação ao escrever que “a ubiqüidade e poder dos computadores embarçam a distinção entre informação pública e privada”; “que a revolução não será apenas juntar dados, mas analisar o que já está prontamente compartilhado”. A informação pública é aquela que está disponível para todos terem acesso livremente. O detalhe é que pela coleta constante de dados públicos é perfeitamente possível chegar à informação privada por simples dedução. Hunter usa o exemplo de uma pessoa que dentro da sua própria casa observa quem caminha pela janela. Fazendo anotações sobre as pessoas e comportamentos e, mais tarde, ao cruzar essas anotações com outras feitas por seus vizinhos chega a traçar perfis de quem trafega pela

---

<sup>20</sup> <http://www.riia.com>

<sup>21</sup> Artigo integrante do livro *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum, editora Prentice Hall, 1995.



região. O mesmo acontece com uma loja de livros, por exemplo. Ao final de determinado período de “observação” já é viável prever que tipos de lançamentos seriam mais interessantes para cada cliente ou mesmo fazer outros tipos de deduções relacionadas com o conteúdo dos livros. Portanto, a partir de diversas peças de informação pública é possível chegar à informação privada. Esse elemento por si só já é poderoso no sentido de direcionar ações que uma empresa (ou seja qual for o órgão) possa tomar. Agora imagine se informações de diversos tipos de serviços fossem cruzadas. Seria um verdadeiro dossiê pessoal sobre cada indivíduo, que possivelmente nem suspeitaria de nada.

Hunter sugere a idéia de que a informação deva ser tratada como propriedade, ou seja, aquilo que se refira a cada pessoa deve pertencer a ela própria. Portanto, se uma livraria que mantém registros sobre compras de clientes decidir fornecer seu banco de dados para outros deve primeiro obter a permissão dos clientes para tal. Ora, isso nada mais é do que um compromisso ético com o tratamento da informação. Além disso, tornaria inválida a prática de algumas empresas de vasculhar correspondência eletrônica ou outros documentos de seus funcionários.

Porém, quando se trata de governo, a coisa pode mudar um pouco. A informatização dos cadastros pessoais de cada indivíduo tornou-se uma questão crucial para a eficiência das suas operações. E isso tanto em nível social quanto estratégico. Seria um retrocesso estipular limites abrasivos que impossibilitassem sua utilização sob pena de voltarmos à chamada “era pré-histórica” do tratamento de informação. Mas como assegurar que cada governo aja de acordo com as regras éticas requeridas nesse caso? Na China, por exemplo, tem havido notório controle sobre o direito de privacidade dos seus cidadãos. Lá um homem foi condenado a ir para a prisão após ter tido suas mensagens eletrônicas (email) vasculhadas. O conteúdo dessas mensagens estava relacionado a conceitos como democracia e liberdade (que soam como “palavrão” nesse país). O mais incrível é que a dita mensagem sequer havia sido enviada. Ela estava no que costumeiramente é chamado de rascunho, uma pré-fase de elaboração do email onde é possível começar a redigi-lo e terminá-lo em outra ocasião. O fornecedor do serviço de mensagens em questão – o portal multinacional Yahoo! – colaborou com o governo chinês de forma amplamente não restritiva e entregou toda informação de que dispunha ambicionando, possivelmente, a entrada no mercado desse país, tido como emergente potência mundial.

É perceptível a completa viabilidade da obtenção de informações pelos fornecedores de serviços on line. Quem garante que nesse momento não estamos sendo monitorados pelo provedor de conteúdo enquanto navegamos inocentemente, checando nossas mensagens

eletrônicas? O caso Yahoo China<sup>22</sup> deu-se por uma jogada estratégica de mercado; colaborando com o governo chinês, este possivelmente seria mais “generoso” no futuro no que diz respeito à abertura de oportunidades futuras. Mas onde fica a Ética nessa situação? Onde está a consciência ética e a política de privacidade que protegem seus usuários? Se de uma hora para outra o governo brasileiro, por exemplo, decidir que deve buscar informações através desses portais multimídia toda a privacidade dos usuários seria jogada no lixo? Voltaríamos à famosa época na qual se guardava dinheiro “embaixo do colchão”, pois ninguém estaria seguro de fato em armazenar seus dados em servidores alvos de espionagem. Mas esse episódio não foi somente ocorrido com o Yahoo. Algo semelhante ocorreu com outro gigante das ferramentas de busca pela internet: o Google<sup>23</sup>. Porém, desta vez não de forma tão acintosa já que o portal resistiu à pressão (no caso do governo dos Estados Unidos) para liberar informações. Mas mesmo assim decidiu aceitar a “proposta” dos chineses em retirar páginas que fizessem menção a assuntos que este governo considerasse “inapropriados” como *liberdade de expressão, democracia*, entre outros.

Mas e quanto às leis sobre privacidade *on line*? Elas existem, é claro. Elas foram desenvolvidas pioneiramente na Europa e Estados Unidos dadas suas condições privilegiadas de desenvolvimento em relação ao resto do mundo. Mas mesmo nestes países estas leis não estão devidamente adequadas com a real necessidade que a internet impõe em termos de privacidade, pois abordam aspectos apenas normativos. Na Europa, por exemplo, a EU Data Protection Directive (1995) pôde ser considerado um bom passo no sentido de regulamentar aspectos relativos à privacidade, muito embora fosse pouco aplicável ao contexto real e tratasse os assuntos de forma generalista. Estas diretivas foram depois revistas e adequadas às telecomunicações com a Diretiva 97/66/EC, e finalmente com a Diretiva 2002/58/EC<sup>24</sup> a menção sobre proteção de dados e privacidade eletrônica foi feita.

Nos Estados Unidos há diversas regulamentações a respeito, desde o famoso Privacy Act de 1974 até as várias ramificações em inúmeras áreas.

No Brasil, segundo o advogado Antônio Ludovino Lopes, em seu artigo para o site *InfoGuerra*<sup>25</sup> citam-se as leis 8078 de 1990 (artigos 43 e 44 tratando da abertura dos bancos de dados por parte de fornecedores e clientes )<sup>26</sup> e a lei 9983<sup>27</sup> de 2000, onde há referência explícita sobre crimes em banco de dados. Embora essas referências sejam apenas superficiais

---

<sup>22</sup> [http://www.usatoday.com/tech/world/2006-04-19-yahoo-china-dissident\\_x.htm](http://www.usatoday.com/tech/world/2006-04-19-yahoo-china-dissident_x.htm)

<sup>23</sup> <http://news.bbc.co.uk/1/hi/technology/4630694.stm>

<sup>24</sup> [http://www.eu.int/eur-lex/pri/en/oj/dat/2002/l\\_201/l\\_20120020731en00370047.pdf](http://www.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf)

<sup>25</sup> <http://www.infoguerra.com.br>

<sup>26</sup> <http://www.presidencia.gov.br/ccivil/leis/L8078.htm>

<sup>27</sup> <http://www010.dataprev.gov.br/sislex/paginas/42/2000/9983.htm>

é possível usar o Código de Defesa do Consumidor, Código Civil ou ainda o Código Penal através de adaptações ao contexto (computacional, no caso) se alguém se sentir prejudicado em termos de privacidade, de acordo com o advogado Amaro Moraes e Silva Neto<sup>28</sup>. Mas isso pressupõe que sempre a parte prejudicada tenha de tomar individualmente a iniciativa de promover uma ação contra quem atentou à sua privacidade.

Retornando ao contexto mundial, é curioso que apesar do esforço em racionalizar o tratamento da privacidade do ponto de vista computacional haja, ao mesmo tempo, outra corrente exatamente no sentido oposto. A National Security Agency (NSA)<sup>29</sup>, dos Estados Unidos, mais um conglomerado de outros países desenvolveram uma espécie de sistema de vigilância mundial batizado de *Echelon*. Por ele todo tipo de transmissão, seja por telefone, internet, satélite, é monitorada em tempo integral, revelando-se numa total inexistência de privacidade. Embora o volume de dados analisados seja gigantesco ainda assim foi possível identificar indícios dos ataques terroristas às torres gêmeas (World Trade Center) em 11 de setembro de 2001, por exemplo. Aliás, o terrorismo tem servido de desculpa para os Estados Unidos apertarem ainda mais o nível de vigilância mundial e principalmente dentro do seu próprio território através da legislação *Mobilization Against Terrorism Act*, (MATA).

O que possivelmente não tem sido bem analisado é que medidas como o MATA ou qualquer outra que agrida os direitos fundamentais dos cidadãos cedo ou tarde passam a ser contestadas. Nas sociedades democráticas o *direito de saber* e a *privacidade* são itens que ficam em lados opostos da “balança”. Há a necessidade de equilíbrio para que a balança não penda só para um lado, terminando por “derrubar” tudo. Seja por espionagem ou processamento de dados, tem de haver a consciência de que há pessoas por trás dos gráficos e números que representem tendências. O controle dessas informações é necessário, mas ao mesmo tempo isso se traduz numa ferramenta que pode alterar de forma substancial a vida das pessoas envolvidas. Como Forrester & Morrison (FORRESTER, MORRISON, 1993) cita sobre a invasão de privacidade, o primeiro passo é estar consciente de que isso existe para então tentar a resolução do problema, o que, diga-se de passagem, é incerta.

---

<sup>28</sup> <http://informatica.terra.com.br/virusecia/spam/interna/0,,OI195624-EI2403,00.html>

<sup>29</sup> <http://www.nsa.gov/>

#### 2.4.1.1.4 *Ética na Internet*

De todos os tópicos sobre violações éticas no contexto computacional, este, sem dúvida, é o mais abrangente de todos. Falar sobre Ética na internet é como abordar o assunto da pirataria, hackerismo, invasão de privacidade e tudo mais relacionado a computadores conectados na rede. Dessa forma um outro enfoque será dado nesse capítulo, tratando a internet por um aspecto mais generalista – mas não sem dar pinceladas mais precisas em determinados assuntos.

A internet existe como ferramenta já faz muito tempo. Na longínqua década de 50 nasceram os primeiros protótipos com propósitos militares e mais tarde, após a ameaça da Guerra Fria enfraquecer, para comunicação entre universidades norte-americanas. Era um sistema de comunicação bem precário, é verdade, e extremamente de uso limitado, longe da acessibilidade que temos atualmente. No Brasil, digamos que este ficou “às moscas” durante boas décadas até o ano de 1989, quando o projeto<sup>30</sup> RNP (Rede Nacional de Ensino e Pesquisa<sup>31</sup>) foi lançado pelo Ministério da Ciência e Tecnologia<sup>32</sup> (MCT) com financiamento do Conselho Nacional de Pesquisa<sup>33</sup> (CNPq). Mesmo assim o acesso a essa rede era destinado ao meio acadêmico brasileiro, sendo liberado ao público somente em 1995 com a concessão de exploração para os provedores comerciais.

Atualmente, com o desenvolvimento crescente da internet, chegou-se a um patamar em que praticamente qualquer informação pode ser obtida com somente alguns cliques de *mouse*. Textos, vídeos, músicas, qualquer coisa é acessível sem que o indivíduo precise sequer tirar o pé da própria casa. A internet deixa, então, de ser um meio alternativo à carta e ao telefone para se tornar um “segundo mundo”, o mundo virtual, o ciberespaço, como já citado anteriormente.

Quando nos sentamos em frente ao computador e conectamos à internet, automaticamente passamos a fazer parte de uma comunidade de alcance global. Não é apenas mais uma máquina ligada, mas um ator desempenhando um papel no contexto virtual. Esse papel pode ser desempenhado de diferentes maneiras e também pode influenciar o pensamento e mudar decisões de outros participantes, assim como ser irrelevante de igual forma.

---

<sup>30</sup> <http://www.rnp.br/noticias/imprensa/2002/not-imp-marco2002.html>

<sup>31</sup> <http://www.rnp.br>

<sup>32</sup> <http://www.mct.gov.br/>

<sup>33</sup> <http://www.cnpq.br/>

Dimitrios Theotokis e Georgios Gyftodimos, no artigo *The role of the Internet both as an ancient agora and a French café for the humanities*<sup>34</sup>, abordam o aspecto abstrato da internet focando os papéis desempenhados pelos internautas. Eles analisam o mundo virtual proporcionado pela rede sob duas variantes: o *agora* e o *café francês*.

Na chamada cidade-estado de Atenas, em períodos antigos, Platão, Sócrates, Demóstenes, entre outros, reuniam-se num local específico para debater questões filosóficas e ensinar seus conceitos. Esse local era o que é chamado de *agora*. De forma análoga, Theotokis e Gyftodimos relacionam o contexto da internet com o dos tempos dos famosos filósofos. Certo, não temos mais Sócrates nem Platão, mas em compensação contamos com a grande vantagem de poder trocar idéias sobre as mais diversas áreas sem o empecilho da localização geográfica. Qualquer pessoa, em qualquer lugar do planeta que tenha acesso à internet poderia, em tese, participar desse debate aumentando de forma estrondosa as possibilidades de alcance do que está sendo discutido. Dentro do *agora* são definidos os atores que fazem parte dessa discussão, que são os transmissores e receptores com tarefas obviamente dedutíveis. Theotokis e Gyftodimos determinaram que no *agora* há sempre o fornecedor do conhecimento e aqueles que entram na discussão apenas para absorvê-lo. Ao contrário de outros tipos de mídia, como a imprensa, por exemplo, em que único meio (ou o mais eficiente) de comunicação do leitor com a mídia seria via editor. O fórum de discussão proporcionado pela internet, ao contrário, permite uma troca de informação muito mais dinâmica e teoricamente sem gargalos. No entanto essa comunicação seria mais para efeito de pequenas interações do que propriamente para contestar propostas feitas pelos transmissores. Dessa forma, o papel em princípio passivo dos receptores pode ser observado sob outro aspecto: o do autodidatismo. O indivíduo, mesmo não tendo voz ativa nas discussões, participa delas no intuito de aprender o que pretende sendo guiado pelas fontes que desejar, constituindo-se assim, uma espécie de livre arbítrio virtual. Mas há também o outro lado, negativo, que é a possibilidade de manipulação de idéias por parte dos transmissores, fazendo com que os receptores sejam guiados de forma errônea se não forem suficientemente conscientes das fontes de informação em que se baseiam. Mas mesmo nesse caso há o “consolo” do exercício da liberdade de expressão e do livre arbítrio, já que o receptor, identificando a deficiência de “conteúdo” da sua fonte, pode simplesmente decidir deixar de usá-la e procurar outras que considere confiáveis.

---

<sup>34</sup> Artigo integrante do livro *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum, editora Prentice Hall, 1995.

Já sobre o outro ponto de vista proposto por Theotokis e Gyftodimos, temos a internet vista como um *café francês*. Usou-se esse termo por referência às famosas cafeterias da França revolucionária do século XVII. Eram, na verdade, mais do que estabelecimentos para servir café e outros petiscos, e sim pontos de encontro para os revolucionários trocarem idéias e organizarem suas ações.

Assim como no *agora*, o *café francês*, em analogia com a internet, tem a mesma propriedade de não possuir limites fronteiriços para suas discussões. Porém, ao contrário do primeiro, seus integrantes têm voz ativa, participando muito mais além do que meros receptores. Dessa forma, receptores e transmissores trocam de papel constantemente e não há alguém considerado como o detentor incontestável do conhecimento, como se observava no *agora*.

Não se pode dizer que *agora* é pior do que *café francês* ou vice versa. Os tipos de comportamento observados no mundo virtual podem ser muito bem o reflexo da nossa conduta no mundo real. Os dois tipos existem concomitantemente e podem ser desempenhados inclusive pelo mesmo ator em contextos diferentes.

Sendo assim podemos ponderar que os rumos que a internet toma estão fortemente relacionados ao tipo de comportamento que desempenhamos nela. Melhor explicando, se quisermos que a Ética seja observada nesse sentido, a “conduta virtual” dos atores é de extrema importância. Então vem a pergunta: deve-se deixar que a internet se auto regule ou seriam necessários meios que garantissem isso? Os defensores da auto regulação usam como argumentos a liberdade de se expressar, o direito a privacidade, de decidir o que é melhor para si. Já os detratores apontam as distorções causadas pela política frouxa de controle como a pornografia, racismo, desrespeito à propriedade intelectual, insegurança, entre outros.

De acordo com Penny Duquenoy em seu trabalho *The Internet: a framework for understanding ethical issues*<sup>35</sup>, temos que o comportamento de cada indivíduo na internet é baseado por princípios éticos (sejam eles quais forem). A regulação justamente entraria para reconhecer esses princípios e “validá-los” ou não, funcionando como uma ferramenta ética.

Duquenoy observou ainda um detalhe interessante: a internet de hoje não é totalmente desregulamentada, havendo elementos de auto regulação mesmo que em níveis mais brandos. Por exemplo, muitos serviços disponíveis virtualmente somente são acessíveis mediante aceitação de termos ou políticas de conduta. Essas políticas não são iguais para todos os fornecedores de serviço, sendo fruto de uma análise individual das empresas no que concerne

---

<sup>35</sup> Disponível em <http://www.cs.mdx.ac.uk/staffpages/penny/allchapters.pdf>

suas necessidades e tipos de comportamentos esperados ou tidos como aceitáveis por parte do cliente.

No entanto, essa auto regulamentação não impede que outros desvios éticos de conduta na internet venham a ocorrer simplesmente por estarem fora do âmbito da empresa fornecedora do serviço. Novamente exemplificando, temos o caso da tentativa de criar um domínio próprio para conteúdos pornográficos<sup>36</sup>. Dessa forma, todos os serviços oferecidos através da internet nessa área estariam com o sufixo “.xxx”, similar ao que temos para sites relativos ao governo “.gov”. Os opositores dessa idéia apontam que isso não resolveria o problema já que o material pornográfico poderia continuar a circular livremente pelas páginas com o sufixo “.com”. Já os defensores acreditam que essa medida ajudaria a identificar mais facilmente os casos de pornografia infantil, um problema amplificado pela alta disponibilidade de conteúdo via internet.

Apesar do exemplo acima citado ter características normativas – afinal de contas, o fato de determinar a mudança do domínio de páginas por conteúdo é um tipo de regulamentação – seus efeitos são parecidos com os da auto regulamentação no sentido de serem extremamente brandos e deixando a tarefa de fiscalizar e punir – se for o caso – por conta de quem se dispor a fazê-lo e da forma que quiser.

O auto regimento tem por princípio a consciência ética de cada indivíduo representado no mundo virtual através dos seus “atos” na internet. É tido para alguns como o meio mais democrático, digamos, para estabelecer limites, respeitando assim o direito da livre expressão. Segundo Duquenoy, outro elemento que conta a favor desse tipo de “controle” é a velocidade com que a tecnologia progride, inviabilizando a concretização de uma legislação sempre a par com as possibilidades disponíveis.

Mas a auto regulamentação nada pode fazer se o indivíduo ignora qualquer princípio ético e decide transgredi-lo propositadamente. É o que acontece com as diversas páginas de conteúdo racista, por exemplo. O Orkut<sup>37</sup>, site de relacionamentos internacional amplamente conhecido no Brasil, é um espaço onde todos os tipos de idéias podem ser veiculados e nele é possível entrar em contato também com todo o tipo de aberração discriminatória; desde comunidades (é como são chamadas as seções de discussão por assunto) abertamente fazendo apologia a discriminação contra negros, adoração ao nazismo, etc.

Por razão desses casos muitos levantam a necessidade de um controle mais rígido para coibir esse tipo de material circulando pela internet, podendo ser acessado por qualquer

---

<sup>36</sup> <http://news.bbc.co.uk/1/hi/technology/4760459.stm>

<sup>37</sup> <http://www.orkut.com>

pessoa, de qualquer idade, bastando para isso estar em contato com um computador conectado.

