Modelos de Confiança para Segurança em Informática

Versão 1.7 – 25/11/2012

Pedro A. D. Rezende *
Departamento de Ciência da Computação
Universidade de Brasília, Brasil
prezende@unb.br

Resumo. Este artigo de pesquisa investiga elementos psicossociais que atuam no processo e no teatro da segurança, e como esses elementos, ao interagirem com a técnica, se aplicam em modelos de confiança para segurança informacional, particularmente na informática. Tais modelos, aqui propostos, exploram fronteiras de confiança que devem ser traçadas na análise de riscos, e formas com que esses traços permitem abordar conflitos de interesse, estendendo e integrando modelagens já conhecidas numa abordagem semiológica, baseada na teoria da Ação Comunicativa de Habermas e na definição de Confiança de Gerck. O artigo contém: I– Introdução; II– Criptografia e a Arte da Guerra; III– O que é Confiança? IV– Modelando Confiança; V– Cadeias de Modelos de Confiança; VI– Conclusão.

Palavras-chave: Segurança Informacional, Segurança em Informática, Modelos de Confiança, Análise Semiológica da Confiança, Análise Sintática de Infraestruturas, Análise Semântica de Riscos.

Abstract. *This research article investigates some psychosocial elements which take part in the security process and theater, and how these elements, upon interacting with techniques, apply to trust models for information security, particularly for cybersecurity. These models, proposed here, explore trust boundaries which shall be traced in risk analysis, and ways by which these traces allow for approaches to conflict of interests, extending and integrating current modeling techniques towards a semiological approach, based on Habermas' theory of Communicative Action and on Gerck's definition of Trust. This article contains the chapters: I– Introduction; II– Cryptography and the Art of War; III– What is Trust? IV– Modeling Trust; V- Chains of Trust Models; VI– Conclusion.*

Key words: Information Security, Cybersecurity, Trust Models, Semiologic Trust Analysis, Syntactic Infrastructure Analysis, Semantic Risk Analysis.

I

1.1 Introdução

Em toda civilização, regras de comportamento (costumes, normas, leis) são estabelecidas, escritas ou subentendidas, para dar segurança (estabilidade, previsibilidade) às práticas sociais. Entende-se por práticas sociais as relações interpessoais, institucionais, de negócio, de produção, etc. Não há segurança sem regras, e isso manifesta-se nos valores de uma cultura, nela possibilitando laços de compromisso e responsabilização. Assim as sociedades complexas se formam e evoluem: com base em engajamento coletivo nessas práticas, em entendimento e aceitação desses laços, e em métodos coercitivos para inibir transgressões. Métodos esses geralmente operados ou sancionados pelo Estado, mas nem sempre. De qualquer forma, seja de onde venha a sanção coercitiva, a coesão social baseia-se em confiança coletiva na eficácia dessas práticas, laços e métodos [1].

Conforme as práticas sociais se fazem intermediar por Tecnologias da Informação e Comunicação (TIC), e essas tecnologias convergem em formas e modos digitais, a ciência da computação é desafiada: pelo Estado e pela sociedade, a encontrar meios de replicar laços de compromisso e responsabilização, na esfera virtual onde imergem, com confiabilidade ao menos equivalente. As TIC evoluem velozmente e, com elas, também uma dependência da nossa civilização a esta *tecno-imersão*. Nos primórdios da informática, a crença na replicabilidade virtual desses laços brotava espontaneamente do fascínio com as tecnologias digitais. Naquele tempo era comum se ouvir que "computador não erra". Não mais.

Conforme os efeitos da dependência a esta tecno-imersão emergem e proliferam, aquela confiabilidade "automática" na informática vai sendo questionada, testada e transformada pelos que nela investem com fins escusos, e pelos que se dedicam a estudos e a práticas de segurança no seu uso. A confiabilidade com as TIC passa então a depender, sempre mais, de como ocorrem os processos de desenvolvimento, fornecimento, mediação e uso de seus artefatos e inovações. Daí, a confiabilidade no que toca ao virtual, ou que se projeta em sua esfera, progride por um caminho (como veremos) sempre mais delicado. Rumo ao que se tem chamado de cibercultura [2], onde o virtual – segundo o filósofo Gilles Deleuze – não é sinônimo de irreal, mas da *indistinguibilidade* entre o real e o irreal [73].

O caminho da confiabilidade no virtual é delicado pois, conforme as técnicas de ataque e de defesa se tornam mais semelhantes [3], e as TIC, mais convergentes e disseminadas, as possibilidades de conflito de interesses, também. Entre os que desenvolvem, fornecem ou usam tecnologias, os que precisam de proteção contra mediações indevidas, os que competem por um desses objetivos, além dos que o fazem para fins ou por meios escusos. Esses conflitos tornam-se então mais decisivos para o processo da segurança, a começar pela influência em estabelecer o que seja coibível, direcionada pelo que seja considerado indevido ou hostil por um ou outro interesse. Técnica, institucional ou legalmente coibível, por quem, com quais métodos de coerção, graus de prioridade, rigor e eficácia.

1.2 O Teatro da Segurança

Neste caminho, surgem então aparentes paradoxos, que convém aqui questionar. Por

que, em média sobre dados gerais pesquisados, quanto mais se gasta com segurança em informática, mais danos se contabilizam com incidentes de segurança, acima do aumento no uso? [4], [5]. Se quisermos entender este e outros enigmas, devemos antes assumir uma postura sensata frente às TIC. Devemos reconhecer que mesmo se as TIC forem consideradas neutras, suas aplicações não o são, pois o uso de uma tecnologia afeta perfis de riscos a que estão sujeitos os envolvidos em suas aplicações. E sobre segurança informacional, devemos aceitar que os elementos básicos de análise são perfis de riscos aos quais se expõem (ao fim e ao cabo) pessoas e entidades, sujeitos em situações diversas que envolvem aplicações tecnológicas. As tecnologias envolvidas são elementos contingentes, por alterarem esses perfis, não devendo portanto ser aí tratadas isolada ou primordialmente.

Em segundo lugar devemos, com esta postura, buscar em estudos de segurança envolvendo TICs conhecimento dos aspectos técnicos com reverente prudência ante os sentimentos pertinentes. E se possível, com humildade; a começar, frente a outras posturas. O criptógrafo Bruce Schneier ensina que qualquer segurança é, ao mesmo tempo, um processo real e um sentimento pessoal [6]. O processo real da segurança é de natureza estatística. É baseado em probabilidades de riscos se materializarem em danos (incidentes), e de eficácia nos procedimentos (protocolos) e mecanismos (métodos) utilizados para se evitar ou se detectar incidentes numa prática sistematizada. O sentimento de segurança é de natureza psicológica. É baseado em reações pessoais a percepções de riscos, e de in/adequação aos riscos percebidos. Tais percepções incluem as de funcionalidade de protocolos e métodos de proteção utilizados numa prática ou sistema, as de in/adequação desses, e as de possível ausência ou deficiência, o desprezo ou a supervalorização dessas percepções. Processo e sentimento constituem, respectivamente, os planos externo e interno da segurança, pela perspectiva de alguém interessado nela (no caso, em segurança informacional).

E esses planos muitas vezes destoam. Alguém pode se sentir inseguro em relação a um sistema cujo uso contabiliza certas probabilidades de incidência de falhas, acidentes, fraudes ou sabotagens, e se sentir seguro em relação a outro sistema com maiores probabilidades de incidentes com potencial de dano equivalentes. Enquanto outrem, vice-versa. Pela falta de calibres aferíveis entre o plano externo (sistêmico, objetivo) e o interno (vivencial, subjetivo), vivemos aquilo que Schneier chama de "teatro da segurança". Nesse teatro, encenam-se relações entre esses dois planos, com cenários, enredos e contextos do primeiro.

Nesta modalidade de teatro, expressões do tipo "sistema não confiável" ou "garantir a segurança", referentes ao uso de sistema ou aplicação tecnológica, ou de protocolo ou método de segurança idem, são proferidas com o objetivo de tão somente alimentar sentimentos de proteção ou desproteção. Sem um correspondente entendimento racional das correlações entre esse uso em práticas e as probabilidades de incidentes que tal uso alteraria, e como, relativamente às mesmas práticas sem tal uso. Um sentimento assim nutrido pode destoar do processo, inclusive porque sistemas e procedimentos técnicos embutem *sempre* riscos próprios, tais como os de falha ou de uso indevido ou ineficaz dos mesmos.

Quando a agudeza de sentimentos pessoais incita rigor no processo real, esta prudência difusa tende a se reverter em benefício coletivo. Como exemplo, consideremos dois sistemas de transporte humano, aéreo e terrestre: o medo de acidente aéreo, mais agudo que o de acidente terrestre, demanda e mantém em uso evolutivo protocolos e métodos de proteção no processo real da segurança de voo, sem correlatos terrestres. Doutra feita, quando os sentimentos pessoais dissipam o rigor do processo, os riscos interagem, se es-

tendem e proliferam. Num exemplo emblemático, em Troia, o difuso sentimento de superioridade dos troianos fê-los desprezar o risco de emboscada no presente dos gregos.

1.3 Cenários, Enredos, Papéis

Devido aos modos como o teatro pode interferir no processo, especialistas costumam opinar que um sentimento relapso de segurança tende a ser, em valores coletivos, mais danoso do que a falta de um processo real planejado. Nesse exemplo dos transportes, dada a proporção de acidentes fatais no trânsito causados por sono, embriaguez ou más condições de veículos e vias, vê-se um sentido nessa opinião. Na falta de procedimentos e mecanismos eficazes, o processo real da segurança se limita a reações *ad-hoc,* em que vítimas reagem a incidentes com recursos disponíveis na ocasião. Doutro lado, o foco nesta limitação pode aguçar a percepção dos riscos. E esta, aguçada, modular o sentimento de adequação aos riscos, tendendo a fiar na prudência a conduta de potenciais vítimas, que assim reagem para evitar perigos, com reflexo em suas probabilidades de sofrer ou causar danos.

E quanto às TIC? Nas sociedades consumistas de hoje, a ideologia dominante vê a inovação tecnológica como um bem em si mesmo. Uma de suas crenças difusas é a de que os riscos embutidos em novas tecnologias e suas aplicações serão superados, em valor coletivo, por eficiência instrumental ou econômica, ou pela satisfação de novas necessidades virtuais. E certamente, se a tecno-imersão das práticas sociais afetadas for guiada por forças de mercado. Esta crença, tecno-triunfalista, manifesta-se no teatro da segurança.

Tecno-imersões capazes de ativar impulsos atávicos (como o medo) numa direção em que o interesse coletivo insta práticas fiscalizatórias eficazes, a nível da prioridade e evolução dessas práticas poderem manter os contextos de uso dessas tecnologias modulados por sentimentos críticos de adequação aos riscos aí embutidos, capazes de manterem distinguíveis nesses contextos o teatro e o processo da segurança (como no transporte aéreo), são a exceção. A regra, sob tal ideologia, é deixar por conta do mercado o ajuste das práticas sociais, transformadas pelas TIC, aos sentimentos de in/adequação a riscos, que foram alterados pela imersão tecnológica. As ações normativas deveriam aí ser pontuais e reativas, para corrigir distorções e "garantir competitividade", é o que fia a cartilha dessa ideologia. Na prática, porém, surgem dois grandes problemas.

O primeiro problema é que, devido à natureza das TIC, essas alterações em perfis e "correções" normativas geram fortes efeitos secundários e indiretos. Efeitos que atingem em cascata até perfis de riscos não envolvidos diretamente no uso da tecnologia regulada, e a própria evolução tecnológica. A volatilidade das moedas e do crédito são exemplos disso: são efeitos-rede difíceis de extricar e quantificar, e fáceis de desprezar ou justificar ante o imperativo da eficiência (mito do progresso), para quem interessa esta ou aquela imersão tecnológica ou agenda política. Aí, ao se combinarem esse viés e a crescente complexidade (com seu gêmeo, o hermetismo) nas TIC, surge a tendência de se tomar por real o respectivo teatro da segurança. Com isso, a percepção dos limites de eficácia em processos de segurança perdem foco; e as reações normativas perdem lastro, de causas mensuráveis e efeitos previsíveis nesses processos, passando a flutuar em causas provocáveis (por fetiches e fobias insufladas) *e* efeitos esperados *nos sentimentos*[*].

* Para um exemplo, vide o do PL 84/99, em http://www.cic.unb.br/~pedro/trabs/AI5d.html

O segundo problema é que essa "regra de mercado", de que ele mesmo seja o tribunal natural para resolver conflitos de interesse irrompidos na tecno-imersão de práticas sociais, se aplica com uma lógica peculiar, da razão instrumental: a de exceções quando esses riscos e distorções, ou seus efeitos, atingem algum interesse concentrador de capital ou poder. Quando esses interesses são atingidos por novos tipos ou graus de risco, o Estado têm sido instado a cumprir sua função normativa e seu monopólio legal da força com alcance, prioridade e rigor proporcionais à concentração, visando a distribuir ou coletivizar esses riscos [7]. Mesmo em afronta ao dogma central do fundamentalismo de mercado, o ideal de Estado mínimo, porquanto ideologias são sempre cegas às suas próprias limitações e contradições; sejam elas de esquerda ou de direita, estando dominantes ou não.

Daí a tendência desse viés político-ideológico da segurança no virtual manifestar-se em modelagens e análises de riscos de forma sanitária ou censora, para que processos de segurança "da informação" não se contaminem ideologicamente; isto é, não sejam influídos por *qualquer outra* ideologia [8]. Para que sigam guiados pela razão instrumental dominante ([62], pp 77). Assim, o gravame em que se desdobram esses dois problemas nos motiva a desenvolver, nesta pesquisa, modelos de confiança para segurança informacional, aplicados à informática (capítulos IV e V). E também, a buscar razões para a escassez de pesquisas frutíferas desse teor: sobre o teor das possíveis modelagens de confiança – *distintas* das modelagens de segurança, na seção 5.0; e sobre escassez de bons frutos dessas modelagens para a segurança no virtual, no capítulo VI.

II

2.1 Criptografia e a Arte da Guerra

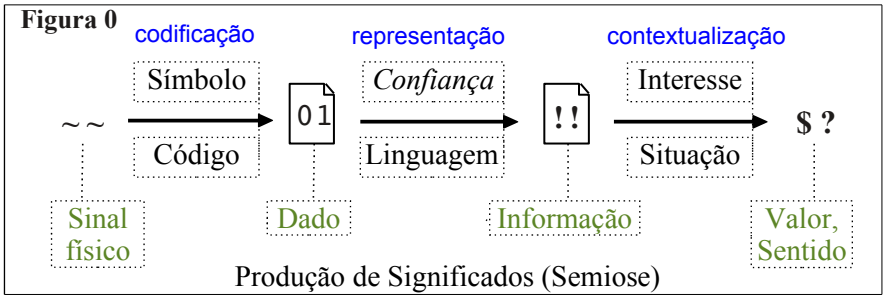
Há mais de 2200 anos, o general Sun Tsu escreveu, no clássico da literatura oriental sobre o tema [9], que a arte da guerra se baseia no logro. Isto é, na capacidade de enganar, ludibriar ou fraudar o oponente, por um lado, e na capacidade de reconhecer, neutralizar ou elidir efeitos dessas artimanhas, quando empregadas por outros. Donde o primeiro e máximo preceito, "conheça teu inimigo", dessa arte que não acredita em garantias de vitória (quando muito, de empate). Na esfera virtual, a arte da guerra de Sun Tsu tem se mostrado sem rival. Nem mesmo na arte da guerra preferida no ocidente desde o século XIX, a do general Clausewitz – que apesar de conter preceitos sagazes, como o de que "a guerra é a continuação da política por outros meios", acredita em vitórias humanas definitivas.

Os desafios para uma arte da guerra na esfera virtual são enormes. No virtual, tudo é simulacro, só possibilidades são concretamente reais. Por isso, conhecer lá o inimigo é tarefa assaz delicada, pois abstrata [74]. E lá a guerra é assimétrica: basta a quem ataca encontrar uma brecha, e cabe a quem defende proteger-se de todas. Nesse domínio da arte da guerra, o único recurso indispensável é o conhecimento; começando pelos métodos viáveis de se identificar *tempestivamente* ações e – se possível – atores hostis, aplicáveis em análise de riscos, seja quantitativa ou psicológica. Na evolução dessa arte, a tecnociência

talhou, com a criptografia, sua mais sofisticada linha de armas[1] semiológicas[2].

Há várias formas de se definir e abordar "criptografia". Para uma abordagem adequada aos motivos desta pesquisa, recorremos a um expoente da Filosofia, um dos mais influentes pensadores contemporâneos. Em sua crítica social da ciência, no livro "Conhecimento e Interesse" [61], Jürgen Habermas deixa claro que há uma relação inevitável entre os métodos e os interesses que guiam o conhecimento. Habermas entende, seguindo a vertente pragmática da semiologia de Peirce, que a análise desta relação revela só ser possível a crítica do conhecimento como teoria da sociedade ([62], pp 62). Sob este prisma, definimos Criptografia como a área da tecnociência que busca oferecer, a quem atribui determinados valores a informações, métodos e mecanismos de proteção a tais *valores*[3].

A Criptografia não pode proteger dados ou informações *em si*. Dados são apenas grupamentos de símbolos, codificados por sinais para representar informações. E símbolos não se quebram nem morrem, não se desintegram nem se deterioram, não vão presos nem à falência (os sinais que os codificam, e o que eles indicam, talvez). Sendo apenas padrões de sinais, símbolos só existem no domínio das formas, e são em si alheios ao que possam representar. Já informação, só existe na mente de quem a percebe de dados, pela instrumentação de códigos e linguagens nalgum contexto[4]. O contexto da comunicação é que gera informação: ele induz um receptor cognitivamente dotado, numa determinada situação transmissiva, a acionar um processo representacional, instrumentado por seleção de competências internas disponíveis, processo que lhe extrairá informação – conforme Shannon [12] – a partir de sinais percebidos, para seus possíveis significados (figura 0).



A Criptografia opera, como elemento desse contexto, recodificando dados, mas apenas para situá-los em distintas linguagens *enquanto transmitidos* por símbolos agrupados. O que a Criptografia pode então proteger são certos valores que certos dados significam

1 Não se trata de mera figura de linguagem: os EUA tratam o comércio desses programas em formato executável como de munição bélica, no *International Traffic and Arms Regulation* (ITAR).

2 Da Wikipedia: Semiologia, ou Semiótica (do grego *semeiotiké* ou "a arte dos sinais"), é a ciência geral dos signos e da semiose (produção de significado, figura 0), que estuda todos os fenômenos culturais como se fossem sistemas sígnicos, isto é, sistemas de significação. Ocupa-se do estudo do processo de significação ou representação, na natureza e na cultura (e, por extensão, na cibercultura). Para uma abordagem sistemática do tema, ver "Tratado Geral de Semiótica" (ref. [36]).

3 Esta definição, baseada na Teoria da Ação Comunicativa de Habermas (ref. [62]), é adequada por melhor permitir a distinção entre teatro e processo real da segurança, foco desta pesquisa.

4 Dentre as várias definições de "informação" proposta na literatura científica (ver ref. [70]), esta resume a mais adequada para o tema e abordagem desta pesquisa (ver também nota de rodapé 9).

para alguém, ao se situarem numa linguagem para representar informações *em algum contexto*. Na informação representável, o que é pois protegível são valores *relativos* a alguma situação *e interesse* (contexto). Protegíveis por relativas garantias de sigilo e/ou de integridade em transmissões, realizáveis através do espaço ou do tempo, e/ou por garantias de acesso controlado a dados em representações, contextualizáveis por quem de direito.

