ÉTICA E INFORMÁTICA

Anne-Marie N. H. Otero

Preliminares

Talvez não seja fácil fixar datas, mas é provável que já em torno dos anos sessenta, pesquisadores brasileiros se tenham dado conta de que as modificações tecnológicas acarretam muitas e profundas alterações comportamentais.

Se a observação vale para inovações do passado – como o automóvel, nos anos 20, o avião, nos anos 50, os foguetes espaciais, nos anos 70 – deve valer, também, para as novidades destes tempos, em especial, para o computador. Convém, pois, de início, fazer ligeiro comentário a respeito das transformações havidas em cada caso, porque isso oferece meios para melhor avaliar o que está por vir.

***

Um ser humano caminha, sem dificuldade, cerca de quatro quilômetros por hora. Mantendo sua locomoção nesse nível, desenhou um tipo de vida que, agora, só vemos retratado nas tribos primitivas.

Com o surgimento dos primeiros automóveis, a velocidade dos movimentos humanos foi multiplicada por dez. Ainda há quem se lembre das alterações que o carro provocou. Até mesmo a ingênua mocinha das pequenas vilas se transformou, para tornar-se uma jovem ousada e agressiva, capaz de disputar, com os moços, alguns serviços que lhe eram vedados.

Os primeiros aviões, deslocando-se a 400 km/h, tornaram a multiplicar por dez a capacidade de movimento. Quero crer que todas as pessoas adultas de hoje têm clara noção das transformações que a sociedade e o mundo sofreram com o advento das aeronaves. Deixamos de pensar em termos locais e passamos a cogitar das coisas e das gentes em termos do planeta. Acontecimentos da China, da Austrália ou da Groelândia, itens remotos para uma vida brasileira, tornaram-se, de súbito, itens presentes, atuantes, influentes em nosso ambiente.

Os foguetes, deslocando-se a quatro mil quilômetros por hora, multiplicando, pois, a capacidade humana por 10^3, provocaram novas alterações em nossas vidas. A globalização ganhou dimensões "escandalosas" e já falamos em termos de universo – ou melhor, de universos (no plural) que a fantasia permitiu entrever e que, possivelmente, a realidade nos levará a conhecer.

Não è preciso esmiuçar o tema para perceber as mudanças que se operaram em nós, nas coisas, nos seres, nos artefatos, na vida... cada vez que a capacidade humana de locomoção foi multiplicada por dez, passando de 4 para 4x10, para $4x10^2$ e para $4x10^3$.

Ora, os primeiros computadores, segundo se afirma, multiplicaram a capacidade de calcular por um fator da ordem de 10^8! Inegavelmente, pois, o computador deveria provocar transformações muito profundas nos seres humanos. Considerando que os computadores mais recentes têm acelerado incessantemente os cálculos viáveis, somente a imaginação será capaz de colocar algum limite nas transformações a que o ser humano estará sujeito nos próximos anos.

Cogitar das transformações que os seres humanos poderão sofrer no início do novo milênio requer, no mínimo, análise do que vem ocorrendo à nossa volta. Essa análise, porém, precisa ver-se mergulhada em algumas considerações filosóficas e talvez deva ser permeada por alguma dose de inventividade. Tentemos.

Problemas trazidos pela disseminação dos computadores

Em nossos dias, o uso de computadores tornou-se comum. As escolas já dispõem desses aparelhos, e os alunos com eles "brincam", em clima de total naturalidade. O computador invadiu os lares e se propaga pelas favelas.

Tais e tantas têm sido as modificações das atitudes das pessoas que lidam com os computadores que as mais avisadas procuram ensinar outras a obter proveitos, sem, no entanto, causar danos a terceiras. Uma espécie de "ecologia computacional" está "no ar", cativando novos usuários das máquinas.

Crescendo o número de interessados envolvidos em alguma atividade, é natural que também cresçam as "áreas de atrito" entre eles. È compreensível, portanto, que os computadores tenham colocado algumas questões muito sérias. Entre elas, as da privacidade (cada vez menor), da confiabilidade (às vezes duvidosa), da propriedade intelectual (difícil de assegurar), da segurança, etc., etc.

