2
Revisão da literatura

2.1.
Comércio eletrônico e sistemas de reputação

A expressão comércio eletrônico é muito ampla, abrangendo lojas virtuais, (como Amazon.com), transações entre empresas conduzidas eletronicamente (*business-to-bussiness* ou B2B) e leilões conduzidos através da Internet, entre outros. Neste trabalho focaremos nos portais de leilão via Internet, dos quais o maior é o eBay. No Brasil, temos o MercadoLivre[5] e, mais recentemente, o TodaOferta[6]. Apesar do nome e de serem muito conhecidos pelos leilões, esses portais albergam hoje uma grande variedade de tipos de negociação. Concretamente, há verdadeiras "lojas" que operam através deles, vendendo um grande volume de produtos a preços fixos. Daqui em diante quando falarmos em mercados eletrônicos estaremos nos referindo a esses portais. Já as entidades que os gerem chamaremos simplesmente de *operadores*.

O diferencial desses mercados é que seus operadores funcionam como *mediadores* nas negociações entre vendedores e compradores, de modo que, quando é efetuada uma compra, o operador toma conhecimento. Além disso, é oferecida às partes envolvidas a possibilidade de manifestar-se sobre o resultado da negociação. Com isso, o operador consegue disponibilizar um histórico da atuação passada de cada uma das partes, permitindo que se desenvolva o efeito da reputação sobre os negócios realizados no mercado. Os *sistemas de reputação* operacionalizam a coleta e disseminação dessas informações.

Há uma variedade de sistemas de reputação utilizados no comércio eletrônico e há também uma extensa literatura sobre o assunto, procurando explicar porque funcionam e como aperfeiçoá-los. Um bom resumo pode ser encontrado em Dellarocas (2006).

Dentro da variedade de sistemas de reputação existentes, focaremos naqueles que possibilitam a realização de negócios entre agentes desconhecidos, como é

[5] www.mercadolivre.com.br
[6] todaoferta.uol.com.br

o caso dos mercados eletrônicos. Esses sistemas de reputação possuem dois papéis distintos (Dellarocas, 2006b):

- O papel de *punidores* de comportamentos inadequados (*sanctioning role*). Esse papel está relacionado com o risco existente em transações nas quais as partes estão separadas no tempo e/ou no espaço: um dos agentes se move primeiro (e.g. efetuando o pagamento) e fica dependendo da ação do segundo. O segundo pode optar por não cumprir o acordo. Quando o não cumprimento do acordo é mais proveitoso que o cumprimento, então se dá o *risco moral* (*moral hazard*).
- O papel de *sinalizadores* das qualidades dos vendedores. Esse papel está relacionado com o problema de *seleção adversa* (*adverse selection*): a falta de informação com relação à qualidade dos vendedores leva os compradores a reduzirem o valor que estão dispostos a pagar. Isso faz com que os bons vendedores não tenham estímulo para permanecer no mercado, que acaba apenas com os piores vendedores.

Os sistemas de reputação ajudam a diminuir o risco moral ao fazer com que o ganho obtido pelo agente desonesto ao descumprir sua parte no acordo seja menor que o ganho descontado das futuras negociações no mesmo mercado. Normalmente isso se consegue publicando o desempenho do vendedor, de modo que suas atuações desonestas diminuam a quantidade de clientes e a margem de lucro, criando um incentivo para que se cumpra sempre o acordado.

Com relação ao problema da seleção adversa, a idéia é similar: publicar o histórico da atuação passada do agente para *revelar* a qualidade do agente, de modo a remover a assimetria de informação e permitir que os melhores vendedores obtenham melhores preços.