Garantias que são também relativas pois um mecanismo criptográfico útil funciona com base em dois fundamentos dos quais ao menos um, como veremos a seguir, será sempre relativo: (a) Controle de custos de de/codificações; e (b) Premissas de confiança. O fundamento (a) se assenta na interação entre combinatória e processo, e o (b), na fronteira entre processo e percepção. Desprezar este relativismo (por exemplo, com ilações do tipo "isso garante a segurança") simplifica, mas ao custo de confusões entre teatro e processo de segurança. Para racionalizar esse custo, meta desta pesquisa, devemos ter em clara evidência o papel essencial da confiança na produção de significados. É ela, segundo Gerck [14], que seleciona e conecta competências cognitivas internas para o processo representacional que gera informação. É ela que situa interesses do receptor no contexto, para relacionar e organizar tal informação em sentidos plausíveis e valores aduzíveis.

Para, por exemplo, no caso acima, classificar a utilidade de mecanismos criptográficos conforme possíveis contextos. Seguindo a analogia legalista americana[1], o uso *eficaz* desse tipo de arma (mecanismos criptográficos) presume que algum material necessário – munição e a própria arma – esteja em condições confiáveis de produção, transporte, armazenagem e operação. Isto significa que esse material (de cunho informacional) deve estar protegido, *antes* e *durante usos,* por controle de acesso, integridade e em certos casos sigilo, para eficácia do mecanismo. O fundamento (b), portanto, é sempre *relativo a percepção*: se a situação em foco atende ou não às premissas de confiança exigidas para eficácia do mecanismo. Desprezar qualquer desses fundamentos é reducionismo, e perigoso.

2.2 Canais de confiança

As armas da Criptografia, como todas (Sun Tsu), podem ser úteis só quando adequadamente empregadas, e, perigosas quando mal utilizadas. Quanto ao poder que esse tipo de arma confere, a Criptografia hoje não apenas permite controlar, na esfera virtual e por força de leis combinatórias, fluxos de significados em fluxos de dados, ela também impõe responsabilidades, no mundo da vida e por força de leis jurídicas, a quem opera esses fluxos ou é levado a agir por eles. Leis e tratados cada vez mais severos e desequilibrados, negociados de formas cada vez mais obscuras [23], com tipos penais cada vez mais amplos e vagos [32], tornando o uso inepto da Criptografia cada vez mais perigoso [10], e essas leis cada vez mais questionáveis sob qualquer ética universalista ou não-cética [11].

Esta pesquisa se baseia em análise de elementos condicionantes à "boa" utilidade da Criptografia, por motivos além do didático. Pela importância atual da Criptografia, e de seus desdobramentos sociojurídicos, na segurança informacional. Pelo papel fundamental das premissas de confiança na sua utilização adequada, *e* na eficácia dos seus mecanismos. Pelo caráter geral e limítrofe desse papel, de conexão entre análises quantitativas de riscos (processo) e avaliações psicológicas de percepções (sentimento). E pelo fato desses elementos condicionarem contextos gerais de tecno-imersão, onde tais conexões tendem a ser racionalizadas. Onde se tende a confundir os dois planos da segurança (o teatro como

processo), e a tratar conflitos de interesses legítimos com reducionismos, levando a práticas que ofuscam distorções daí decorrentes, e que assim sucumbem a tais distorções.

Sabemos que a utilidade da Criptografia requer condições específicas de confiabilidade no preparo do material que habilita ao uso dos mecanismos escolhidos, e que o uso eficaz desses mecanismos presume uma situação que atenda a tais condições. Sabemos também que o uso adequado a uma situação presume, antes, escolhas adequadas à *natureza* da proteção demandada. Mas é fato que há contextos onde *dos mesmos dados e ao mesmo tempo* um interesse interlocutor demanda sigilo enquanto outro demanda transparência (integridade apenas), e desses dados, nenhum interessado é mais "legítimo dono" do que o outro[5]. E este fato, por ser tradicionalmente desprezado ou ofuscado, torna-se emblemático da importância da análise em que se baseia esta pesquisa, focada no fundamento (b) .

Ante uma escolha de mecanismos, as condições necessárias para que o uso dos mesmos seja eficaz são as premissas de confiança *referentes à tal escolha*. Em informática, o material requerido para habilitar uma escolha de mecanismos inclui, via de regra, cadeias de bits em codificações próprias (cifradores, chaves, etc). Se nelas houver o que transportar, o material a transportar terá a mesma forma que os dados nos quais irão operar os mecanismos escolhidos: cadeias de bits. Neste caso as premissas de confiança colocam, para eficácia dos mecanismos, um problema recursivo: para proteger um interesse num canal de comunicação digital, parece ser necessário um canal digital *já* protegido.

Ou seja, um canal por onde o uso digital da Criptografia é habilitado deve ser confiável em relação às premissas para eficácia dos mecanismos escolhidos, e por isso, esse canal habilitante deve ser diferente daquele onde esses mecanismos irão operar. Pois do contrário tal uso seria ou desnecessário ou ineficaz. Entender isto é essencial, um teste de dissonância cognitiva frente ao hábito de se confundir confiança com segurança, porquanto nesta abordagem elas *não* são sinônimas, mas, aquela pré-condição para esta.

Na literatura, usa-se o termo "em banda" (*in-band*) ou canal inseguro (*insecure channel*) para designar um canal de comunicação onde um ou mais mecanismos irão operar, canal confiável (*trusted channel*) para um canal já protegido de certos riscos, fora de banda (*out-of-band*) para um canal diferente do canal em banda, e problema da distribuição de chaves (*key distribution problem*) para designar o problema recursivo mencionado acima, referente à habilitação de mecanismos criptográficos para uso digital eficaz.

Na figura 1 e nas seguintes, *canal de confiança* designa um canal de comunicação, no tempo ou no espaço, fora de banda e confiável em relação às premissas para eficácia do/s mecanismo/s de proteção em banda. Ainda sobre convenções adotadas nas figuras:

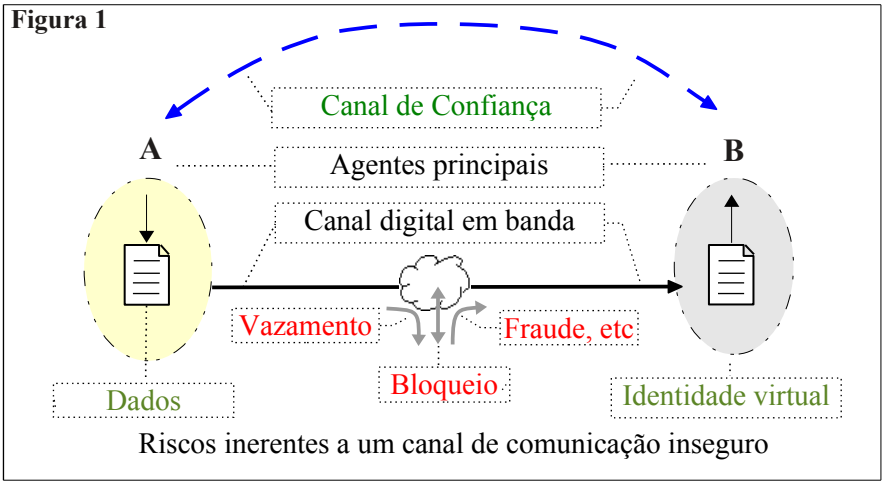
- Apenas na figura 1, para ilustrar alguns aspectos inerentes a canais inseguros, a

5 Por isso é útil, quando necessário, distinguir entre *segurança da informação* (termo que pressupõe tacitamente inexistirem conflitos de interesses legítimos entre interlocutores quanto a valores nela representados a proteger), *segurança informacional* (relativa a informação) e *segurança na informática* (relativa a contextos informatizados). Confusões entre esses tipos de contexto assumem postura ideológica ao reduzir todos ao primeiro, o qual ignora conflitos entre interesses legítimos, desprezando as consequências. Tais confusões, intencionais ou não, sempre dificultam a distinção entre teatro e processo real de segurança. Onde há conflitos de interesse, entre sigilo e transparência por exemplo, o foco da proteção em dados ou informação – e não em interesses – ofusca os conflitos e os consequentes empoderamentos (ver nota 8 e ref. [43]), nos quais, via de regra, favorecimentos são confundidos com proteções 'neutras' enquanto teleologia da segurança.

comunicação de dados em banda tem uma direção, originando-se no perímetro de um interesse a proteger. Nas demais, o fluxo de dados em banda é bidirecional.

- Um agente com interesses a proteger numa situação em foco, relativa aos quais se analisa as condições para eficácia de mecanismo/s de proteção em banda, tem sua identidade virtual como interlocutor (e interesses pertinentes) demarcados por um perímetro amarelo. Outros agentes principais para a comunicação em banda, por cinza, ou rosa se o contexto admitir significativo conflito de interesses entre principais.

Figura 1



Riscos inerentes a um canal de comunicação inseguro

2.3- Habilitando à Criptografia (Distribuição de Chaves)

A Figura 1 ilustra situações típicas: um agente (**A**) deseja enviar dados a um agente (**B**) por um canal digital. Se **A** quiser usar Criptografia para se proteger contra algum dos riscos inerentes à transmissão neste canal, e ainda ser entendido por **B**, terá que combinar *previamente* com **B** o uso de algum mecanismo, o que pode requerer o transporte de algum *material habilitante*, necessário ao uso desse mecanismo (chave, etc). Para sua eficácia, *antes do uso* **A** precisa saber que esse material teve origem e destino certos. Mas, ainda, **B** também pode querer enviar dados, e ter interesses a proteger em banda. Se aí houver conflito de interesses[4], quem seria "mais dono" dos dados é percepção irrelevante.

Importa quem (**A** e/ou **B**) conseguirá efetivamente proteger o que, e do que. Isto significa: escolha adequada de mecanismos criptográficos, relativa aos quais presume-se haver, *antes do seu uso*, correta percepção, para um eventual remetente de material habilitante, da identidade do destinatário e/ou vice-versa, e da origem, da integridade e talvez do sigilo desse material *enquanto em uso*. Com vistas a justificar uma hipótese de pesquisa que cubra os possíveis objetivos da segurança em informática, ilustramos com exemplos o que a figura 1 pode representar. Como é comum na literatura, chamaremos os interlocutores principais para a comunicação em tela, os agentes **A** e **B**, de **A**lice e **B**ob respectivamente.

Se o canal em banda se estende sobre o tempo, os interlocutores principais são via de regra o mesmo agente (**A**=**B**). Digamos que seja Alice. Alice protege dados valiosos, en-

quanto armazenados, contra vazamento cifrando-os. Parte do material habilitante necessário para a decifragem, resumidamente chamado aqui de "chave", normalmente é protegido por senha. Quando quer recuperar o que antes protegeu cifrando, Alice precisa confiar em sua memória: para localizar o que procura, para evitar o risco desta senha ter se degradado (caso a esqueça), e para evitar o risco desta senha ter vazado (caso a anote). Neste caso, o canal que a habilita a de/cifrar é a sua memória, que conecta Alice a si mesma no tempo.

Se o canal em banda se estende no espaço, os interlocutores principais são via de regra distintos (**A≠B**). Para que Bob decifre transmissões digitais, a chave para Bob decifrar deve estar com ele. Via de regra, ou esta chave teria sido enviada antes a ele, talvez por Alice, ou a chave que Alice usou para cifrar teria sido enviada a ela, talvez por Bob, ou essas duas chaves teriam sido antes geradas pela ação de algum protocolo criptográfico entre ambos (i.e. Diffie-Hellman)[6]. Assim, o canal que os habilita conectou-os no espaço.

Se essas duas chaves (a que Alice vai usar e a que Bob vai usar) forem idênticas, ou se uma delas for facilmente dedutível da outra (chaves simétricas), a geração, transporte e armazenamento de chave deve ocorrer sob sigilo (chaves simétricas devem ser secretas). Se for inviável deduzir-se uma dessas chaves da outra (chaves assimétricas), então a chave que Alice usa para cifrar poderia ser-lhe enviada às claras (chave pública), mas mesmo assim, também neste caso Alice precisa saber quem detém a chave decifradora correspondente (chave privada), presumivelmente o remetente da chave pública (talvez Bob).

Em todos esses casos, o problema da distribuição de chaves ocorre: ao menos na necessidade de alguém saber com que/m está se comunicando para habilitar-se ao uso de um mecanismo criptográfico, enquanto o canal em banda, onde esse mecanismo irá operar, ainda está sujeito a fraudes, e portanto, a erros na identificação do interlocutor. Alice não quer esquecer sua senha, nem enviá-la ao site de um falso Bob, nem via SSL[7]. Se houver entre ambos um canal fora de banda confiável em relação às premissas do mecanismo que querem usar, Alice e Bob podem antes, por esse canal de confiança, ficar sabendo com que/m se comunicarão pelo mecanismo em banda. Cabe indagar se haveria um tal canal confiável entre ambos (se temporal, entre a Alice que cifra hoje e a que decifrará depois).

Ou antes, cabe indagar se carece haver: pode a Criptografia ser eficaz *sem* canais de confiança? Pode a segurança informacional?[8] Se a resposta for não, como avaliar se há ou

6 Esquema de derivação de chaves simétricas, precursor da criptografia assimétrica. Suas premissas não requerem prévia comunicação sigilosa, exceto para identificação mútua dos principais.

7 *Secure Sockets Layer*, protocolo criptográfico que emprega certificados digitais x509 para autenticação e sigilo, usado por navegadores e servidores web na Internet através do protocolo https.

8 Um exemplo didático da importância de canais de confiança para a segurança informacional (além da informática) surgiu durante a negociação de um pacote para socorrer bancos e instituições financeiras de iminente colapso, em setembro de 2008. O então secretário do Tesouro dos EUA, Henry Paulson, e o presidente do *Federal Reserve* (Fed), Ben Bernanke, demandavam que o Congresso aprovasse um orçamento emergencial de US$ 700 bilhões, para ser gasto sem restrições, e com imunidade jurídica para ambos (os que iriam decidir como gastá-lo), sob ameaça de decretação de lei marcial se não fossem atendidos (ver ref. [41]). O Congresso resistiu e, durante a negociação, conseguiu extrair em depoimento de ambos, sob juramento, a promessa de transparência nas aplicações deste fundo de emergência. Mas a lei emergencial foi aprovada sem nenhum condicionante de instalação ou de operacionalização de procedimento capaz de produzir essa transparência. Apenas a promessa sob juramento parece que bastou, no caso, para gerar sentimentos de que o negócio seria assim, de que os gastos deste fundo emergencial seriam transpa-

não canal de confiança disponível, e se houver, como seu uso é presumido pela situação em foco? Se não houver, como criar? E se não houver como criar, como lidar com a situação? Estas são questões programáticas para a pesquisa que buscamos desenvolver. Neste artigo, abordamos as três primeiras. Para a terceira propomos, no capítulo V, cadeias de modelos de confiança em (e para) sistemas de comunicação e de significação.

III

3.1 O que é Confiança?

Até onde sabe o autor, qualquer procedimento ou mecanismo que emprega Criptografia para fins de segurança, dentre os descritos na literatura ou em uso até hoje, requer algum canal de confiança para habilitar seu uso eficaz. Os que, por exemplo, não são divulgados "por razões de segurança", *nisso* estão a requerer canal *sigiloso*: para instalações visando o uso eficaz (ver [60]). A hipótese basilar desta pesquisa generaliza esta observação empírica: *Qualquer* procedimento ou mecanismo que vise alguma forma de segurança in-

rentes. E esses sentimentos foram tomados como garantias do negócio, ou seja, da (futura) transparência das informações sobre os gastos desse fundo. Depois, quando agentes da imprensa quiseram informar-se sobre onde e como estavam sendo gastas quantias desse fundo, Paulson e Bernanke recusaram-se a revelar, alegando "segredos comerciais" (ver seção 4.1). Se foi tida como canal de confiança para habilitar a tal transparência, a promessa sob juramento nasceu morta. Inócua, pois as escolhas de onde e como gastar dinheiro em sigilo terão produzido efeitos ocultos antes que alguma decisão judicial, em processo já iniciado, obrigue-os finalmente a divulgar informações sobre o negócio, sobre quem recebeu quanto e em que termos. Trata-se de efeitos que podem ser benéficos para quem recebe dinheiro em sigilo, mas danosos para quem compete com os destinatários do dinheiro – sem saber desse recebimento – e para quem o provê (*taxpayers*) – sem saber desses termos. Tal situação estimula e amplia a capacidade de tráfego de influência que um tal sigilo proporciona a quem pode decidir como gastar dinheiro público desta forma (ver ref. [42]).

Outra situação com interesses conflitantes sobre *o mesmo dado ao mesmo tempo* surge em junho de 2009, num contexto de investigações parlamentares acerca de alegadas irregularidades na empresa Petrobrás. Um jornalista, com possível agenda oculta, quer sigilo sobre suas perguntas via e-mail ao presidente da empresa, alegando o seu direito a tal proteção em contatos com fontes jornalísticas, enquanto a fonte quer transparência, sobre essas perguntas e suas respostas, para evitar possíveis consequências desta agenda oculta (deturpação da narrativa por meio de descontextualização de trechos). A tempestividade favoreceu primeiro o interesse da fonte (que tinha as perguntas antes do jornalista ter as respostas): o entrevistado abriu um blog corporativo, e lá postou tudo antes do jornalista publicar sua matéria. Mas o jornal, controlando o canal de confiança formado pela credibilidade junto ao público, diante disso, ao invés de publicar sua versão editada da entrevista, desqualificou em editorial a sua fonte: o editorialista denunciou, com interpretação jurídica fantasiosa, suposta violação do direito autoral do jornalista na postagem do blog corporativo (ref. [58]), desprezando o fato de que uma entrevista é uma obra autoral coletiva.

Temos aqui exemplos que mostram como o teatro pode ser confundido com o processo real de segurança, e como um contexto pode induzir conflito, entre interesses envolvidos na situação, relativo à natureza da proteção almejada sobre o mesmo dado ao mesmo tempo (ver nota 5). Esses exemplos mostram também como, neste tipo de conflito, o controle do canal de confiança capaz de habilitar mecanismo(s) de proteção é decisivo para o tipo de proteção que poderá ter eficácia.

formacional, também requer. Com tal hipótese investigaremos as formas em que procedimentos e mecanismos de segurança informacional, análises de riscos que os tornam úteis, e políticas de segurança que os situem com eficácia na informática, modelam-se ou se deixam modelar, explicita ou tacitamente, por alguma noção de confiança aplicável a transmissões e interesses contemplados no procedimento, mecanismo ou política de segurança.

O objetivo geral desta pesquisa é abrir a análise de riscos e a gestão de políticas de segurança informacional para a sua dimensão semiológica, ampliando seus horizontes tecnológicos e ideológicos. É dar assim a elas novos instrumentos para descrever fenômenos e efeitos psicossociais que atuam em processos reais de segurança, incluindo interferências às quais esses processos se expõem no teatro correspondente, e para entender e explicar como interagem esses elementos em contextos computacionais.

A fundamentação conceitual para esta pesquisa encontra-se na Teoria da Ação Comunicativa de Jürgen Habermas [62], na Teoria Matemática da Informação de Claude Shannon [13], e no trabalho pioneiro de Ed Gerck no *Meta-Certificate Group* sobre modelagem de Confiança [14]. A hipótese acima surge, como contribuição originária do autor, de uma conjugação analítica de fundamentos que abordam, respectivamente, o que é ação comunicativa, o que é informação, o que é confiança, e como estas se relacionam.

Em 1948, Shannon inovou ao abordar o problema de como definir o que é "informação". Ele buscou uma definição que fosse, ao mesmo tempo, precisa para a engenharia das telecomunicações e significativa para o mundo da vida. Por abstração, ele evitou se basear na estrutura interna, na função cognitiva ou na dimensão semântica da informação.

> *"In Information Theory, information has nothing to do with knowledge or meaning. In the context of Information Theory, information is simply that which is transferred from a source to a destination, using a communication channel. If, before transmission, the information is available at the destination then the transfer is zero. Information received by a party is that what the party does not expect – as measured by the uncertainty of the party as to what the message will be."* [12]

Na teoria de Shannon, Informação é o que é transferido de uma fonte a um destino por um canal de comunicação, medido pela incerteza (probabilidade) do que *não é antecipável* em relação ao que *pode ser esperado e entendido* pelo receptor (ou destinatário)[9]. Na relação "ao que pode ser esperado e entendido", é onde Gerck situa a noção de confiança.