Mas como promover esse controle através de regimentação sem agredir a liberdade de informação? Se já não bastasse esse elemento, ainda há outro que é a pouca definição e ambigüidade dos termos relativos à computação. Não existem certezas absolutas quanto a abordagem a ser tomada em casos de propriedade intelectual, privacidade, entre outros. Devo ou não devo ceder meu software adquirido por mim a terceiros sem custos? Devo ou não transformar um cd de áudio em arquivos de mp3 para que sejam compatíveis com outros equipamentos como players portáteis? Apesar de nos casos de propriedade intelectual haver legislação proibindo esses atos, o ato de distribuição de arquivos em massa pela internet age como um fator “justiceiro” na medida em que prega que essas leis criadas para restringir acessos são abusivas. Isso não quer dizer que a regulamentação da internet seja somente para efeito de fazer valer tais leis restritivas (apesar de certos setores da indústria possivelmente pensarem desse jeito). Como já abordado, há inúmeras distorções causadas por desvios de conduta que poderiam ser evitadas se uma regulamentação mais firme estivesse em vigor.

Por ser um assunto relativamente novo não há consenso em relação a qual caminho se deva seguir. A própria internet representa uma incógnita atualmente na medida em que não temos certeza de como estaremos interagindo com ela, mesmo a curto prazo. Nascida com propósitos fixos e, depois de cumprida sua tarefa, digamos, militar, ela foi deixada “sozinha” para que pudesse caminhar com suas próprias pernas. E ela está realmente fazendo isso. A famosa frase utilizada por Eric E.Schmidt, na época chefe executivo da Sun Microsystems, encaixa-se muito bem nessa situação: “A internet foi a primeira tecnologia que nós humanos construímos sem entendê-la realmente.” “...Cada vez que ela começa a fazer sentido, então muda”.



### 2.4.1.2 Códigos de Ética na computação

De acordo com Ferrell, Fraedrich e Ferrel, no livro *Ética Empresarial - Dilemas, Tomadas de Decisões e Casos* (FERREL, FRAEDRICH & FERREL, 2001), um código de ética nada mais é do que “um acordo explícito entre membros de um grupo social, uma categoria profissional, um partido político, uma associação civil, etc”. Ainda segundo este mesmo autor:

Seu objetivo é explicitar como aquele grupo social que o constitui, pensa e define sua própria identidade política e social; e como aquele grupo social se compromete a realizar seus objetivos particulares de um modo compatível com os princípios universais da Ética. Um código de Ética começa pela definição dos princípios que o fundamentam e se articula em torno de dois eixos de normas: direitos e deveres. Ao definir direitos, o código de Ética cumpre a função de delimitar o perfil do seu grupo. Ao definir deveres, abre o grupo à universalidade. Esta é a função principal de um código de Ética. A definição de deveres deve ser tal que, por seu cumprimento, cada membro daquele grupo social realize o ideal do ser humano. (FERREL, FRAEDRICH & FERREL, 2001).

É interessante lembrar que códigos de Ética não têm “poder de polícia”, ou seja, não são juridicamente válidos por si mesmos exceto que haja uma lei calçando o princípio em questão. Dessa forma, os códigos de Ética adquirem um aspecto mais informativo do que qualquer outra coisa. A decisão pela correção ou não da ação, na maioria das vezes, ficaria por conta da própria pessoa que estivesse envolvida na situação.

Como já argumentado, a área computacional ainda não possui regulamentação no Brasil, o que resulta na inexistência de um código de Ética específico. Fora do país existem esforços para tentar pelo menos delimitar certas questões e estabelecer alguns princípios considerados básicos. É o que se verifica nos códigos de Ética da ACM<sup>38</sup> (Association for Computing Machinery) e do IEEE-CS<sup>39</sup>/ACM, que são na verdade sociedades ativas com uma certa quantidade de agregados. No mundo, essas associações são as que produziram os códigos de Ética mais difundidos, apesar de existirem outras, como a Association of Information

---

<sup>38</sup> [www.acm.org](http://www.acm.org)

<sup>39</sup> <http://www.computer.org> (Institute of Electrical and Electronics Engineers – Computer Society)

Technology Professionals (AITP), a British Computer Society (BCS) e a Canadian Information Processing Society (CIPS). (MASIERO, 2000).

No Brasil também se pode encontrar associações similares, como a Sociedade Brasileira de Computação<sup>40</sup> (SBC) ou ainda a Sociedade dos Usuários de Informática e Telecomunicações<sup>41</sup> (Sucesu), sendo que nenhuma delas possui um código de Ética formal. A SBC se posiciona explicitamente contrária à regulamentação da profissão, segundo ela, nos “moldes tradicionais”, por julgar que tal atitude gera uma reserva de mercado e induz a um endeusamento do diploma universitário, mesmo que sem a competência técnica para tal. Mas ao mesmo tempo defende a criação de código de Ética elaborado por um conselho, ao qual denomina Conselho Nacional de Auto-Regulação, baseado em princípios que julga serem corretos.

Apesar de não haver uma regulamentação própria para a profissão na área da computação no Brasil, não se pode dizer que não existe nenhum aspecto normativo. Leis como a do software (Nº 9.609, de 19 de Fevereiro de 1998), muito embora não cubram como se desejaria todos os elementos relacionados ao assunto, pelo menos os cercam em termos gerais.

Voltando aos códigos da ACM e IEEE-CS/ACM, estes também cometem o “pecado” de serem generalistas demais. Algumas vezes os regimentos ali encontrados são conflitantes entre si e no fim das contas os casos omissos dependem sempre da conduta ética do usuário para serem solucionados. É reconhecível, mesmo assim, a dificuldade residente na elaboração de um conjunto de normas que preveja com total precisão todas as possibilidades. É praticamente impossível que isso seja concretizado sem que brechas apareçam. Há ainda o complicador que é a mudança constante da tecnologia, fazendo que certos preceitos tenham de ser incessantemente atualizados.

Os dois códigos – ACM e IEEE-CS/ACM – têm uma característica em comum, conforme observa Masiero que consiste numa “hierarquia crescente de valores, que vai do interesse individual ao interesse geral da sociedade”. Completando, quando houver impossibilidade de conciliação entre esses dois interesses, o da sociedade deve sempre prevalecer.

O código da ACM foi um dos pioneiros ao delimitar as primeiras linhas relativas à conduta ética na computação, sendo inicialmente produzido na década de 1990, com um enfoque amplamente generalista. Mais tarde, ao fim dessa mesma década, através de uma

---

<sup>40</sup> <http://www.sbc.org.br/>

<sup>41</sup> <http://www.sucesu.org.br/>

força tarefa entre a ACM e o IEEE, chegou-se ao que é reconhecido como o código unificado IEEE-CS/ACM. O enfoque, nesse caso, seria específico para os profissionais que lidam com software, tanto que a referência “engenharia de software” é feita de forma explícita no título do código.

É possível distinguir quatro partes bem distintas no código da ACM<sup>42</sup>: os imperativos morais gerais, as responsabilidades profissionais mais específicas, os imperativos sobre liderança organizacional e a submissão ao código de Ética em si.

O primeiro – imperativos morais gerais – prega sobre elementos considerados bem subjetivos, como “contribuir para o bem estar da sociedade”, “evitar danos a terceiros”, “ser honesto e confiável”, “ser justo e agir de forma não discriminatória”, “honrar direitos de propriedade”, “dar crédito apropriado à propriedade intelectual”, “respeitar a privacidade dos outros”, “honrar a confidencialidade”. Talvez a idéia dessa primeira parte do código tenha sido a de “preparar o terreno” para entrar em atribuições mais específicas. Elementos como “ser justo e confiável” são coisas bem superficiais e podem invariavelmente serem aplicadas em diferentes contextos. Os imperativos morais são, portanto, uma espécie de “framework ético” similar aos dez mandamentos para os cristãos, onde o caráter do indivíduo influencia diretamente no resultado.

O segundo – responsabilidades profissionais mais específicas – segue a linha dos imperativos morais, porém com um enfoque mais específico nas atribuições relativas às atividades exercidas no âmbito computacional. Como exemplos, citam-se “adquirir e manter competência profissional”, “honrar contratos, atribuições e responsabilidades” e inclusive uma que propõe ao indivíduo uma reflexão sobre as responsabilidades, conseqüências e limitações da computação em relação à sociedade.

O terceiro – imperativos da liderança organizacional – se refere ao profissional como parte de um time, e como tal deve estimular o senso de responsabilidade do grupo a que pertence. Há também a visão de quem necessariamente não está com a “mão na massa” na hora de projetar sistemas, que são aqueles que gerem uma determinada equipe. Nesse caso, o imperativo diz que se deve “construir sistemas de informação que melhorem a qualidade de vida no trabalho”.

O quarto e último – submissão ao código – prega a obediência aos itens até aqui explanados e invalida a afiliação ao grupo da ACM caso se detecte alguma contravenção às normas.

---

<sup>42</sup> Disponível na versão original em Anexo III

Com exceção a uma menção sobre as leis de propriedade intelectual e exclusão do grupo, nenhuma sanção adicional está prevista por esse conjunto de regras. Há referência clara a respeito do detalhe dos conflitos entre preceitos. A saída encontrada pelos elaboradores do código ACM foi recorrer aos princípios básicos de conduta.

Já o código de Ética resultante da força-tarefa entre IEEE e ACM<sup>43</sup> está subdividido em princípios, sendo que cada um deles concerne a uma gama de atuação específica do chamado engenheiro de software. Assim, no primeiro princípio, o engenheiro de software se compromete a agir consistentemente com o interesse público, ou seja, desenvolver seu software de maneira que venha a garantir segurança, satisfação do cliente.

O segundo princípio cita a relação que deve existir entre o engenheiro de software e clientes e empregadores. Por esse princípio, por exemplo, o profissional deve “fornecer serviços em suas áreas de competência sendo honesto e franco sobre qualquer limitação de sua experiência e educação”. Também há a menção sobre o uso da propriedade, seja de cliente ou empregador, que deve ser feito de forma autorizada e responsável. Observa-se também a referência à utilização de software obtido ou mantido sob forma ilegal. Por esse princípio o profissional estaria impedido de fazê-lo.

O princípio três tem a ver com a competência técnica do engenheiro de software. Diz que todos os esforços devem ser feitos em ordem de se obter um produto com o máximo de confiança e alto padrão profissional. É bem similar ao princípio cinco, porém, este tem outro enfoque que é o gerencial.

O quarto princípio diz que o engenheiro de software tem que estar apto a julgar de forma ética os eventos que venham ocorrer no dia a dia do seu trabalho. Inclusive há uma citação referindo-se que o profissional deve sempre considerar o fator humano nas questões em que uma decisão ética deve ser tomada.

Os princípios seis, sete e oito são similares entre si e referem-se, respectivamente, à profissão, aos colegas de trabalho e em última instância, ao próprio profissional. Este último diz que o engenheiro de software deve procurar continuamente seu aperfeiçoamento, tanto técnico quanto humano.

O que se pode perceber analisando os dois códigos de Ética é que, pela condição generalista das suas proposições, estes são basicamente aplicados de forma inspirativa pelos profissionais da área de computação. As situações propostas são sempre as ideais, como por exemplo, “não seja desonesto”, “não utilize software ilegal”. Agora tente aplicar isso a um

---

<sup>43</sup> Disponível na versão original em Anexo IV

caso em que o profissional, dependente do seu emprego, é obrigado por seu empregador a utilizar determinado programa (obtido ou mantido ilegalmente) para desempenhar determinada tarefa. A visão realista sobre o código de Ética, nesse caso, é que ele será sempre respeitado, enquanto for possível fazê-lo.

Porém, teoricamente, o código serve, sim, para promover inspiração e orientação, como propõem Michael Martin e Roland Schinzinger, em *Codes of Ethics*<sup>44</sup>. Segundo eles, o código de Ética deve ser mesmo o mais breve possível para que seja efetivo de fato. As especificidades deveriam ser apontadas pelas empresas, portanto, cada um adotando sua maneira de trabalhar, mas sempre tendo como *framework* o código de Ética.

Mas como os próprios autores relatam, a relativa incerteza provocada pelo pouco aprofundamento em cada caso tem seu lado negativo: a multiplicidade de interpretações. Nada impediria, portanto, que abusos fossem cometidos por empresas na elaboração de sua regimentação, já que contariam basicamente com seus sentidos de responsabilidade, somente.

Além disso, deve-se levar em consideração a geração de conflitos entre proposições do próprio código. Não há orientação nesse sentido a não ser seguir princípios morais próprios, o que pode levar a uma cadeia recursiva de dilemas morais. Essas distorções podem acontecer ainda de forma externa, ou seja, entre códigos produzidos por empresas distintas.

A questão é, enquanto não houver o embasamento jurídico necessário comentado no início deste capítulo, códigos de Ética apenas e tão somente servirão para orientar os profissionais em nível informativo.

---

<sup>44</sup> Artigo integrante da obra *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum

### 3 Pesquisa

#### 3.1 Procedimentos

Como segunda parte deste trabalho, desenvolveu-se uma pesquisa através de entrevista entre os estudantes da UFSC. A idéia foi elaborar um conjunto de questões<sup>45</sup> relacionadas à Ética e moral e aplicá-lo em dois grupos diferentes: os acadêmicos do curso de Sistemas de Informação e os demais acadêmicos da universidade reunidos num segundo grupo. O intento desse procedimento foi o de estabelecer uma comparação descritiva entre esses dois elementos e tentar estabelecer ligações com o que vem sendo discutido em torno de ética profissional e computacional.

O primeiro passo foi mensurar a população envolvida, ou seja, determinar a quantidade de alunos matriculados em cada centro do campus da Universidade Federal de Santa Catarina. Esta informação foi obtida com auxílio do Núcleo de Processamento de Dados<sup>46</sup> da UFSC, o que resultou no seguinte quadro:

**Tabela 1 – Número de acadêmicos por centro da UFSC em 2006/1**

<b>Centro</b>	<b>Alunos</b>
Ciências Agrárias - CCA	844
Ciências Biológicas - CCB	353
Comunicação e Expressão - CCE	2263
Ciências Jurídicas - CCJ	941
Ciências da Saúde - CCS	2413
Centro de Desportos - CDS	579
Ciências da Educação - CED	910
Centro Filosofia e Ciências Humanas - CFH	2273
Ciências Físicas e Matemáticas - CFM	2697
Centro Sócio-Econômico - CSE	3585
Centro Tecnológico - CTC	5591
<b>Total</b>	<b>22449</b>

<sup>45</sup> Os questionários encontram-se em anexo

<sup>46</sup> <http://www.npd.ufsc.br/>

Dentre os matriculados no Centro Tecnológico estão os do curso de Sistemas de Informação, que são o alvo da segunda parte da pesquisa. A tabela a seguir mostra esse dado:

**Tabela 2 – Número de acadêmicos do Centro Tecnológico em 2006/1**

<b>Centro Tecnológico</b>	<b>Alunos</b>
Outros cursos	5036
Sistemas de Informação	<b>555</b>
<b>Total</b>	5591

Decidiu-se por usar o método da amostragem aleatória simples para realizar as entrevistas, dado o tamanho da população consideravelmente grande. Uma avaliação por amostragem nada mais é que o estudo de uma porção representativa da população ao invés de tomá-la por inteiro. Segundo Barbetta, esse tipo de amostragem tem a propriedade de que “qualquer subconjunto da população, com o mesmo número de elementos, tem a mesma probabilidade de fazer parte da amostra”. (BARBETTA, 2002).

Para chegar ao tamanho da amostra a utilizar, segundo Barbetta, é preciso estipular o que se chama de *erro amostral tolerável*, que nada mais é do que “o quanto se admite errar na avaliação dos parâmetros de interesse”.

Para este trabalho adotou-se o valor de 10% como erro amostral tolerável. Este dado é aplicado à fórmula para o cálculo do tamanho mínimo da amostra mostrada a seguir:

$$n = N.n_0 / (N + n_0)$$

**Equação 1 – Cálculo do tamanho mínimo da amostra**

Onde:

N – tamanho da população;

n – tamanho da amostra;

$n_0$  – primeira aproximação para o tamanho da amostra ( $n_0 = 1 / E_0^2$ )

$E_0$  – erro amostral tolerável

Considerando os dados disponíveis para os acadêmicos da UFSC (sem os do curso de Sistemas de Informação), temos então a aplicação da fórmula:

$$n = (21894 \cdot (0,1)^2) / (21894 + 100) = 99,55$$

Portanto, de acordo com o valor da amostra calculado, é necessário, no mínimo, 100 entrevistas (arredondando) para que haja representatividade com o erro amostral em questão. De forma a manter a proporcionalidade de estudantes por centro, foi rearranjada a seguinte tabela:

**Tabela 3 – Valores de amostragem por centro**

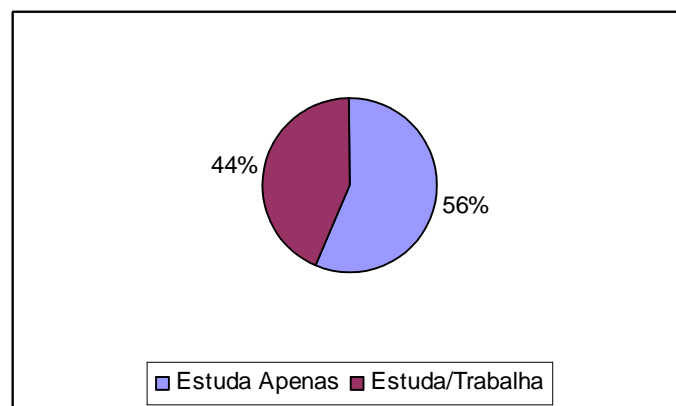
<b>Centro</b>	<b>Alunos</b>
Ciências Agrárias - CCA	3,84
Ciências Biológicas - CCB	1,60
Comunicação e Expressão - CCE	10,29
Ciências Jurídicas - CCJ	4,28
Ciências da Saúde - CCS	10,97
Centro de Desportos - CDS	2,63
Ciências da Educação - CED	4,14
Centro Filosofia e Ciências Humanas - CFH	10,33
Ciências Físicas e Matemáticas - CFM	12,26
Centro Sócio-Econômico - CSE	16,30
Centro Tecnológico - CTC	22,90
<b>Total</b>	<b>99,55</b>

No caso dos acadêmicos de Sistemas de Informação, optou-se por consultar aproximadamente metade das 555 pessoas matriculadas em situação regular, no intuito de se obter um resultado mais apurado do que simplesmente aplicar a técnica de amostragem.

### 3.2 Resultados Obtidos

#### 3.2.1 Questionário aplicado na UFSC (sem Sistemas de Informação)

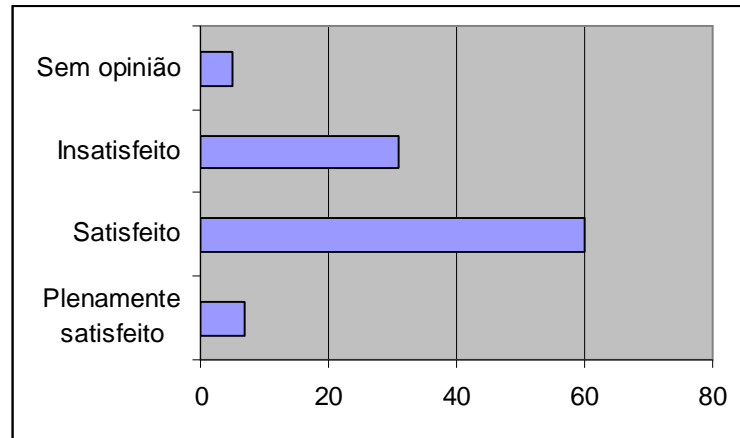
A primeira pergunta do questionário se refere à ocupação do acadêmico.