No que respeita à segurança, convém notar que o Inglês distingue 'safety' e 'security', exigindo longas frases a fim de que as noções sejam convenientemente trazidas para o nosso idioma. Não esquecer, paralelamente, que as relações entre usuários de computadores sofreram e continuam sofrendo alterações a que caberia dar atenção. Em planos mais vastos, também é preciso atentar para certos problemas de grande alcance, como, digamos, o do apoio institucional a oferecer aos responsáveis pelo desenvolvimento da informática; o da formação de pessoal habilitado; e mesmo o da justiça social.

Comportamento ético

Conflitantes posições têm sido defendidas, quando se analisa a "neutralidade" da ciência e da tecnologia. Para uns, essa neutralidade é mera fantasia. Para outros, é defensável. Conseqüências morais de uma inovação tecnológica dependem do *uso* que dela se faça -- não dependem dela mesma. Dependem, em suma, de como o ser humano dela se serve. Os seres humanos podem agir com isenção, pensando no bem-estar alheio, podem agir com parcialidade, cogitando apenas de seus próprios interesses.

Está em tela, naturalmente, um comportamento moral ou imoral dos sujeitos. É tema que requer atenção.

Sem pretender chegar às minúcias e colocando como (quase) sinônimos os termos 'ética' e 'moral', diremos que a Ética diz respeito ao mau ou bom; ao injusto ou justo; às condutas irresponsáveis ou responsáveis; ao digno de reprimendas ou digno de elogios; ao proibido, ao facultativo (permitido) ou ao obrigatório. Em tal sentido, associa-se, claramente, à culpa, à vergonha, ao ressentimento, à empatia, à compaixão, aos cuidados dispensados a terceiros. Envolve, por certo, questões relativas às diretrizes públicas, assim como questões de ordem pessoal.

Inegavelmente, a Ética recebe apoio do ambiente social, de práticas estabelecidas, da lei, da religião e da consciência individual. Inegavelmente, porém, examina criticamente todas essas fontes de apoio. Não deve provocar espanto, pois, o fato de ser matéria imersa em controvérsias, incapaz de se ver confinada a uma definição. Todavia, a Ética é algo com que nos familiarizamos desde a mais tenra infância.

As crianças estão constantemente sujeitas a receber reprimendas ou estímulos – vindos de pais, professores, parentes ou companheiros. Reprimendas e estímulos encorajam as crianças a crer que estejam capacitadas a executar ações de maneira responsável. Elas sentem vários tipos de reações de caráter moral e, em especial, sentem a indignação e os ressentimentos manifestados pelos adultos com os quais convivem. De maneira recíproca, também as crianças, dirigindo-se às pessoas que as cercam, manifestam indignação e ressentimentos.

A par disso, certos estudos recentes atestam que as crianças adquirem, já com quatro a cinco anos de idade, uma compreensão intuitiva das diferenças que cercam o convencional (por exemplo, o uso de uniformes coloridos) e o moral (por exemplo, não jogar tinta no rosto de colegas).

***

A utilização generalizada de redes e da Internet deu origem a novas questões éticas em sistemas de informação. Novas ferramentas de softwares permitem que os empregados sejam supervisionados eletronicamente de várias maneiras.

A tecnologia do sistema telefônico, na maioria das grandes empresas comerciais, registra a hora, a duração e o destino das chamadas telefônicas feitas pelos empregados. Permite, com facilidade, ouvir as conversas que funcionários venham a manter com os clientes.

Não raro, afirma-se que a monitoração dos telefones, por meio dos computadores, è uma valiosa técnica de controle de qualidade. Em vista disso, cabe ao departamento de sistemas de informação de uma empresa, deixar explícito, para os funcionários dessa empresa, que eles serão monitorados. Cabe informar que a monitoração tem por objetivo garantir o êxito das iniciativas da firma e que os dispositivos de monitoramento não serão usados com o propósito de prejudicar os funcionários.

Algumas empresas, entre as quais podem ser citadas a Federal Express, a Eastman Kodak e o Bank of Boston, emitiram informações normativas, instruindo seus empregados sobre o direito da empresa de interceptar e ler suas mensagens de *e-mail*.