Como fronteira conceitual na ciência, "confiança" parece ser algo de difícil definição, até mais do que as ideias de tempo e espaço. Com a pecha de subjetivo e impreciso, o conceito de confiança era um "patinho feio" para a ciência [15], até o advento da Internet. Com a Internet, o conceito cresce em importância.

Consideremos a seguinte síntese da evolução das TIC:

---

9 Esta tradução, do autor, considera que Shannon emprega o verbo "*expect*" com acepção de "contar com" ou "aguardar" (ver *The New Michaelis Dictionary, Eng.-Port. 20th ed.*), portanto, traduzível por *antecipar*, em contextos onde algo pode ser esperado – de uma situação comunicativa – e entendido – por um interesse cognitivo dotado de uma linguagem comum: "*as to what the message will be*". O que pode assim ser esperado e entendido está, portanto, em uma mente. Ainda, *"destination"* cobre, por polissemia, tanto a acepção de uma transferência intencional do emissor quanto a de uma percepção interessada do receptor dissociada de intencionalidade na origem.

Ciclo Década	Inovação principal	Paradigma: Como pode ser...	Regime produtivo / negocial prevalecente
1940	Arquiteturas	a máquina programável?	Artesanal: Hardware <-> Software
1950	Transistores	a programação viável?	
1960	Linguagens	a viabilidade útil?	Monolítico: Hardware+software+SLA[10]
1970	Algoritmos	a utilidade eficiente?	
1980	Redes	a eficiência produtiva?	Proprietário: Software = EULA[11]<->SLA
1990	Internet	a produtividade confiável?	
2000	Cibercultura	a confiança virtualizável?	Difuso: *Software as Service. Cloud.* FOSS[12] ?
2010	Ciberguerra	a virtualização destrutível?	

Se for mesmo paradigmático para a cibercultura e para a ciberguerra, como sugerem esta síntese histórica e o conceito deleuziano de virtual, então ambos desafiam a ciência da computação para uma definição cuidadosa e inovadora de confiança. Nesse contexto, e nesse sentido, a definição dada por Gerck segue a de Shannon:

> "*Confiança é aquilo que é essencial para um canal de comunicação mas que não pode ser transferido da fonte para o destino através desse canal*."

3.2 Uma hipótese semiológica

A definição de Confiança proposta por Gerck, derivada de uma teoria que se tornou basilar para a Criptografia[13], é de natureza semiológica. Como tal, é um conceito abstrato, enquanto permite que se derive dele várias definições concretas, quando modelado por situações distintas, envolvendo sistemas de comunicação e de significação específicos[13].

---

10 Tipo de contrato de suporte em TI conhecido por "*Service Level Agreement.*"

11 Tipo de contrato de adesão ou licença de uso conhecido por "*End User License Agreement.*"

12 Modelos de desenvolvimento e licenciamento conhecidos por *"Free and Open-Source Software*"

13 A teoria da Informação de Shannon é hoje basilar para a Criptografia, dentre outras razões, porque sem seus conceitos e métodos não seria possível a Criptografia assimétrica, esta essencial ao processo de segurança em redes abertas (vide seção 5.3). Em [13], Gerck cita várias possíveis definições concretas de confiança derivadas da definição conceitual abstrata:
"Trust about an entity's behavior on matters of x is that which an observer has estimated at epoch T with a variance as small as desired",
"trust is a set of natural and logical connections between expected and actual behavior",
"trust is expected fulfillment of behavior",
"trust is to expect all previously observed behavior",
"trust is to expect absence of any previously unobserved behavior",
"trust is an inter-subjective statement that stands behind an authorization",
"trust is an open-loop control process of an entity's response on matters of x",
"trust is to rely upon actions at a distance",
"trust is to rely upon reactions at a distance",
"trust is to rely upon actions or reactions at a different point in space or time",
"trust is qualified reliance on information, based on factors independent of that information",
"trust is reliance on received information, coherently with some extent";

Em processos reais de segurança informacional, este conceito nos leva a deduzir o seguinte: se um procedimento ou mecanismo escolhido (por uma política de segurança explícita ou subentendida, em conjunto com outras medidas) requer transmissões bem sucedidas para habilitar seu uso eficaz, tais transmissões precisam ocorrer fora de banda relativamente ao canal onde tal procedimento ou mecanismo irá operar. Generalizam-se os aqui chamados "canais de confiança" para uso eficaz da Criptografia, descritos na seção 2.2.

Completando a hipótese central deste trabalho, pressupomos ainda, para fechar a extensão desta generalização, que na definição de Gerck "essencial" tem sentido amplo, universal. Ou seja, que os procedimentos e mecanismos úteis à segurança informacional, quaisquer que sejam ou venham a ser, *sempre requerem*, dentre suas premissas de confiança, *entendimento prévio* para sua eficácia; isto é, requerem canal de confiança. A hipótese responde negativamente às duas primeiras questões programáticas erguidas no cap. II.

No seu trabalho pioneiro, Gerck reconhece o contexto hiperconectado da cibercultura como formado por comunidades virtuais que se agregam em torno de algum interesse comum, extraindo daí motivos para uma conceituação de confiança que permita modelagens próprias para sistemas de comunicação ou de significação específicos. Porém, suas abordagens visam – ao contrário desta pesquisa – antes o caráter virtual dessas comunidades, do que o potencial de conflito entre interesses diversos, percebíveis em vários contextos.

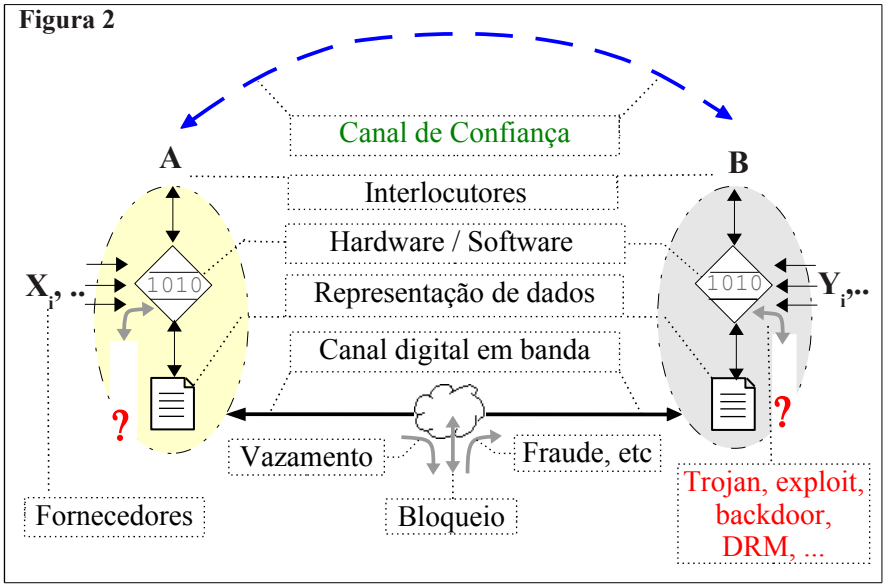
Para mostrar a utilidade virtual da conceituação que propõe, Gerck busca abordar situações nas quais não vem ao caso a forma representacional dos agentes; seja qualquer deles pessoa, *software* ou máquina. Tanto o agente que confia como aquele no qual se confia, ou demais envolvidos (mediador, fornecedor, etc). Nesta pesquisa, pelos motivos expostos no capítulo I e para responder à terceira questão programática em II, buscamos abordar situações nas quais algum interesse do agente que confia, em algo ou alguém sobre algum assunto, se encontra em potencial conflito com outro interesse (pertinente ao contexto)[14]; esteja qualquer desses interesses representado no processo real por pessoa,

---

"trust is that which an observer can rely upon to some known extent regarding a subject matter";
"trust is what an observer knows about an entity and can rely upon to a qualified extent";
"trust is received information which has a degree of belief that is acceptable to an observer";
"trust is knowledge acceptable by an observer";
"trust is knowledge about one's perception of a fact";
"trust is that which provides meaning to information";
"trust is a link between a local set of truth-values and a remote set of truth-conditions";
"trust is a link between reference and referent";
"trust is a link between referent and sense";
"trust is a link between reference and sense";
"trust is measurable by the coherence of understanding",
"trust is that which absence can make any state possible",
"trust is that which absence can make any state transition possible",
"trust is that which absence cannot justify reliance";
"trust is time measured without a clock and/or space measured without a scale";
"trust is a link between conceptual and perceptual realities";
(objective) "trust is a coherent collective agreement";
(inter-subjective) "trust is a bilateral agreement, not necessarily balanced";
(subjective) "trust is what you know that you know that you know" – i.e., you know, you can recall at will and you know how to use.

14 Confiança não pode ser forçada (Gerck). Assim, quando um agente *sente-se obrigado* a agir co-

software ou máquina, percebíveis inclusive no contexto hiperconectado da ciberguerra.



Assim, ilustramos a abordagem *orgânica* desta pesquisa em refinamentos da figura 1 onde estejam representados os mediadores da comunicação e da significação que influem na virtualização de práticas sociais em situações diversas. Tais refinamentos se referem a contextos computacionais, mas a abordagem também se aplica, com menos detalhes, a contextos gerais e alheios à informática. Em refinamentos, face ao caráter abstrato e universal da confiança (como essência da significação em comunicações), seguimos Garfinkel & Spafford [26]: consideramos interesses de fornecedores das tecnologias intermediadoras, e dos que atuam na operacionalização destas, como pertinentes à análise de riscos.

3.3 Interesses e riscos

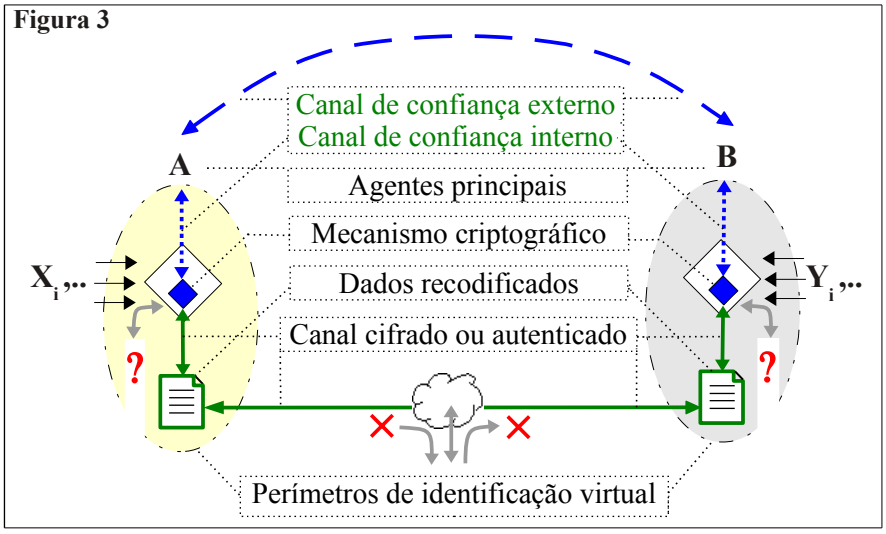
Nas figuras 2 e 3 estão indicadas as mediações e os agentes mediadores (**X**$_i$,.., **Y**$_i$..., todos ali chamados "fornecedores") com interesses relacionados ao uso das tecnologias que fornecem ou suportam, para os agentes principais, em situações e contextos a analisar. Das análises cabíveis num refinamento inicial podemos destacar, desde logo, alguns aportes à especificidade dos riscos. Ao situarmos as intermediações tecnológicas, com seus fornecedores, entre os agentes principais (**A**lice e **B**ob) e o canal digital pelo qual esses agentes se comunicam em banda, identificam-se novos tipos de risco.

Novos riscos que são inerentes às respectivas intermediações tecnológicas, tais como os de invasão ou intrusão (na figura 2, em vermelho) sobre canais laterais (*side channel*

mo se confiasse noutro, tal situação indica potencial conflito de interesses, modelável pelas distintas percepções da *extensão* da confiança que ambos presumem do contexto, isto é, pelas diferenças entre a "confiança" que um agente presume ser demandada de si pelo outro, e a oferecida de si para o outro, *relativamente* ao assunto em tela e em expectativa a esse agir (ou ao não-agir).

attacks), mas não só. Vislumbram-se também novas interações entre riscos[15], e entre possíveis efeitos destas interações em premissas de confiança no processo da segurança[16] .

Figura 3



Quanto aos riscos inerentes ao canal em banda (vazamento, fraude e bloqueio), indicados na figura 1 como abordáveis com mecanismos criptográficos (×), cabe observar que:

- Vazamentos só serão neutralizáveis; e só se as premissas de confiança para uso eficaz do mecanismo de cifragem escolhido valerem *também* no canal de confiança interno a cada plataforma usada por principais, isto é, valerem também nos canais laterais utilizados, na situação em foco, entre os agentes principais e os respectivos dispositivos (hardware ou *software*) que operam tal mecanismo (indicados na fig. 3).
- Fraudes só serão detectáveis; e só se as premissas de confiança para uso eficaz do mecanismo de autenticação escolhido valerem *também* no canal de confiança interno a cada plataforma usada por principais (como indicado na fig. 3).

Dentre as possíveis interações envolvendo riscos de vazamento ou de fraude, podemos aqui já destacar algumas, por impactarem as premissas de confiança em contextos onde se situam, através da severidade (potencial de dano ou probabilidade) dos riscos recombinados ou propagados por vulnerabilidades em canais laterais (*side channel attacks*):

- Se um ataque ocorrer via vulnerabilidade lateral, sobre o canal de confiança interno à plataforma usada por um agente principal, portanto dentro do perímetro de uma identificação virtual deste agente, o risco desse tipo de ataque estende e propaga

15 Para exemplos corriqueiros, e cada vez mais complexos, desse tipo de interação na esfera digital consulte-se, por exemplo, literatura sobre os tipos de ataque conhecidos como *Cross-Site Scriping* (XSS) ou os conhecidos como *Cross-Site Request Forgery* (CSRF).

16 Idem, sobre ataques conhecidos como *Zero-day exploits* (0-D), ou sobre ferramentas do tipo *Metasploit* (*frameworks* para penetração, que varrem alvos identificados por endereço IP em busca de vulnerabilidades conhecidas, e nelas descarregam *payloads* de *exploits* conhecidos, a partir de menus e códigos executáveis selecionáveis de um banco de dados), disponíveis na web.

seus efeitos (potencial de danos), atingindo interesses relacionados a ambos principais (**A**lice e **B**ob), conforme os valores aduzíveis no contexto em tela. Isto porque os principais, via de regra, só perceberão a perda de eficácia do mecanismo em uso depois das consequências, devido à natureza do mecanismo e da proteção possível[17].

- Se uma invasão ou intrusão ocorrer num ponto do fluxo de dados anterior ao do acionamento do dispositivo que cifra ou autentica, ou posterior ao do dispositivo que decifra ou verifica/valida, ou dentro (ou de dentro) de um desses dispositivos (na fig. 3, num ponto azul do canal lateral), tal ataque lateral (*side channel*) via de regra torna o respectivo mecanismo ineficaz. Se este for seu propósito, o ataque será furtivo: tenderá a ocorrer da forma que lhe for mais fácil para disfarçar indícios e despistar rastros na plataforma (por exemplo, através de uma *backdoor* ou de um *exploit*)[15, 16].

- Sob regimes normativos, administrativos ou jurídicos, que imputam responsabilidades pelo uso de tais mecanismos sob a premissa implícita de confiabilidade nessas plataformas [10], [32], ou que estendem esta imputação incluindo responsabilidade pela validade de tal premissa (ver nota 48), ou ainda, que obrigam a utilização ou a habilitação para práticas sob tal premissa, tácita ou explicitamente assumida pela norma [16], as consequências dessa propagação agrava os riscos, individual e coletivamente, em paralelo à sensibilidade valorativa no contexto jurisdicional em tela.

A progressiva tecno-imersão de práticas sociais judicadas por regimes assim distorcidos parece imparável, devido à lógica da eficiência, guiada pela ética utilitarista que domina o capitalismo tardio [11]. Nesta dinâmica, tais interações e propagações tendem a escalar e a persistir, gerando novos tipos de risco (APT), ampliando o potencial de dano e as probabilidades de incidência dos riscos assim "diluídos". Enquanto nessa escalada, mais valores passam à tutela desses regimes jurisdicionais, os quais refluem à esfera de influência virtual sobre os processos normativos desses regimes, realimentando essas distorções.

- Os desequilíbrios entre riscos e responsabilidades (direitos de acusação, de defesa e de causa) sob tais regimes geram, em par com mais oportunidades negociais para mediadores, na forma de mercados cativos via *vendor lock-in*, de blindagem normativa e desregulamentação seletiva contra riscos jurídicos, novas oportunidades para organizações virtuais clandestinas. Para espionagem privada (com fins diretos ou terceirizáveis), sabotagem via *botnets* (com fins extorsivos ou político-econômicos [64]), intermediação para fraudes em transações e contratos eletrônicos, com fé ou garantias públicas [10], [50], [51] ou com lavra e execução automatizadas[18]. Sem fa-

17 Ao tentar sensibilizar legisladores sobre distorções e perspectivas de insegurança jurídica na Medida Provisória que instituiu a ICP Brasil (MP 2.200, ainda em vigor na data desta versão), o autor foi informado de que, ao abordar membros da Comissão de Ciência e Tecnologia da Câmara dos Deputados, teria chance de ser ouvido se resumisse o problema em quinze segundos. A metáfora escolhida foi: Criptografia é como linguiça (mas não pelo sentido óbvio da metáfora, o da "tripa de bits"): só se distingue a boa da estragada pelos efeitos colaterais posteriores (ref. [18]).

18 Decisões erráticas, inócuas ou contraproducentes, tomadas por autoridades para debelar a crise econômica global eclodida em 2008 têm, em boa medida, plausível racionalidade na necessidade de se seguir ocultando e/ou fomentando, destruindo ou bloqueando acesso a provas de fraudes financeiras e contábeis que podem vir à tona em falências catastróficas ou em regimes estatizados, fraudes que alguns *insiders* estimam ultrapassar quatro trilhões de dólares. Para estimativas, ver ref. [37], [38]; sobre incidência no mercado de *subprimes*, ver ref. [39]. Para um estudo detalhado do acolhimento jurídico de contratações lavradas e executadas automaticamente, ver ref. [40].

lar do extravazamento da ciberguerra à ação clandestina de Estados nesse teatro [78]

- Tal dinâmica se sustenta na ética utilitarista, e reflui por vias de risco moral [11]. Ela estimula interesses aparentemente (ou noutras situações) conflitantes a promoverem, coludidos, mais confusões entre teatro e processo de segurança, as quais ampliam esses desequilíbrios. Esses desequilíbrios seguem assim transferindo novos riscos, que tendem a se tornar sistêmicos, expandindo velhos riscos, que seriam inerentes à realização negocial desses interesses, e coletivizando os que cabem. Os efeitos dessa dinâmica ao final incluem a politização e a erosão do Direito (capítulo VI).

Esta análise preliminar já indica importantes papéis que a arquitetura tecnológica dos sistemas de comunicação, a estrutura axiológica dos sistemas de informação, os modelos negociais que viabilizam sua operacionalização, os ordenamentos normativos a eles aplicáveis, e as interações entre esses, podem desempenhar em pesquisas sobre segurança no virtual. E também em análise de riscos, em políticas e gestão de processos reais de segurança informacional que pretendam algum fôlego. Antes de abordarmos esses papéis, porém, encerramos esta análise preliminar sobre interações entre riscos inerentes a canais digitais e a intermediações tecnológicas com algumas observações sobre riscos de bloqueio.