Os mecanismos de reputação efetivamente produzem confiança entre compradores e vendedores, como é demonstrado pelo constante crescimento do volume de negócios nos principais sítios de vendas que utilizam sistemas de reputação. Todavia, o problema das fraudes continua e afeta uma parcela não-desprezível desse mercado (Internet Crime Complaint Center, 2007). Isto ocorre porque os fraudadores procuram aproveitar-se das limitações do sistema para enganar os compradores. Os pontos frágeis comumente explorados são os seguintes:

- Identidades baratas (Friedman & Resnick, 2001): o custo para cadastrar-se nos mercados eletrônicos é muito baixo. Normalmente esse custo reduz-se

à exigência de informar algum tipo de identidade real (número de cartão de crédito, por exemplo), o que pode ser contornado pelo fraudador utilizando identidades roubadas. Outros serviços exigem apenas um endereço eletrônico válido. Esse baixo custo permite que um fraudador se cadastre no sistema, aplique golpes e volte a se cadastrar utilizando outra identidade, recomeçando com uma reputação limpa que lhe permite repetir os golpes. As identidades baratas também facilitam a formação de diversos tipos de conluios; por exemplo, um fraudador pode cadastrar-se diversas vezes, simular negociações para melhorar a reputação de uma de suas identidades e depois, quando aparecerem os clientes verdadeiros, aplicar o golpe.

- Monitoramento imperfeito das negociações (Dellarocas, 2006b): o sistema não monitora diretamente o desempenho dos vendedores; ele depende de que os compradores informem o resultado de suas negociações. Isso abre espaço para informes incorretos, seja por uma falha de comunicação entre vendedor e comprador (expectativas excessivas), seja por uma atuação maliciosa do comprador. Além disso, nem todos os compradores informam o resultado da negociação.
- Lentidão na atualização da reputação (Dellarocas, 2005): os mercados eletrônicos normalmente permitem a venda concomitante de muitas unidades do mesmo produto. Como há uma demora normal entre a venda e a entrega do produto, o fraudador pode vender diversos produtos sem entregar nenhum (ou entregando alguns poucos), já que as pontuações negativas demoram a aparecer.

Há diversas propostas para melhorar o funcionamento dos sistemas de reputação. Abaixo apresentamos uma classificação dessas propostas com uma breve descrição.

- **Soluções baseadas em *side-payments***. Essas abordagens incluem no funcionamento do mercado alguns pagamentos extras em certas situações, de forma a conseguir que a melhor estratégia para os agentes seja a de cooperar, cumprindo sua parte no contrato e relatando de modo veraz sua opinião sobre os produtos/serviços adquiridos. Jurca (2007) oferece um bom resumo dessas soluções.
- **Sistemas de detecção de fraudes**. Visam descobrir possíveis fraudadores através da análise da rede social subjacente nos mercados eletrônicos, for-

mada a partir da relação de compra e venda de produtos e serviços. A análise da rede pode revelar padrões de relacionamento típicos de conluios (Pandit, Chau, Wang et al., 2007).

- **Reputação amortecida**. Várias abordagens procuram introduzir algum fator de amortecimento na reputação, de modo a manter o incentivo dos vendedores a serem honestos ao longo do tempo: uma elevada reputação conquistada no passado não consegue mascarar um mau desempenho presente (Fan, Tan & Whinston, 2005; Srivatsa, Xiong & Liu, 2005).
- **Uso de identidades fortes**. Algumas abordagens propugnam meios para reforçar as identidades utilizadas nos mercados eletrônicos, como o uso de identidades persistentes (Friedman & Resnick, 2001) ou terceiros confiáveis – *trusted third parties* (Ba, Whinston & Han Zhang, 2003).
- **Ressarcimento por perdas**. Alguns sítios cobrem os prejuízos de compradores em caso de fraude, caso se cumpram algumas condições[7]. Há propostas de mecanismos nessa linha (Zhao, Fang & Whinston, 2006), mas dependem de identidades fortes.
- **Soluções baseadas em redes sociais**. O cálculo da reputação passa a levar em conta a rede social subjacente juntamente com as reputações dos outros agentes (Chen & Singh, 2001).