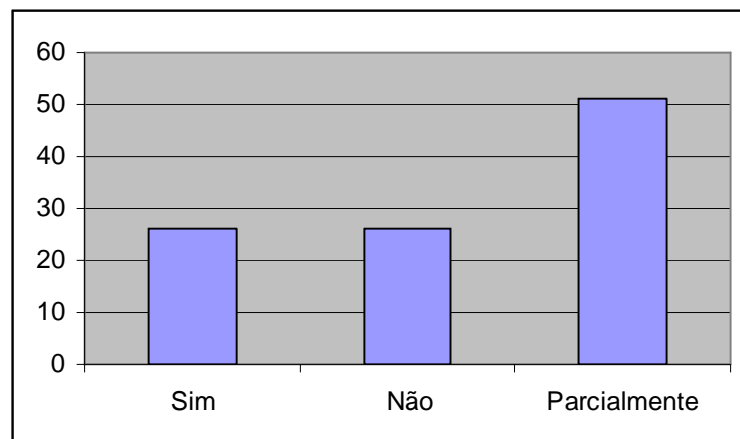
**Ilustração 1 – Ocupação dos acadêmicos**



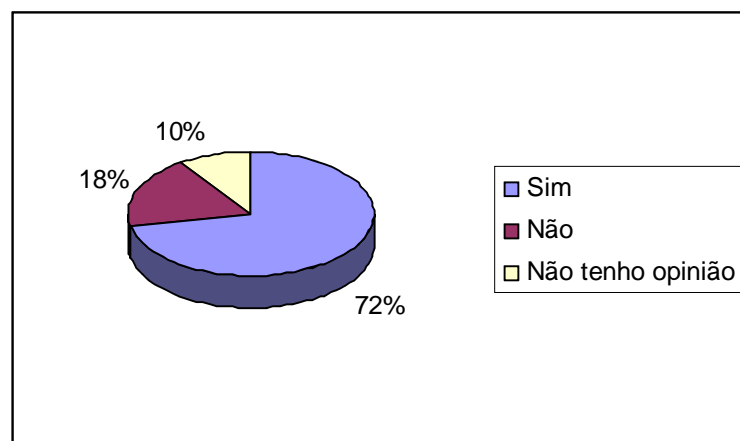
Pelo gráfico da *ilustração 1* é possível perceber que a maioria das pessoas apenas estuda, sem nenhuma ocupação extra, seja esta estágio ou emprego de qualquer natureza. No entanto, a diferença para aqueles que trabalham não é tão díspar a ponto de caracterizar a população como não-ativa.



**Ilustração 2 - Nível de satisfação em relação ao curso**

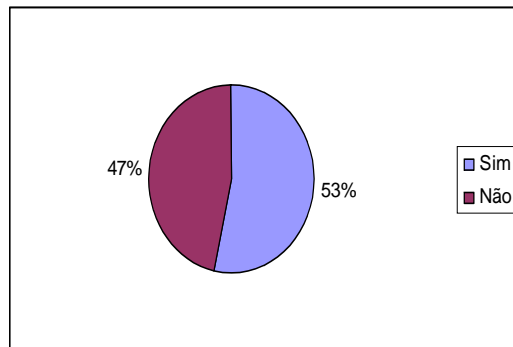


**Ilustração 3 – Capacidade de preparação ético-cidadã do curso (%)**

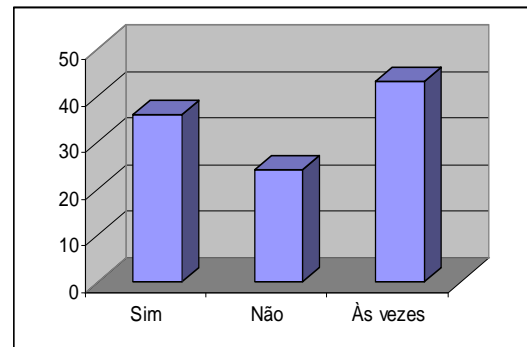


**Ilustração 4 – Necessidade de uma disciplina de Ética no curso**

Pelas duas ilustrações anteriores, nota-se que embora a maioria se considere satisfeita com o curso em que estuda (60%), aponta ainda para a deficiência deste em termos de formação ético-cidadã (mais de 50%). Isso se reforça pela preferência da necessidade de uma disciplina específica de Ética no curso (esmagadores 72%). Os gráficos a seguir se destinam a verificar se o acadêmico, embora identifique tais problemas em relação ao ensino da Ética, procura se manter informado sobre o assunto.

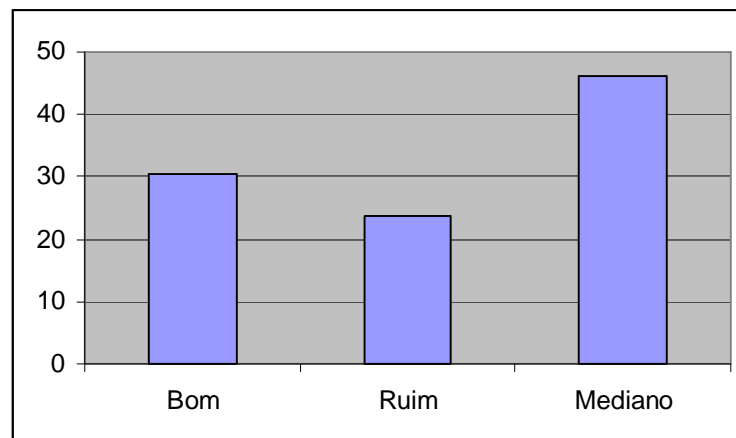


**Ilustração 5 – Ciência de um código de Ética na área**

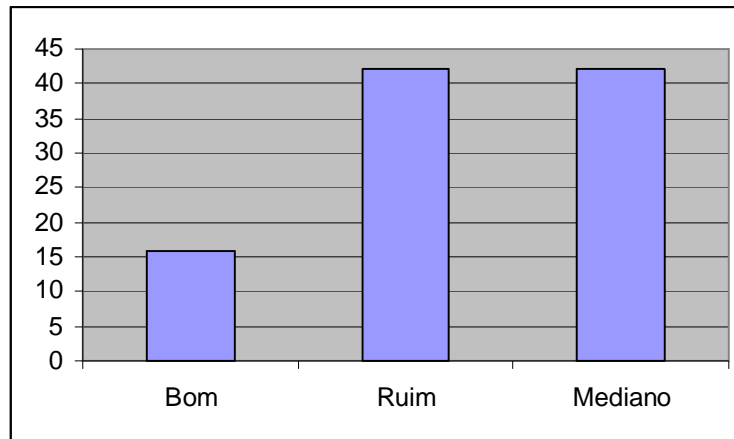


**Ilustração 6 – Frequência (%) de leitura sobre Ética**

O próximo gráfico mostra a relação entre aqueles que marcaram a necessidade da existência de uma disciplina sobre Ética no curso e a atual condição deste no que diz respeito à formação ético-cidadã oferecida. Em seqüência a este gráfico, está outro na mesma condição, mas para aqueles que acham tal disciplina não é requerida.



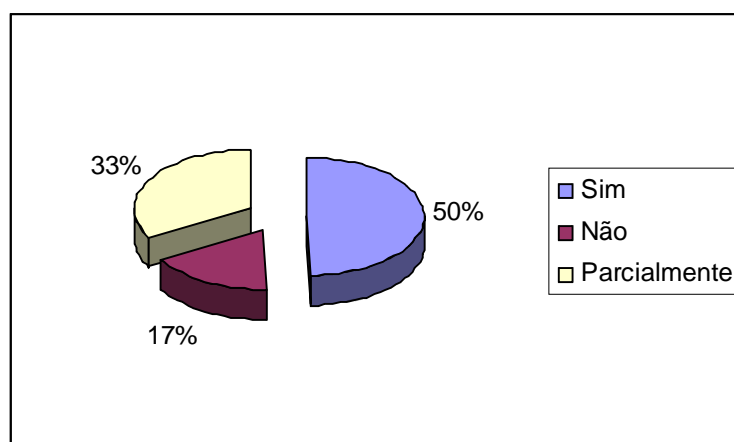
**Ilustração 7 - Nível de conhecimento ético oferecido pelo curso pelos defensores da existência de uma disciplina específica no assunto (%)**



**Ilustração 8 - Nível de conhecimento ético oferecido pelo curso pelos não defensores da existência de uma disciplina específica no assunto (%)**

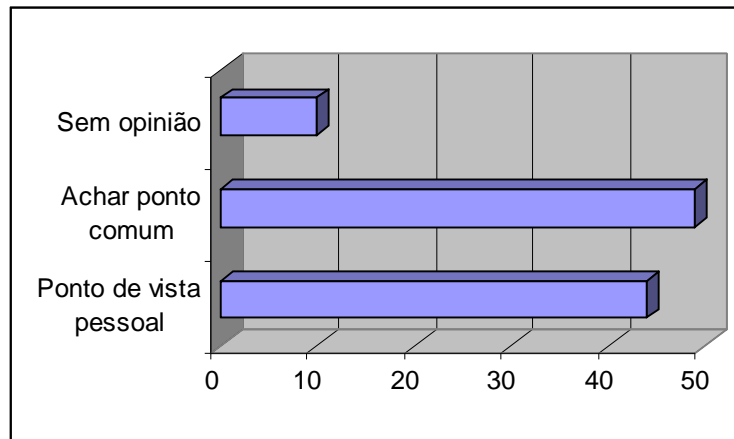
Vê-se no primeiro gráfico (entre aqueles que aprovam a existência de uma disciplina sobre Ética) que os acadêmicos, em sua maioria, apontam para um desempenho apenas mediano no que diz respeito ao conteúdo ético recebido no curso. Essa tendência é similar ao gráfico geral (o que não poderia ser muito diferente, já que representam a grande maioria). A surpresa veio com o gráfico daqueles que não acham importante ter a disciplina sobre Ética no curso. Esperar-se-ia um percentual maior do item “Bom”, considerando que a preferência pela por essa opção implicaria na não necessidade de uma disciplina sobre o assunto. No entanto, poderia também significar que os acadêmicos, optando, por exemplo, que assuntos éticos fossem abordados dentro de certas disciplinas (como se fosse um capítulo especial) não estivessem recebendo o conteúdo ao nível que esperavam.

O próximo gráfico mostra como os acadêmicos enxergam a diferença entre práticas que envolvem ou não uma discussão moral.



**Ilustração 9 - Consciência entre práticas que envolvem ou não discussões morais**

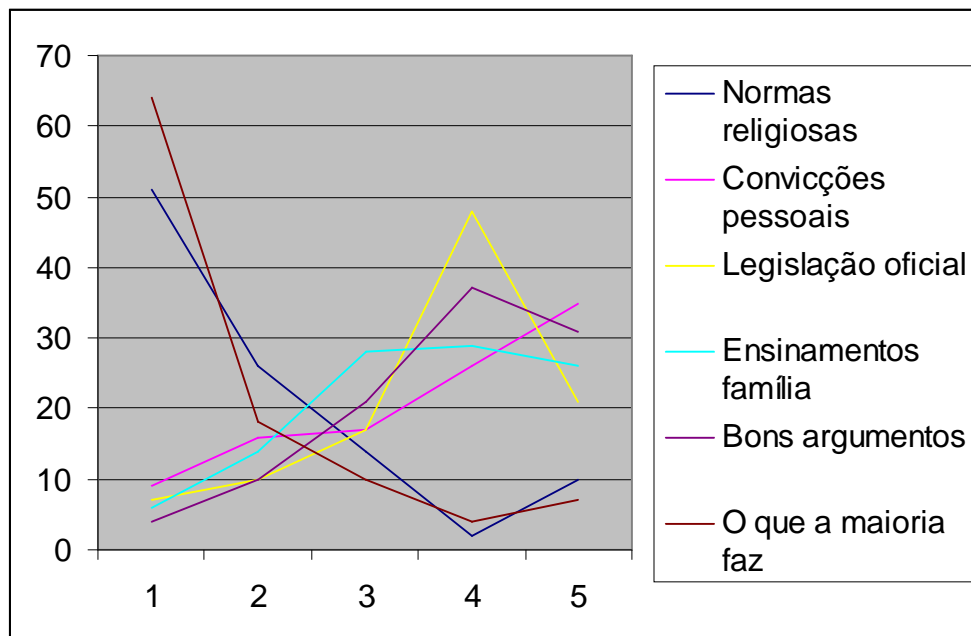
O resultado mostra que há uma parcela considerável de pessoas que não têm total clareza sobre a questão moral dos atos praticados, seja no cotidiano ou na vida profissional.



**Ilustração 10 – Entendimento sobre questões morais (em porcentagem)**

Mesmo com um percentual alto de não esclarecidos sobre a moral na prática, a maioria decidiu pelo coletivo ao fator individual.

A seguir estão os resultados referentes à questão que solicitou ao entrevistado que ordenasse os critérios que julgasse essenciais para o tratamento de problemas morais que aparecem na sociedade:



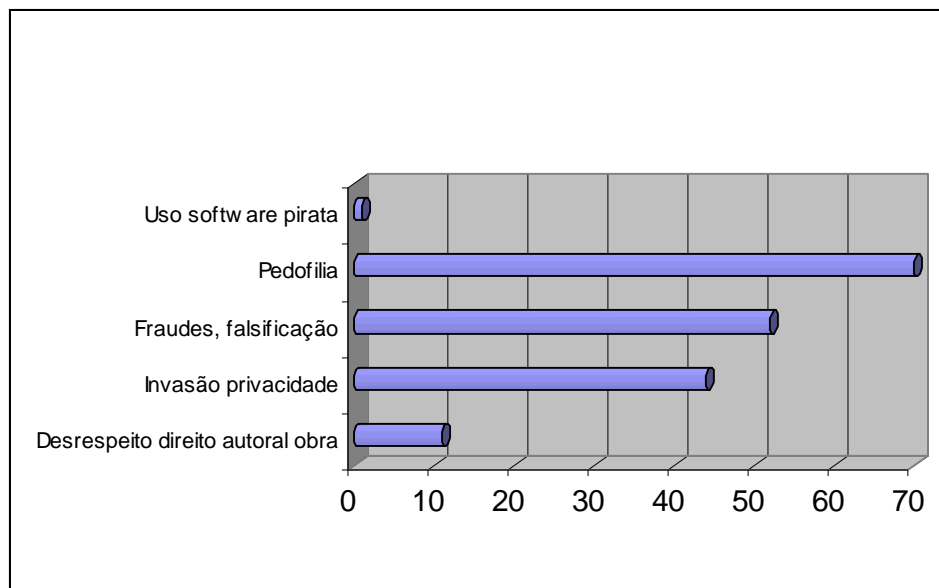
**Ilustração 11 – Avaliação de critérios morais (Num Pessoas x Critério)**

Pela ilustração é possível notar uma rejeição considerável à utilização de critérios baseados em normas religiosas, ou seja, houve uma boa parcela (praticamente 50%, considerando um total de 100 entrevistados) de pessoas que marcaram “1” ao classificar entre

1 e 5 o critério em questão. Porém, o maior percentual de rejeição foi, sem dúvida, atribuído à opção “o que a maioria faz”. Mas isso não vai contra ao questionamento anterior, onde houve uma inclinação para as decisões coletivas? Não necessariamente. O item “o que a maioria faz” pressupõe certo descaso com a avaliação crítica dos atos pela moral, diferentemente de uma discussão em grupo de forma consciente.

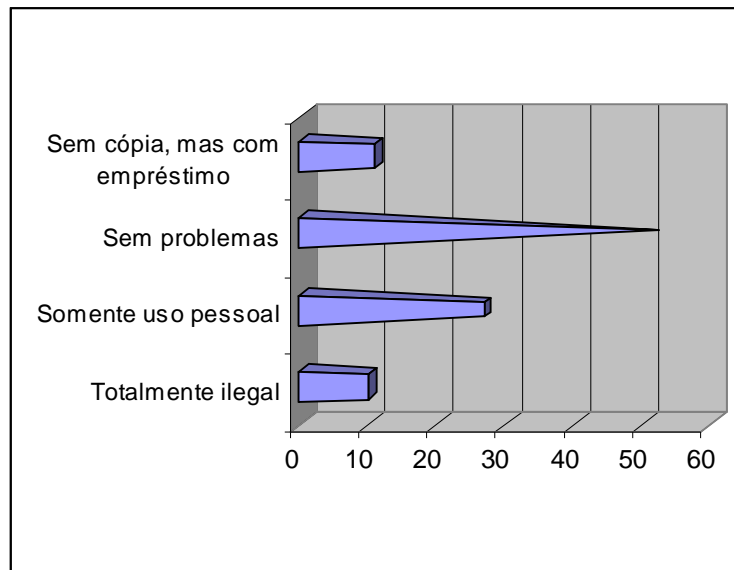
Percebe-se a importância dada pela avaliação baseada em legislação, bem classificada pelo critério de ordenação 4, apesar da queda no patamar seguinte. Os critérios “convicções pessoais” e “ensinamentos familiares”, em tese considerados subjetivos, obtiveram muito boa conceituação nas entrevistas entre os acadêmicos.

O critério mais nobre, em princípio, (“convicções justificadas por bons argumentos”), se é que se pode usar este tipo de classificação, esteve bem colocado no lugar esperado. Quando se diz que uma convicção é justificada por um bom argumento, nesse caso, pressupõe-se que a situação em questão foi ao menos analisada segundo algum critério moral válido.



**Ilustração 12 – Tipos de contravenções mais anti-éticas (número de pessoas)**

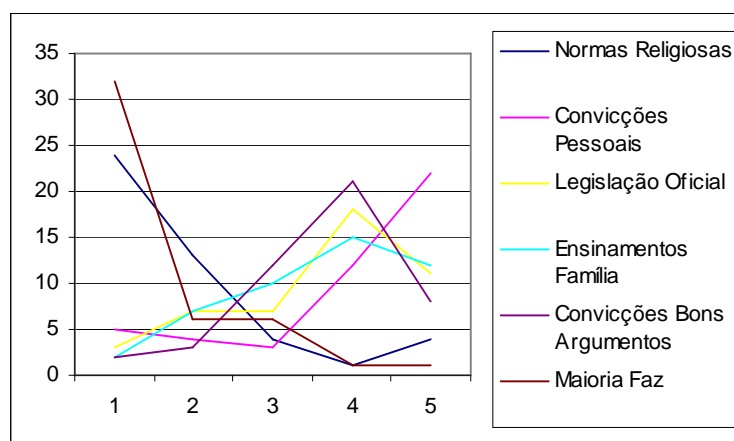
A questão do gráfico acima pedia que fossem marcadas no máximo duas contravenções das que estavam listadas. A primeira opção selecionada pelos entrevistados já era esperada (distribuição de material pedófilo). Percebe-se que os acadêmicos quase não consideram errados aqueles que usam softwares piratas, mas condenam os que praticam o ato da falsificação e fraudes. Ficou clara a preocupação com o individual no sentido de apenas reprovar itens que vão contra o coletivo (pedofilia, fraudes e falsificações e invasão de privacidade). (não entendi o argumento??).