Pela natureza de ambos, os mecanismos criptográficos não podem inviabilizar, nem neutralizar ou refinar o rastreamento de ataques de bloqueio, cujos alvos são *fluxos* de dados. Quando muito só podem, em certas situações específicas, despistar a identificação de alvos potenciais, para tentar reduzir a probabilidade de ocorrerem. Os protocolos e métodos de anonimização conhecidos, que se valem de agentes intercessores e/ou de técnicas de ofuscamento local de dados referentes a tráfego, são capazes de apenas atenuá-los.

- Bloqueios só serão atenuáveis; e só se as premissas de confiança para uso eficaz do mecanismo de anonimização escolhido valerem também nos canais formados, na situação em foco, por encapsulamentos do fluxo de sinalização (entre os agentes principais), operáveis também por agentes intercessores em banda.

  Cabe aqui destacar a diferença entre proteção *contra* acesso indevido ao *conteúdo* dos dados (às informações que eles representam), e proteção *para* acesso ao *fluxo* esperado dos dados (aos sinais que lhes codificam): o primeiro tipo de proteção (à confidencialidade, contra *vazamento*) é diretamente abordável pela Criptografia: com uso adequado de cifragem *para sigilo,* se o canal de confiança presumido estiver disponível e sob controle do interesse a proteger; já o segundo (proteção à disponibilidade, contra *bloqueio*), o é apenas indireta e parcialmente, com uso adequado de cifragem *para anonimização*, se suas premissas de confiança estiverem atendidas.

  Sobre interações envolvendo riscos de bloqueio, cabe por fim observar que são fontes ricas de conflitos de interesse. A anonimização é vista com desconfiança em processos normativos, pois seus métodos também servem a interessados em evadir sanções, para despistar a identificação de agentes principais em situações ilícitas de varejo (geralmente em contextos que envolvem compartilhamento de dados). A viabilidade técnica desses métodos, e a baixa relação benefício/custo para reverter sua eficácia nesses usos, leva outros interesses – inclusive de mediadores que noutras situações conflitariam – a buscar juntos estratégias para neutralizar esses métodos.

  Tendo percebido que com tecnologia apenas não se impõem, essas estratégias passam então a atuar em processos normativos de forma a conduzi-los (através de licen-

ças [59] e de atos administrativos [68]) ou a cooptá-los (através de leis e tratados internacionais [65]) em direções que, seja por efeito colateral ou intencional, bloqueiam direitos à privacidade e à autonomia da vontade em meio digital [63]. Direitos antes ou noutras situações exercíveis pelos principais [17], cerceados à revelia de legítimas funções do anonimato e do compartilhamento na esfera virtual[19]. Assim, tais estratégias agravam interações e conflitos de interesses entre os perfis atingidos.

Como se vê, o gravame descrito na introdução atinge perfis de riscos inerentes à intermediação tecnológica, na esfera virtual e na comunicação digital, com interações e propagações que se realimentam em cascata. Porém, pela dimensão político-econômica desse gravame, sua dinâmica tende a ser "des"ideologizada. Trivializada ou racionalizada com reducionismos guiados por utilitarismos míopes. Muitas vezes a pretexto de se facilitar ou simplificar a "solução tecnológica", como se a agilidade, a hiperconectividade e outras facilidades oferecidas pelas TIC não tivessem contrapartida; no caso, em complexidade semiológica. Extravasando essa dimensão, tal gravame passa a atuar, em teatros da segurança, no papel de alguma evolução inevitável, a exigir dos principais mais "investimento", e de todos, mais apoio ao vesgo furor normativo da vez. Sob esta perspectiva, observa-se:

1. Uma enxurrada de jurisdoutrinas que, envernizadas com tênue saber jurídico, seguem flutuando, embarcando as TIC como fenômeno mágico-triunfalista, e arremedando, sem a menor crítica ou constrangimento, a marquetagem de encastelados mediadores monopolistas ou a verve de seus prepostos;

2. O uso de tais doutrinas, como pretensas legitimadoras desta "des"ideologização instrumental, para alavancar, ora aventuras normativas radicalizantes, que flutuam em efeitos fóbico-sentimentalistas (vide 1.3), ora políticas de segurança ortodoxas ou terceirizadas, que acabam desapontando quanto à eficácia.

IV

4.1 O que é Política de Segurança?

Política de segurança é, em três palavras, definição de restrições. Ir além disso requer alguma taxonomia, pois ambos os substantivos nesse termo têm dupla tradução ao idioma nativo da cultura onde a computação digital originou-se: *policy, politics; safety, security*. Porém, uma taxonomia para segurança ou políticas de segurança não é meta desta pesquisa, pelo que nos limitamos a propor conceituações pertinentes ao aporte dos modelos de Confiança aqui descritos, no processo de formação e gestão de políticas de segurança informacional. Essas políticas serão daqui em diante referidas pela sigla "PSI".

19 Devido à tendência monopolizante do mercado de *softwares*, decorrente do efeito rede associado à natureza não-rival ou antirrival do tipo de bem simbólico mercadejado, usuários são via de regra hiposuficientes perante fornecedores. Com *vendor lock-in,* as proteções jurídicas perdem eficácia (ref. [11]). Porém, em contextos de licenciamento FOSS o anonimato (do licenciado a usar o *software*) protege o usuário, em par com a *garantia* de acesso ao código-fonte, contra o potencial de abusividade que a posição de tecnomediador dominante habilita a esses fornecedores.

Uma PSI define, principalmente, prioridades. Com sentido de *policy*, ela contempla ou formaliza, em linhas gerais, crenças, princípios, metas e objetivos gerenciais, procedimentos e mecanismos aceitáveis ou mandatórios para agentes numa entidade (que a adota), incluindo modos de ação visando a sancionar desvios, enfrentar contingências e reformular-se com aferições [19]. Para situá-las nesta pesquisa, podemos entender uma PSI como um mapeamento dinâmico de interesses, da entidade ou relacionados a seu negócio ou função, sobre o processo (e o teatro) da segurança, concernentes a seus ativos e sistemas de informação. Particularmente, para máxima aplicação da modelagem aqui proposta, concernentes a ativos e sistemas relacionados a tecnologias digitais. Não ter uma PSI própria, ou não seguir uma que se diz ter, pode então ser entendido como uma política (ainda no sentido de *policy*) que visa priorizar e/ou ofuscar interesses do agente que assim decide.

A natureza da entidade aí se reflete. Quando ela é simples, o informalismo ou a terceirização de sua PSI reflete um alinhamento de interesses entre a entidade e quem a dirige ou por ela responde. Quando ela é não trivial ou complexa, como uma empresa de capital aberto ou ente estatal por exemplo, a produção e gestão de sua PSI, formal ou não, própria ou não, insere-se no processo político – aqui no sentido de *politics* – que distribui competências a seus agentes internos. Neste caso, esse processo político projeta na PSI alguma priorização de interesses, a começar pela autoridade para formular e decidir sobre PSI.

No caso das empresas de porte considerável, uma tática hoje ortodoxa, em voga para projetar e acionar interesses relacionados às TIC, é conhecida por "inteligência competitiva" [20]. Porém, o que esse termo vem significar tem como referência a competição em mercados. Ao passo que, quando se trata de ente estatal o "mercado" em que seus interesses competem tem (ou deveria ter) como referência a missão do Estado, e não a mercantilização das funções de seus agentes ou sua fetichização negocial. Estados nacionais, por exemplo, competem por soberania, não por lucro a curto, médio ou longo prazos (os quais podem advir da soberania, segundo o mercantilismo). E esta soberania tem custo, cada vez mais ampliado por concessões e por dependência a tecnologias não livres [8].

Confundir esses tipos ou referentes, pode sinalizar alguma inteligência neoliberal, mas, não é sadio para PSIs – especialmente em um ente estatal – devido aos conflitos de interesse que tais confusões ofuscam[20]. Principalmente quando fornecedores monopolistas nos mercados de TIC agem politicamente para ideologizar assim suas práticas negociais "modernizadas" e disputas a respeito delas[21]. Em contextos onde esse ofuscamento é denso, a modelagem aqui proposta permite desembaçar a formação e gestão da PSI e seus processos de segurança, ante as distorções inerentes ao fundamentalismo de mercado.

---

20 Em 1938 o presidente dos EUA Franklin Roosevelt alertou o Congresso: "*...the liberty of a democracy is not safe if the people tolerate the growth of private power to a point where it becomes stronger than their democratic state itself. That, in its essence, is fascism -- ownership of government by an individual, by a group, or by any other controlling private power."* (ref. [21])

21 Recentes demandas ao governo de Quebec solicitando informações sobre contratos "guarda-chuva" firmados com grandes fornecedores, IBM, Novell e Microsoft, foram atendidas apenas parcialmente. As informações solicitadas envolvendo IBM e Novell foram atendidas, mas a Microsoft se opôs. Os advogados da empresa interferiram, com o argumento de que a divulgação dos documentos poderia prejudicar a "competitividade" do cliente (governo de Quebec, cuja função constitucional é regida pelo princípio da publicidade). No original: "*[releasing the documents] would likely risk to cause serious prejudice to our client and would procure the competition an appreciable advantage and would substantially undermine the competitivity of our client.*" (ref. [25])

4.2 Modelando Confiança para Políticas de Segurança

A ideia básica é simples. Seguir o preceito máximo de Sun Tsu, "conheça teu inimigo", adaptando-o para inimigos virtualizados: abstraindo-os. Se a segurança é no sentido de *safety*, uma ação fortuita, de efeito virtual e com potencial de dano, manifesta-se conforme as "leis de Murphey". Para enfrentá-las, medidas de contingência são escolhidas, tais como *back-ups, no-breaks,* redundância de componentes, apólices de seguro, etc. Se a segurança é no sentido de *security*, uma ação deliberada e virtualmente hostil manifesta-se conforme a primeira hipótese metafísica de Descartes. Se o demônio tem toda a inteligência e poder de disfarce que lhe atribui o dogma da Igreja, com o que concorda Descartes, a primeira questão a se enfrentar no processo é: como saber se nossa percepção do que é real – ou fático, para os juristas – não está sendo ocultamente manipulada em nossa mente? Com a tecno-imersão de práticas sociais onde chegou, na esfera virtual precisamos de um arsenal adequado e eficaz para termos chance de saber, do que ali é real.

Porém, esta chance está limitada não só pelo que Deleuze nos ensina sobre o virtual, mas também pelo fato do jogo ali ser com gênios do mal. Voltando a Descartes, ele responde àquela questão primeira, sem se queimar na fogueira, com a hipótese que separa o saber fundado em validação pelo método científico, do saber fundado em dogma. E assim a ciência chega onde chegou, ocultando o seu (dogma) na validade do (seu) método. E por aí, quem se fia em percepção dela transmitida para explicar a si o que é real, raramente a validou por esse método; e quem assim a validou, ou revalidou, tinha aí seus interesses, seu próprio entendimento do método científico, o de seus revisores e o de seus editores, em contexto. Tinha-os, portanto, como condições "de contorno" para o explicar-se. É o que destaca, em sintonia com Habermas, o filósofo da ciência Paul Feyerabend [46].

A definição de Gerck cabe aqui perfeitamente. Na segurança informacional, essas condições de contorno se aduzem como premissas de confiança. E pela hipótese central deste trabalho, no processo real da segurança essas premissas *sempre requerem* canal de confiança. Tê-los (os canais de confiança) mal ou não reconhecidos como presumidos, ou mal ou não disponíveis e controlados como necessários, são ações para enredos trágicos no teatro da segurança, realmente encenáveis quando esse teatro se confunde com o processo.

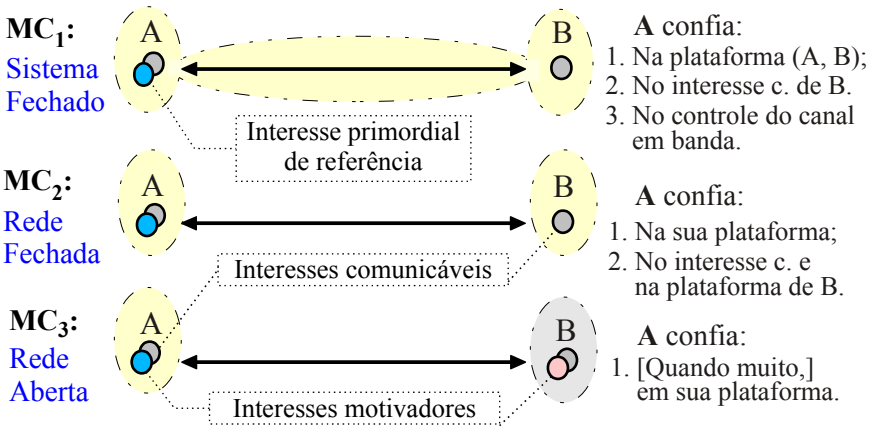
Precisamos saber identificar os canais de confiança presumidos por processos reais de segurança, para podermos aferir se uma dada situação concreta, centrada em interesses a proteger, dispõe deles *e como*. Para isso, investigamos como as premissas de confiança – que por hipótese demandam algum canal de confiança – se aduzem da arquitetura dos possíveis sistemas de comunicação, e na estrutura dos possíveis sistemas de significação existentes. Para esse fim, propomos uma classificação para essas arquiteturas e estruturas.

Uma taxonomia que classifique tais arquiteturas e estruturas conforme possam distinguir premissas de confiança, e demandá-las *minimamente* a quem faz uso dos respectivos sistemas. Esta classificação, talvez por uma variante do paradoxo Sausurreano[22], é de natureza semiológica, pois só conseguimos realizá-la a contento fixando referenciais para uma classe de sistemas (de comunicação) na outra classe de sistemas (de significação) e vice-versa. A ideia é aplicar a Teoria dos Atos de Fala de John Austin [79], precursor de

22 William Labrov, fundador da sociolingúistica, assim nomeia a co-dependência, constatada por Sausurre, em só se poder estudar o aspecto social duma linguagem no indivíduo, enquanto o aspecto individual só poder ser estudado por observações da linguagem em seus contextos sociais.

Habermas e pioneiro da “virada linguística” na Filosofia, ao domínio das tecno-imersões.

Figura 4



Modelos de Confiança para sistemas de Comunicação (sintáticos)

Começamos pela classe dos sistemas de comunicação, que chamamos sintática. Para descrever as premissas de confiança que tais sistemas demandam, fixamos o referencial para uma dada situação em um interesse primordial: no propósito que motiva intimamente a entidade em foco (**A**) a buscar comunicação em banda. Os sentidos desse propósito, basilar para a PSI dessa entidade porquanto *telos* de sua ação comunicativa [62], determinam premissas acerca dos outros interlocutores legítimos, isto é, acerca de outros agentes principais para comunicações que podem ser significativas no contexto em tela, a começar de suas localizações: espacial, temporal, cognitiva e volitiva (quem poderia se interessar).

Na modelagem para análise de riscos, esse interesse primordial, indicado por um ponto azul na identidade virtual do agente principal em foco (A), não precisa coincidir com interesses que possam ser comunicados nesta sua busca, isto é, percebidos em atos pelos quais este agente se oferece para engajar-se em comunicação com outro principal (**B**). Nem com interesses que possam vir a ser comunicados em consequentes interlocuções entre ambos (pontos cinza), esteja qualquer desses interesses explícito ou implícito na oferta e nas interlocuções[23]. Nem tampouco, em princípio, com o interesse íntimo que motive um agente a engajar-se em banda como principal, aceitando e respondendo a tal oferta[24] (ponto rosa).

Este referencial, fixado num interesse primordial que motiva o agente em foco a engajar interlocutores como principais, pode encontrar, sob o prisma desta proposta, distintos tipos de situação, conforme as características do sistema de comunicação subjacente ou

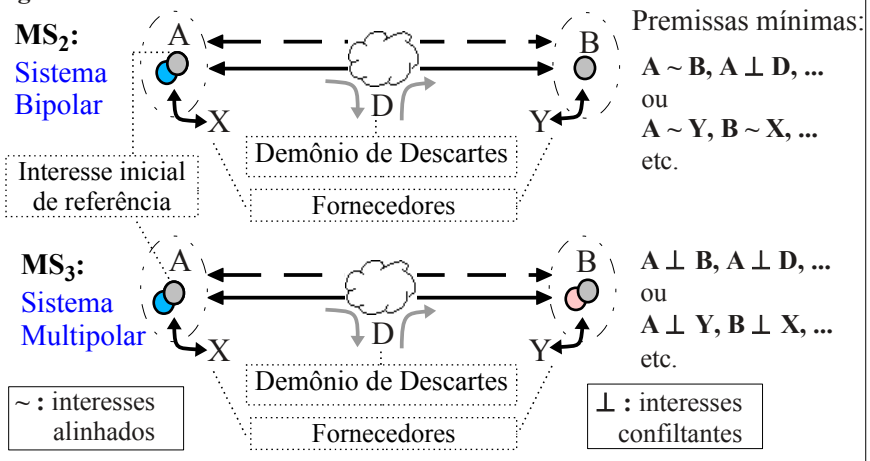
23 A arte de fazer os interesses motivador e comunicável parecerem o mesmo enquanto divergem, sem dizer aquele ou ambos, ocorre na área de *marketing* e em tipos penais (estelionato, etc). Na Teoria da Ação Comunicativa, se o agente inclui em seu cálculo possíveis decisões do outro interlocutor, seu agir é dito *estratégico*, em distinção ao agir teleológico e ao normativo, nos quais se baseiam a teoria neoclássica da escolha econômica e a teoria clássica dos jogos ([62], pp 101).

24 Hipótese necessária para modelar riscos inerentes a certas condutas criminosas, como estelionato

necessário a tais engajamentos, as quais distinguem o sistema quanto às premissas de confiança que sua arquitetura minimamente demanda. Esses tipos se configuram nos modelos sintáticos **MC1**: Sistema Fechado; **MC2**: Rede Fechada; e **MC3**: Rede Aberta.

Em paralelo, classificamos os sistemas de significação, que chamamos semânticos. Para descrever as premissas de confiança que esses sistemas distinguem, fixamos o referencial noutro interesse: no propósito que o agente principal em foco comunica, explícita ou tacitamente, ao se expressar inicialmente sobre dado assunto[25]. O contexto das ofertas ou interlocuções pelas quais esse agente busca se expressar, determina premissas sobre outros agentes a considerar, isto é, sobre agentes com acesso aos sinais transmitidos nos canais (em banda ou fora, externos ou internos) envolvidos na situação em foco, aptos a contemplar interesse/s pertinente/s à análise de riscos. Isto é, tal contexto determina possíveis interesses em interferir ou se locupletar da comunicação praticável entre principais.

Figura 5



Modelos de Confiança para sistemas de Significação (semânticos)

Para a modelagem em tela, esse interesse inicial, propósito comunicável indicado por um ponto cinza na identidade virtual do agente em foco (**A**), não precisa coincidir com o interesse primordial que o motivou a se oferecer para comunicar-se (ponto azul), esteja qualquer desses interesses explícito ou implícito em suas ofertas e interlocuções[22]. Nem tampouco, em princípio, com o interesse íntimo que motiva outro agente (**B**) a engajar-se na comunicação em banda[23] (ponto rosa), e nem com o interesse que este outro agente expressa, ou insinua aderir[26], ao engajar-se como principal (ponto cinza junto ao rosa).

Este referencial, fixado num interesse que o agente em foco comunica ao se expressar

25 O interesse inicial comunicável é como a "persona" do interesse primordial motivador: ele propõe, explícita ou tacitamente, intenção de expressar, em determinada modalidade ilocucionária, um certo conteúdo proposicional; ou seja, ele é o elemento ilocutivo inferível de uma ação comunicativa compreensível, necessário ao entendimento conforme a Teoria de Habermas ([62] pp 87)

26 Hipótese necessária para modelar certos modos de agir estratégico, como os intimidatórios, e *situações interlocutórias degradáveis em desentendimento, por exemplo em trolling ou flaming.*

inicialmente sobre dado assunto, pode encontrar, sob o prisma desta proposta, distintos tipos de contexto, conforme os valores aduzíveis no sistema de significação situado por tais ações comunicativas e pelo assunto, os quais demandam o sistema quanto às premissas de confiança que sua estrutura minimamente distingue. Esses tipos de contexto se caracterizam pela polarização de interesses que, na semântica de riscos do sistema, estejam em significativo conflito[27]. Esses tipos se configuram nos modelos semânticos **MS_2:** Bipolar, com dois polos de interesses conflitantes; e **MS_3:** Multipolar, com três ou mais.