As soluções que visam "reequilibrar" o mercado normalmente presumem que o vendedor se comporta de modo estratégico, visando maximizar o valor presente do seu ganho ao longo do tempo. No entanto, a possibilidade de abandonar uma identidade e reentrar com outra, juntamente com a possibilidade de criar múltiplas identidades, torna esse equilíbrio difícil de ser alcançado, pois quando a reputação do fraudador cai, ele pode "reconstruí-la", ainda que com algum custo. Esse estratagema não é totalmente seguro, pois obviamente os operadores do sistema empregarão técnicas para tentar descobrir essas identidades falsas (análise de redes sociais, registros de endereços IP, valores das transações etc.). Todavia, é suficientemente lucrativo para manter elevado o número de fraudes.

Com isso, uma dificuldade persistente dos sistemas de reputação é a demora para a fraude manifestar-se e o volume de vendas que um vendedor consegue ob-

[7] Cfr. Programa de Proteção ao Comprador do MercadoLivre (http://www.mercadolivre.com.br/org-img/html/MLB/ppc_programa.html) e do ebay (http://pages.ebay.com/help/tp/isgw-buyer-protection-steps.html). Há também meios mais seguros, como o oferecido pelo BuySAFE (http://www.buysafe.com).

ter durante esse tempo, tendo uma reputação relativamente barata de se obter. Como veremos no Capítulo 3, bastam poucos dias para que um fraudador receba vários pagamentos de produtos.

Outra vertente de pesquisa é a dos sistemas de reputação distribuídos. Nos sistemas de reputação utilizados comercialmente, há sempre um operador do sistema que deve ser considerado confiável por todos os que participam nas negociações. Esse operador é quem centraliza as informações (anúncios, qualificações, dados pessoais etc.), funcionando como um grande banco de dados confiável. No entanto, há cenários em que isso não é possível ou não é desejável. Por exemplo, há diversas propostas de sistemas de reputação para redes p2p (Aberer & Despotovic, 2001). O desafio de se fazer um sistema de reputação nessas condições é ainda maior, dada a ausência de entidades que possam ser confiadas por todos.

2.2. Mercados eletrônicos e atividade fraudulenta

Deter-nos-emos agora a analisar a atividade fraudulenta que ocorre nos mercados eletrônicos, dos quais o mais conhecido mundialmente é o eBay, com um valor bruto de mercadorias negociadas de US$ 16 bilhões no primeiro trimestre de 2008 (eBay, 2008). No Brasil, o maior portal desse tipo é o MercadoLivre[8], com um valor bruto de mercadorias negociadas de US$ 449 milhões no mesmo período (MercadoLivre, 2008a). Recentemente foi lançado o portal TodaOferta[9], promovido pelo UOL (Universo Online).

Há uma premissa fundamental para o funcionamento dos sistemas de reputação: que os agentes tenham perspectivas de *permanecer* no mercado e sofrer no futuro as conseqüências de suas ações no presente. Quando isso não é o caso, esses sistemas tornam-se pouco eficazes (Resnick et al., 2000). O problema em questão revela-se na possibilidade de repetir indefinidamente o ciclo *construir reputação – explorar reputação – abandonar mercado – reentrar com uma nova identidade*, ciclo esse que é viabilizado pela ausência de mecanismos de identificação que sejam ao mesmo tempo fortes e bastante disseminados (Friedman & Resnick, 2001). Esse ciclo em si não é novidade, já que os golpes e fraudes praticados antes do advento da Internet também faziam uso dessa estratégica. Todavia, a reputação "virtual" pode ser adquirida a um custo relativamente baixo, já que

[8] www.mercadolivre.com.br
[9] todaoferta.uol.com.br

seu processo de construção é determinístico: qualquer agente pode construir a reputação que quiser, ao menos teoricamente, bastando para isso interagir com o sistema de forma adequada; por exemplo, um agente pode cadastrar-se diversas vezes em um portal e efetuar negociações entre as identidades criadas, de forma a "inflar" a reputação de uma delas (Dellarocas, 2000; Cheng & Friedman, 2005; Douceur, 2002). Certamente que esse estratagema vai implicar custos, pois normalmente os portais cobram comissões das vendas efetuadas. Ainda assim, esses custos podem ser desprezíveis diante do lucro que se pode auferir com um grande golpe.