A *Internet* apresenta desafios adicionais de privacidade, principalmente quanto ao uso crescente da *World Wide Web* (www). *Sites* da www podem ser programados para acompanhar não somente o número de vezes que tenham sido acessados por outros computadores, mas também para localização desses outros computadores acessados. Essas informações ajudam os profissionais de marketing a direcionar seus anúncios.

Ainda mais controvertidos são os "*cookies*", uma tecnologia que permite que os sites da *Web* rastreiem usuários individuais. Um pequeno arquivo è colocado no computador que acessar um determinado site. O arquivo contém o nome do site da *Web*, um código de identificação, exclusivo do arquivo, e alguns outros dados. Quando alguém utiliza seu computador para acessar um site da *Web* que já tenha armazenado um *cookie*, qualquer pessoa poderá procurar o computador daquele alguém e achar seu *cookie*. Saberá, portanto, o que esse alguém fez e poderá, naturalmente, fazer uso do *cookie* descoberto.

***

Em verdade, è claro que "hackers", de todos os tipos imagináveis, nada fazem para que os elogiemos. Na melhor das hipóteses, podem ser comparados a doenças -- males que despertam, em alguns pesquisadores, o desejo de erradicá-los...

***

Alguns filósofos e psicólogos (e.g., Piaget e Kohlberg) estudaram questões dessa natureza e ressaltaram aspectos notáveis do desenvolvimento cognitivo e do desenvolvimento moral. As idéias de Kohlberg despertaram numerosas adesões e críticas. Sem cogitar desses aspectos, note-se apenas que o psicólogo estipula seis fases de desenvolvimento moral

e cognitivo. Nas duas primeiras fases domina o interesse pessoal. Na primeira, há o medo da punição e a alegria da premiação; na segunda, prevalecem os "acordos mútuos" ("Você me dá isso, eu lhe dou aquilo"). Nas duas fases seguintes manifesta-se a "moralidade convencional". A fase três apoia-se em aprovação ou reprovação de colegas e amigos. A fase quatro acolhe "regulamentos" (leis), admitindo que sejam indispensáveis para a coesão e a ordem social. Somente nas duas últimas fases se apresenta a moralidade que Kohlberg denomina "crítica", ou pós-convencional. Em resumo, trata-se de agir em consonância com princípios livremente escolhidos que possam ser empregados, entretanto, para avaliar a adequação das respostas surgidas nas quatro fases anteriores.

E' claro que o desenvolvimento moral (bem como o cognitivo) prossegue ao longo de toda a vida. Segundo se observa, parece existir um conjunto mínimo de valores que qualquer sociedade viável precisa acolher, caso pretenda sobrevivência coletiva. Esse conjunto mínimo incluirá, sem dúvida, "deveres positivos" (entre os quais estariam apoio mútuo, lealdade e reciprocidade), bem como "deveres negativos" (entre os quais estariam não provocar danos a terceiros, normas para procedimentos corriqueiros e padrões destinados a dirimir pendências relativas ao justo).

***

Deve estar claro que um conjunto mínimo de valores é necessário, porém não suficiente, para assegurar a coexistência dos seres humanos – em nível pessoal, familiar, profissional, comunitário, nacional e internacional.

Também deve estar claro que o conjunto mínimo precisa ser identificado a fim de tornar possíveis as análises de abusos e de contravenções. Sem o conjunto mínimo de valores, não haveria maneira de criticar e condenar as contravenções.

Parece lícito, por conseguinte, afirmar que o comportamento ético pode ser visto como algo que se acha "embutido" nos seres humanos, dispensando minuciosas caracterizações – a menos que estejamos interessados nos meandros da Filosofia. Sabemos perfeitamente o que é desrespeitar um código de boa conduta. Não há necessidade de longos debates para saber se algumas (provavelmente a maioria) das ações dos indivíduos merecem aplausos ou reprimendas.

***

Hackers

Recente exame dos sites da www, realizado por Dan Farmer, perito em segurança, concluiu que aproximadamente 2/3 dos sites comerciais e governamentais mais populares da *Web* estão amplamente abertos à penetração e ao mau uso. Farmer é um dos que desenvolveram o SATAN

(Security Analysis Tool for Auditing Networks), um pacote de software que analisa as redes de computadores UNIX, em busca de falhas de segurança. Ele relata informações sobre serviços de redes mal-configurados e falhas em utilitários de sistemas ou de redes, como protocolos de transferência de arquivos, envio de mensagens e o sistema de arquivos de redes. Embora reconhecido como valiosa ferramenta de diagnóstico, o SATAN também pode ser usado por *hackers* para ajudá-los a descobrir meios de penetrar ilicitamente em redes.