Na figura 5 a modelagem de um alinhamento de interesses é indicada pelo sinal ~, e a de um plausível ou significativo conflito de interesses, pelo sinal ⊥ entre agentes principais ou coadjuvantes nas comunicações em tela. Um conflito pode ocorrer entre interesses comunicáveis, motivadores ou cruzados (entre um interesse comunicável e um interesse motivador), entre qualquer par de agentes em tela, inclusive cruzados no mesmo agente[28].

4.3 Usando Modelos de Confiança

A ideia é situar os interesses mapeáveis pela PSI em modelos adequados, para que esses modelos possam melhor instruir (com métricas aferíveis e *feedback*) decisões ao longo da formação e gestão da PSI, da análise de riscos e do processo de segurança correspondentes. Esta modelagem permite, de saída, delinear as fronteiras virtuais do processo real da segurança, que *são* os canais de confiança presumidos pela situação em foco. Isto é importante porque esses canais são calcanhares de Aquiles do processo da segurança, especialmente em contextos computacionais. Vejamos algumas explicações e justificativas.

Começamos pelo rótulo dado ao agente apto a praticar vazamentos ou fraudes em canais de comunicação em banda, na figura 5. "Demônio de Descartes", em referência à hipótese metafísica do filósofo, sinaliza o interesse do agente **D** em ocultar ou disfarçar identificações suas, de sua ação e/ou de seus interesses no contexto em tela. Embora o interesse motivador da ação de D possa ser inefável (não comunicável), pode estar implícito[29], podendo assim ser modelado pela natureza desses tipos de ataque. Ou seja, é plausível supor que o autor de ataques desse tipo esteja motivado a agir camufladamente.

Entretanto, o risco de bloqueio não está ali associado ao agente D, nem a qualquer outro agente. Isto por várias razões: esse tipo de ataque, via de regra, identifica a ação (bloqueio) para a vítima (quando a vítima não encontra razão acidental para a interrupção de um fluxo esperado); mas mesmo assim permite, ao agente que ataca, ocultar seu interesse motivador. Até mesmo quando esse agente, fora de banda, se identifica e expressa um in-

27 Confiança não pode ser forçada. Por isso, um conflito de interesses indicado, por exemplo, por divergência nas percepções sobre a extensão da confiança presumida no contexto (ver nota 14), pode situar-se entre qualquer dos 4 interesses em foco (motivador e comunicável dos principais).

28 Alinhamento entre dois interesses comunicáveis é necessário (mas não suficiente) para o *entendimento,* denominado "razão discursiva" na Teoria da Ação Comunicativa. Num mesmo agente é possível o conflito cruzado, necessário para colusões e outras modalidades do agir estratégico (ref. [62]). O único tipo de conflito talvez não situável (sem utilidade nesta modelagem) seria entre um interesse motivador explícito e um interesse comunicável tácito no mesmo agente.

29 Sob a ética utilitarista subjacente a teorias econômicas clássicas, um interesse implícito é indicado pela questão: quem poderia lucrar com *isso*, quanto e a que custo? Sob éticas universalistas ou cognitivistas, por pesquisas sobre o agir normativo: sobre históricos de condutas conflituosas em situações ilocucionárias equivalentes, para se aduzir padrões de reputabilidade *fora de banda.*

teresse comunicável para sua ação bloqueante. Pois um interesse comunicável pode ser explicitado para despistar o interesse motivador do mesmo agente. Essa tática pode camuflar ataques de bloqueio[30], por exemplo, induzindo a vítima a perceber o bloqueio como algum colateral de interferências entre mediações tecnológicas ou de outros conflitos. Tal enredo tem sido útil, no teatro da segurança, para camuflar interesses inefáveis mas implícitos como motivos plausíveis para agentes mediadores[31] (**X**, **Y**). Devido à sua natureza peculiar, fronteiriça entre *safety* e *security* (entre o acidental e o intencional), o risco de bloqueio será melhor compreendido com a análise de modelos multipolares.

Cabe aqui destacar a natureza orgânica da modelagem proposta, cujos modelos se imbricam, permitindo-nos abordá-los e analisá-los ora em paralelo, ora em *feedback*, ora em refinamentos. Mais precisamente, um modelo sintático (de confiança em comunicação) sempre se acopla a um modelo semântico (de confiança em significação), pelo referencial fixado para o primeiro, num interesse primordial motivador: o que se quer *ao se* comunicar também orienta a PSI sobre demais interesses relacionáveis no contexto. E vice-versa, pelo referencial fixado para o segundo, num interesse inicial comunicável: o que se quer comunicar também indica meios de transmissão viáveis para a situação. Ainda, uma modelagem $\mathbf{MC_i}$ sempre encadeia modelos $\mathbf{MC_{i-1}}$, e uma modelagem $\mathbf{MS_3}$ sempre refina modelos $\mathbf{MS_2}$, por meio da arquitetura ou da estrutura interna dos respectivos sistemas.

Ao abordarmos as possíveis cadeias de modelos sintáticos, identificamos as fronteiras do processo real da segurança em situações modeláveis. Essas fronteiras *são* os canais de confiança presumidos por cada modelo da cadeia sintática que representa a situação em foco. E, ao abordarmos os possíveis refinamentos em modelos semânticos, mapearemos as premissas de confiança, inclusive as demandadas pela cadeia sintática situada, para o contexto em tela. Esse mapeamento indica como as premissas mínimas podem ser atendidas, como elas devem estar disponíveis na situação em foco, e como elas devem ser controladas pela entidade a proteger no contexto em tela, calibrando seu perfil de riscos em sua PSI. Por fim, para o alcance desta proposta, cabe aplicar a hipótese de trabalho da qual partimos: quaisquer situações e contextos informacionais seriam assim modeláveis.

Antes do detalhamento para contextos computacionais, cabem algumas observações sobre modelagem semântica. Esta proposta exclui o tipo de modelo semântico unipolar porque sua semântica de riscos os mapearia a um perfil utópico, no qual todos os interesses relacionáveis se alinham, sem conflitos significativos com o principal em foco. E ela conflui as possíveis semânticas com mais de dois polos de interesses possivelmente conflitantes, em um único tipo multipolar (**$\mathbf{MS_3}$**), porque o refinamento de dois para três polos introduz um novo tipo de risco, o de colusão (conluio)[32], que interage com outros tipos

30 Uma tática comum para camuflar interesses consiste em transmitir um interesse comunicável, explícito e verossímil, que cruza em contradição *performativa* com um interesse motivador, inefável mas implícito no contexto (ver nota 29) como plausível para o mesmo agente, que assim age estrategicamente (ver ref. [62]). Uma espécie de álibi motivacional.

31 Quando, por exemplo, o interesse motivador do fornecedor incluir a obsolescência programada ou o *vendor lock-in* de seus clientes, como no caso do Service Pack 3 para o MS Office 2003: à guisa de proteger clientes contra "formatos inseguros" (ref. [43]). Ver também o caso dos sistemas de votação totalmente informatizados (DREs), que bloqueiam meios de recontagem pelo eleitor (transparência) à guisa de proteger-lhes contra "eleitores mal intencionados" (ref. [31]).

32 Numa palestra para alunos de engenharia, em que o tema escolhido por eles era segurança no processo eleitoral eletrônico, ao tentar explicar a gravidade dos riscos de conluio o autor perce-

de risco em modos que ofuscam até a análise da polarização [74]; para ser eficaz, uma conspiração deve parecer apenas mera "teoria da" conspiração. A mera possibilidade de colusões já se constitui, pois, em vetor para refinamentos na análise de riscos, em **MS3**.

Modelos unipolares, como base para refinamentos, serviriam tipicamente para representar um perfil de riscos em contextos computacionais onde a situação envolve computadores desligados e trancados em cofre com a chave perdida, e onde o demônio de Descartes estaria de folga. A segurança se resumiria a *safety*. Trata-se, portanto, de modelagem inútil para processos reais de segurança no estágio atual das tecno-imersões de práticas sociais; apesar de estar implícita em abordagens *bottom-up* na PSI de entidades não triviais que desconsideram, talvez deliberada ou casuisticamente, ataques origináveis em agentes internos ("todos aqui são honestos, alguém duvida?"). Estas assim modelam-se com enredos trágicos, onde papéis centrais são encenados sob o efeito Dunning-Kruger [75].

Tais enredos servem também de modelagem para entidades complexas cuja abordagem a riscos é excessivamente simplista. Entidades cuja PSI mapeia interesses[33] conforme uma lógica binária ("nós contra eles"), em situações onde uma tal semântica de riscos, de **MS2**, é reducionista demais. Tais enredos tendem a encenar suas tragédias em situações que envolvem sistemas sensíveis em rede aberta[34], ou sistemas em rede fechada que atendem a interesses conflitantes e oponíveis ao interesse superveniente (do dono do sistema). Ao não contemplar refinamentos multipolares em sua análise de riscos (como em **MS3**), por orientação precária ou por outra razão, essas entidades se expõem, junto com outras relacionadas no contexto e talvez despreparadamente[35], à condição de reféns, a armadilhas de colusão envolvendo mediadores e terceiros[36], ou sob ambos perfis (como em [31]).

---

beu dificuldades na plateia em acompanhar a explicação. Perguntados a respeito, 9 entre 10 não sabiam o que significa a palavra "conluio" (ver ref. [31]). Um estudo sério do processo da segurança requer bagagem intelectual considerável (ver seção 1.2), para se evitar nele as possíveis ciladas do demônio de Descartes; e humildade, para se avaliar honestamente a bagagem que se traz e ao que ela serve, para se evitar o efeito Dunning-Kruger (ref. [75]). Desqualificar os aportes deste requisito como *antibusiness*, paranoia, esquerdismo, eruditismo, antididatismo, amadorismo, desinformação, teoria da conspiração, autopromoção, embromação, impropério, vitupério, desacato ou insulto, só tisna a seriedade da abordagem, mas elide substância para a crítica sadia a pesquisas como esta, enquanto dificulta a distinção entre teatro e processo real de segurança.

33 Quando a PSI não existe formalmente, ou não é seguida, esse mapeamento estará implícito.

34 A dinâmica de riscos com as *mortgage-backed securities* na crise econômica pós 2008, que os espalhou e amplificou através de colusões entre agentes envolvidos, exemplifica, com a confissão de erros do ex-presidente do *Fed* Alan Greenspan (ver ref. [44]), a importância da adequada modelagem de interesses em contextos onde a semântica de riscos é inerentemente multipolar.

35 O teatro "realista" da segurança induz o risco desta espécie de transtorno bipolar contaminar a psique de quem responde pela PSI, se esta estiver debilitada por imprudência solipsista, seja de natureza ideológica ou narcísica (vide refs. [74], [75]), impedindo um diagnóstico interno adequado e uma evolução favorável desse quadro. Para agravar, tal quadro é indistinguível de estratégia ou esquema para acobertar corrupção, corroborando a definição deleuziana do virtual.

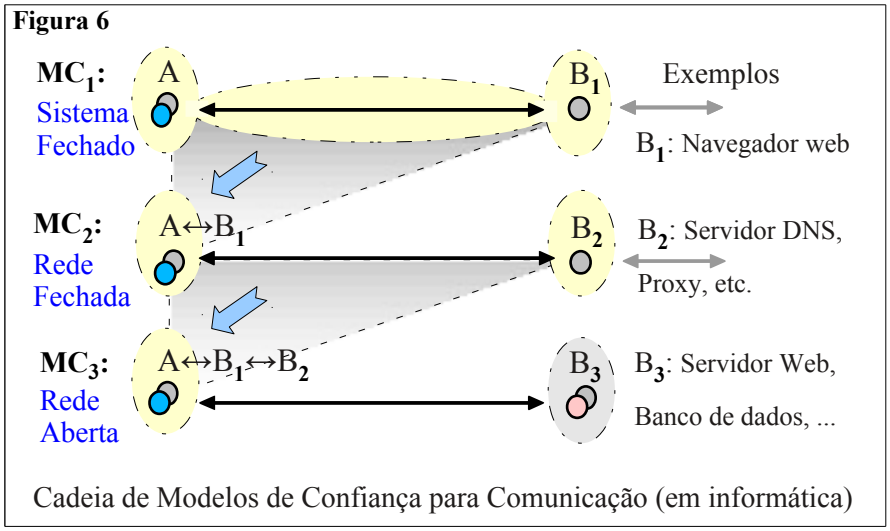
36 Riscos desse tipo se agravam nas situações em que possíveis agentes achacantes (que podem fazer reféns, por exemplo com *vendor lock-in*) ou coludentes (que podem agir em colusão, como analisado em [47], pp 119) encontram táticas para dissipar elementos que poderiam informar objetivamente sua culpabilidade (fazer prova criminal) e que estariam ao alcance da vítima, tornando assim a ação intencional indistinguível da acidental, e a prática conspiratória indistinguível de uma mera e surrada "teoria". Um exemplo didático (mas não digital): um agente de uma empresa contratada para reformas deixou, ao final do expediente, uma empilhadeira estacionada em posi-

V

5.0 Cadeias de Modelos de Confiança em Informática

A ideia de se encadear modelos de confiança, representada na figura 6, é similar à ideia conhecida em análises de riscos tradicionais e em PSI ortodoxas como segurança em profundidade, ou em camadas (*in-depth security*). A diferença é que nas abordagens ortodoxas os únicos referenciais estruturantes são as arquiteturas dos sistemas de comunicação – sejam os internos às plataformas computacionais, como nos modelos OSI e "*orange book*" (DoD 5200.28-STD), sejam os internos a redes digitais corporativas, como nos padrões ISO 27K (topologias de segurança, norma ABNT NBR ISO/IEC 17799) [27].

Figura 6



Cadeia de Modelos de Confiança para Comunicação (em informática)

A noção de confiança em abordagens ortodoxas é intuitiva, rudimentar face aos desafios, às vezes fundada em ideologia ou marquetagem, induzindo um caráter implicitamente bipolar à respectiva semântica de riscos. Ou então, quando o conceito de confiança é tratado formalmente (geralmente para sistemas distribuídos), a modelagem tem, via de regra (com Capra, Shand, Patel, por exemplo), fundamentação puramente semântica. Isso as limita no potencial para se refinarem com análises de características topológicas (e semiológicas, quando aquela se imbrica com estas) dos canais envolvidos, relativas aos de confiança presumidos pelas situações modeláveis e aos disponíveis nos contextos em tela.

ção que encobria a câmera do circuito interno de vigilância na sala-cofre do Banco Central em Fortaleza. Durante a noite, a empresa de vigilância encarregada nada fez a respeito. Naquela noite, uma quadrilha assaltou a sala-cofre por um túnel subterrâneo. Doutra feita, em contextos digitais é mais fácil para uma vulnerabilidade "tunelizável" (*backdoor*) fazer-se passar, se descoberta (por potenciais vítimas), como erro de programação ou de operação, enquanto permite, antes disso, a quem a conheça invadir sistemas. Para um exemplo do que pode ter sido mesmo um erro de programação, ver ref. [49], e para um que talvez não (*backdoor* oculta no WMF por quinze anos até ser descoberta por um pesquisador de segurança em 2006), ver refs. [24], [59].

Nada das abordagens tradicionais, entretanto, precisa ser descartado para a introdução e utilização de um conceito mais cuidadoso, funcional e eficaz de confiança. Apenas adaptado, visando a uma análise de riscos mais elaborada e uma relação custo/benefício mais estável para a gestão de PSIs. Precisamos, por exemplo, entender melhor as consequências semiológicas do advento da Internet, isto é, as consequências *para estratégias*, como sinalizam o crescimento concomitante de gastos com segurança em informática e de danos com incidentes reportados apontando para o demônio de Descartes [4], [5], de um lado, e de outro lado, o uso político que vem sendo feito disto [7], [18], [22], [23].

Uma postura cética, inercial, conservadora ou ortodoxa pode, todavia, racionalizar ou desprezar tais sinalizações, que indicam crescente ineficiência das abordagens tradicionais à segurança no virtual em sua evolução. Uma tal postura tenderá a considerar esses sinais insuficientes ou irrelevantes para se privilegiar abordagens semiológicas ao tema da confiança. Ou pior, quando a crescente ineficiência atual é reconhecida, a considerar como única alternativa a radicalização normativa [17]. Mas, antes, podemos agregar a esses sinais outras evidências empíricas. No plano teórico, com uma avaliação do estado da arte na abordagem sociológica; e no *front* pragmático, do estado da arte na engenharia de software.

Para a primeira, analisaremos uma contribuição da sociônica[37] à economia de bens simbólicos, que explora formalmente o conceito de confiança com latitude inédita [76]. Esta análise será incluída [na versão seguinte deste relatório de pesquisa] em seguida à descrição da modelagem semiológica aqui proposta. Para a segunda, analisaremos uma contribuição oferecida pelo principal cientista da empresa líder em certificação digital no planeta, co-projetista de boa parte das tecnologias sob fogo de batalha (HTTP, PKIX, SAML), em um congresso científico cuja temática se aproxima da pretendida nesta pesquisa. Começamos então pela segunda, a seguir.

No resumo da palestra "*From CyberCrime to CyberConflict: The Infrastructure of Crime and Worse to Come*", proferida em abril de 2009 no seminário "*Cyber International Relations*" promovido pela *Harvard Kennedy School of Government* junto ao *Center for International Studies* do MIT, Phillip Hallam-Baker se expressa nesses termos [52]:

> "*[...T]he documented and proven capabilities of the infrastructure that has developed to support Internet crime are real and deserve attention as an urgent national security issue. The Internet has revolutionized every other aspect of modern life, it must revolutionize warfare. If the idea of cyber-warfare appears fantastical, it is because we are mischaracterizing the nature of the threat. .... We face a large number of challenges.*
>
> *The information we have on opposition activities is highly unsatisfactory. By the time an Internet crime trend can be reliably quantified it is obsolete. And even though we have no shortage of technical countermeasures, we have only succeeded in deploying measures that provide a short term tactical benefit to the deploying party rather than strategic measures that could defeat or at the very least dramatically raise the bar for the opposition.*"

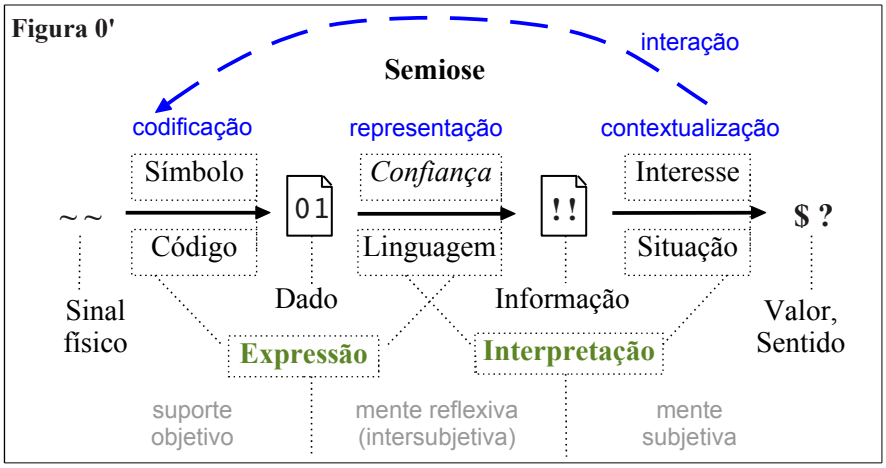
cujo último parágrafo pode ser assim traduzido: "A informação que temos sobre ativi-

37 Conforme a ref. [76], Sociônica é a área Inteligência Artificial dedicada ao estudo e construção de sistemas capazes de gerenciar 'sociedades de agentes computacionais autônomos em ambientes informacionais abertos operando em larga escala'.

dades hostis é *altamente insatisfatória*. Quando um novo padrão de prática criminosa na Internet chega a ser *confiavelmente* quantificado, esta prática *já está obsoleta*. Embora não haja nenhuma escassez de medidas tecnológicas à disposição para enfrentá-las, só temos alcançado sucesso produtivo com medidas que proporcionam benefício tático de curto prazo a quem as adota, mas não medidas estratégicas que possam vencer essas atividades ou ao menos erguer barreiras significativas contra elas."