2.2.1. Fraudes em números

Segundo o *Crime Report* do Internet Crime Complaint Center (2007) dos Estados Unidos, que coleta queixas sobre atividades criminosas relacionadas com a Internet, 35,7% das reclamações recebidas referiam-se a fraudes em leilões online; entre as reclamações que incluíam informação do valor perdido, a mediana foi de US$ 483,95. Em uma pesquisa sobre as reclamações registradas pelos usuários do eBay no sistema de reputação, a maior parte das reclamações (cerca de 36%) referia-se à não-entrega dos itens adquiridos (Gregg & Scott, 2008).

Com relação ao percentual de anúncios relacionados com atividade fraudulenta, vários autores repetem a informação divulgada pelo eBay de que menos de 0,01% dos anúncios estão relacionados com algum tipo de fraude (Gregg & Scott, 2006; Gavish & Tucci, 2008; Fan et al., 2005). Esses mesmos autores colocam esse número em dúvida, propondo estimativas como 0,62% (Gavish & Tucci, 2008), 5% (Fan et al., 2005) e 0,211% (Gregg & Scott, 2006). Um fator importante é a prevalência de reclamações de fraude em algumas categorias específicas, como a de produtos eletrônicos e de informática (Gavish & Tucci, 2008).

2.2.2. Anatomia das fraudes

Diversos tipos de fraude são cometidos nos mercados eletrônicos. As mais conhecidas são aquelas perpetradas contra os compradores (não-entrega, propaganda enganosa etc.). Contudo, há também fraudes contra vendedores: compradores que dizem não ter recebido e solicitam estorno das operadoras de cartão de crédito; compradores que pagam com cartões de crédito roubados etc. Boa parte da literatura se dedica a analisar as fraudes contra compradores, já que estes são

mais vulneráveis, seja pela inexperiência, seja pela praxe de que os produtos devem ser pagos antes de serem enviados.

Gregg & Scott (2008) apresentam uma tipologia das reclamações típicas de compradores no eBay, construída com base em dados coletados em 2003 e 2005. As reclamações são divididas nas seguintes categorias:

- Problemas relacionados com a recepção do produto (e.g. não-entrega, envio para endereço errado, sobretaxas no envio).
- Problemas com o produto (e.g. produto errado, de má qualidade ou falsificado).
- Problemas com ressarcimento (e.g. ressarcimento recusado ou parcial).
- Problemas de comunicação (e.g. vendedor não responde, é rude, usa termos que o comprador não entende).
- Problemas com leilão (e.g. leilões cancelados antes do prazo).

Cada uma dessas categorias possui outras subdivisões. Observando a quantidade de reclamações em cada subdivisão, aquela que agregava mais queixas era a relacionada com não-entrega de produtos (cerca de 36%); em segundo lugar vinha aquela que agregava queixas de que os produtos entregues não correspondiam ao anunciado (em torno de 16%).

Com relação ao *modo* como as fraudes são perpetradas, Nikitkov & Stone (2005) classificam em oito tipos as estratégias utilizadas no eBay por fraudadores. Essa classificação é baseada em outra mais geral (Grazioli & Jarvenpaa, 2003). Essas estratégias visam dificultar, de um modo ou de outro, a percepção da realidade por detrás da oferta: pode ser a realidade de um produto inexistente, de um produto de má qualidade, de um vendedor que não aceita devolução etc. Com isso, além de enganar mais facilmente sua vítima, o fraudador pode ganhar tempo e até mesmo evitar uma denúncia de fraude, o que lhe permite enganar mais pessoas. Segue a relação das estratégias descritas por eles, junto com uma breve explicação e um exemplo:

- Mascarar (*masking*): consiste em omitir ou obscurecer informações relevantes. Um exemplo é anunciar um produto usado colocando uma foto do sítio do fabricante.
- Re-embalar (*repackaging*): disfarçar a realidade com informações que sugerem o contrário. Um exemplo é atuar como vendedor exi-

bindo uma reputação elevada obtida apenas com compras de valor baixo. A reputação obtida "disfarça" um vendedor novato como se fosse experiente.