Farmer usou o SATAN para examinar furtivamente 1.735 sites da *Web* em busca de falhas de segurança. A pesquisa mostrou que 68% dos sites dos bancos e 62% dos sites do governo dos EUA eram vulneráveis, prova que foi confirmada quando os *hackers* penetraram no site da Força Aérea dos EUA, desfigurando a home-page.

Esta história mostra como os sistemas computadorizados são vulneráveis ao roubo, a estragos, à destruição ou ao mau uso. Mostra, ainda, que utilização e operação apropriadas dos sistemas de informação dependem do comportamento das pessoas.

Os problemas de segurança e crimes por computador são de especial importância para os usuários de sistema de informação. Os sistemas de informação devem ser salvaguardados contra acessos não autorizados, alterações e roubos. Embora o roubo monetário seja a maneira mais comum de crime por computador, ele também pode envolver o furto de serviços, de informações ou de programas, alterações de dados e danos ao *software*.

Como exemplo recente, podemos citar a fraude em IR pela *Interne*t ocorrida aqui no Brasil há não muito tempo. Grupos criminosos tiveram acesso a dados cadastrais de contribuintes isentos, cuja renda era inferior a R$ 10.800,00 por ano. Com as informações, eles montaram declarações fraudulentas, lançando receitas e despesas fictícias, de modo que a conta resultasse em imposto a restituir. O único ponto que exigiu cuidado foi manter o valor a restituir em nível que não fosse enquadrado na chamada “malha fina”. Depois, bastou (com o número do CPF) fazer uma consulta na *Internet* para saber se o dinheiro já havia sido liberado.

O Brasil foi o primeiro país do mundo a adotar a declaração de renda pela rede, há cerca de quatro ou cinco anos. Ainda hoje é um dos poucos a utilizá-la. Para o supervisor nacional de Imposto de renda da Receita Federal, Luiz Carlos Rocha de Oliveira, a *Internet* è a forma mais segura para o envio da declaração de renda ao fisco, porque evita a interferência de terceiros no processo.

*

**

Enfim, são os conjuntos mínimo de valores que possibilitam gerar uma base genérica sobre a qual assentar

debates que “atravessam fronteiras”, isto è, debates que girem em torno de questões de dimensões internacionais ou universais.

Comércio eletrônico

A *Interne*t está, hoje, aberta a todos. Qualquer informação passa por vários sistemas computacionais da *Net* antes de chegar a seu destino. Pode ser monitorada, capturada, armazenada em qualquer destes lugares. Dados importantes que podem ser capturados incluem o seu nome o número de seu cartão de crédito, dados pessoais, contratos, negociações, etc. Por causa da forma de pagamento na rede, o comércio eletrônico não cresceu mais.

Em verdade, a tecnologia é uma faca de dois gumes. Pode ser a fonte de muitos benefícios. Um deles é a facilidade com que a informação digital se transmite e será compartilhada com outras pessoas. Mas, ao mesmo tempo, a tecnologia criou muitas oportunidades de quebrar a lei e tirar proveito de trabalhos alheios...

Muitas das leis americanas e européias sobre privacidade estão baseadas na Fair Information Practices (FIP), com um primeiro relatório escrito em 1973. O FIP é um conjunto de princípios que regem a coleta e o uso das informações sobre os indivíduos. Os cinco princípios do FIP são:

1. Não deve haver registros pessoais cuja existência seja secreta.

2. As pessoas devem ter direito de acessar, inspecionar, revisar e corrigir os sistemas que contêm informações sobre elas mesmas.

3. Sem prévio consentimento, não se pode fazer uso das informações para outros objetivos que não os que permitiram armazenar as informações.

4. Administradores de sistemas de 5. informação são seus responsáveis e podem ser responsabilizados pelos danos que vierem a causar.