Para que as informações sobre atividades hostis se tornem satisfatórias, o que falta? Pela abordagem aqui proposta, o que falta é Confiança. Ou melhor: falta uma adequada aferição daquela que se tem, e da que é possível ter. Falta isto em relação à fonte (de dados expressivos), à identificação dos tipos (de atividade hostil) e à interpretação (da dinâmica de hostilidade face às situações e contextos). A questão que no fundo se insinua, seguindo Gerck, é como então alcançar satisfatórias extensões[14, 26] da Confiança possível.

Esta questão se torna crucial quando entendemos o que diz Sun Tsu sobre a natureza da guerra (seção 2.1), cabalmente manifesta na análise de Hallam-Baker. Porém, respostas satisfatórias (que evitem, por exemplo, circularidades, comuns em abordagens tradicionais à conceituação de confiança) requerem antes uma percepção da natureza semiológica da questão. Para isso convém situar "expressão" e "interpretação" na produção de significados (fig. 0'), etapas internas ao processo representacional que demandam Confiança para a interação simbólica necessária ao entendimento mútuo e à coesão social ([62], pp 66).



Conceituações puramente semânticas da noção de confiança, embora tradicionais, são reducionistas, e nalgum ponto autorreferenciadas. Por isso elas nada tem oferecido, e sob esta perspectiva nada têm a oferecer no limiar de sua aplicabilidade, em resposta ao impasse apontado por Hallam-Baker. Elas só oferecem mitigações minguantes, porquanto a natureza semiológica da noção de confiança, como indica a "virada linguística" da Filosofia, é imanente [72, III]. A ideia de Confiança transcende tanto a semântica quanto a sintaxe, pois, na semiologia, semântica (relação dos signos com o que designam), sintaxe (relação dos signos entre si) e *praxis* (relação dos signos com quem os usa) não são autônomas. Na dúvida, se não sabemos bem o que ela é, valeria a pena reduzir "confiança" a um conceito apenas técnico? Como saber se a que julgamos poder ter, em alguém sobre

algo situado no virtual, nos satisfaria afinal? E o Demônio de Descartes, nesse impasse?

Tomando por base comparativa a mais antiga referência tecnocientífica à noção de confiança abordada em contextos computacionais que pudemos localizar [53], e seus mais celebrados desenvolvimentos no campo atual da segurança em informática [54], podemos ilustrar mais concretamente a natureza das limitações intrínsecas às abordagens ortodoxas. Nestas, o conceito de confiança é algo contextualmente restrito a valores inter/subjetivos atribuídos a expectativas de adequação. Especificamente, expectativas de adequação *sintática e tempestiva* de interlocuções a algum protocolo de comunicação digital, significando que o propósito do interlocutor seria presumível pelo mero engajamento no protocolo.

O celebrado modelo de Patel – *Trust and Reputation model for Agent-based Virtual Organizations* (TRAVOS) [55] – e suas extensões baseiam-se num sentido quantitativo de confiança, calculável por meio de probabilidades dos agentes engajados se comportarem conforme esperado, relativamente a algum protocolo de comunicação predeterminado. Essas probabilidades são quantizadas para decisões interativas sobre subsequentes engajamentos. Esse sentido é aduzido com avaliações comportamentais de terceiros, sobre prévias interações destes com o agente avaliado (reputações). Nessas modelagens, o problema da recursividade (como interromper as regressões), que vem da demanda circular por prévias interações em predeterminado protocolo, é redutível à premissa de que os agentes engajáveis como principais fazem parte de uma organização (os modelos são para estas).

Tal redução pode ser compatível com o conceito semiológico de Confiança, que adotamos, desde que a apresentação dos agentes se dê por canais de confiança adequados e disponíveis à organização modelada (mais na seção 5.3). Porém, das aplicações do modelo TRAVOS, as que prometem utilidade abordam situações onde a forma de organização opera no virtual (o modelo é para estas). Ou, em extensões do modelo, onde "organização" se reduz a uma mera predeterminação protocolar em rede aberta (como em redes P2P). Nessas situações, o lastro hermenêutico das prévias interações, suporte para o cálculo de e com reputações (como métrica para confiança), se agrega com semântica para interlocuções praticadas *em banda*, violando o conceito semiológico de Confiança. Com isso inviabiliza-se, segundo a hipótese central desta pesquisa, ou a utilidade ou a eficácia dessas abordagens. E de fato, essas abordagens não alcançam modelar interesses hostis dotados de estratégias adaptativas, que submergem sob a superfície tecida pela hermenêutica das interações da vez; nem situações em que a comunicação com agentes inconfiáveis faz-se inevitável (por exemplo no e-comércio), como bem diagnostica Hallam-Baker.

No limiar funcional das abordagens tradicionais à noção de confiança, a necessária identificação de atividade hostil ou oponente ainda se baseia em hermenêuticas de comportamento identitário *on-line* (*profiling*), ou seja, em interpretações de interações para apresentação e para validação de identificações (ver seção 5.1) *tudo em banda*. Donde o déficit de Confiança diagnosticado. Se as estratégias possíveis com as abordagens tradicionais fossem úteis e eficazes nesse limiar, as listas negras de endereços IPs, por exemplo, formariam uma barreira significativa contra o spam e pragas congêneres (*phishing*, etc). Entretanto, esta barreira é facilmente contornada, por exemplo, com engenharia social de varejo (*spear phishing*) e por ágil rotatividade (*churning*) em *botnets*, as quais vem sendo observadas, por seus efeitos indiretos, em larga atividade na Internet [71].

Tais limitações advém do fato das abordagens semânticas tratarem comunicação e significação como processos estanques ou independentes. Então, se de "confiança" entender-

mos tudo isso mas racionalizarmos ou desprezarmos as consequências, teremos que enfrentá-las sem estratégias eficazes, mitigando apenas. Haverá quem prefira apenas mitigar, ou convencer clientes à mitigância mais rala e cara, ou a si e a estes de que só resta a radicalização normativa – em termos habermasianos, a "juridificação" – como saída. Dentre as vítimas da Síndrome de Estocolmo Digital [11], decerto. Mas, haverá alternativa?

Para o escopo desta pesquisa, a semiologia quer dizer que o processo de comunicação e o de significação *não podem* ser compreendidos a contento separadamente. Que esses dois processos são como forma e função de um todo orgânico. Para quem interessa entender melhor as consequências disto, os canais de confiança presumidos pelos processos da segurança *em informática* oferecem perspectivas instigantes. Para explorá-las[38], examinamos a cadeia de tipos de modelos sintáticos sob este prisma: o da imbricação com tipos de modelos semânticos. Nas figuras 7 a 9 esses canais de confiança terão legendas em verde.

O tipo básico desta cadeia (**MC1**) modela sistemas fechados. A situação típica a ser modelada – em informática – é a de uma plataforma formada por computador, sistema operacional e recursos nele instalados (aplicativos, etc.). Esse tipo básico cobre também dispositivos móveis e *firmware* (roteadores, etc.) que disponham de mecanismo de controle de acesso baseado em segredo compartilhado (senha) ou em identificador único (dispositivo biométrico, *token* de chave privada, etc). A modelagem é ilustrada na figura 7.

O tipo intermediário desta cadeia (**MC2**) modela redes fechadas. Para os referenciais aqui considerados, uma rede fechada é uma rede que tem dono. A situação típica a ser modelada é a de uma rede de sistemas fechados na qual seja inviável o controle físico sobre os canais de comunicação digital da rede. Por exemplo, uma LAN ou VPN (figura 8).

O tipo final desta cadeia (**MC3**) modela redes abertas. Para os referenciais aqui considerados, uma rede aberta é uma rede formada por acordo tácito. A situação típica a ser modelada é a de uma rede de redes digitais fechadas que funciona por adesão voluntária a um conjunto de protocolos de comunicação e formatos digitais abertos, como a Internet, ou qualquer rede de serviço oferecido e prestado nela (figura 9).

5.1 MC1: Sistemas Fechados, Identificação e Autorização

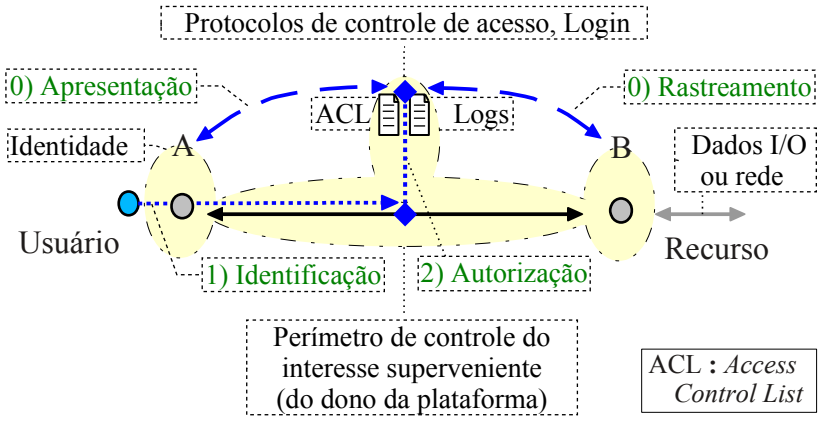
Neste tipo de modelo, o processo real de segurança é delineado por protocolos de controle de acesso [29]. Os canais de confiança presumidos por tais protocolos, e que portanto demarcam as fronteiras do processo de segurança na plataforma modelada[39], são os demandados por seus subprocessos. Os canais de confiança externos são os demandados pelos subprocessos limítrofes: 0) de Apresentação e de Rastreamento. Os canais de confiança internos à plataforma modelada, cuja confiabilidade depende da eficácia dos subprocessos limítrofes, são os dos subprocessos 1) de Identificação e 2) de Autorização.

38 Motivação para explorar essas perspectivas exige coragem. Coragem intelectual para dominar o medo irracional dos limites racionais da confiança (ver ref. [74]). Medo que pode estar condicionado ao hábito de se tomar por real o teatro da segurança. O verdadeiro "teatro de guerra" da segurança informacional (o dos processos reais) tem pesadas baixas, no teatro da "segurança da informação" (o dos sentimentos pessoais), entre aqueles que fixam a segurança no inanimado. Ou, em jargão militar, no teatro da antiquada "guerra de trincheiras", entre os que se entrincheiram no terreno dos dados, oblívios aos interesses por ali legítimos mas conflitantes.

39 Conforme a definição de Confiança de Gerck e a hipótese central deste trabalho de pesquisa.

Identificar é reconhecer, conhecer *outra* vez. Na situação mais simples, o sistema e o agente se reconhecem por nome de usuário e senha, através do subprocesso 1), delineado por um protocolo de *login*. No caso, o *login* presume a senha como segredo compartilhado entre apenas o agente e a plataforma do sistema (até o ponto do fluxo de dados onde o *hash* da senha é calculado), para fins de identificação mútua. Se 1) retiver registro confiável das identificações, diz-se autenticação. O que não inclui o conhecer pela *primeira* vez.

Figura 7



MC$_1$: modelo de confiança para sistemas fechados

Quando uma conta de usuário é criada, presume-se que um (novo) agente está sendo apresentado à plataforma, que assim o conhece pela primeira vez. Este subprocesso limítrofe, 0) de Apresentação, é de natureza administrativa. Ele tem um lado que se executa dentro da plataforma, e um lado que se executa fora. O lado executado na plataforma é para habilitar este usuário ao *login*, e ocorre fora do *login* (quem cria a conta tem que já estar logado). O lado executado fora da plataforma é para justificar o uso que tal agente deve ou pode fazer da plataforma, a quem responde por ela. Quem responde pela plataforma deve presumir que alguns registros desse uso podem ser rastreados na plataforma (por exemplo, em *logs*). Este lado conecta o processo de segurança nesta plataforma a outros relacionados. Por exemplo, se tal plataforma estiver em rede, esta modelagem se encadeia à desta.

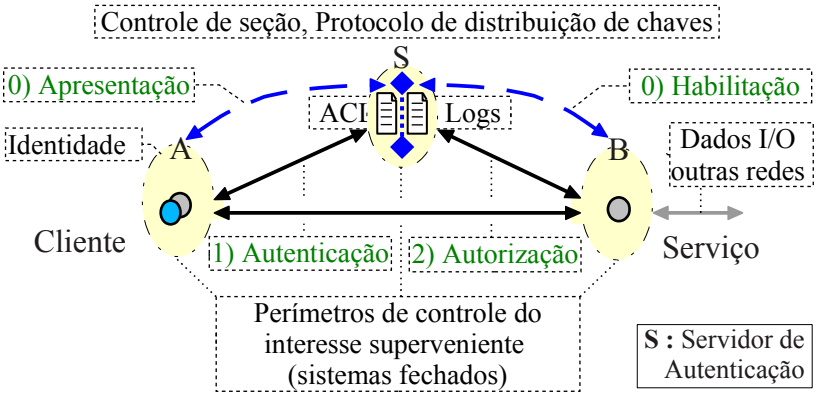
O outro subprocesso limítrofe, 0) de Rastreamento, também administrativo, também tem um lado que se executa dentro da plataforma e outro que se executa fora. O lado que é executado na plataforma delineia seu gerenciamento (administração de contas de usuários, de *logs*, de *back-ups*, etc.), conforme o interesse superveniente do dono da plataforma. Este pode incluir a retenção de registros em 1) e 2) (cuja confiabilidade depende da eficácia dos subprocessos 0), das identificações bem sucedidas e dos acessos autorizados e executados ou não. O lado do Rastreamento que é executado fora da plataforma conecta-se a outros processos de segurança relacionados (por exemplo, de recuperação por *back-up*, auditoria, etc.), inclusive aos regidos por normas jurídicas que visam a proteger o valor probante desses registros, se e quando dela extraídos (forênsica, perícia judicial, etc.) [30].

No caso mais simples, por exemplo, em que o *login* não é usado, é usado anonimamente ou sem eficácia para o subprocesso 2), ou em que o próprio interesse superveniente à plataforma for alvo de suspeição de terceiros, tal proteção pode requerer a busca, o flagrante e apreensão desta plataforma quando um indício externo a investigar indicá-lo.

5.2 MC_2: Redes Fechadas, Autenticação Subjetiva e Cifragem

Neste tipo de modelo, o processo de segurança é delineado por protocolos de controle de seções, que habilitam usos da Criptografia na rede modelada. Esses protocolos, comumente chamados "de distribuição de chaves", geralmente são implementados por um serviço de diretórios (por exemplo, LDAP + SSL, *Active Directory*, etc). As fronteiras desse processo são demarcadas pelos canais de confiança externos, demandados por seus subprocessos limítrofes: 0) de Apresentação (de usuários que se habilitam aos serviços) e de Habilitação (de serviços a serem disponibilizados na rede, para seções sob tal controle).

Figura 8



MC_2: modelo de confiança para redes fechadas

Os canais de confiança internos à rede modelada, cuja confiabilidade depende da eficácia dos subprocessos limítrofes, são os demandados pelos serviços de integridade e de sigilo 1) e 2), que visam a oferecer: a) Para o dono da rede: confiabilidade na identificação de usuários e de serviços, e no controle de autorizações para seções entre estes; b) Para um usuário ou serviço da rede: confiabilidade na identificação mútua de interlocutores autorizados, e na integridade das transmissões entre ambos.

Numa rede fechada a modelagem distingue, como estrutura de referência, um interesse superveniente – do dono da rede – sobre a função desta rede. Esse interesse pode incluir a modulação de possíveis conflitos de interesses nesta rede. Esta modulação ocorre pela escolha de normas administrativas, medidas internas e serviços a operar. Os canais de confiança externos, por onde o dono da rede instala e opera tais escolhas, servem também a que cada agente, indicado nessas normas, as conheça (cliente **A**) e se adapte, ou seja instalado

(serviço **B**) em conformidade (lado "de fora" dos subprocessos limítrofes). Para que, pelo lado "de dentro" desses subprocessos, cada um estabeleça uma chave mestra, compartilhada (só) com o servidor de autenticação **S**, na Apresentação (de A) ou Habilitação (de B).

As chaves mestras servem para habilitar os serviços internos de integridade e de sigilo para sessões autorizadas, nos subprocessos 1) e 2), necessários aos objetivos do protocolo. Estes operam com chave de seção distribuída aos interlocutores (A e B) pelo servidor de autenticação (S), sob cifragem com as respectivas chaves mestras, quando uma solicitação de cliente é autorizada. Assim, a confiabilidade de um agente na identificação de outro via canal inseguro pode ser mediada, com lastro em segredo previamente compartilhado (com S). Ainda, se tal rede fechada estiver em rede aberta, esta modelagem se encadeia à desta.

Antes de passarmos ao próximo tipo de modelo sintático, cabem duas observações sobre chaves mestras e modos de confiabilidade na identificação (modalidades de autenticação). Se uma chave mestra for simétrica (como por exemplo, no protocolo Kerberos), será presumidamente um segredo inicial (i.e., material habilitante) compartilhado entre o respectivo par de agentes. Nada impede, porém, que uma rede fechada utilize chaves assimétricas em seu protocolo de controle de acesso (como por exemplo, no serviço LDAP com protocolo SSL). Por razões históricas é que alguns desses protocolos não as utilizam[40]. Doutra feita, se a identificação de um interlocutor pelo outro, através de um canal inseguro, baseia-se em prévio compartilhamento de segredo, tal mecanismo autentica apenas uma identidade, e a integridade de transmissões, de um interlocutor *para o outro*. Essa modalidade de autenticação tem, pois, sentido intersubjetivo, ou, subjetivo para ambos.

Em situações que envolvem potencial conflito de interesses entre interlocutores a autenticação subjetiva é ineficaz, visto que terceiros supostamente neutros não poderiam decidir sobre um tal conflito baseado nesta modalidade de autenticação. Isto porque um dos interlocutores, de posse do segredo que serve tanto para autenticar quanto para verificar autenticidade, poderia forjar emissões, isto é, mensagens autenticadas, e alegar que uma tal mensagem teria sido originada e transmitida pelo outro (por aquele com quem ele compartilha tal segredo), de forma trivial e indistinguível ao protocolo. Nessas situações, a autenticação deve ser objetiva, dita "oponível a terceiros" (*erga omnes*) em contextos jurídicos. Na modalidade objetiva, o sentido da autenticação deve excluir a possibilidade de um agente poder forjar, através de um ataque ou subversão ao protocolo com custo/benefício viável, a identificação de outro emissor, a partir da sua necessidade de (e habilitação para) validar a autenticidade de emissões alheias, transmitidas ou armazenadas.

Na modalidade objetiva, o segredo em que se baseia a identificação para autenticações não pode, por isso, ser compartilhado. Ainda, um esquema de autenticação objetiva precisa oferecer alguma garantia de irretratabilidade[41], para ser eficazmente oponível a terceiros (para que o protocolo possa distinguir entre forjas e falsas acusações de forja). O que nos remete, se acolhida a lei ou princípio de Kerckhoffs[42], à Criptografia assimétrica, com

40 Alguns protocolos, como Needham-Schroeder (o primeiro para distribuição de chaves a ser publicado), antecedem a descoberta do primeiro sistema criptográfico assimétrico (RSA, em 1978).