- Ofuscar (*dazzling*): misturar informações relevantes com outras pouco importantes. Um exemplo seria dar uma explicação confusa acerca das formas de pagamento.
- "Levantar a bandeira vermelha" (*red flagging*): esconder a realidade manifestando um ponto negativo inócuo. Um exemplo seria anunciar que o aparelho tem pequenos arranhões, quando esses pequenos arranhões são pouco relevantes para o produto em questão.
- Imitar (*mimicking*): copiar informações de vendedores honestos. Um exemplo seria copiar o anúncio de um vendedor já consagrado.
- Inventar (*inventing*): apresentar uma realidade falsa. Um exemplo seria inventar uma explicação plausível para uma qualificação negativa anteriormente recebida.
- Lançar iscas (*decoying*): enganar comprador atraindo sua atenção para outra coisa, por exemplo, para um brinde ou uma vantagem oferecida àqueles que comprem as primeiras unidades do produto anunciado.
- "Jogo duplo" (*double play*): reforçar uma interpretação incorreta do anúncio sugerindo uma interpretação correta. Por exemplo, informar após a compra que talvez algum dos itens entregues não funcione bem (reforça a interpretação incorreta de que o vendedor queria entregar o produto).

Essa classificação visa ser bastante abrangente, capturando diversos tipos de atuação fraudulenta.

2.2.3. Impacto das fraudes nos operadores

Os operadores dos mercados eletrônicos sofrem diversos prejuízos com as fraudes (Gavish & Tucci, 2008): comissões não pagas, custos para prevenir fraudes, consumidores que desistem de comprar, ressarcimento de consumidores no caso de compras seguradas, aumento do risco percebido, diminuição dos preços. Todavia, não encontramos na literatura informações acerca da magnitude dessas perdas.

Em alguns casos, como no das fraudes de não-entrega seguidas de abandono do sistema, podemos estimar o valor mínimo das perdas que ocorrem por conta do não-pagamento de comissões. Nos casos de fraudadores que desaparecem após o golpe, podemos assumir que não serão pagas as comissões devidas ao operador pelas vendas fraudulentas. Se também assumirmos que os compradores adquiririam o produto de outro vendedor caso não tivessem fechado negócio com o fraudador e que não tornarão a comprar no mesmo mercado após o engano, então podemos dizer que o operador perdeu no mínimo o valor das comissões não-pagas.

2.2.4. Identificando fraudes

As qualificações dos usuários com relação aos seus parceiros nas negociações são registradas pelos portais de leilão e funcionam como um mecanismo importante para melhorar a confiabilidade desses portais (Resnick et al., 2000). Essas qualificações também servem como fonte de informação para estudar atividades fraudulentas, já que freqüentemente elas serão o único registro de que ocorreu algo de errado em uma negociação (Gregg & Scott, 2006).

Todavia, as qualificações devem ser utilizadas com cautela, já que não há nenhuma garantia de que reflitam a realidade, ao menos se analisadas isoladamente: bons vendedores podem ser difamados pelos seus concorrentes (Dellarocas, 2000), usuários ansiosos podem qualificar apressadamente por conta de uma demora normal na entrega etc. É necessário analisar o conteúdo e o contexto em torno da qualificação para alcançar uma maior segurança de que nela reflete-se uma possível conduta fraudulenta (Gregg & Scott, 2006): uma qualificação negativa tem muito mais peso quando vem acompanhada por várias outras de diferentes usuários e em momentos diferentes; mais peso ainda tem quando o usuário em questão é descredenciado pelo operador do portal.