**Ilustração 13 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (%)**

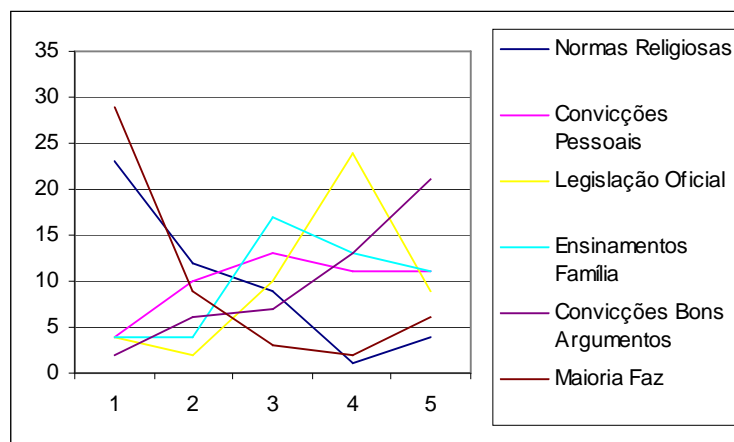
Nota-se que a maioria não vê problemas em transformar áudio e ainda repassá-lo a terceiros. As opções restritivas (“sem cópia, mas com empréstimo” (sob condição deste também não copiar) e “totalmente ilegal”) ficaram bem atrás das mais liberais. É o retrato atual da indefinição sobre direitos autorais relativos ao conteúdo digital e possivelmente um recado claro dos usuários relacionado ao uso justo.

A seguir, mostra-se o gráfico dos acadêmicos que assinalaram que cada um tem seu ponto de vista, quando se trata de questões morais, cruzado com os critérios que utilizam para julgá-las.



**Ilustração 14 – Pessoas que assinalaram que, em se tratando de questões morais, cada um tem seu ponto de vista, e seus critérios que utilizam para julgá-las**

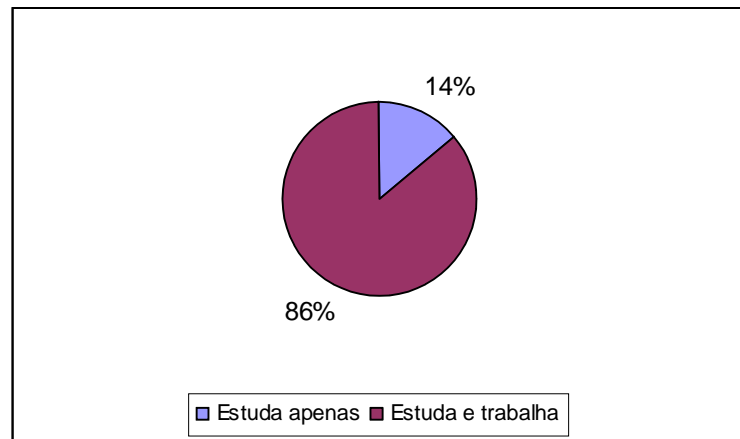
É possível perceber que os critérios “normas religiosas” e “O que a maioria faz” foram cotados com os escores mais baixos e a partir daí só caíram. O critério que se esperaria forte, entre os acadêmicos que acreditam que as questões morais dependem do ponto de vista pessoal de cada um, seria “convicções pessoais”, o que realmente se confirmou. Apesar do item “convicções justificadas com bons argumentos” apresentar uma boa escalada entre os escores 2 e 4, no quinto apresentou queda, ao passo que “convicções pessoais” continuou firme. Nota-se também que “legislação oficial” seguiu de perto estes dois últimos, assim como “ensinamentos da família”. Esses são a base teórica e empírica de cada um no que se trata de questões morais.



**Ilustração 15 - – Pessoas que assinalaram que, em se tratando de questões morais, deve-se discutir e chegar a um ponto comum, e seus critérios que utilizam para julgá-las**

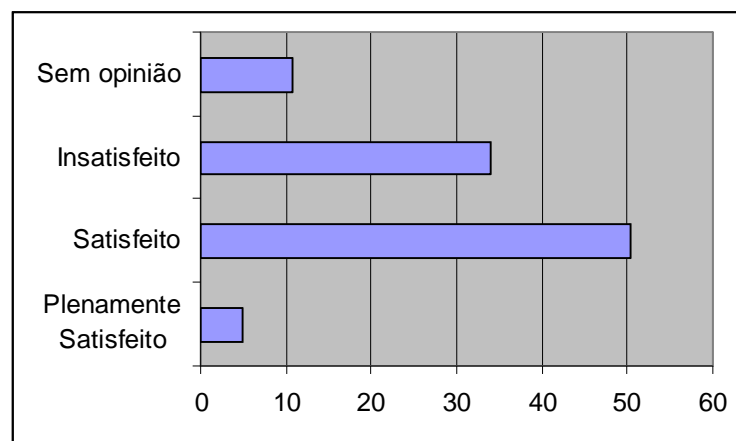
O item esperado, nesse caso, seria “convicções justificadas com bons argumentos” (o que se confirmou), pois pressupõem uma discussão prévia do impasse antes de tomar uma decisão. Novamente “normas religiosas” e “o que a maioria faz” foram mal cotados. Nota-se ainda que “legislação oficial” apresentou um crescimento constante até o escore 4 e depois uma queda quase abrupta no último.

### 3.2.2 Questionário aplicado no curso de Sistemas de Informação

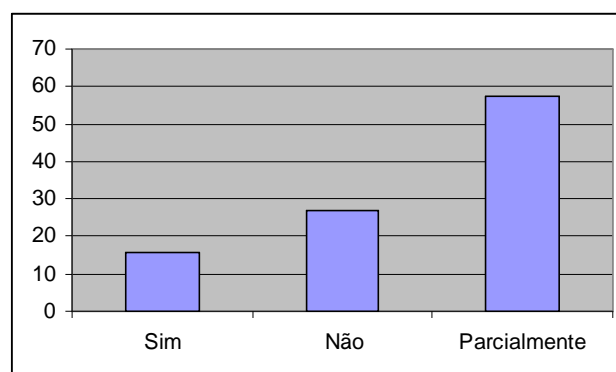


**Ilustração 16 - Ocupação dos acadêmicos de Sistemas de Informação**

Observa-se que o perfil dos acadêmicos de Sistemas de Informação em relação ao trabalho é bem diferente se comparado ao resto da UFSC. Apenas 14% das pessoas entrevistadas dedicam-se exclusivamente aos estudos, sem nenhum trabalho ou estágio.

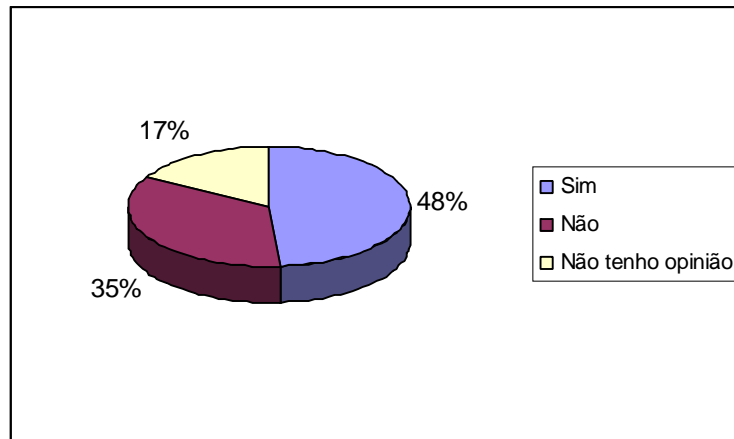


**Ilustração 17 – Nível de satisfação em relação ao curso de Sistemas (%)**



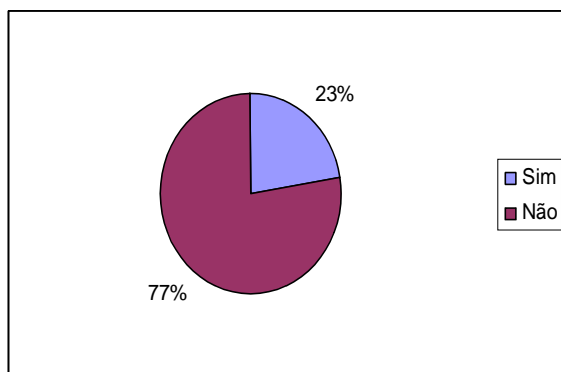
**Ilustração 18 – Capacidade de preparação ético-cidadã do curso de Sistemas (%)**



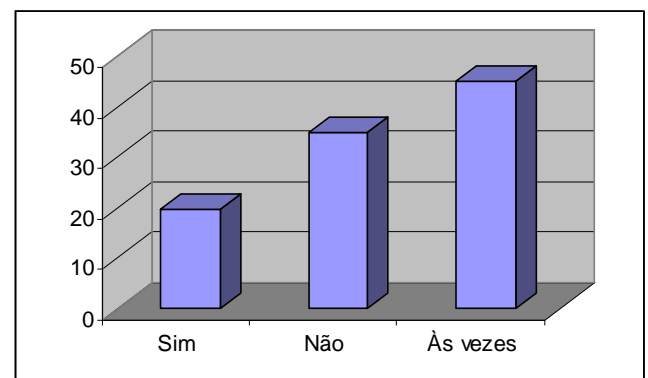


**Ilustração 19 – Necessidade de uma disciplina de Ética no curso de Sistemas**

Da mesma forma como no resto da UFSC, em Sistemas de Informação a maioria se declara satisfeita com o curso, mas acha que há deficiência no que diz respeito à formação ético-cidadã oferecida. Já o fato de se ter uma disciplina específica no assunto é vista com olhos mais conservadores, considerando que 48% são a favor e 35% contra, com um nível de indecisos relativamente alto (17%).



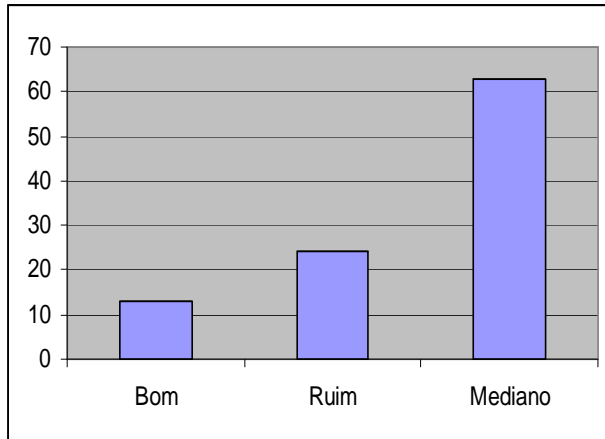
**Ilustração 20 – Ciência de um código de Ética na área**



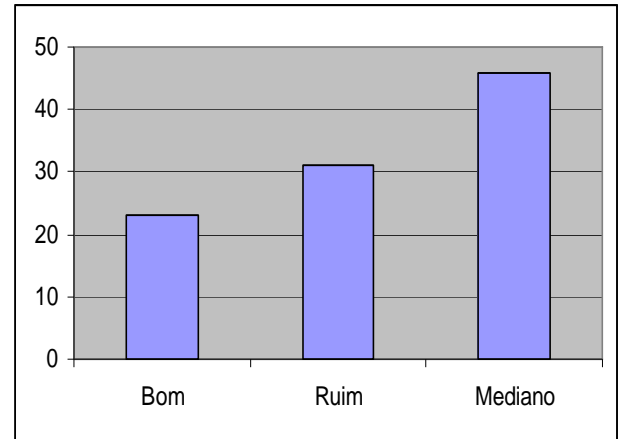
**Ilustração 21 – Frequência de leitura sobre Ética (%)**

A ilustração 20 mostra o contraste entre a esfera de Sistemas e as restantes. No resto da UFSC há certo equilíbrio entre a ciência ou não de um código de Ética da área, ao passo em que Sistemas a predominância pelo não conhecimento é bem maior. A leitura de obras no assunto também apresenta dados piores, o que pode explicar o certo desinteresse na área da Ética.

Do mesmo jeito que anteriormente, serão comparadas as respostas obtidas nas questões referentes à necessidade ou não da existência de uma disciplina sobre Ética no curso, com as obtidas ao perguntar se o curso está proporcionando uma formação ético-cidadã adequada.

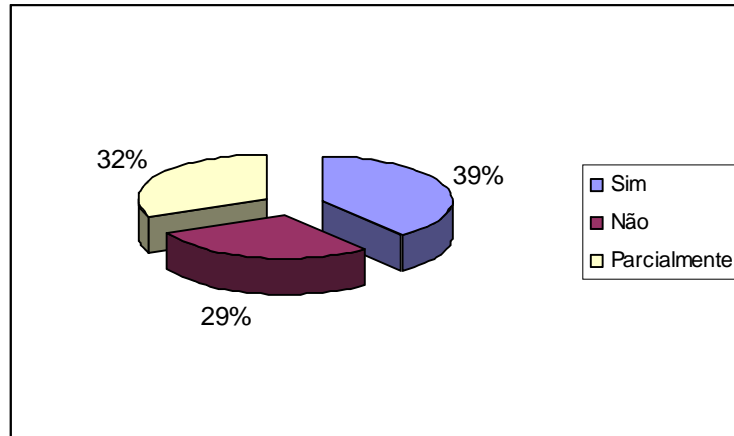


**Ilustração 22 – Nível de conhecimento ético em Sistemas de Informação, pelos defensores da existência de uma disciplina específica no assunto (%)**



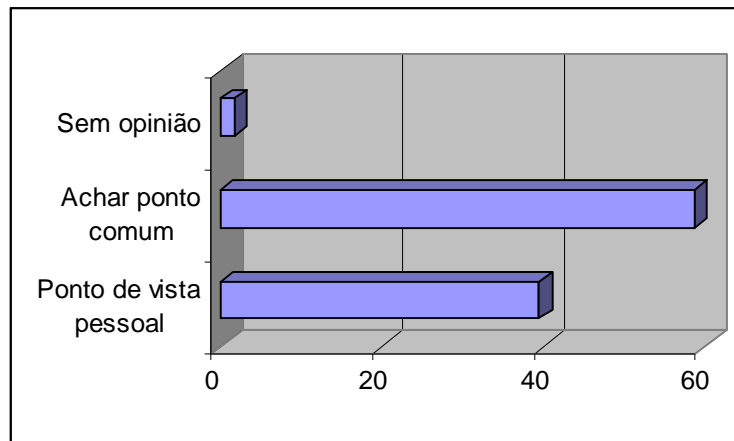
**Ilustração 23 - Nível de conhecimento ético em Sistemas de Informação, pelos não defensores da existência de uma disciplina específica no assunto (%).**

Os dois gráficos são bem parecidos entre si, mostrando que o curso não tem agradado à maioria de forma satisfatória no que se refere ao ensino da Ética em Sistemas de Informação. Independente de se ter ou não uma disciplina específica no assunto, tanto para Sistemas quanto para o restante dos cursos, revela-se que ainda há pontos a melhorar.



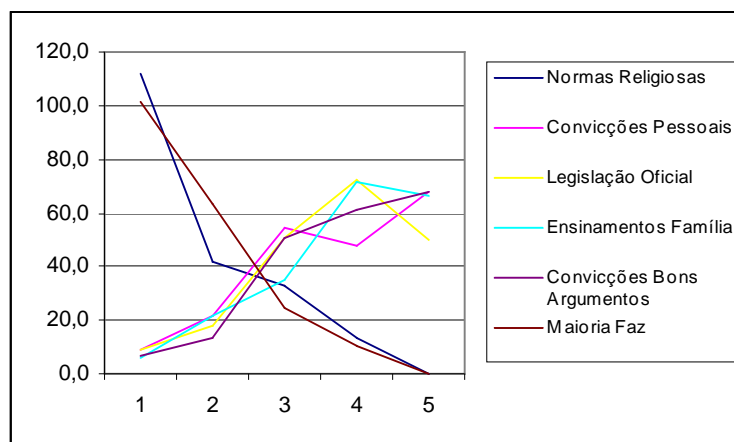
**Ilustração 24 – Consciência entre práticas que envolvem ou não discussões morais (Sistemas de Informação).**

A margem entre as pessoas que conhecem ou não a diferença entre práticas que envolvem ou não discussões morais é mais estreita nesse caso. Isso é particularmente preocupante no sentido que há a tendência de agir sem necessariamente levar em conta as conseqüências que a ação em questão possa trazer para si mesmo e para os que o cercam.



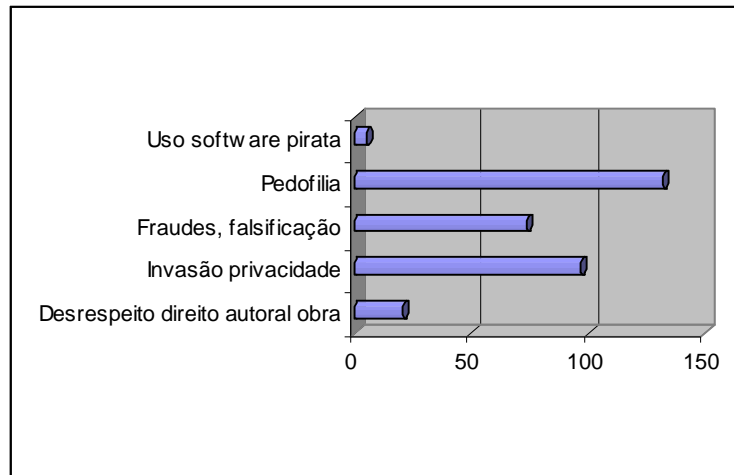
**Ilustração 25– Entendimento sobre questões morais em Sistemas de Informação (%).**

Percebe-se que a porcentagem de pessoas sem opinião clara sobre o assunto caiu em Sistemas de Informação. Mas, do mesmo jeito que antes, a discussão em grupo em busca de um ponto em comum continua na dianteira.



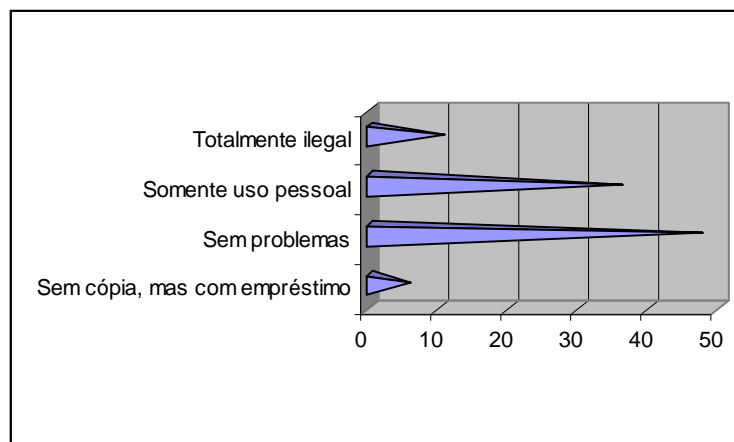
**Ilustração 26 – Avaliação de critérios morais em Sistemas de Informação (Num. Pessoas x Critério).**

Temos duas situações bem curiosas aqui. Primeiro a quase linearidade decrescente na avaliação dos critérios “normas religiosas” e “o que a maioria faz”. Apesar de ser uma tendência observada no restante da UFSC, aqui ficou bem reforçada. Segundo, a convergência dos outros critérios para mais ou menos o mesmo ponto do gráfico. Num aspecto geral foi surpreendente que isso tenha acontecido, revelando a variedade de fontes que os acadêmicos levam em questão em se tratando de avaliar uma situação.