41 Condição muita vez chamada de "não repúdio", termo este que confunde sua recepção jurídica.

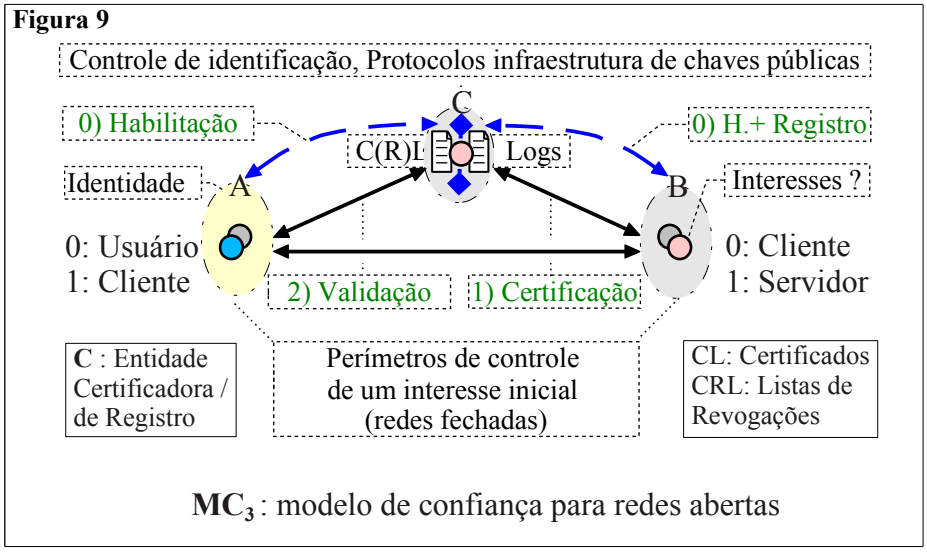
42 Auguste Kerchoffs formulou, no século XIX, o axioma que diz que a eficácia de um sistema criptográfico pode ser independente do conhecimento público de tudo sobre o sistema exceto as chaves. Reformulado (talvez independentemente) por Shannon (ver ref. [12]), como a premissa de que "o inimigo conhece o sistema", é um princípio acolhido pela grande maioria dos

a qual a chave privada (do emissor) autentica, e a chave pública correspondente verifica[43]. E donde o nome "assinatura digital" para esta modalidade objetiva de autenticação[44].

5.3 MC3: Redes Abertas, Autenticação Objetiva e Certificação

Neste tipo de modelo, o processo de segurança é delineado por protocolos de identificação e distribuição de chaves públicas, que habilitam usos da Criptografia na rede modelada. Tais protocolos, referidos em conjunto como uma "infraestrutura de chaves públicas" (por exemplo, PKIX, SPKI), ou por siglas genéricas como ICP ou PKI, são às vezes implementados sob a jurisdição de uma norma civil superveniente (por exemplo, ICP-Brasil, sob a MP 2.200) [10]. As fronteiras desse processo são demarcadas pelos canais de confiança externos, demandados por seus subprocessos limítrofes: 0) Habilitação (de titulares e usuários à validação e utilização de certificados digitais de chave pública) e Registro (de titulares a serem identificados na rede aberta através desses certificados).

Figura 9



Os canais de confiança internos à rede aberta, cuja confiabilidade depende da eficácia

criptógrafos (traduzido de *Wikipedia*). A alternativa de se rejeitar este princípio remete, neste contexto, a um axioma do fundamentalismo de mercado que, aqui aplicado, aduz ao negócio da intermediação criptográfica um rótulo de neutralidade semântica (face a riscos). Tal alternativa é o que propõe o modelo de lei UNCITRAL, no Brasil tramitado (em tradução sofrível) no agora dormente PL 672 /99 do Senado. UNCITRAL diz basicamente ser o mercado quem escolhe o que pode substituir, na esfera virtual para o Direito, a assinatura de punho como instrumento de manifestação da vontade (de agentes juridicamente capazes), ficando desde logo invertido o ônus da prova (de falsificações) sob tal escolha (mais sobre Kerckhoffs em [60]).

43 Se, no futuro, algo como a computação quântica tornar ineficaz o algoritmo RSA como hoje ele é usado, isso significa que o RSA como hoje usado deixaria de ser um algoritmo assimétrico, e não que a autenticação objetiva sob Kerckhoffs deixaria de remeter-se à Criptografia assimétrica.

44 O termo "assinatura digital" foi assim empregado pela primeira vez por W. Diffie e M. Hellman, num artigo que descrevia, em 1976, possíveis usos da Criptografia assimétrica, (ver ref. [28])

dos subprocessos limítrofes, são os demandados pelos serviços de integridade 1) e 2) que visam a oferecer: a) ao titular de um certificado: confiabilidade na apresentação desta titularidade, visando a utilização adequada da chave pública transportada no certificado, para fins ou de transmissões sigilosas de usuários a si, ou de verificação da autenticidade de emissões suas a usuários; b) ao usuário de certificados: confiabilidade na apresentação do titular do certificado, visando a utilização adequada da chave pública nele transportada.

Numa rede aberta, a modelagem distingue, como estrutura de referência, apenas um acordo tácito sobre como se comunicar nela. Não havendo dono da rede, não haverá escolha possível para norma administrativa; só para protocolos e serviços de comunicação tecnicamente acordados e nela operáveis. Como num idioma. Numa rede aberta, portanto, nada impede ou modula potenciais conflitos de interesses em interlocuções. A começar pelos interesses envolvidos em apresentações. Se "compartilhar segredo" não for, nesse contexto, entendido como oxímoro (sentido paradoxal), então o termo presumiria mútua identificação confiável, ali uma premissa circular. Por isso, em rede aberta, a confiabilidade de um agente na identificação de outro *não pode* lastrear-se em partilha de segredo.

Temos então, com o advento das redes digitais abertas, uma inédita versão do problema que *antecede* o da distribuição de chaves, que é o da apresentação: como conhecer pela primeira vez alguém, agora numa rede aberta, sem mediações do demônio de Descartes? Os canais de confiança presumidos pela rede fechada da qual participa **A**lice, pela qual Alice pode se comunicar em rede aberta, cobrem apenas a primeira, sua rede fechada.

Se houver um canal de confiança pelo qual Alice possa conhecer (pela primeira vez) seu potencial futuro interlocutor **B**ob, isto situaria Bob ao alcance da rede fechada de Alice, ou a rede fechada de Alice ao alcance de uma federação de redes fechadas da qual a de Bob poderia participar [27]. Isto solucionaria um caso particular (federado), mas não o caso geral do problema da apresentação em rede aberta. Um caso particular para situações restritas, como as que se adequam à modelagem semântica bipolar ou nas quais pode ser propício utilizar, como mecanismo de apresentação, o conceito e modelos de *reputação*.

De qualquer forma, mesmo uma tal federação *já presume* mediação e arbitragem por terceiros, pelo que, já nela, mesmo com mecanismos de reputação, a confiabilidade na identificação (autenticação) deve ser oponível a terceiros. Assim, tanto nessas federações quanto em redes abertas no *latu* sentido, a autenticação eficaz deve ser objetiva (por Criptografia assimétrica, via assinatura digital), e não subjetiva (por compartilhamento ou delegação de segredo)[45]. Nelas, portanto, segredos compartilhados não podem ser "mestres", isto é, material inicial habilitante. Donde o nome para o tipo de agregado de protocolos capaz de delinear o processo de segurança em redes abertas (ICP). E onde tal processo tem seu calcanhar de Aquiles, muito bem camuflado pelo correspondente teatro da segurança, no canal de confiança externo demandado para a Habilitação (ao uso da ICP).

Quando um certificado digital (x.509) é emitido, presume-se que um agente, nomeado *titular* desse certificado, está sendo apresentado na rede aberta pela ICP. Para isso, este agente precisa antes se habilitar como usuário e cliente na ICP. O subprocesso para isso, de Habilitação, sendo limítrofe, tem um lado interno, que ocorre na rede aberta, e um lado externo, que deve ocorrer fora da rede aberta. O lado interno serve para usuários (como

45 As áreas não clássicas da Criptografia (quântica, por exemplo) não oferecem, nem apresentam perspectivas de oferecer, mecanismos alternativos *para autenticação*.

Bob) se habilitarem como titular de um certificado, que será servido a usuários da ICP (como Alice). Numa plataforma sob seu controle, Bob precisa instalar um dispositivo que opere com chaves assimétricas, gerar um par de chaves (pública e privada) e armazenar a chave privada para si. Esta chave privada tem ação inversa à da chave pública que seu certificado transportará. Dessa chave privada, presume-se que somente Bob controlará o uso, para eficácia de identificações atribuídas a ele, via assinaturas lavradas com tal chave, e/ou para eficácia do sigilo em transmissões endereçadas a ele, via cifragens com a chave pública correspondente. Este uso começa com uma solicitação para emissão do certificado

No lado interno da Habilitação, Bob atua como cliente de uma certificadora da ICP: ele envia uma solicitação contendo seu nome e sua chave pública, assinada com sua chave privada, à certificadora. Já Alice, se ela for apenas usuária da ICP (não for titular de certificado), nesse lado interno da Habilitação ela atua como cliente apenas de um fornecedor: basta-lhe instalar, como fez Bob, numa plataforma sob seu controle, um dispositivo que opere com chaves assimétricas e que armazene certificados de chave pública.

Para atender à solicitação de Bob, a certificadora executará o outro subprocesso limítrofe, o de Registro. Que também tem dois lados; um interno, que ocorre na rede aberta, e um externo, que ocorre fora da rede aberta. O lado interno serve para a certificadora executar uma verificação sintática nos dados do certificado. Isto inclui: se o solicitante controla a chave privada correspondente (via verificação da assinatura digital na solicitação para emissão do certificado); se o nome fornecido pelo solicitante (Bob) é único no cadastro de certificados emitidos (*distinguished name*); e, em caso afirmativo, o preenchimento de outros campos do certificado, conforme a política de certificação desta certificadora, mais o lado externo do Registro. O lado externo serve para validação semântica desses dados. Para isso a certificadora aciona uma entidade "de registro", que irá verificar, *fora de banda*, se, conforme critérios daquela política de certificação, o solicitante faz jus ou não em ser apresentado pela certificadora, a usuários da ICP, através do certificado solicitado, com o nome e atributos que ele apresentou à certificadora. A resposta encerra o Registro.

A partir da resposta do Registro, a certificadora passa então a executar o seu lado do subprocesso 1), de Certificação. Conforme a resposta, ela emite ou não o certificado solicitado. Se for emiti-lo, ela assina digitalmente o certificado (com sua chave privada), publica-o (ou dispõe-o numa base de dados designada em sua política de certificação), e envia-o ao solicitante (Bob), que assim toma ciência de haver se tornado titular desse certificado. Se não, comunica ao solicitante o motivo da negativa. Numa analogia simplista, o certificado digital seria um tipo de documento que tem o sentido de "colar" uma chave pública ao nome do seu titular, e de "selar" essa colagem. Tendo recebido seu certificado, Bob pode então distribui-lo a usuários da ICP: no seu lado deste subprocesso 1), Bob atua como servidor para os que queiram usar seu certificado, e Alice, como cliente.

Para utilizar com eficácia um certificado recebido, porém, usuários da ICP devem antes validá-lo. Para isso a certificadora que emitiu o certificado, digamos **C**larisse, precisa antes ser apresentada a usuários, como Alice. Isto para que os clientes de Clarisse (como Bob) possam ser apresentados a usuários da ICP (como Alice) através da verificação de sua assinatura digital (de Clarisse) em certificados que ela emitiu. Isto para que usuários (como Alice) possam identificar o titular do certificado (Bob) por meio da respectiva chave pública (de Bob): seja em documentos que o titular (Bob) tenha assinado digitalmente, seja em mensagens destinadas ao titular (Bob) sob sigilo.

Ainda, para verificar com eficácia a autenticidade de um tal documento (a vontade que o signatário "Bob" expressa num documento digital), ou para cifrar-lhe com eficácia uma mensagem sigilosa (que só o destinatário "Bob" poderá ler), a chave pública de Bob (transmitida no certificado emitido em nome dele) deve ser validada também contra respectivas listas de revogação de certificados, emitidas periodicamente pela certificadora designada (por Clarisse). Essas verificações – da assinatura digital de um signatário, da integridade do certificado que transporta a chave pública deste signatário (ou de um destinatário), e da não revogação desse certificado – compõem o lado interno (*downstream*) do subprocesso 2), de Validação, para o qual um certificado válido de Clarisse é necessário.

Para completar (*upstream*) a Validação, resta saber: quem emitirá o certificado de Clarisse? Se for **D**aniel (ou Dantas), quem emitirá o Dele? Em algum ponto esta cadeia de emissões, conhecida como *trust path*, a ser também verificada por Alice, há que parar. Com alguém, digamos Daniel, tendo emitido seu próprio certificado, por isso chamado "raiz". Então, voltemos... Aceitar um certificado raiz (de "D"), que qualquer um pode emitir com qualquer nome, e avaliar o que ele e o ato de usá-lo em validações significam, é o outro lado – externo – da Habilitação. Precisamente, o lado externo de um subprocesso de segurança limítrofe, o qual demanda um canal de confiança fora de banda relativamente à rede modelada, e portanto, fora da rede aberta. Mas enfim, que canal seria esse, e como ocorre esse lado do processo? (Afinal, D também designa "Demônio de Descartes")

Numa ICP, os certificados raiz funcionam como âncoras de confiabilidade para identificação: de signatários, em esquemas de autenticação, e de destinatários, em esquemas de cifragem. Um certificado raiz forjado, aceito por quem precisa identificar por meio digital um interlocutor virtual, permite ao falsário se passar por qualquer um na rede aberta, perante a Validação (falsificando toda a cadeia de certificados, a partir de um par raiz, com os nomes do titular falsos). A vítima, servida com a cadeia falsa, pode cair no golpe com um mero *click-through*[46], ou nem isso[47] [33], [77]. Da mesma forma, o uso da chave privada funciona como âncora para a confiabilidade na identificação do seu titular. O acesso à *tua* chave privada por um interesse inefável, manipulada por quem queira forjar uma identidade virtual atribuída a você, permite ao falsário passar-se por *você* perante qualquer usuário da ICP. De forma indistinguível antes das consequências, e com inversão do ônus da prova (da falsificação) em jurisdições como a da ICP-Brasil[48]. Que canal, esse?

---

46 Tendência de se responder, movido pela pressa, frustração ou impulso, "OK" a alertas na tela, por vezes sem ler ou buscar entender a mensagem que se responde ou as consequências da ação.

47 Por exemplo: quando uma página web é solicitada a um *site* "seguro" (i.e., acessível via protocolo https) e o navegador web, ao tentar validar o certificado recebido, não consegue montar um *trust path* ancorado em um certificado raiz que ele já possua, pode ser que o próprio *site* ofereça ao navegador também o certificado raiz faltante: mas em banda, antes do uso da Criptografia se iniciar. Neste caso haverá um alerta do tipo "você tem certeza que conhece este *site*?", já que toda a cadeia enviada pode aí estar forjada. E mesmo com atenção, há risco: a pesquisa em [33] mostra como um código malicioso pode suprimir tal alerta no navegador usado pela grande maioria dos internautas. Ainda, se o serviço DNS ou o proxy da rede fechada do internauta também estiver comprometido, a forja poderá ser indetectável antes das consequências para a vítima, por mais cuidadosa que esta seja (devido ao risco de ataques do tipo *man-in-the middle*).

48 Interpretação provável dos efeitos combinados do § único do Art. 6º e do § segundo do Art. 10º da Medida Provisória 2.200-2 de 2001, sendo, ainda, a pretendida pelo legislador à luz do Art. 1º e de opiniões publicamente circuladas por lobbistas que promoveram e/ou que defendem este di-

VI

6 Conclusão

Uma norma social ou jurídica não pode alterar leis físicas naturais. Seria absurdo, por exemplo, pretender-se alterar a constante gravitacional – que determina a aceleração de corpos em queda livre – por decreto ou dispositivo constitucional. Entretanto, a norma jurídica que institui a a ICP-Brasil (MP 2.200-2) contém dispositivos cujo sentido de conexão tecno-jurídica tem o condão de pretender alterar leis naturais. Leis combinatórias pelas quais a possibilidade técnica da eficácia probante da assinatura digital é racionalmente atribuída, através da relação lógica destas com leis estatísticas. Tem o condão de pretender alterá-las banalizando-as, ofuscando elos causais para responsabilizações. Elos que deveriam ser fundados em cautelas plausíveis, mas não o são, como mostra a seção 5.3. Nessa norma, as responsabilizações emanam de causas técnicas fundadas em cautelas incomensuráveis com os riscos e competências que tocam aos agentes envolvidos; seja diretamente, pela necessária custódia de material criptográfico habilitante em ambientes virtuais hostis, a maior, seja em suporte a tais ambientes, pelas mediações tecnológicas, a menor.

Sob a hermenêutica positivista dominante, a pretensão mágico-triunfalista erguida com esta e outras banalizações afins [7] poderá cobrar seu custo social em insegurança jurídica. Custo este faturável na medida em que a lógica e a organização da mentalidade criminosa ou anti social fluírem para debitá-lo, pela via da sua própria evolução tecnológica clandestina, irrigada pela tecno-imersão de práticas sociais sob jurisdição de regimes

---

ploma. Seguramente a interpretação cabível sob a égide do positivismo jurídico, como em [35]: "*Dispõe o art. 116 da Lei 8112/96 (RJU) que são deveres do servidor:...VII-zelar pela conservação do material e a conservação do patrimônio público. Este item adquire especial significação no que diz respeito à utilização de hardware e software, ambas passíveis de danificação em caso de mau uso (sic.). Aqui podem ser enquadradas as condutas irregulares do funcionário que, por grave descuido, ou mesmo voluntariamente, facilita a 'infecção' de computadores e redes por códigos maliciosos, inclusive pela utilização de procedimentos e softwares em desconformidade com o marco da ICP-Brasil, instituída pela MP 2.200-2.*"
Indaga-se, aqui, em que sentido a conformidade com tal marco regulatório preveniria contra infecções capazes de produzir falsificações, ou contra falsificações rastreáveis a "mau uso" na conduta do funcionário; e em que sentido a não conformidade com tal marco seria causa facilitadora de infecções capazes de causar falsificações. Sobre esta ilação, a lógica da mentalidade criminosa, que só cresce em sofisticação e especialização na esfera virtual (ver ref. [4], [5]), indica justamente o sentido contrário: haverá mais interesse em se desenvolver código malicioso, invisível e sorrateiro (ver ref. [33]), contra softwares que se conformam em dar fé pública a documentos eletrônicos (valor sob risco) do que contra softwares que não se conformam em dá-la. Sobre tal fé pública: "... [Dispõe o art. 117 da Lei 8112/96 (RJU)] *que são ilícitos passíveis de responsabilização pelo servidor: III- recusar fé a documentos públicos. ... Situação ainda mais grave será a daquele servidor ou autoridade pública que negue fé quando confrontado com documento produzido por órgão público e 'assinado' com as características da ICP-Brasil, instituída pela MP-2200-2, que prescreve, em seu art. 10º:...*".
Cristalina, aqui, a hermenêutica produzida por um Mestre do Direito Constitucional e Advogado da União em [35]. Restou-lhe esclarecer, todavia, se tal fé pública decorre do citado artigo 10º (situação que daria fé pública *também* aos documentos eletrônicos privados sob o mesmo regime jurídico), ou se da titularidade da assinatura (agente de órgão público), ou se decorre de ambos.

normativos tão distorcidos. É possível, e fácil, deduzir quem poderá com isso ganhar; Trasímaco o mostrou a Platão, em *República*. É possível, também, observar isso fluir; o curso da crise econômica eclodida em 2008 o vai mostrando, a quem quiser ver[49].

Uma ICP não resolve, apenas traduz o problema da apresentação em rede aberta. Traduz para o problema da distribuição de certificados raiz, para o da custódia de chaves privadas, e para o da integridade das plataformas onde chaves criptográficas operam. Uma ICP, ou qualquer agregado de mecanismos e medidas de segurança informacional, não pode proteger quem quer que seja além de suas fronteiras virtuais. Nem pode impedir que sejamos atacados através dessas fronteiras. Se assim pretender, é só teatro. No processo real, tais ataques serão tão plausíveis quanto indicarem as relações custo/benefício em se penetrar essas fronteiras – os canais de confiança externos (5.3) –, que estão sob recrudescente cerco do risco moral ante à disseminada tecno-imersão de práticas sociais [11].