Outra opção é a de entrevistar usuários que negociam nos portais (Gavish & Tucci, 2008). A dificuldade está em conseguir entrar em contato com um número razoável de usuários, o que pode não ser viável; no caso do MercadoLivre, só é possível a comunicação direta entre usuários caso haja uma compra.

2.3. Limitações das soluções existentes

A informação mais importante que o sistema tem para calcular a reputação do vendedor é o histórico de qualificações, isto é, o conjunto de opiniões dadas pelos compradores acerca do produto comprado ou serviço prestado. A premissa básica é que certo número de negociações bem-sucedidas indicam que o vendedor em questão comporta-se bem e que pode então merecer a confiança do comprador.

O problema fundamental está em que o operador não tem como saber quais das negociações qualificadas efetivamente ocorreram. O fraudador, através do uso de múltiplas identidades ou de conluio com outros agentes, pode construir um bom histórico de qualificações. Há um custo nesse processo, pois para cada negociação através do operador é paga uma comissão. Esse custo poderia teoricamente deter o fraudador, mas na prática o aumento de taxas reflete-se na diminuição do número de vendedores, já que aqueles que possuem uma margem de lucro pequena podem abandonar o mercado, caso as comissões absorvam seu lucro. Logo, a solução de cobrar comissões elevadas não é viável (Zhao et al., 2006).

Outra solução é a de cobrar uma taxa de inscrição. Isso aumentaria o custo de se obter novas identidades, todavia com uma dificuldade similar: taxas elevadas o suficiente para deter os fraudadores também espantariam os vendedores com lucratividade menor ou de ocasião, impactando a eficiência do mercado (Friedman & Resnick, 2001).

O perfil do vendedor, que inclui o histórico de qualificações e outras informações como volume de vendas, não deixa de ser relevante, pois há combinações de fatores que diminuem a probabilidade de um fraudador forjá-lo: grande quantidade de qualificações, dispersão temporal das mesmas, valor alto dos produtos negociados, além dos mecanismos de controle empregados pelo sistema. É fácil perceber que esses fatores aumentam significativamente o custo de perpetrar a fraude, não só por conta do valor a ser gasto, mas também por conta do tempo requerido para prepará-la.

Há uma série de perfis de vendedores que, se verdadeiros, produzem confiança no comprador. Isso significa que, para fazer um julgamento correto acerca do vendedor, o comprador teria que examinar com cuidado o seu perfil. Como essa tarefa não é fácil para um comprador comum, o operador oferece medidas agregadas de reputação, que tentam resumir as informações relevantes do perfil e apre-

sentá-las de modo mais facilmente compreensível. Porém nesse processo há perda de informação: perfis verdadeiros e forjados podem acabar recebendo o mesmo valor de reputação. Como os operadores dos mercados eletrônicos se isentam de responsabilidade com relação à conduta dos vendedores, o comprador assume totalmente o risco da negociação e acaba tendo que fazer uma opção difícil: utilizar as medidas de reputação fornecidas e expor-se a perder tempo e dinheiro, ou então analisar cuidadosamente o perfil dos vendedores, gastando um tempo adicional nas suas compras. Mesmo nesse segundo caso o comprador não tem garantias tão sólidas, devido à escassez de informações (Nikitkov & Stone, 2006), e pode acabar agindo com excesso de confiança, tornando-se vítima dos fraudadores do mesmo modo (Grazioli & Jarvenpaa, 2000).

Essa situação afeta o próprio mercado eletrônico, já que os compradores defraudados podem, com o passar do tempo, alterar a percepção de risco dos usuários atuais e também dos possíveis novos usuários, prejudicando o crescimento do mercado (Gavish & Tucci, 2008).