6. O Governo tem o direito de intervir na relação da informação veiculada em reuniões privadas.

Conclusões (provisórias)

Já sublinhamos acima que o crescimento das populações (em uma empresa, em uma cidade, em um país) acarreta um aumento das áreas de atrito entre os indivíduos.

Tendo em conta as diferenças profundas que se apresentam entre pessoas de variadas tradições étnicas e religiosas, pode parecer muito complicado um discurso relativo a va

lores morais comuns. Entretanto, as pessoas têm enfrentado, ao longo da História, alguns problemas que não respeitaram fronteiras nacionais, étnicas ou religiosas.

Entre esses problemas podem ser lembrados, a título de exemplo, as alterações no ambiente (e o ajuste a elas); a hostilidade; as guerras; as epidemias; a superpopulação; a miséria; a fome; os "desastres naturais" (terremotos, inundações, tornados); e, recentemente, os "desastres tecnológicos" (de que Chernobyl seria ilustração adequada).

O fato de que encaramos esses vários itens como problemas que a todos afetam, sugere que existem, efetivamente, alguns valores básicos – e.g., a saúde, a segurança e um desejo (mínimo que seja) de bem-estar.

Na Grécia Antiga, os conflitos entre Atenas e Esparta defluiam das diferentes formas de encarar o ser humano – ora como um pensador ou um artista, ora como um soldado estóico. Nos feudos medievais, os grandes senhores mantinham os campesinos no trabalho, deles arrancando o sustento. Lutas entre feudos eram inevitáveis, na constante busca de poder. Em tempos modernos, aumentando o número de países, as rivalidades não desapareceram. Ao contrário, aí estão os ricos e os subdesenvolvidos, uns com suas avançadas tecnologias, outros com a fome destruidora.

Em geral, seja nas lutas entre cidades, seja nas divergências entre feudos, seja nas dissensões entre países, leva a melhor o possuidor das tecnologias aperfeiçoadas. A tecnologia serve, quase sempre, como indicador claro de capacidade de dominação.

O futuro da humanidade não parece promissor. Como sempre, os fracos sentir-se-ão prejudicados. A fim de superar suas dificuldades, unir-se-ão para combater os fortes. As revoluções suceder-se-ão, sem cessar. Fases de equilíbrio serão alcançadas, durante as quais algumas divergências tenderão a desaparecer, ao passo que outras emergirão – até que novos conflitos se tornem inevitáveis.

***

Contornar ou aliviar um pouco os dramas que os seres humanos estão fadados a enfrentar é tarefa incontornável. Essa tarefa exigirá, sem dúvida, uma educação continuada – que terá início no berço, prolongando-se até a morte – envolvendo um pouco de Ética, uma dose crescente de capacitação profissional, e, quem sabe, uma carinhosa atenção para com os "fracos", isto é, os irmãos, os colegas de trabalho, os subordinados – e mesmo os rivais.

E ficam as perguntas:

Em que extensão devem seus registros de saúde ficar ao dispor de chefes?

Até que ponto devem arquivos financeiros (cartão de crédito) ficar disponíveis para qualquer um que esteja disposta a pagar pela informação?

Até que ponto as conversas telefônicas no trabalho devem ser monitoradas?

Até que ponto deve haver limites para os tipos de informação que outros podem coletar sobre você sem lhe dizer o que estão fazendo?

***

Atualmente a discussão sobre os limites do direito e o controle jurisdicional no espaço virtual cibernético está na ordem do dia.

"Pequena história da internet": A internet interligava originalmente laboratórios de pesquisa e se chamava Arpanet. O Departamento de Defesa norte-americano e os cientistas queriam uma rede que continuasse atuante em caso de um bombardeio. Surgiu então o conceito central da *internet*: è uma rede em que todos os pontos se equivalem e não há um comando central. Hoje ela è um conjunto de mais de 40 mil redes no mundo inteiro."

Instalou-se, em São Paulo, uma delegacia virtual, especializada em combater delitos via internet: o Setor de Investigação de Crimes de Alta Tecnologia e Meios Eletrônicos da Polícia Civil. Ela era comandada pelo delegado Mauro Marcelo de Lima e Silva. Combatia crimes cibernéticos tais como: trotes por e-mail, sites racistas, páginas de pedofilia e piratarias em cartões de crédito utilizados em compras feitas pela rede. Segundo o delegado "Não dá para praticar crimes pela *internet* sem deixar rastros".