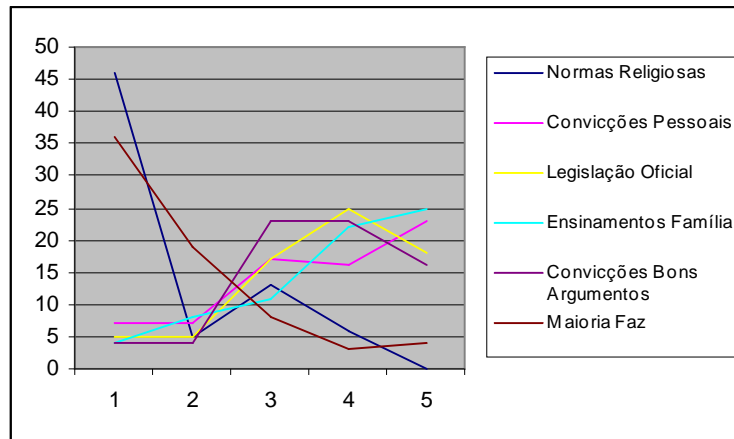
**Ilustração 27 – Tipos de contravenções mais anti-éticas para Sistemas de Informação (Num. Pessoas).**

O gráfico para Sistemas ficou bem parecido com o restante da UFSC, com exceção da inversão de posições entre “fraudes e falsificações” e “invasão de privacidade”, reforçando o aspecto individualista dos acadêmicos. O gráfico a seguir também tem resultado similar fora do curso de Sistemas de Informação, como se pode observar.

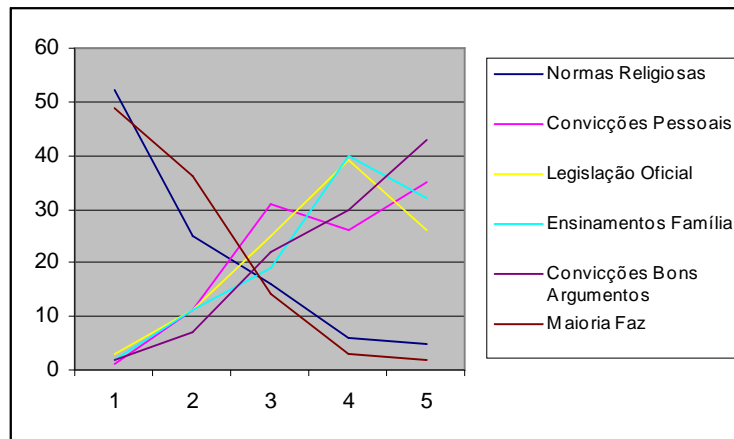


**Ilustração 28 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (%)**

A seguir estão cruzadas as questões referentes ao entendimento das questões morais (ponto de vista individual ou coletivo) e ao uso dos critérios mais relevantes na resolução dos problemas envolvendo conflitos morais.



**Ilustração 29 - Pessoas que assinalaram que, em se tratando de questões morais, cada um tem seu ponto de vista, e seus critérios que utilizam para julgá-las (Sistemas de Informação)**



**Ilustração 30 – Pessoas que assinalaram que, em se tratando de questões morais, deve-se discutir e chegar a um ponto comum, e seus critérios que utilizam para julgá-las (Sistemas de Informação)**

Em ambos os gráficos observa-se a pouca validade dada pelos acadêmicos de Sistemas de Informação aos critérios religiosos e também ao que a maioria faz. É possível perceber que aqueles que preferem uma discussão em busca de um ponto comum têm um desenho mais parecido com o gráfico geral, e, assim como no caso do restante dos cursos, há uma predominância de “convicções fundamentadas por bons argumentos”. No caso do primeiro gráfico, referente às convicções pessoais, nota-se que tem um desempenho bem parecido com o anterior, com exceção de que “ensinos da família” tem um desempenho levemente melhor.

#### 4 Considerações Finais

Seria pretensão querer finalizar a discussão sobre Ética computacional com apenas um trabalho. É um campo tão inexplorado que mesmo os princípios básicos já definidos são discutíveis dependendo do prisma da observação. Mas mesmo dessa forma é interessante apontar alguns itens que puderam ser observados.

Dois fatores têm colaborado para a multiplicação da complexidade da delimitação dos preceitos éticos: a evolução do hardware, das mídias de armazenamento e a internet. São os meios que massificaram a troca de arquivos, seja de forma legal ou não. Mas o que é eticamente legal tratando-se de software? A cultura que predomina é a de que o total controle do produto deva estar “nas mãos” daquele que o fez. Os chamados gerenciamentos das propriedades intelectuais são, infelizmente, baseados na linha de pensamento da Revolução Industrial. Os consumidores eram limitados a manusear exclusivamente aquilo que conseguiam obter dos fornecedores, ou seja, não havia como “tratar” o produto, criar novas coisas a partir dele. Enfim, era do jeito que os produtores sempre desejavam: uma “folha impressa em fonte de jornal” somente poderia ser obtida de quem a manufaturasse. A modernização dos equipamentos, a introdução do computador, da internet, mudaram totalmente as possibilidades. Qualquer um pode criar seu próprio jornal on line, imprimi-lo tão igual ou melhor ao que é distribuído nas bancas, produzir seu próprio filme independente, produzir seu próprio software.

Mas o que aconteceu com os produtores? Continuaram a achar que estávamos na época da Revolução Industrial e, como tal, impõem regras que agridem o livre desenvolvimento da criatividade. Essa divergência de ideologias tem gerado muitos conflitos e por consequência, muita indefinição do que pode ser considerado como correto ou não no que concerne à Ética computacional e direitos autorais.

Mas os produtores não esperneiam à toa ou totalmente sem razão. Ninguém gosta de ter seu trabalho “roubado” e usado de forma diferente do que tinha pensado desde o início. Afinal de contas, não há como concordar que pessoas que copiem o software de alguém de forma não autorizada passem a lucrar sem nenhum mérito. Isso embora haja alternativas interessantes como a adoção do copyleft e do chamado uso justo – no caso do uso justo nem toda a cópia seria ilegal, dependendo da situação.

E o que dizer da informação pessoal? A quem pertence? Àquele que se diz empregador e, portanto, se acha no direito de verificar toda a correspondência pessoal dos seus

empregados simplesmente pelo fato destes usarem os equipamentos da empresa? Ou à empresa fornecedora de serviços que registra cada movimento dos seus clientes, seja de forma on line (através da navegação no web site da empresa, por exemplo) ou das compras que eles efetivamente realizam ou não? Há quem defenda que a informação pessoal deva ser o que o nome sugere: pessoal. Então, se a partir da informação pública é possível deduzir a informação privada, a partir do momento que essa dedução pode ser realizada de forma a obter consistência, passa a pertencer àquele que está sendo referenciado. É interessante que ao passo em que a modernização dos meios de comunicação trouxe à tona o obsoletismo do gerenciamento de direitos autorais, no que se refere à privacidade vem exatamente no sentido contrário, mais conservador. Mas nesse entremeio existem aqueles que não concordam com esse conservantismo e acham que informação alguma deva ser omitida do conhecimento público: *hackers*. Amados por uns, odiados por outros, são comumente confundidos com arruaceiros e propagadores de pragas pela internet. *Crackers* e seu desdobramento amador – os *script kiddies* – são os vilões da estória da invasão virtual e conectam-se à internet com o propósito maléfico de destruir, fraudar e roubar. Movidos por uma espécie de sentimento de impunidade proporcionado pelo aparente anonimato da internet – resultantes do ciberespaço – tomam liberdades que possivelmente nunca as fariam no mundo real. E isso independente de ser hacker ou cracker. Na verdade a chamada ética hacker tem alguns pontos que não convencem o público leigo e muito menos os mais céticos. Mas mesmo estes últimos concordam que os hackers são importantes na medida em que podem detectar falhas em sistemas contribuindo para o aumento da segurança do produto final. Essa é, no entanto, uma medida contraditória já que seus serviços ora são tidos como antiéticos ora de estimada importância.

Mas o que fazer para que não sejam cometidos atos considerados antiéticos no mundo dos computadores (ou pelo menos que haja punição para quem os cometer)? Seria necessária uma normatização mais consistente e pró ativa para que usuários de tecnologia pensassem duas vezes antes de fazer algo? O problema disso é que não é possível – ou viável – estabelecer limites precisos em cada situação analisada. Um controle rígido implicaria possivelmente na perda do livre arbítrio na internet, da liberdade de expressão, até. Acredita-se que por essa razão muitos ainda consideram a auto-regulamentação o melhor caminho para controlar os abusos que acontecem na internet. As chamadas políticas de privacidade, costumeiramente referenciadas por inúmeras empresas como uma garantia, um atestado de idoneidade ao público que utiliza seus serviços, são falhas no sentido de depender da linha de pensamento da organização – que pode conter distorções (vide caso Yahoo! e Google).

Apoiando as políticas de privacidade, os códigos de Ética entrariam com um suporte a nível mais básico e teórico. Tidos como generalistas e frequentemente com cláusulas conflitantes entre si mesmas, servem mais como um guia de conduta àquele que se vê frente dilemas morais durante a vida profissional ou não, ao manipular computadores. No fim, o que acaba realmente valendo é a lei com valor jurídico, e daí a necessidade de estudar melhor o assunto, mapear as adversidades e então partir para uma regulamentação mais específica na área (ou pelo menos uma tentativa de fazê-lo).

Sobre os questionários, estes foram aplicados com o intuito de se ter uma noção de como o acadêmico da UFSC enxerga a situação sobre a Ética na profissão. Porém, o foco residiu mais nos acadêmicos de Sistemas de Informação, que além de usuários possivelmente serão profissionais na área de computação e lidarão com diversas situações em que alguma decisão moral tenha de ser tomada.

Sistemas de Informação tem um perfil de pessoas diferente do resto da universidade, no sentido de que são, em sua grande maioria, pessoas que conciliam trabalho e estudos. Isso pode ter refletido no desenvolvimento de “técnicas” baseadas na experiência, por exemplo, para resolver conflitos morais diversos. O gráfico geral de critérios usados para avaliar esses conflitos foi bem balanceado nos critérios “convicções pessoais”, “legislação oficial”, “ensinamentos familiares”, “convicções baseadas em bons argumentos”. Embora no resto da UFSC essa tendência seja também observada, talvez tenha sido motivada não tanto pelo empirismo, mas por algum *background* teórico, já que são pessoas que lêem mais sobre Ética e optam com mais certeza pela existência de uma disciplina específica sobre o assunto no currículo.

Os critérios “normas religiosas” e “o que a maioria faz” foram avaliados sempre como não confiáveis para discussão sobre valores morais, tanto na UFSC quanto em Sistemas de Informação. Tratando-se do primeiro item, não foi um resultado tão inesperado assim, já que em meios acadêmicos há uma tendência natural, num aspecto geral, em refutar argumentos baseados em princípios religiosos. Mas não se deve esquecer que em muitos casos os ensinamentos familiares são fortemente baseados em preceitos de religiões diversas. Frequentemente foi encontrado um item “extra” de mensuração – “0” (zero) - de critério (e assinalado) na folha do questionário, ao lado esquerdo do escore “1”.

A respeito das contravenções, observou-se pouca atenção com a questão de direitos autorais. Melhor dizendo, diante de proposições como “pedofilia”, “invasão de privacidade” e “fraudes e falsificações diversas”, tornou-se menos atraente - ou até menos “necessário” – apontar fatores ligados a direito de propriedade intelectual. Isso pode pressupor que mesmo



no mundo virtual da computação costumamos aplicar os princípios básicos da forma hierárquica com que fazemos no mundo dito real. Distribuir material pornográfico pela internet é algo que causa repulsa à maioria das pessoas, assim como ter sua conta bancária invadida também poderia ser. Apesar de certas correntes da Ética apontarem esse fato como uma característica individualista e egoísta (a Ética Estóica diz que nos indignamos com situações como as apresentadas não pelo fato de estarmos preocupados com o semelhante, mas pelo desejo de que não aconteçam conosco), manifesta-se o desejo primário pelo estabelecimento do bem comum (e por consequência, o próprio). Isso não quer dizer que direitos de propriedade intelectual sejam mais ou menos importantes que a perda da privacidade por efeito de uma invasão, por exemplo. Porém, na prática, o que pode acontecer é uma priorização de princípios.

A última pergunta do questionário tratava exclusivamente de direitos autorais. A maioria decidiu que transformar áudio de um cd comercial para o formato mp3 ou similar e ainda cedê-lo a terceiros é algo normal, tanto para Sistemas de Informação quanto para o restante da UFSC. Isso não pressupõe distribuição em massa de conteúdo protegido, mas apenas que possa ser considerado como o uso justo de algo adquirido legalmente. A segunda corrente, segundo os acadêmicos, é de que apenas deva ser feito um backup pessoal, sem direito a empréstimos. Nesse quesito é complicado dizer quem está certo ou errado, se é que há como fazê-lo. Produtores e consumidores brigam como vizinhos que disputam onde colocar a cerca que delimita o território de ambos. Sabe-se que o conteúdo digital não pode ser tratado como “mercadoria física”, como querem os produtores e nem como totalmente “abstrata” como quer a maioria dos consumidores. Como já referenciado, alternativas extras não faltam (como o copyleft, por exemplo). Assim como na definição de direitos autorais, a área ético-computacional como um todo carece de um melhor estudo e atenção. Do resultado desse estudo mudanças significativas nas vidas das pessoas podem acontecer, já que estamos caminhando inevitavelmente para a total dependência da automatização computacional dos processos.

## 5 Bibliografia

BARBETTA, Pedro Alberto. **Estatística Aplicada às Ciências Sociais**. Florianópolis: Ed. da UFSC, 2002

BARROCO, Maria Lucia Silva. **Ética e Serviço Social: Fundamentos Ontológicos**. São Paulo: Cortez, 2003.

BERLEUR, Jacques; BRUNNSTEIN, Klaus. **Ethics of Computing**. Londres, Inglaterra: Chapman & Hall, 1996.

BERLEUR, Jacques; WHITEHOUSE, Diane. **The Ethical Global Information Society – Culture and democracy revisited**. Londres, Inglaterra: Chapman & Hall, 1997.

CAMARGO, Marculino. **Fundamentos de Ética Geral e Profissional**. Petrópolis, RJ : Vozes, 1999.

DIBONA, Chris; OCKMAN, Sam; STONE, Mark; BEHLENDORF, Brian. **Open Sources: Voices from the Open Source Revolution**. California, USA: O'Reilly & Associates, Inc, 1999.

FERREL, FRAEDRICH & FERREL. **Ética Empresarial: Dilemas, Tomadas de Decisões e Casos**, Rio de Janeiro, Brasil: Reichmann & Afonso, 2001.

FORESTER, Tom; MORRISON, Perry. **Computer Ethics**. Massachusetts, EUA: The MIT Press, 1993.

HEXSEL, Roberto A. **Software Livre**. Departamento de Informática da Universidade Federal do Paraná, 2003.

HIMANEN, Pekka. **A Ética dos Hackers e o Espírito da Era da Informação**. Editora Campus, 2001.

JOHNSON, Deborah G.; NISSENBAUM Helen. **Computers, Ethics & Social Values**. USA: Prentice Hall, Inc, 1995.

LESSIG, Lawrence. **Cultura Livre – Como a mídia usa a tecnologia e a lei para barrar a criação cultural e controlar a criatividade**. New York, USA: The Penguin Press, 2003.

MASIERO, Paulo César. **Ética em Computação**. São Paulo: Editora da Universidade de São Paulo, 2000.

MING, Wu. **O Copyleft explicado às crianças**. Ano: 2003. Disponível em: [www.wumingfoundation.com](http://www.wumingfoundation.com)

MITNICK, Kevin D.; SIMON William L. **Mitnick – A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação.** São Paulo: Pearson Education, 2003.

NALINI, José Renato. **Ética Geral e Profissional.** São Paulo: Editora Revista dos Tribunais, 2001.

RAUBER, Jaime José; ZANATTA, Alexandre Lazaranetti. “A Ética na Computação: Uma análise descritiva justifica sua presença”. Rio Grande do Sul: Universidade de Passo Fundo.

STALLMAN, Richard M. **Free Software, Free Society: Selected Essays of Richard M. Stallman.** Boston, USA: GNU Press, 2002.

STERLING, Bruce. **The Hacker Crackdown: Law and Disorder on the Electronic Frontier.** New York, USA, 1993.

VALLS, Álvaro L.M. **O que é Ética.** São Paulo: Editora Brasiliense S.A., 1986.

VÁRIOS. **Serviço Social e Ética: convite a uma nova práxis.** São Paulo: Cortez, 2003.

VAZQUES, Adolfo Sanches. **Ética.** Rio de Janeiro: Civilização Brasileira, 1970.

ZILLI, Daniel. **Mundo Livre – 3ª Edição.**

WILLIAMS, Sam. **Free as in Freedom: Richard Stallman’s Crusade for Free Software.** California, USA: O’Reilly & Associates, Inc, 2004.

## 6 Anexos

### **Anexo I – Questionário sobre Ética para acadêmicos de Sistemas de Informação**

**1. Atualmente, sua ocupação é:**

- autônomo
- estuda apenas
- estuda e trabalha (estágio)
- estuda e trabalha (emprego fixo)

**2. Quanto ao nível de satisfação em relação ao curso de Sistemas de Informação da UFSC, você diria que se sente (ou sentiu):**

- plenamente satisfeito
- satisfeito
- insatisfeito
- não tenho opinião formada

**3. Na sua opinião, há necessidade de uma disciplina específica sobre ética no curso de Sistemas de Informação?**

- sim
- não
- não tenho opinião a respeito

**4. Você tem conhecimento da existência de um Código de Ética específico da área da computação a nível nacional ou internacional?**

- sim
- não

**5. Você considera que os conhecimentos adquiridos no curso de Sistemas de Informação foram (são) suficientes no que diz respeito à formação ético-cidadã, tratando-se do seu desempenho profissional?**

- sim
- não
- parcialmente

**6. Você conhece a diferença entre práticas que envolvem e práticas que não envolvem uma discussão moral?**

- sim
- não
- parcialmente

**7. Você costuma ler artigos de jornais ou revistas que tratam de questões éticas?**

- sim
- não
- às vezes

8. **Alguém que, alcoolizado, sai dirigindo um carro e mata uma pessoa sem intenção, deve sentir-se moralmente responsabilizado pela morte daquela pessoa?**

- sim  
 não  
 depende da situação

9. **Qual o seu entendimento sobre questões morais?**

- Cada um tem o seu ponto de vista  
 Deve-se discutir o problema para chegar-se a um ponto de vista comum  
 Não tenho opinião formada

10. **Na sua opinião, um Código de Ética e Conduta Profissional é essencial para o bom andamento de uma profissão?**

- sim  
 não

11. **Frente a problemas morais que aparecem na sociedade, que critério você usa ou usaria para julgá-los? (Indique sua preferência por cada uma delas, atribuindo uma nota de 1 a 5, sendo 1 o valor mínimo e 5 o máximo). Observa-se que é possível marcar dois ou mais itens com a mesma nota.**

Itens	Aspectos avaliados	Nota				
a)	Normas religiosas	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
b)	Convicções pessoais	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
c)	Legislação oficial	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
d)	Ensinamentos aprendidos na família	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
e)	Convicções justificadas com bons argumentos	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
f)	O que a maioria faz	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

12. **Qual tipo de contravenção você acha mais antiética hoje em dia (cite duas, no máximo)?**

- Desrespeito aos direitos autorais de obras  
 Invasão de privacidade para tomar posse de dados confidenciais  
 Fraudes, falsificações diversas  
 Pedofilia  
 Uso de software pirata

13. **Posso, ao comprar um cd de áudio, transformar seu conteúdo para mp3 (ou similar) para que seja compatível com outros equipamentos (mp3 player, por exemplo)? Posso ainda cedê-lo a terceiros?**

- De jeito nenhum. É totalmente ilegal.  
 Sim, desde que seja para uso pessoal. Ceder a terceiros, nem pensar.  
 Sim, não há problema algum.  
 Não posso copiar, mas posso emprestá-lo sob a condição de que não copiem.