O operador do mercado tem que manter-se num equilíbrio difícil ao lidar com o enorme número de vendedores presentes no mercado: tratá-los de forma mais rigorosa, correndo o risco de que bons vendedores injustamente atingidos migrem para outros mercados eletrônicos, ou então adotar uma postura mais cautelosa, que garante um bom relacionamento com os vendedores, mas facilita as tentativas de fraude.

Em última análise, o operador enfrenta um problema de classificação dos vendedores: quer encontrar o maior número possível de fraudadores minimizando a quantidade de vendedores normais afetados. Fazendo uma analogia com a área de recuperação de informação, o operador deve equilibrar a recuperação com a precisão.

Há uma pesquisa em andamento visando a descoberta de fraudadores através de mineração de dados em redes sociais (Chau & Faloutsos, 2005; Pandit et al., 2007; Bin Zhang, Zhou & Faloutsos, 2008). A idéia básica é revelar uma das estratégias usadas por fraudadores em sítios de leilão, que leva à formação de um grafo bipartido de negociações, com identidades “honestas” de um lado e identidades fraudulentas do outro. As identidades “honestas” são utilizadas para elevar a reputação das identidades fraudulentas através de negociações simuladas, de forma a obter a reputação necessária para cometer uma fraude bem-sucedida. As

identidades “honestas” são utilizadas também em negociações normais, tornando difícil revelar sua ligação com a atividade fraudulenta. Essas identidades podem ser reutilizadas várias vezes pelos fraudadores, reduzindo o custo total para levar a cabo os golpes.

Essa pesquisa oferece uma solução interessante para o problema da descoberta dos fraudadores. Todavia, ela se limita a uma única estratégia de fraude, não oferecendo uma solução geral: basta que os fraudadores descubram outra estratégia para que a solução proposta por eles deixe de funcionar.

2.4. Mecanismos de revelação de informação

Existe um problema relacionado com o de sistemas de reputação que é o da *revelação veraz de informação privada*: um determinado agente possui uma informação sobre algo que outro agente deseja obter; como garantir que ele revelará honestamente a informação? Esse é o caso mais geral do problema de seleção adversa. Esse problema tem duas vertentes:

- O agente tem que ter incentivo para manifestar-se: se ele não recebe nada em troca da informação dada, a tendência é não fornecê-la (problema dos bens públicos em Economia).
- O agente tem que ter incentivo para revelar *honestamente* a informação: se a informação que vai ser revelada pode interferir com a remuneração futura do agente, então ele tenderá a reportar a informação que maximiza a sua lucratividade, ao invés de reportar aquilo que efetivamente sabe.

No caso dos sistemas de comércio eletrônico, a lucratividade do vendedor muitas vezes é uma função das características do que ele está anunciando. Na ausência de um sistema de reputação, ele terá incentivo para omitir informações que diminuam o preço que os compradores estão dispostos a pagar. Outro exemplo desse problema ocorre mesmo na presença de sistemas de reputação: um comprador pode qualificar negativamente um vendedor não devido à qualidade do produto recebido, mas porque qualificando-o negativamente ele melhora a situação de um amigo seu, que é um vendedor concorrente do primeiro. Isto ocorre nos mecanismos de busca na internet com o nome de *link spam*. Também os sistemas de recomendação sofrem do mesmo problema: usuários podem manipular o resultado do sistema através das suas opiniões (Dellarocas, 2006a).

De modo geral, qualquer mecanismo onde sejam necessárias afirmações verazes de agentes para decidir algo (qualidade de um produto ou serviço, relevância de uma página na web, importância de determinado autor etc.), emergirá o problema descrito.