A delegacia recebia, em média, uma denúncia por dia, que podia ser feita no local, por telefone ou por e-mail (webpol@policia-civ.sp.gov.br). Um dos casos mais rumorosos que elucidou foi o que envolvia o empresário Ricardo Mansur, dono dos laticínios Leco e Vigor, do banco Crefisul e das cadeias de lojas Mappin e Mesbla. Utilizando nome falso, Mansur teria enviado mensagens eletrônicas para executivos, espalhando o boato infundado de que o Bradesco estaria com grande capital negativo. Movia o empresário o fato de estar devendo uma grande soma de dinheiro ao banco.

Não há lei específica para o mau uso da rede de computadores. Os crimes são enquadrados de acordo com o Código Penal, por isso a punição dos responsáveis è complicada.

O que se faz hoje é adaptar o código vigente às armadilhas que a *Internet* apresenta. "A grande maioria das condutas criminosas pode ser aplicada ao mundo virtual. Mas, para efeitos penais, è necessária uma conduta específica, ou seja, que aquele fato criminoso esteja previsto em uma lei específica", explica o advogado Renato Opice Blum, especialista em direito na *Internet*.

A Polícia Federal também conta com equipes especializadas em crimes eletrônicos, tendo particular preocupação com os sistemas informatizados do Governo – em especial Receita Federal e tribunais eleitorais. São elas a Secretaria de Segurança Pública do Rio de Janeiro (www.delegaciavirtual.rj.gov.br) e a Polícia Militar de São Paulo (www.polmil.sp.gov.br). Há cerca de três anos, a PF informou que *hackers* brasileiros haviam participado de 41 dos 66 ataques em todo o mundo, em apenas quatro dias de um só mês.

O vírus "Iloveyou" infectou 45 milhões de máquinas, causou prejuízos da ordem de US$ 5 bilhões a US$ 10 bilhões, segundo o instituto Computer Economics.

O (Senador) Renan Calheiros, ex-ministro da justiça, é autor de um projeto de lei que define 20 tipos de crimes cometidos via computador, prevê multas e prisão de seis meses a quatro anos para os que forem enquadrados, com ênfase nos ataques de *hackers*.

Outros projetos de lei estavam ou estão sendo analisados pelo Senado. Um deles (do deputado Luiz Piauhylin) parecia o mais avançado do ponto de vista criminal. Dele constam alguns itens interessantes:

1. Pena de prisão de um a três anos e multa para quem apagar, destruir, modificar ou inutilizar, indevidamente ou sem autorização, total ou imparcialmente, dados ou programas de computador.

1. Detenção de seis meses a um ano e multa para quem obtiver acesso, indevido ou não autorizado, a computador ou rede.
2. Detenção de um a três anos e multa para quem obtiver segredos, de indústria ou comércio, em computador ou rede, de forma indevida ou não autorizada.
3. Reclusão de um a quatro anos e multa para quem criar, desenvolver ou inserir, dado ou programa em computador ou rede, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar o uso de computador ou rede.

Outro projeto de lei é do deputado Walter Pinheiro.

O FBI (Federal Bureau of Investigation) lançou, no mês de maio 2000, a Central de Fraude de Internet com 161 funcionários investigando denúncias. A Central trabalharia em parceria com as polícias federais e estaduais – que por sua vez estavam instituindo núcleos de ciber-investigação nas cidades do interior.

Para o diretor do FBI, a onda de recentes ataques de *hackers* aos grandes sites da Web – Yahoo, E-bay e Amazon – apenas comprovam a necessidade de se criarem legislações federais que possam acompanhar o desenvolvimento da tecnologia. O FBI trabalha com o Departamento de

Justiça em um pacote legislativo para atualizar as leis regendo crimes eletrônicos.

Um dos grandes obstáculos legislativos para o combate ao crime na *Web* è o fato de que as ordens de prisão devem ser aprovadas, *antes do início de uma investigação*, nos distritos judiciais onde o delito foi cometido. Em casos de fraude que envolvem mais de um país, a situação se agrava por questões de soberania nacional.

Legislação adequada ainda está em fase de elaboração.