## **Anexo II - Questionário sobre Ética para acadêmicos da UFSC**

**1. Atualmente, sua ocupação é:**

- autônomo
- estuda apenas
- estuda e trabalha (estágio)
- estuda e trabalha (emprego fixo)

**2. Quanto ao nível de satisfação em relação ao seu curso na UFSC, você diria que se sente (ou sentiu):**

- plenamente satisfeito
- satisfeito
- insatisfeito
- não tenho opinião formada

**3. Na sua opinião, há necessidade de uma disciplina específica sobre ética no seu curso?**

- sim
- não
- não tenho opinião a respeito

**4. Você tem conhecimento da existência de um Código de Ética específico da sua área a nível nacional ou internacional?**

- sim
- não

**5. Você considera que os conhecimentos adquiridos no seu curso foram (são) suficientes no que diz respeito à formação ético-cidadã, tratando-se do seu desempenho profissional?**

- sim
- não
- parcialmente

**6. Você conhece a diferença entre práticas que envolvem e práticas que não envolvem uma discussão moral?**

- sim
- não
- parcialmente

**7. Você costuma ler artigos de jornais ou revistas que tratam de questões éticas?**

- sim
- não
- às vezes

**8. Alguém que, alcoolizado, sai dirigindo um carro e mata uma pessoa sem intenção, deve sentir-se moralmente responsabilizado pela morte daquela pessoa?**

- sim
- não
- depende da situação

**9. Qual o seu entendimento sobre questões morais?**

- Cada um tem o seu ponto de vista
- Deve-se discutir o problema para chegar-se a um ponto de vista comum
- Não tenho opinião formada

**10. Na sua opinião, um Código de Ética e Conduta Profissional é essencial para o bom andamento de uma profissão?**

- sim
- não

**11. Frente a problemas morais que aparecem na sociedade, que critério você usa ou usaria para julgá-los? (Indique sua preferência por cada uma delas, atribuindo uma nota de 1 a 5, sendo 1 o valor mínimo e 5 o máximo). Observa-se que é possível marcar dois ou mais itens com a mesma nota.**

Itens	Aspectos avaliados	Nota				
a)	Normas religiosas	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
b)	Convicções pessoais	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
c)	Legislação oficial	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
d)	Ensinos aprendidos na família	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
e)	Convicções justificadas com bons argumentos	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5
f)	O que a maioria faz	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5

**12. Qual tipo de contravenção você acha mais antiética hoje em dia (cite duas, no máximo)?**

- Desrespeito aos direitos autorais de obras
- Invasão de privacidade para tomar posse de dados confidenciais
- Fraudes, falsificações diversas
- Pedofilia
- Uso de software pirata

**13. Posso, ao comprar um cd de áudio, transformar seu conteúdo para mp3 (ou similar) para que seja compatível com outros equipamentos (mp3 player, por exemplo)? Posso ainda cedê-lo a terceiros?**

- De jeito nenhum. É totalmente ilegal.
- Sim, desde que seja para uso pessoal. Ceder a terceiros, nem pensar.
- Sim, não há problema algum.
- Não posso copiar, mas posso emprestá-lo sob a condição de que não copiem.

## **Anexo III - ACM Code of Ethics and Professional Conduct**

*Adopted by ACM Council 10/16/92.*

- **Preamble**

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. [Section 1](#) outlines fundamental ethical considerations, while [Section 2](#) addresses additional, more specific considerations of professional conduct. Statements in [Section 3](#) pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in [Section 4](#).

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondly, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of [Section 1](#), the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.



## 1. GENERAL MORAL IMPERATIVES.

*As an ACM member I will ....*

### 1.1 Contribute to society and human well-being.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

### 1.2 Avoid harm to others.

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See [principle 2.5](#) regarding thorough evaluations.

### **1.3 Be honest and trustworthy.**

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

### **1.4 Be fair and take action not to discriminate.**

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

### **1.5 Honor property rights including copyrights and patent.**

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

### **1.6 Give proper credit for intellectual property.**

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

### **1.7 Respect the privacy of others.**

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from

unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

### **1.8 Honor confidentiality.**

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

## **2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.**

*As an ACM computing professional I will ....*

### **2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.**

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

### **2.2 Acquire and maintain professional competence.**

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

### **2.3 Know and respect existing laws pertaining to professional work.**

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

#### **2.4 Accept and provide appropriate professional review.**

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

#### **2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.**

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in [imperative 1.3](#).

As noted in the discussion of [principle 1.2](#) on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for [imperative 1.2](#) for more details concerning harm, including the reporting of professional violations.

#### **2.6 Honor contracts, agreements, and assigned responsibilities.**

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

### **2.7 Improve public understanding of computing and its consequences.**

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

### **2.8 Access computing and communication resources only when authorized to do so.**

Theft or destruction of tangible and electronic property is prohibited by [imperative 1.2](#) - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle ([see 1.4](#)). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

## **3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.**

*As an ACM member and an organizational leader, I will ....*

**BACKGROUND NOTE:** This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context "leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context "organizations" are corporations, government agencies, and other "employers," as well as volunteer professional organizations.

### **3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.**

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

### **3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.**

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

### **3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.**

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

### **3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.**

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

### **3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.**

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

### **3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.**

This complements the imperative on public understanding [\(2.7\)](#). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

#### **4. COMPLIANCE WITH THE CODE.**

*As an ACM member I will ....*

##### **4.1 Uphold and promote the principles of this Code.**

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

##### **4.2 Treat violations of this code as inconsistent with membership in the ACM.**

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, Chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund. This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice. Copyright ©1997, Association for Computing Machinery, Inc.

## **Anexo IV – IEEE-CS/ACM Code of Ethics**

### **Software Engineering Code of Ethics and Professional Practice IEEE-CS/ACM Joint Task Force on Software Engineering Ethics and Professional Practices Full Version (5.2)**

#### **Preamble**

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer's humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for



the health, safety and welfare of the public is primary; that is, the "Public Interest" is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

## **Principles**

### **Principle 1: Public**

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

- 1.01. Accept full responsibility for their own work.
- 1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.
- 1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.
- 1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.
- 1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.
- 1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.
- 1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.
- 1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

**Principle 2: Client and Employer**

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

- 2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.
- 2.02. Not knowingly use software that is obtained or retained either illegally or unethically.
- 2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.
- 2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.
- 2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.
- 2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.
- 2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.
- 2.08. Accept no outside work detrimental to the work they perform for their primary employer.
- 2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

**Principle 3: Product**

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

- 3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.
- 3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.
- 3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

- 3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.
- 3.05. Ensure an appropriate method is used for any project on which they work or propose to work.
- 3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.
- 3.07. Strive to fully understand the specifications for software on which they work.
- 3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.
- 3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.
- 3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.
- 3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.
- 3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.
- 3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.
- 3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.
- 3.15. Treat all forms of software maintenance with the same professionalism as new development.

#### **Principle 4: Judgment**

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

- 4.01. Temper all technical judgments by the need to support and maintain human values.
- 4.02. Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.
- 4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.
- 4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

### **Principle 5: Management**

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance . In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with this Code.

5.12. Not punish anyone for expressing ethical concerns about a project.

**Principle 6: Profession**

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

- 6.01. Help develop an organizational environment favorable to acting ethically.
- 6.02. Promote public knowledge of software engineering.
- 6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.
- 6.04. Support, as members of a profession, other software engineers striving to follow this Code.
- 6.05. Not promote their own interest at the expense of the profession, client or employer.
- 6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.
- 6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.
- 6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.
- 6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.
- 6.10. Avoid associations with businesses and organizations which are in conflict with this code.
- 6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.
- 6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.
- 6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

**Principle 7: Colleagues**

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

**Principle 8: Self**

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06. Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

This Code was developed by the IEEE-CS/ACM joint task force on Software Engineering Ethics and Professional Practices (SEEPP):

Executive Committee: Donald Gotterbarn (Chair), Keith Miller and Simon Rogerson;

Members: Steve Barber, Peter Barnes, Ilene Burnstein, Michael Davis, Amr El-Kadi, N. Ben Fairweather, Milton Fulghum, N. Jayaram, Tom Jewett, Mark Kanko, Ernie Kallman, Duncan Langford, Joyce Currie Little, Ed Mechler, Manuel J. Norman, Douglas Phillips, Peter Ron Prinzivalli, Patrick Sullivan, John Weckert, Vivian Weil, S. Weisband and Laurie Honour Werth.

## **Anexo V – Artigo**

# **Ética Computacional: um estudo das violações à ética pelos profissionais e estudantes de informática**

**Crystie Allan Rosa**

**Universidade Federal de Santa Catarina**  
**Departamento de Informática e Estatística – INE**  
[crystie@inf.ufsc.br](mailto:crystie@inf.ufsc.br)

### *Resumo*

*Este trabalho visa o estudo das violações éticas cometidas por profissionais e estudantes na área de informática, através da análise dos problemas éticos mais comuns, a destacar: pirataria, hackerismo, invasão de privacidade e Ética na internet. Constitui-se, ainda, na aplicação de um questionário entre os acadêmicos de Sistemas de Informação e o restante da Universidade Federal de Santa Catarina com o intuito de saber a opinião dos acadêmicos em relação à Ética tanto no estudo quanto na profissão, com uma posterior análise descritiva. Além de incentivar um estudo mais aprofundado da Ética no curso de Sistemas de Informação, reforça ainda a necessidade da elaboração de um código de Ética na área da Computação, que, por razão da sua constante evolução, torna a tarefa extremamente complicada.*

## **1- Introdução**

Os computadores se tornaram uma ferramenta indispensável para todas as pessoas do chamado mundo moderno, e é justamente por esse motivo que eles foram fazendo parte, mesmo que de forma um tanto imperceptível, de nossas vidas. A informatização dos elementos que nos rodeiam não é, portanto, algo que se deva condenar. Todavia, ela traz novas variáveis no que diz respeito a optar pelo o que é certo ou errado em nossas decisões. Falar de Ética em Computação é algo realmente complicado. Primeiro que a Ética em si não é uma ciência tida como de conceitos “sólidos e indiscutíveis”, algo que contrasta com a precisão exigida pela Computação. No entanto, essa precisão torna-se maleável no mesmo sentido em que inovações vão sendo constantemente introduzidas na área. Obviamente isso não aplica aos conceitos elementares da Computação, mas às condições a que são submetidos seus usuários em razão de supostas inovações. Segundo, a área computacional, em relação às profissões mais tradicionais como medicina e advocacia, por exemplo, está na sua infância. Praticamente não houve tempo para criar uma regulamentação num ambiente em que novas descobertas alteram constantemente o paradigma de atuação do profissional e usuários.

A idéia principal deste trabalho consiste justamente na discussão dos fatores que envolvam computação e princípios éticos em situações como cópia de softwares, hackerismo, invasão de privacidade (virtual) e comportamento e conduta na internet, seguida pela demonstração de resultados da aplicação de um questionário sobre Ética Geral e Computacional entre os acadêmicos de Sistemas de Informação e restante da Universidade Federal de Santa Catarina (UFSC).

## **2 - Pirataria de Software**



Pode-se dizer que o software é uma das principais “peças” de um computador e sem ele a máquina não passa de um entulho com pouca utilidade. A valorização atual desse elemento contrasta com períodos mais longínquos, onde o hardware em si era muito mais importante que todo o resto. Dada a inversão de valores, outra coisa passou a ser percebida: a maior facilidade em manipular programas de forma a burlar proteções e assim usá-los sem pagar nada para seus desenvolvedores tomou conta, de forma globalizada, do pensamento dos usuários. A chamada pirataria está presente em todos os campos da informática e qualquer outro de criação intelectual. Mas isso não é um problema recente. Segundo Forrester e Morrison (FORESTER, MORRISON, 1993) essa questão existe desde a Idade Média e as autoridades da época já tinham dificuldades de controle nesse aspecto. No âmbito atual, o recurso mais utilizado para proteger as criações intelectuais é, sem dúvida, o copyright. Traduzido como o “direito de cópia”, o copyright assegura por lei que a permissão de copiar, reproduzir, expor publicamente e derivar o trabalho são exclusivas daquele que o criou. Assim, se alguém se interessar por qualquer uma das opções anteriores precisa obter o consentimento do criador, que não raro, exigirá uma compensação financeira em troca. Esta talvez seja uma das principais motivações para pessoas que desejam alterar softwares indevidamente e lançar versões na internet, ou ainda alimentar o mercado negro de vendas desse nicho. Citam-se como outras formas de proteção do trabalho intelectual as patentes – que vêm sendo utilizadas por alguns setores para softwares- e também os trademarks.

O período de proteção que o copyright oferece ao produto não é eterno, assim como não é uniforme em todos os países, havendo variações em diferentes aspectos. Nos Estados Unidos, de acordo com o website *U.S. Copyright Office*, todas as obras criadas em ou depois de 1 de Janeiro de são automaticamente protegidas desde o momento da sua criação perdurando por toda a vida do criador mais um adicional de setenta anos após sua morte. Se houver mais de um autor, essa regra se aplica ao último sobrevivente. Já no Brasil, no que se diz respeito aos softwares, estão protegidos por cinquenta anos sob o domínio do autor, de acordo com a lei 9609/98.

O copyright conta ainda com outro reforço: o DRM – Digital Rights Management. Isto funciona mais ou menos como um reforçador das restrições do copyright, usando para isso meios que assegurem – ou pelo menos tentem assegurar – as condições iniciais de direito de cópia. O controle da transformação do conteúdo de mídias de áudio para formatos comprimidos é um exemplo bem comum nesse sentido.

## 2.1 - O Copyleft

De acordo com o coletivo WuMing (MING, 2003), o copyleft é o copyright virado do avesso, ou seja, ao invés de restringir a cópia e derivação do trabalho, ele o libera sob a condição deste também permanecer livre. Embora pareça loucura para alguns, o copyleft ganhou um enorme número de adeptos representados, na área do software, pela comunidade do software livre. Idealizado por Richard Stallman, o software livre vem conquistando espaço em diversos setores da produção de programas, sempre sob a bandeira da disponibilização e possibilidade de derivação do código fonte sem ônus. Em outros setores como áudio, vídeo e texto, destaca-se a figura de Laurence Lessig, conhecido por seus trabalhos relacionados à dita cultura livre (Creative Commons). Embora atuem em diferentes áreas da produção intelectual, tanto Lessig quanto Stallman chegam à mesma conclusão que o cenário atual tende a levar à monopolização. A dificuldade, ou mesmo impossibilidade, de reutilizar elementos na criação de novos condiciona a uma estagnação do processo criativo, e a um conseqüente afunilamento do curso da produção. Este aspecto do monopólio também é reproduzido, no setor de softwares, pela pirataria. Tida para muitos como a principal desculpa para explicar números

negativos de vendas, a pirataria pode agir como elemento propagador e condicionante. Propagador porque os indivíduos que se utilizam de programas sem pagar acabam passando a informação para seus conhecidos, que então repassam à frente, formando uma rede de conhecimento a respeito do produto. Condicionante porque esses mesmos usuários se tornam dependentes dos softwares e, em um cenário empresarial, essa dependência é traduzida na compra das licenças originais sob o risco de se ter funcionários produzindo abaixo do esperado (por estarem condicionados a um determinado padrão de software) e de estar sujeito às penalidades da lei caso não o faça.

## 2.2 - É ético copiar softwares?

A cópia de softwares, no que se diz respeito à validade moral, é condenada na maioria das situações. Mas não em todas. De acordo com Helen Nissebaum (Nissebaum, XXXX) essa avaliação deve ser feita de forma contextual. Não é concebível que se alterem as propriedades de um programa e/ou disponibilizem-no pela internet, por exemplo. Mas se alguém que tenha adquirido um software dentro da legalidade sentir a necessidade de cedê-lo para outra pessoa que, estando em dificuldades e precisando dele, não tenha condições de obtê-lo, aí a ação seria moralmente aceitável. Mas esse é um caso particular, não devendo ser estendido de forma “maliciosa” para justificar a distribuição em massa de propriedade intelectual.

## 3 - Hackers

O termo hacker é geralmente evocado nas principais manchetes na mídia envolvendo crimes virtuais de diferentes tipos. O que talvez muitos não saibam é que o uso da palavra hacker não é adequado para esse caso, e sim cracker. A denominação *hacker* pouco ou nada tem a ver, em princípio, com delitos computacionais e sua origem é antiga, não estando necessariamente relacionada com computadores. A palavra já existia mesmo antes de alguém pensar em computação. Os antigos artesãos tinham como principal utensílio de trabalho o machado, e, justamente o ato de talhar, ou ainda de cortar lenha era a denominação original de *hacker*. A associação desse termo com a computação se deu por uma analogia feita com programadores que mergulhavam fundo nas suas atividades, buscando cada detalhe para tornar um programa sempre melhor. Essa dedicação além do nível normal acabou por cunhar o termo *hacker* no sentido computacional. Então podemos observar que ser *hacker* é apenas ser “fuçador”, extremamente ligado ao trabalho que se executa.

Se ser hacker é ser no máximo um trabalhador esforçado, como atualmente este termo adquiriu sentido de invasor, malfeitor, criminoso em termos computacionais? Difícil dizer, mas a partir do momento em que hackers começaram a mudar seus comportamentos e invadir causando danos aos sistemas, ou seja, tornando-se crackers, a atribuição possivelmente começou a ser feita.

Aparentemente é possível identificar duas linhas de atuação entre *hackers* e *crackers*. A primeira é o ato de propriamente invadir um sistema (ou ainda vasculhar as linhas de código de um programa por meio de engenharia reversa, por exemplo) e o segundo o que fazer depois que essa invasão for bem sucedida. Do ponto de vista ético, essa última (se executado alguma ação maléfica em seguida) aparentemente não provoca maiores discussões relacionadas com sua identificação. Afinal de contas, trata-se de um ato danoso contra terceiros. Mas e quanto à invasão? Seria eticamente correto uma pessoa aproveitar-se de falhas em sistemas ou programas e ter acesso à informação que em tese deveria ser confidencial? Essa é uma questão polêmica e embora o senso comum aponte para a ilegalidade do ato, há quem defenda que o simples ato de invadir sem causar danos não é necessariamente um crime. Um dos

fatores que por certo incentiva o procedimento de invadir é chamado efeito ciberespaço. Pode-se dizer que é um mundo virtual, onde há a abstração de valores e compromissos éticos, bem similar à sensação causada por vídeo games, para citar um exemplo.

### 3.1 - Ética Hacker

Independente de o invasor ser classificado como *hacker* ou *cracker*, ambos têm raízes em comum, ou pelo menos concordância em alguns itens pré-estabelecidos, mesmo que informalmente. Argumentos baseados nesses itens são usados para justificar as ações de hackers e crackers (no sentido da invasão) e são relacionados ao que se chama de ética hacker. O primeiro e mais “famoso” deles é o de que toda informação deve ser livre. O segundo argumento refere-se à exploração de falhas em sistemas.

## 4 - Invasão de privacidade

É comum se dizer que o direito à privacidade é uma das benesses trazidas a tiracolo pela democracia. Em tempos modernos, teoricamente, o direito a esse item de maneira geral é assegurado por lei na maioria das sociedades. No entanto, com o advento da computação a visão em torno dessa questão passou a mudar significativamente, considerando que praticamente tudo está guardado em bancos de dados, sejam nossos dados pessoais, contas no comércio, etc. Aparentemente não há regras definidas para o manuseio desses bancos de dados, apenas políticas de privacidade que variam de acordo com a empresa que as manipula. Diante dessa variável, como delimitar o acesso e exploração dessas informações (se é que se deve fazer isso) no intuito de preservar a privacidade das pessoas?