Existem alguns sistemas em operação na web que procuram obter informações verdadeiras a partir de interações virtualmente anônimas:

- O sítio epinions[10], que agrega resenhas sobre produtos e serviços diversos, enfrenta o problema descrito com duas medidas: remunera os autores das melhores resenhas e avalia a qualidade das resenhas feitas, considerando as vendas associadas com a leitura das resenhas e as opiniões dos demais usuários sobre o autor (grau de confiança).
- ESP game[11]: esse sítio oferece um "jogo" no qual pares de usuários escolhidos aleatoriamente tem que prover rótulos descritivos para uma determinada imagem. Quando os rótulos fornecidos coincidem, ambos ganham pontos. A idéia é colocar os usuários para executar a tarefa de descrever uma imagem, mas com um mecanismo de incentivo para efetuarem-na bem (ou seja, "inteligentemente"). O mecanismo nesse caso é o incentivo para recorrer ao conhecimento compartilhado acerca da imagem, de modo a garantir que haja coincidências nas respostas de dois usuários sem comunicação.
- O sítio Mechanical Turk[12] é um mercado onde se disponibilizam uma série de tarefas que podem executadas por quaisquer pessoas, normalmente tarefas fáceis para pessoas, mas difíceis para o computador. Se a tarefa for resolvida adequadamente, o usuário recebe uma determinada remuneração. Aqui o problema básico é o de garantir que de fato a tarefa foi executada "inteligentemente". Um dos mecanismos utilizados para isso é atribuir a mesma tarefa para vários usuários: a "resposta" mais popular é considerada vencedora e só os usuários que a escolheram são remunerados.

[10] www.epinions.com
[11] www.gwap.org
[12] www.mturk.com

2.4.1. Computação humana

Os dois últimos exemplos de sistemas construídos para extrair respostas verazes de agentes humanos são casos particulares da chamada *computação humana* (Ahn & Dabbish, 2004; Gentry et al., 2005), que consiste em resolver problemas computacionais com o auxílio de agentes humanos, normalmente recorrendo a estes para resolver subproblemas que são muito difíceis para o computador, mas relativamente fáceis para seres humanos, como é o caso do ESP game, que se propõe a obter rótulos textuais para imagens da Internet.

Com relação à viabilidade da computação humana, temos que o sítio Mechanical Turk, que segue o paradigma da computação humana, disponibiliza tarefas não-triviais por pagamentos módicos. As tarefas, chamadas de HITs – human intelligence tasks – são propostas por clientes, publicadas no sítio e usuários cadastrados podem aceitar essas tarefas, para as quais eles têm um determinado tempo para dar a resposta. Se a resposta for considerada satisfatória, então o pagamento é efetuado.

A solução que propomos para o problema de identificação de fraudadores (o jogo "pega ladrão") se encaixa nesse paradigma, ainda que com uma diferença importante: uma das premissas utilizadas nos trabalhos de computação humana é a de que as tarefas a serem resolvidas pela parte "humana" do sistema são fáceis para seres humanos, mas extremamente difíceis para o computador. Em uma primeira análise, o problema que estamos investigando (detecção de fraudadores) não se enquadra nessa categoria, precisamente pelo fato dos fraudadores procurarem enganar os clientes (humanos). Tampouco é uma tarefa que exija conhecimentos muito específicos ou pouco acessíveis, como se pode depreender da literatura (Grazioli & Jarvenpaa, 2003; Nikitkov & Stone, 2006).

Gentry et al. (2005) propõem um modelo para a computação humana chamado *Secure Distributed Human Computation* (SDHC). Os elementos mais importantes do modelo são os *fornecedores de problemas*, os *distribuidores de problemas* e os *clientes*. Os fornecedores de problemas são as pessoas ou organizações que desejam resolver problemas computacionalmente difíceis através da computação humana. Esses problemas são descritos de forma conveniente e repassados aos distribuidores, que por sua vez interagem com os clientes de forma a

conseguir que resolvam os problemas, possivelmente mediante algum tipo de pagamento ou premiação.

A interação entre distribuidores e clientes é descrita por um protocolo com duas fases: a de *registro*, onde o cliente se habilita perante o distribuidor, e a de *operação*, na qual o distribuidor repassa os problemas para os clientes, coleta respostas, monitora a qualidade dos resultados e efetua os pagamentos.