Por exemplo, há empresas que não hesitam em vasculhar a comunicação eletrônica dos seus funcionários em busca de qualquer informação valiosa. Embora o ambiente de trabalho e maquinário sejam proporcionados pela empresa, quem os opera são os funcionários, que em tese deveriam ter a privacidade respeitada. Não seria muito diferente de ter seus dados observados a partir do computador caseiro, por pessoas estranhas. Outra situação comum é a venda de cadastros com dados de clientes por empresas, o que se traduz na prática no envio de spam direcionado.

Mas nem tudo é negativo nesse prisma. Através da possibilidade de procurar registros em bancos de dados poder-se-ia facilitar a localização de um criminoso, por exemplo. Um dos grandes males da humanidade alavancados pela internet é a pedofilia e, indivíduos que procuram esse tipo de material geralmente lançam mão de ferramentas de busca como Google, Yahoo, etc. O propósito de ter acesso aos registros de mecanismos de busca é tentador, mas ao mesmo tempo representa um rompimento, uma abertura de possibilidades relacionadas com a privacidade *on line* dos usuários que até então se escondia no obscurantismo. De repente o usuário que transferia seus arquivos confidenciais para contas de email com alta capacidade de armazenamento passa a questionar se esses dados estão mesmo seguros e fora do alcance de outras pessoas. Estando cada computador por trás de um número IP, é perfeitamente viável a identificação do usuário (ou pelo menos de alguém responsável), embora essa técnica possa levar a distorções.

Larry Hunter, em seu artigo *Public Image*<sup>47</sup>, aborda bem a questão da informação ao escrever que “a ubiquidade e poder dos computadores embaraçam a distinção entre informação pública e privada”; “que a revolução não será apenas juntar dados, mas analisar o que já está prontamente compartilhado”. A informação pública é aquela que está disponível para todos

---

<sup>47</sup> Artigo integrante do livro *Computers, Ethics & Social Values*, de Deborah Johnson e Helen Nissenbaum, editora Prentice Hall, 1995.

terem acesso livremente. O detalhe é que pela coleta constante de dados públicos é perfeitamente possível chegar à informação privada por simples dedução. Hunter sugere a idéia de que a informação deva ser tratada como propriedade, ou seja, aquilo que se refira a cada pessoa deve pertencer a ela própria.

Porém, quando se trata de governo, a coisa pode mudar um pouco. A informatização dos cadastros pessoais de cada indivíduo tornou-se uma questão crucial para a eficiência das suas operações. E isso tanto em nível social quanto estratégico. Seria um retrocesso estipular limites abrasivos que impossibilitassem sua utilização sob pena de voltarmos à chamada “era pré-histórica” do tratamento de informação.

Mas e quanto às leis sobre privacidade *on line*? Elas existem, é claro. Na Europa, por exemplo, há a EU Data Protection Directive 2002/58/EC. No Brasil, segundo o advogado Antônio Ludovino Lopes, em seu artigo para o site *InfoGuerra*<sup>48</sup> citam-se as leis 8078 de 1990 (artigos 43 e 44 tratando da abertura dos bancos de dados por parte de fornecedores e clientes)<sup>49</sup> e a lei 9983<sup>50</sup> de 2000, onde há referência explícita sobre crimes em banco de dados. Embora essas referências sejam apenas superficiais é possível usar o Código de Defesa do Consumidor, Código Civil ou ainda o Código Penal através de adaptações ao contexto (computacional, no caso) se alguém se sentir prejudicado em termos de privacidade, de acordo com o advogado Amaro Moraes e Silva Neto.

Nas sociedades democráticas o *direito de saber* e a *privacidade* são itens que ficam em lados opostos da “balança”. Há a necessidade de equilíbrio para que a balança não penda só para um lado, terminando por “derrubar” tudo. Como Forrester & Morrison (FORRESTER, MORRISON, 1993) cita sobre a invasão de privacidade, o primeiro passo é estar consciente de que isso existe para então tentar a resolução do problema, o que, diga-se de passagem, é incerta.

## 5 - Ética na Internet

A internet existe como ferramenta já faz muito tempo. Na longínqua década de 50 nasceram os primeiros protótipos com propósitos militares e mais tarde, após a ameaça da Guerra Fria enfraquecer, para comunicação entre universidades norte-americanas. Atualmente, com o desenvolvimento crescente da internet, chegou-se a um patamar em que praticamente qualquer informação pode ser obtida com somente alguns cliques de *mouse*. Textos, vídeos, músicas, qualquer coisa é acessível sem que o indivíduo precise sequer tirar o pé da própria casa. Quando nos sentamos em frente ao computador e conectamos à internet, automaticamente passamos a fazer parte de uma comunidade de alcance global. Não é apenas mais uma máquina ligada, mas um ator desempenhando um papel no contexto virtual. Esse papel pode ser desempenhado de diferentes maneiras e também pode influenciar o pensamento e mudar decisões de outros participantes, assim como ser irrelevante de igual forma. Sendo assim podemos ponderar que os rumos que a internet toma estão fortemente relacionados ao tipo de comportamento que desempenhamos nela. Os tipos de comportamento observados no mundo virtual podem ser muito bem o reflexo da nossa conduta no mundo real. Os dois tipos existem concomitantemente e podem ser desempenhados inclusive pelo mesmo ator em contextos diferentes.

<sup>48</sup> <http://www.infoguerra.com.br>

<sup>49</sup> <http://www.presidencia.gov.br/ccivil/leis/L8078.htm>

<sup>50</sup> <http://www010.dataprev.gov.br/sislex/paginas/42/2000/9983.htm>

De acordo com Penny Duquenoy em seu trabalho *The Internet: a framework for understanding ethical issues*<sup>51</sup>, temos que o comportamento de cada indivíduo na internet é baseado por princípios éticos (sejam eles quais forem). A regulação da internet justamente entraria para reconhecer esses princípios e “validá-los” ou não, funcionando como uma ferramenta ética. Duquenoy observou ainda um detalhe interessante: a internet de hoje não é totalmente desregulamentada, havendo elementos de auto regulação mesmo que em níveis mais brandos. Por exemplo, muitos serviços disponíveis virtualmente somente são acessíveis mediante aceitação de termos ou políticas de conduta. Essas políticas não são iguais para todos os fornecedores de serviço, sendo fruto de uma análise individual das empresas no que concerne suas necessidades e tipos de comportamentos esperados ou tidos como aceitáveis por parte do cliente. No entanto, essa auto regulamentação não impede que outros desvios éticos de conduta na internet venham a ocorrer simplesmente por estarem fora do âmbito da empresa fornecedora do serviço.

O auto regimento tem por princípio a consciência ética de cada indivíduo representado no mundo virtual através dos seus “atos” na internet. Porém, nada pode fazer se o indivíduo ignora qualquer princípio ético e decide transgredi-lo propositadamente. Por ser um assunto relativamente novo não há consenso em relação a qual caminho se deva seguir. A própria internet representa uma incógnita atualmente na medida em que não temos certeza de como estaremos interagindo com ela, mesmo a curto prazo. A famosa frase utilizada por Eric E. Schmidt, na época chefe executivo da Sun Microsystems, encaixa-se muito bem nessa situação: “A internet foi a primeira tecnologia que nós humanos construímos sem entendê-la realmente.” “...Cada vez que ela começa a fazer sentido, então muda”.

## 6 - Códigos de Ética na Computação

Um código de ética nada mais é do que “um acordo explícito entre membros de um grupo social, uma categoria profissional, um partido político, uma associação civil, etc”, segundo Ferrell, Fraedrich e Ferrel (*FERREL, FRAEDRICH & FERREL, 2001*).

É interessante lembrar que códigos de Ética não têm “poder de polícia”, ou seja, não são juridicamente válidos por si mesmos exceto que haja uma lei calçando o princípio em questão. Dessa forma, os códigos de Ética adquirem um aspecto mais informativo do que qualquer outra coisa. A decisão pela correção ou não da ação, na maioria das vezes, ficaria por conta da própria pessoa que estivesse envolvida na situação.

No Brasil não há códigos de Ética na área da Computação. Mesmo no exterior não existe algo consistente nesse sentido, mas pode-se citar os códigos de Ética da ACM<sup>52</sup> (Association for Computing Machinery) e do IEEE-CS<sup>53</sup>/ACM. Estes dois exemplos cometem o erro de serem generalistas demais em suas proposições. Algumas vezes os regimentos são conflitantes entre si e no fim das contas os casos omissos dependem sempre da conduta ética do usuário para serem solucionados. É reconhecível, mesmo assim, a dificuldade residente na elaboração de um conjunto de normas que preveja com total precisão todas as possibilidades. É praticamente impossível que isso seja concretizado sem que brechas apareçam. Há ainda o complicador que é a mudança constante da tecnologia, fazendo que certos preceitos tenham de ser incessantemente atualizados.

<sup>51</sup> Disponível em <http://www.cs.mdx.ac.uk/staffpages/penny/allchapters.pdf>

<sup>52</sup> [www.acm.org](http://www.acm.org)

<sup>53</sup> <http://www.computer.org> (Institute of Electrical and Electronics Engineers – Computer Society)

Da análise dos dois códigos de Ética é que, pela condição generalista das suas proposições, estes são basicamente aplicados de forma inspirativa pelos profissionais da área de computação. As situações propostas são sempre as ideais, como por exemplo, “não seja desonesto”, “não utilize software ilegal”. Além disso, relativa incerteza provocada pelo pouco aprofundamento em cada caso tem seu lado negativo: a multiplicidade de interpretações.

A questão é, enquanto não houver o embasamento jurídico necessário comentado no início deste capítulo, códigos de Ética apenas e tão somente servirão para orientar os profissionais em nível informativo.

## **7 - Pesquisa**

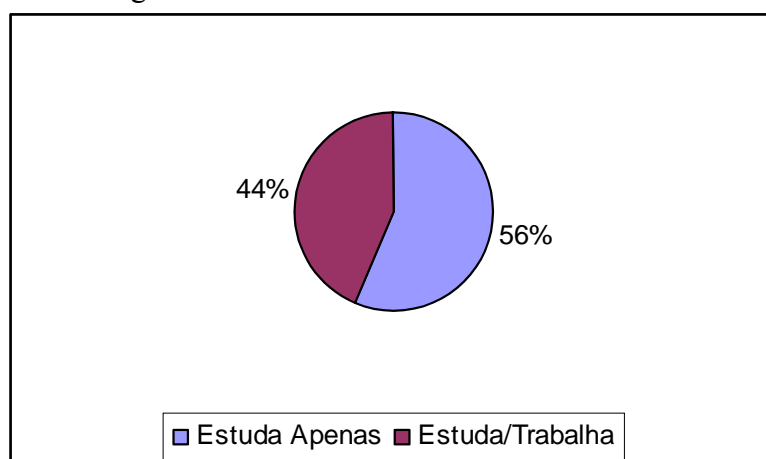
A parte da pesquisa foi realizada através de um procedimento de entrevista entre os estudantes da UFSC. A idéia foi elaborar um conjunto de questões relacionadas à Ética e moral e aplicá-lo em dois grupos diferentes: os acadêmicos do curso de Sistemas de Informação e os demais acadêmicos da universidade reunidos num segundo grupo.

Decidiu-se pela utilização do método da amostragem aleatória simples para realizar as entrevistas no âmbito da UFSC (sem Sistemas de Informação), adotando-se o valor de 10% como erro amostral tolerável. Para a parte dos acadêmicos de Sistemas de Informação, optou-se por consultar aproximadamente metade das 555 pessoas matriculadas em situação regular, no intuito de se obter um resultado mais apurado do que simplesmente aplicar a técnica de amostragem. A tabela abaixo mostra como ficou a distribuição pelos centros da UFSC pela técnica de amostragem aleatória simples:

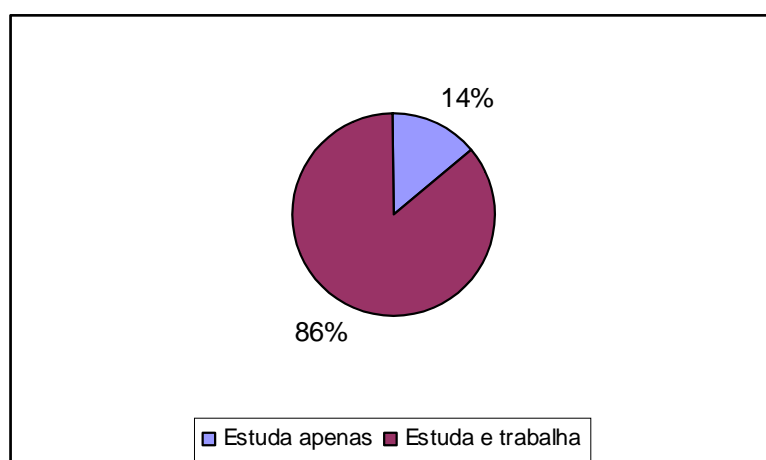
Tabela 4 – Valores de amostragem por centro

<b>Centro</b>	<b>Alunos</b>
Ciências Agrárias - CCA	3,84
Ciências Biológicas - CCB	1,60
Comunicação e Expressão - CCE	10,29
Ciências Jurídicas - CCJ	4,28
Ciências da Saúde - CCS	10,97
Centro de Desportos - CDS	2,63
Ciências da Educação - CED	4,14
Centro Filosofia e Ciências Humanas - CFH	10,33
Ciências Físicas e Matemáticas - CFM	12,26
Centro Sócio-Econômico - CSE	16,30
Centro Tecnológico - CTC	22,90
<b>Total</b>	<b>99,55</b>

Os resultados estão a seguir:

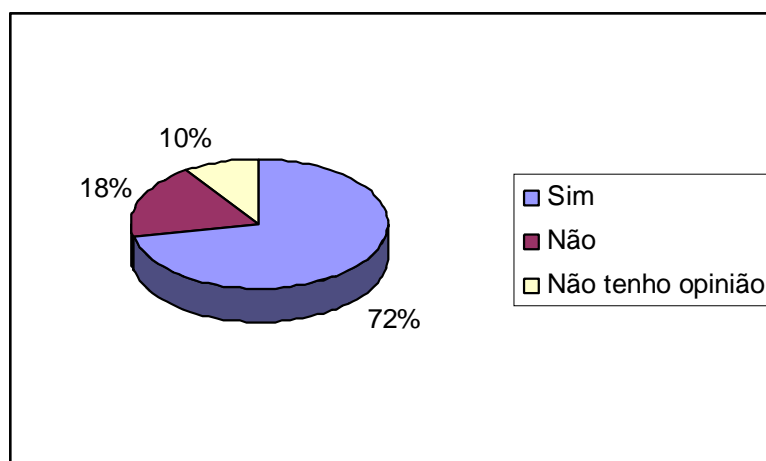


**Ilustração 31 – Ocupação dos acadêmicos UFSC (sem Sistemas de Informação)**

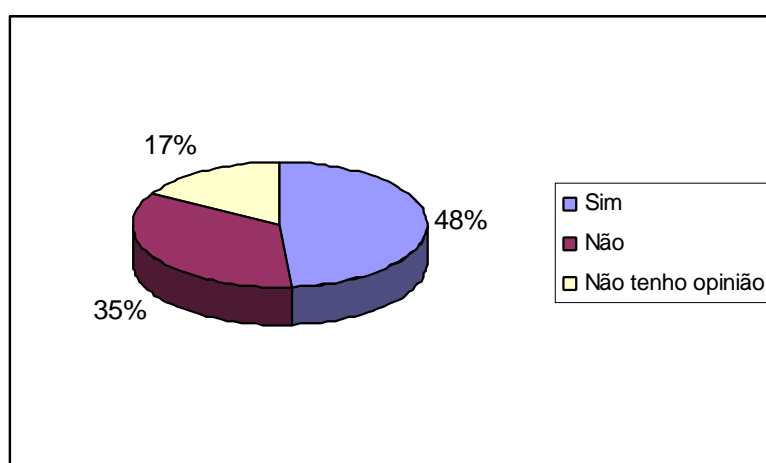


**Ilustração 2– Ocupação dos acadêmicos de Sistemas de Informação**

Pelo gráfico da *ilustração 1* é possível perceber que a maioria das pessoas apenas estuda, sem nenhuma ocupação extra, seja esta estágio ou emprego de qualquer natureza. No entanto, a diferença para aqueles que trabalham não é tão dispar a ponto de caracterizar a população como não-ativa. Já em Sistemas de Informação o quadro é diferente: apenas 14% das pessoas entrevistadas dedicam-se exclusivamente aos estudos, sem nenhum trabalho ou estágio.



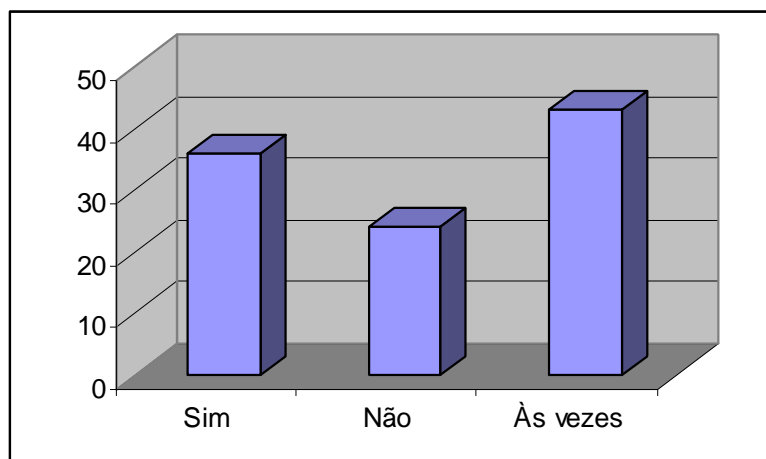
**Ilustração 3 – Necessidade de uma disciplina de Ética no curso**



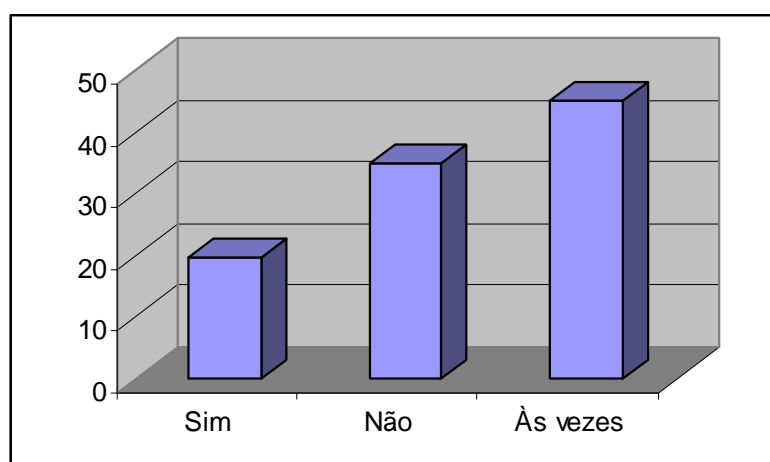
**Ilustração 4 – Necessidade de uma disciplina de Ética no curso de Sistemas**

A respeito de se ter uma disciplina específica sobre Ética no curso, a questão é vista com olhos mais conservadores, considerando que 48% são a favor e 35% contra, com um nível de indecisos relativamente alto (17%). Não é uma tendência observada no restante da UFSC, onde 72% aprova a existência da Ética no currículo.



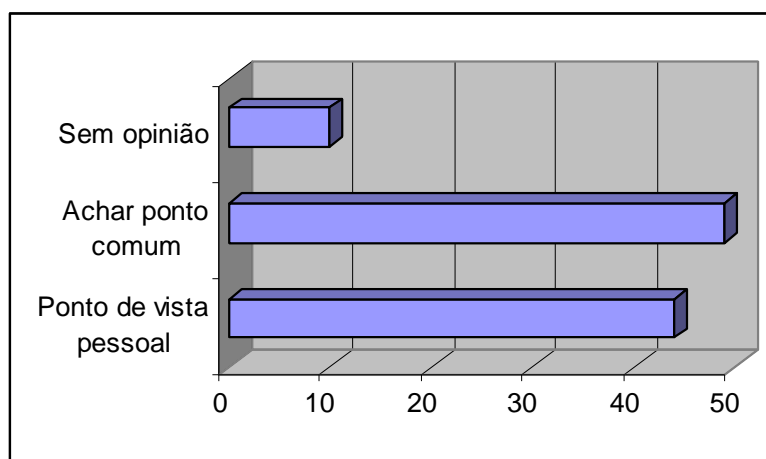


**Ilustração 32 – Frequência (%) de leitura sobre Ética no curso**

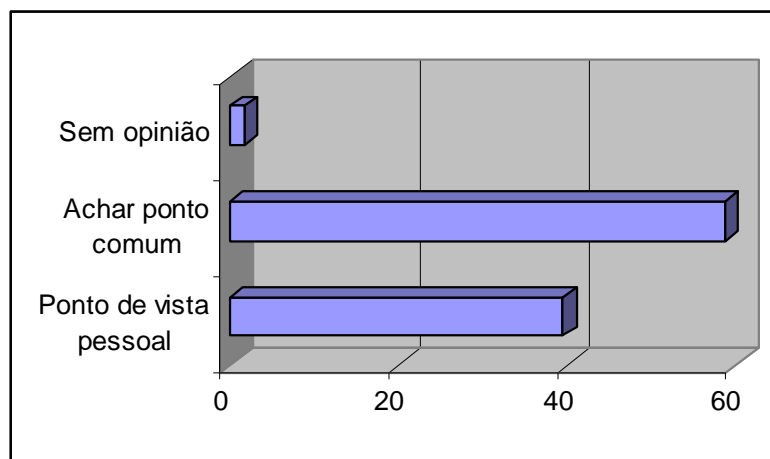


**Ilustração 33 – Frequência (%) de leitura sobre Ética no curso de Sistemas de Informação**

Sobre a frequência de leitura em Ética, nota-se que o acadêmico de Sistemas de Informação não possui o hábito de fazê-lo tanto quanto o restante dos acadêmicos da UFSC. Isso pode se converter num fator preocupante, pois o conhecimento teórico sobre a Ética pode melhorar e muito a formação da consciência do indivíduo e futuro profissional.

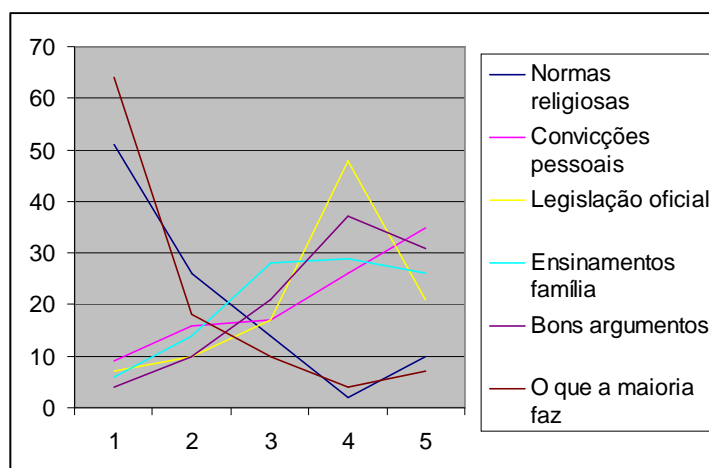


**Ilustração 4 – Entendimento sobre questões morais (restante UFSC) %**

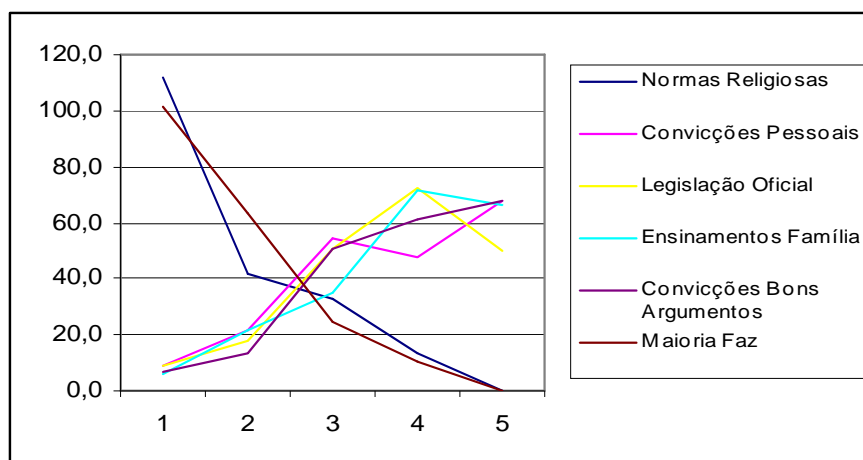


**Ilustração 5 – Entendimento sobre questões morais (Sistemas de Informação) %**

Tratando-se do entendimento sobre questões morais, percebe-se que os resultados foram um tanto parecidos, com prevalência do debate em busca do ponto comum e não apenas com base em elementos individuais.



**Ilustração 6 – Avaliação de critérios morais restante UFSC (Num Pessoas x Critério)**



**Ilustração 7 – Avaliação de critérios morais Sistemas de Informação (Num Pessoas x Critério)**

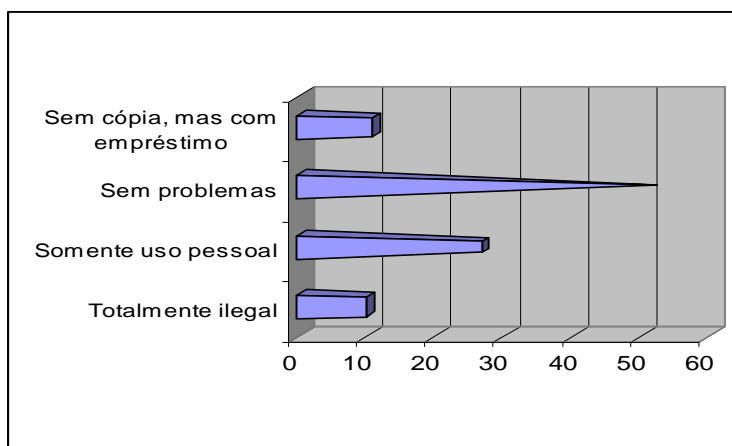
Pela ilustração 6 é possível notar uma rejeição considerável à utilização de critérios baseados em normas religiosas, ou seja, houve uma boa parcela (praticamente 50%,

considerando um total de 100 entrevistados) de pessoas que marcaram “1” ao classificar entre 1 e 5 o critério em questão. Porém, o maior percentual de rejeição foi, sem dúvida, atribuído à opção “o que a maioria faz”. Mas isso não vai contra ao questionamento anterior, onde houve uma inclinação para as decisões coletivas? Não necessariamente. O item “o que a maioria faz” pressupõe certo descaso com a avaliação crítica dos atos pela moral, diferentemente de uma discussão em grupo de forma consciente.

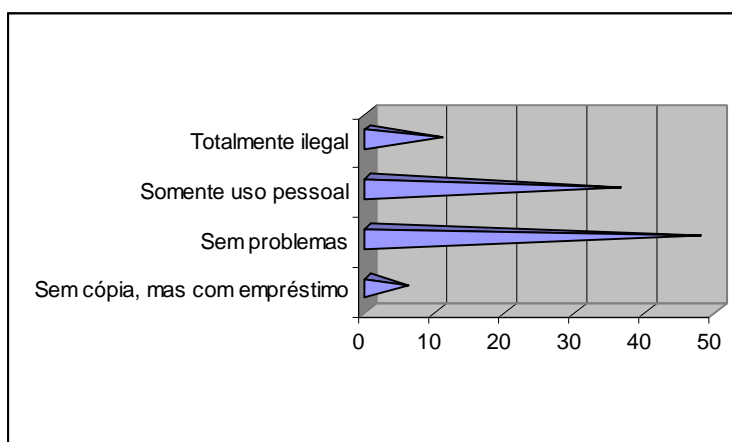
Percebe-se a importância dada pela avaliação baseada em legislação, bem classificada pelo critério de ordenação 4, apesar da queda no patamar seguinte. Os critérios “convicções pessoais” e “ensinamentos familiares”, em tese considerados subjetivos, obtiveram muito boa conceituação nas entrevistas entre os acadêmicos.

O critério mais nobre, em princípio, (“convicções justificadas por bons argumentos”), se é que se pode usar este tipo de classificação, esteve bem colocado no lugar esperado. Quando se diz que uma convicção é justificada por um bom argumento, nesse caso, pressupõe-se que a situação em questão foi ao menos analisada segundo algum critério moral válido.

Já na ilustração 7 temos duas situações bem curiosas. Primeiro a quase linearidade decrescente na avaliação dos critérios “normas religiosas” e “o que a maioria faz”. Apesar de ser uma tendência observada no restante da UFSC, aqui ficou bem reforçada. Segundo, a convergência dos outros critérios para mais ou menos o mesmo ponto do gráfico. Num aspecto geral foi surpreendente que isso tenha acontecido, revelando a variedade de fontes que os acadêmicos levam em questão em se tratando de avaliar uma situação.



**Ilustração 8 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (restante UFSC) (%)**



**Ilustração 9 – Transformar cd de áudio para mp3 ou similar e cedê-lo a terceiros (Sistemas de Informação)**

A maioria não vê problemas em transformar áudio e ainda repassá-lo a terceiros nos dois gráficos. As opções restritivas (“sem cópia, mas com empréstimo” (sob condição deste também não copiar) e “totalmente ilegal”) ficaram bem atrás das mais liberais. É o retrato atual da indefinição sobre direitos autorais relativos ao conteúdo digital e possivelmente um recado claro dos usuários relacionado ao uso justo.

## 8 - Considerações Finais

Seria pretensão querer finalizar a discussão sobre Ética computacional com apenas um trabalho. É um campo tão inexplorado que mesmo os princípios básicos já definidos são discutíveis dependendo do prisma da observação. Mas mesmo dessa forma é interessante apontar alguns itens que puderam ser observados.

Dois fatores têm colaborado para a multiplicação da complexidade da delimitação dos preceitos éticos: a evolução do hardware, das mídias de armazenamento e a internet. São os meios que massificaram a troca de arquivos, seja de forma legal ou não. Mas o que é eticamente legal tratando-se de software? A cultura que predomina é a de que o total controle do produto deva estar “nas mãos” daquele que o fez. Os chamados gerenciamentos das propriedades intelectuais são, infelizmente, baseados na linha de pensamento da Revolução Industrial. Os consumidores eram limitados a manusear exclusivamente aquilo que conseguiam obter dos fornecedores, ou seja, não havia como “tratar” o produto, criar novas coisas a partir dele. A modernização dos equipamentos, a introdução do computador, da internet, mudaram totalmente as possibilidades. Qualquer um pode criar seu próprio jornal on line, imprimi-lo tão igual ou melhor ao que é distribuído nas bancas, produzir seu próprio filme independente, produzir seu próprio software. Mas o que aconteceu com os produtores? Continuaram a achar que estávamos na época da Revolução Industrial e, como tal, impõem regras que agridem o livre desenvolvimento da criatividade. Essa divergência de ideologias tem gerado muitos conflitos e por conseqüência, muita indefinição do que pode ser considerado como correto ou não no que concerne à Ética computacional e direitos autorais.

E o que dizer da informação pessoal? A quem pertence? Há quem defenda que a informação pessoal deva ser o que o nome sugere: pessoal. Então, se a partir da informação pública é possível deduzir a informação privada, a partir do momento que essa dedução pode ser realizada de forma a obter consistência, passa a pertencer àquele que está sendo referenciado. É interessante que ao passo em que a modernização dos meios de comunicação trouxe à tona o obsolescimento do gerenciamento de direitos autorais, no que se refere à privacidade vem exatamente no sentido contrário, mais conservador. Mas nesse entremeio existem aqueles que não concordam com esse conservantismo e acham que informação alguma deva ser omitida do conhecimento público: *hackers*. Amados por uns, odiados por outros, são comumente confundidos com arruaceiros e propagadores de pragas pela internet. Na verdade a chamada ética hacker tem alguns pontos que não convencem o público leigo e muito menos os mais céticos.

Mas o que fazer para que não sejam cometidos atos considerados antiéticos no mundo dos computadores (ou pelo menos que haja punição para quem os cometer)? Seria necessária uma normatização mais consistente e pró ativa para que usuários de tecnologia pensassem duas vezes antes de fazer algo? . Um controle rígido implicaria possivelmente na perda do livre arbítrio na internet, da liberdade de expressão, até. Acredita-se que por essa razão muitos ainda consideram a auto-regulamentação o melhor caminho para controlar os abusos que acontecem na internet. As chamadas políticas de privacidade, costumeiramente referenciadas por inúmeras empresas como uma garantia, um atestado de idoneidade ao público que utiliza seus serviços, são falhas no sentido de depender da linha de pensamento da organização – que pode conter distorções. Apoiando as políticas de privacidade, os códigos de Ética entrariam

com um suporte a nível mais básico e teórico. Tidos como generalistas e frequentemente com cláusulas conflitantes entre si mesmas, servem mais como um guia de conduta àquele que se vê frente dilemas morais durante a vida profissional ou não, ao manipular computadores. No fim, o que acaba realmente valendo é a lei com valor jurídico, e daí a necessidade de estudar melhor o assunto, mapear as adversidades e então partir para uma regulamentação mais específica na área (ou pelo menos uma tentativa de fazê-lo).

Sobre os questionários, estes foram aplicados com o intuito de se ter uma noção de como o acadêmico da UFSC enxerga a situação sobre a Ética na profissão. Sistemas de Informação tem um perfil de pessoas diferente do resto da universidade, no sentido de que são, em sua grande maioria, pessoas que conciliam trabalho e estudos. Isso pode ter refletido no desenvolvimento de “técnicas” baseadas na experiência, por exemplo, para resolver conflitos morais diversos. O gráfico geral de critérios usados para avaliar esses conflitos foi bem balanceado nos critérios “convicções pessoais”, “legislação oficial”, “ensinamentos familiares”, “convicções baseadas em bons argumentos”. Embora no resto da UFSC essa tendência seja também observada, talvez tenha sido motivada não tanto pelo empirismo, mas por algum *background* teórico, já que são pessoas que lêem mais sobre Ética e optam com mais certeza pela existência de uma disciplina específica sobre o assunto no currículo.

A última pergunta do questionário tratava exclusivamente de direitos autorais. A maioria decidiu que transformar áudio de um cd comercial para o formato mp3 ou similar e ainda cedê-lo a terceiros é algo normal, tanto para Sistemas de Informação quanto para o restante da UFSC. Isso não pressupõe distribuição em massa de conteúdo protegido, mas apenas que possa ser considerado como o uso justo de algo adquirido legalmente. A segunda corrente, segundo os acadêmicos, é de que apenas deva ser feito um backup pessoal, sem direito a empréstimos. Nesse quesito é complicado dizer quem está certo ou errado, se é que há como fazê-lo. Sabe-se que o conteúdo digital não pode ser tratado como “mercadoria física”, como querem os produtores e nem como totalmente “abstrata” como quer a maioria dos consumidores. Assim como na definição de direitos autorais, a área ético-computacional como um todo carece de um melhor estudo e atenção. Do resultado desse estudo mudanças significativas nas vidas das pessoas podem acontecer, já que estamos caminhando inevitavelmente para a total dependência da automatização computacional dos processos.

## 9 - Bibliografia

BARBETTA, Pedro Alberto. **Estatística Aplicada às Ciências Sociais**. Florianópolis: Ed. da UFSC, 2002

BARROCO, Maria Lucia Silva. **Ética e Serviço Social: Fundamentos Ontológicos**. São Paulo: Cortez, 2003.

BERLEUR, Jacques; BRUNNSTEIN, Klaus. **Ethics of Computing**. Londres, Inglaterra: Chapman & Hall, 1996.

BERLEUR, Jacques; WHITEHOUSE, Diane. **The Ethical Global Information Society – Culture and democracy revisited**. Londres, Inglaterra: Chapman & Hall, 1997.

CAMARGO, Marculino. **Fundamentos de Ética Geral e Profissional**. Petrópolis, RJ : Vozes, 1999.

- DIBONA, Chris; OCKMAN, Sam; STONE, Mark; BEHLENDORF, Brian. **Open Sources: Voices from the Open Source Revolution**. California, USA: O'Reilly & Associates, Inc, 1999.
- FERREL, FRAEDRICH & FERREL. **Ética Empresarial: Dilemas, Tomadas de Decisões e Casos**, Rio de Janeiro, Brasil: Reichmann & Afonso, 2001.
- FORESTER, Tom; MORRISON, Perry. **Computer Ethics**. Massachusetts, EUA: The MIT Press, 1993.
- HEXSEL, Roberto A. **Software Livre**. Departamento de Informática da Universidade Federal do Paraná, 2003.
- HIMANEN, Pekka. **A Ética dos Hackers e o Espírito da Era da Informação**. Editora Campus, 2001.
- JOHNSON, Deborah G.; NISSENBAUM Helen. **Computers, Ethics & Social Values**. USA: Prentice Hall, Inc, 1995.
- LESSIG, Lawrence. **Cultura Livre – Como a mídia usa a tecnologia e a lei para barrar a criação cultural e controlar a criatividade**. New York, USA: The Penguin Press, 2003.
- MASIERO, Paulo César. **Ética em Computação**. São Paulo: Editora da Universidade de São Paulo, 2000.
- MING, Wu. **O Copyleft explicado às crianças**. Ano: 2003. Disponível em: [www.wumingfoundation.com](http://www.wumingfoundation.com)
- MITNICK, Kevin D.; SIMON William L. **Mitnick – A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Education, 2003.
- NALINI, José Renato. **Ética Geral e Profissional**. São Paulo: Editora Revista dos Tribunais, 2001.
- RAUBER, Jaime José; ZANATTA, Alexandre Lazaranetti. “A Ética na Computação: Uma análise descritiva justifica sua presença”. Rio Grande do Sul: Universidade de Passo Fundo.
- STALLMAN, Richard M. **Free Software, Free Society: Selected Essays of Richard M. Stallman**. Boston, USA: GNU Press, 2002.
- STERLING, Bruce. **The Hacker Crackdown: Law and Disorder on the Electronic Frontier**. New York, USA, 1993.
- VALLS, Álvaro L.M. **O que é Ética**. São Paulo: Editora Brasiliense S.A., 1986.
- VÁRIOS. **Serviço Social e Ética: convite a uma nova práxis**. São Paulo: Cortez, 2003.
- VAZQUES, Adolfo Sanches. **Ética**. Rio de Janeiro: Civilização Brasileira, 1970.

ZILLI, Daniel. **Mundo Livre** – 3ª Edição.

WILLIAMS, Sam. **Free as in Freedom: Richard Stallman's Crusade for Free Software.**  
California, USA: O'Reilly & Associates, Inc, 2004.