O que nos conduz a mais questões programáticas para esta pesquisa:

1. Como vem sendo, na prática hoje, distribuídos e recepcionados certificados raiz, geradas e custodiadas chaves privadas, à luz desta modelagem?
2. Como vem sendo instruídos e responsabilizados os que usam ou são compelidos a usar tais teconolgias, pelo uso inepto, inadequado ou incauto delas?
3. Como vem sendo fiscalizados e responsabilizados os que lucram ou empoderam-se com tais usos, pela mediação inepta, inadequada ou incauta dos mesmos?

À guisa de pista para respostas, cabe comentar que, em seu trabalho seminal sobre modelagem de Confiança, Gerck considera a propensão de se pensar ou se tratar a Internet como se fora uma rede fechada[50], o verdadeiro Bug do Milênio [34]. Como sinal desta propensão, destacamos o excessivo reducionismo em aplicações do modelo TRAVOS, na seção 5.0, e a ela acrescentamos, acima, a propensão de se legislar e se jurisdoutrinar da mesma forma. Como reflexos dessas propensões, observamos desinteresse ou desconforto, e até desdém ou repulsa, por pesquisas deste teor. Postura que sustenta a tendência atual de se tomar o teatro pelo processo real na segurança em informática, sob a mítica miragem coletiva da tecnologia como panaceia mágica e triunfal.

A ressaca dos efeitos dessa miragem coletiva pode atingir áreas fundamentadas em avaliação de riscos e colonizadas por tecno-imersões fantasiosamente autônomas, nas quais a segurança informacional é crucial, com desilusão catastrófica. Em janeiro de 2008, por sinal, uma das principais agências de avaliação de riscos na economia de mercado globalizada publicou um relatório afirmando que tais avaliações "se inviabilizaram talvez para sempre" [56]. Assinado por seu economista-chefe internacional, diz:

> "*It is extremely unlikely that in today's markets we will ever know on a timely basis where every risk lies*."

Trata-se de uma das cinco grandes agências que, com avaliações fantasiosas sobre instrumentos derivativos e suas fiadoras, precipitaram a eclosão da turbulenta crise econômica iniciada em 2008, corroborando a análise evolutiva da segurança no virtual destacada na seção 5.0. Isso apenas dois anos depois de Ben Bernanke, então presidente da Reserva

49 Para um panorama, ver estudo sobre capitalismo de mercado em [45]; para um exemplo, ver [48]
50 Talvez por ser a Internet pioneira e "mãe" dentre as redes digitais abertas.

Federal dos EUA (banco central), ter afirmado o seguinte:

> "*The management of market risk and credit risk has become increasingly sophisticated. ... Banking organizations of all sizes have made substantial strides over the past two decades in their ability to measure and manage risks.*"[51]

Reguladores, legisladores, acadêmicos, e formadores de opinião na mídia, quase todos presumiam que os gerentes de bancos e instituições financeiras sabiam o que estavam fazendo. Mas, em retrospectiva, eles não sabiam. A divisão de produtos financeiros da AIG, por exemplo, que em 2008 arrastou a empresa à situação falimentar, em 2005 havia lucrado US $2.5 bilhões vendendo, em mercados financeiros globais, apólices mal precificadas de seguro contra *default* de instrumentos financeiros complexos e mal compreendidos.

Nessa turbulência, caso algum interesse superveniente consiga coligar-se para se apoderar da infraestrutura semiológica formada pela primeira rede digital aberta e global – a Internet –, terá em mãos um instrumento de colusão e controle social inédito, formidável e sub-reptício [51]. Enquanto isso ainda não ocorre, avolumam-se as normas, doutrinas, jurisprudências e ações políticas que o facilitam. Que entendem a Internet como recurso a ser apropriado, e que rejeitam – pelo viés ideológico do que propõem [66], [67] – tratá-la como um meio semiológico[52] inédito e comum à cibercultura, um instrumento insuperável ao mesmo tempo de liberdade e de controle. Aduzidas pela mente de agentes que se iludem em fúteis contorções retóricas, inebriados pela dogmática do fundamentalismo de mercado, tentando conciliar esses entendimentos opostos como se desastrosa distopia isto não fosse. Numa postura que, em suma, infecta o organismo social com o verdeiro *bug* do Milênio, numa febre que catalisa tal coalizão e empoderamento, fenômeno que o filósofo Paul Virilio chama de "totalitarismo como nunca houve" ([69], pp 38). Que se torna tanto mais factível e perigoso quanto mais se aprofunda a atual crise sistêmica do capitalismo.

Modelos negociais de fornecedores, contextos normativos, e meios substancialmente racionais de se influir neles devem ser considerados em PSIs e em análises de riscos, mas não só nas PSIs de fornecedores monopolistas. Se com teorias, práticas, ferramentas e estratégias tradicionais, ou se com outras mais afeitas ao desafio a enfrentar, é questão metodológica que ultrapassa o escopo desta pesquisa. Aqui, a humildade recomendada na seção 1.2 faz-se prudente e necessária, pelo que retornamos a Habermas, naquilo que o contrapõe ao pessimismo de seus colegas da escola filosófica de Frankfurt. Frente à marcha triunfal da razão instrumental, que nos aliena em relações de dominação num capitalismo em recorrentes crises, Habermas propõe a razão e a ética discursivas, como instrumentos de emancipação humana e de re/integração entre sistema e mundo vivido ([62], pp 77).

Como a premissa de confiança implícita no Discurso habermasiano é o interesse motivador dos interlocutores pelo entendimento mútuo, convém dar o exemplo e já testá-la, mesmo que empiricamente, com alguém que guiou metodicamente o sucesso do fundamentalismo de mercado rumo à catastrófica crise econômica iniciada em 2008, manipulando percepções "autônomas" de confiança. Um dos co-autores do método universalmente usado em mercados financeiros para precificar instrumentos derivativos (Black-

51 http://www.federalreserve.gov/newsevents/speech/Bernanke20060612a.htm

52 Um dos fundadores da Semiologia como ciência, Ferdinand de Sausurre, teria defendido, no seu "Curso Linguística Geral" no início do século XX, a tese de que não é a linguagem que é natural ao homem, e sim a capacidade de constituí-las como sistemas de símbolos associados a ideias.

Scholes), laureado com o prêmio Nobel de economia por esta autoria, dá a seguinte resposta em entrevista a uma jornalista do *New York Times* [57]:

> Deborah Solomon: *Some economists believe that mathematical models like yours lulled banks into a false sense of security, and I am wondering if you have revised your ideas as a consequence*.
>
> Myron Scholes: *I haven't changed my ideas. A bank needs models to measure risk. The problem, however, is that any one bank can measure its risk, but it also has to know what the risk taken by other banks in the system happens to be at any particular moment.*

Na segunda frase de sua resposta, Sholes oferece um diagnóstico que indica, para enfrentar a crise, um novo método. Por esse novo método, cada agente precisaria conhecer os riscos de todos os agentes a todo tempo. Enquanto a primeira frase da mesma resposta sinaliza que seu laureado método anterior, indutor da crise, seria extensível ao novo método que logo indica. Porém, basta que os riscos se comportem mecanicamente, à maneira de corpos celestes, para que um mínimo de três agentes com interesses independentes inviabilizem matematicamente esta indicação[53], e esta presumida extensibilidade.

Disso tudo, percebe-se que esta relação patológica entre processo real e sentimento de segurança, entre o processo no virtual e o sentimento na vivência, induz riscos locais a se recombinarem em riscos sistêmicos, para os quais a tecno-imersão contribui, especialmente a informatização; e que riscos sistêmicos requerem abordagem pragmático-holista, para as quais a tecno-imersão "autônoma" – guiada pela razão instrumental – não contribui, ao contrário. E finalmente, percebe-se que essas contradições não se dissipam com reducionismo mágico-triunfalista, com mais "autonomia" tecnológica. Bem ao contrário.

Mais uma vez, parece ser da incompletude que surgem os piores problemas em reducionismos científicos. Tratar a segurança informacional ou no virtual como algo impessoal[54], tomar seu teatro pelo processo real, ou a abordagem aqui proposta como ataque ideológico ou pessoal, é fechar os olhos ou dar as costas para a marcha histórica aqui exposta. É insensatez. Todavia, mesmo que sua pretensa utilidade ou relevância seja descartada, esta pesquisa nos conduz, ao menos, à sua derradeira e inarredável questão: como identificar o controle da História?

---

53 Em mecânica celeste, sabe-se que o "problema dos três corpos" só admite solução aproximada, que dissipa sua precisão ao longo da variável que simula o tempo.

54 Como assunto "eminentemente técnico" ou "sério demais" para ser tratado doutra forma na prática (razão instrumental), deliberadamente optando-se pelo inanimado como objeto da proteção, reduzindo-se a segurança informacional ou a segurança em informática à segurança "da informação" quando couber distinção. Quando, por exemplo, a modelagem de riscos adequada for multipolar, como em casos afetos ao comentário da seção 2.2 (conforme indicado na nota de rodapé 5) e exemplificado na seção 4.3 (na nota de rodapé 34); quando não couber (sem evocar tragédias) a modelagem dos conflitos de interesse relacionados numa única polarização, entre "nós" e "o cibercrime" ou entre Estado e Mercado por exemplo, onde o dogma central do fundamentalismo deste reza caberem (e resolverem-se) todos.

Referências

1. Robert Wright: Não Zero. A Lógica do Destino Humano.
   (*Nonzero*) Ed. Campus (2001).
2. André Lemos e Paulo Cunha: Olhares sobre a Cibercultura.
   Ed Sulina (2003).
3. Bruce Schneier: Dual-Use Technologies and the Equities Issue.
   Crypto-gram Newsletter, May 2008.
   http://www.schneier.com/crypto-gram-0805.html#2
4. FBI - IC3: Internet Crime Complaint Center Annual Reports
   http://www.ic3.gov/media/annualreports.aspx
5. Symantec: Internet Security Threat Report Tracks Notable Rise in Cybercrime
   www.symantec.com/about/news/release/article.jsp?prid=20060307_01
6. Bruce Schneier: In praise of security theater
   Crypto-gram Newsletter, Feb 2007.
   http://www.schneier.com/crypto-gram-0702.html#1
7. Pedro A D Rezende: Cibercrime, Megalobby e Sottogoverno
   Ensaio para o portal Observatório da Impensa.
   http://www.observatoriodaimprensa.com.br/artigos.asp?
   cod=500IPB006
8. Pedro A D Rezende: Ideologias e Bits.
   http://www.cic.unb.br/~rezende/trabs/jcsbc21.htm.
9. Sun Tzu: A Arte da Guerra
   (*The Art of War*) Ed. Martin Claret, 2001.
10. Pedro A D Rezende: Responsabilidade e Escolhas num mundo de Chaves Públicas.
    http://www.cic.unb.br/~rezende/trabs/ITI.htm
11. Pedro A D Rezende: The Digital Stockholm Syndrome .
    http://www.cic.unb.br/~rezende/trabs/Stockholm.html
12. Claude Shannon: A Mathematical Theory of Communication
    Bell System Technical Journal, vol. 27, pp. 379-423, 623-656, July, October, 1948.
    http://plan9.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf
13. Robert Gray: Entropy and Information Theory
    Stanford University - Springer-Verlag, 1991.
    http://www-ee.stanford.edu/~gray/it.pdf
14. Ed Gerck: Toward Real-World models of Trust.
    http://mcwg.org/mcg-mirror/trustdef.htm
15. Harrison McNight and Norman Chervany: The meanings of Trust
    School of Management, Universitiy of Minnesota.
    http://www.misrc.umn.edu/wpaper/wp96-04.htm
16. Pedro A D Rezende: Impedimento ao Uso Restrito de Assinatura Digital na ICP-BR.
    http://www.cic.unb.br/~rezende/trabs/impedimento.html.
17. Pedro A D Rezende: Software, Cultura e Liberdade.
    http://www.cic.unb.br/~rezende/trabs/goethe.html
18. Pedro A D Rezende: Totalitarismo Digital.
    http://www.cic.unb.br/~rezende/trabs/ditadura.htm

19. Directory of Information Security Policies.
www.information-security-policies-and-standards.com/index.htm

20. Cláudia Canongia: Inteligência Competitiva.
Notas do Curso de Especialização em Gestão de Segurança na Informação, Universidade de Brasília, 2008

21. Time Magazine: Anti-Monopoly (May 8, 1938).
http://www.time.com/time/magazine/article/0,9171,759590,00.html

22. James Love: The Counterfeit treaty (June 3, 2008)
http://www.huffingtonpost.com/james-love/the-counterfeit-treaty_b_104831.html

23. Aaron Shaw: Acta and the Threat of Global Governance.
http://fringethoughts.wordpress.com/2008/06/04/acta-and-the-threat-to-credible-global-governance/

24. Slashdot: Quadrilha russa vende vírus de WMF no mercado negro por US$ 4000
http://it.slashdot.org/article.pl?sid=06/02/02/215210

25. Cyrille Béraud: Sur ordre de Microsoft, le gouvernement du Québec refuse de divulguer les informations sur le contrat le liant à ce fournisseur.
http://blogs.savoirfairelinux.net/cyrilleberaud/2008/05/sur-ordre-de-microsoft-le-gouv.html

26. Simon Garfinkel e Gene Spafford: Practical Unix and Internet Security (Chapter 27).
O'Rilley & Associates (1996)

27. Organization for Advancement of Structured Information Standards (OASIS).
Technical Committee on Security Assertion Markup Language (SAML).
www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

28. W. Diffie and M.E. Hellman: New directions in cryptography
IEEE Transactions on Information Theory 22 (1976), 644-654.

29. Comptia Security Tech Notes – Access Control.
www.techexams.net/technotes/securityplus/mac_dac_rbac.shtml

30. National Institute of Justice. Electronic Crime Scene Investigation
A Guide for First Responders (July 2001).
http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

31. Pedro A D Rezende: Electronic Voting, a Balancing Act.
www.cic.unb.br/~rezende/trabs/Brazil_election.html

32. Pedro A D Rezende: The Possible Laws on Digital/Electronic Signature: On the Proposed UNCITRAL Model. 5th World Multiconference on Systemics, CyberneTIC and Informatics, EUA, July 2001. Proceedings of SCI'2001 (vol X, pp 87-92).
www.cic.unb.br/~rezende/trabs/laws.htm

33. Marchesini, J & Smith, S.& Zhao M, Dartmouth College: Keyjacking: Risks of the Current Client-side Infrastructure Proceedings of the 2nd Annual PKI Research Workshop, NIST.
http://middleware.internet2.edu/pki03/presentations/11.pdf

34. Pedro A D Rezende: Risco, Confiança e Responsabilidade na Internet.
www.cic.unb.br/~rezende/trabs/risco.htm

35. Luiz F T Vergueiro: Internet e seus reflexos estruturais no Direito Processual.
Em "Direito e Internet, Vol. II", pp. 325-354. Ed. Quartier Latin (2008).

36. Umberto Eco: Tratado Geral de Semiótica.
(*Tratatto di semiotica genrale*) Ed. Perspectiva, São Paulo (1976).

37. Brian Grow & Jessica Greenberg: FHA-Backed Loans, the New Subprime (Business Week, 2008).
www.businessweek.com/magazine/content/08_48/b4110036448352.htm

38. Catherine Fitts: Dillon, Read & Co. and the Aristocracy of Stock Profits (2006)
http://dunwalke.com/1_Brady_Bush_Bechtel.htm

39. Mara Der Hovanesian: Sex, Lies and Subprime Mortgages (Business Week, 2008).
www.businessweek.com/print/magazine/content/08_47/b4109070638235.htm

40. Ivo Gico Teixeira Jr.: Responsabilidade Civil dos Robôs (2008).
http://www.cic.unb.br/~rezende/trabs/gico.pdf

41. Michael Shedlock: Read and Weep for the USA (set 2008).
http://seekingalpha.com/article/96510-read-it-and-weep-for-the-usa

42. Yves Smith: Fed Reverses Self on Promises of Transparency, Continues to Stonewall on Collateral, Lending Disclosure; (Nov 10, 2008).
www.nakedcapitalism.com/2008/11/fed-reverses-self-on-promises-of.html

43. Rob Weir: Legacy Format FUD (jan 2008).
http://www.robweir.com/blog/2008/01/legacy-format-fud.html

44. Associated Press: Greenspan Admits Mistake in Subprime Mess (set 2007)
http://www.msnbc.msn.com/id/20759709

45. Henry K C Liu: Killer Touch for Market Capitalism (Asia Times, out 2007)
http://www.atimes.com/atimes/Global_Economy/JJ30Dj04.html

46. Paul K C Feyerabend: Realism, Rationalism & Scientific Method. Philosophical Papers vol 1. Cambridge University Press (1981).

47. Fritz Machlup: The Political Economy of Monopoly: Business, Labor and Government Policies. The John Hopkins Press (1952).

48. Andy Greenberg | Forbes.com: Is your account safe? Newsweek, Dec 8, 2008.
http://www.newsweek.com/id/172902

49. John Leyden | The Register: Lehman Excel snafu could cost Barclays dear. Oct 15, 2008.
http://www.theregister.co.uk/2008/10/15/lehman_buyout_excel_confusion

50. George Akerlof & Paul Romer | National Bureau of Economic Research: Looting: The Economic Underworld of Bankrupcy for Profit. April, 1994.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=227162

51. Catherine Austin Fitts: The Slow Burn. April, 2009.
http://solari.com/blog/?p=818&ref=patrick.net

52. Phillip Hallam-Baker: From CyberCrime to CyberConflict: The Infrastructure of Crime and Worse to Come.
http://www.csail.mit.edu/events/eventcalendar/calendar.php?show=event&id=2188

53. Marsh, S.: Formalising Trust as a Computational Concept.
PhD Thesis. University of Sterling, UK, 1994 *apud* Albuquerque R. *et al*, Int. Journal of Forensic Computer Science (2008) V.3 N.1 pp.75-85.

54. Sabater, J. & Sierra, C.: Reveiw on Computational Trust and Reputation Models.
Artificial Intelligence Review (2005) 24:33-60 *apud* Albuquerque R. *et al*, Int. Journal of Forensic Computer Science, V.3 N.1 (2008) pp.75-85.

55. Patel, J.: A Trust and Reputation Model for Agent-Based Virtual Organizations.
Thesis of Doctor of Phylosophy. Faculty of Engineering and Applied Science. University of Southampton, January, 2007 *apud* Albuquerque R. *et al*, Int. Journal of Forensic Computer Science, V.3 N.1 (2008) pp.75-85.

56. Sorkin, A.: Has Measuring Risk changed "Forever"?
The New York Times, January 7, 2008.
http://dealbook.blogs.nytimes.com/2008/01/07/risk-cannot-be-measured-anymore-moodys-says/

57. Solomon, D.: Crash Course. Questions for Myron Scholes.
The New York Times, May 14, 2009
http://www.nytimes.com/2009/05/17/magazine/17wwln-q4-t.html?_r=1

58. Túlio Vianna: O Globo se supera e diz que perguntas são propriedade do jornalista. 9 de junho de 2009 http://tuliovianna.wordpress.com/2009/06/09/o-globo-se-supera-e-diz-que-perguntas-sao-propriedade

59. Pedro A D Rezende: Diálogo sobre WGA.
www.cic.unb.br/~rezende/trabs/debateHF.html

60. Pedro A D Rezende: A Lei de Kerckhoffs.
www.cic.unb.br/~rezende/trabs/kerckhoffs.html

61. Jurgen Habermas: Conhecimento e Interesse. Trad. J. N. Heck *Apud* Alessandro Pinzani: Habermas Ed. Artmed, São Paulo, 2009.

62. Alessandro Pinzani: Habermas.
Ed. Artmed, São Paulo, 2009.

63. Markoff, J.: Internet's Annonimity Makes Cyberattack Hard to Trace
The New York Times, July 16, 2009.
http://www.nytimes.com/2009/07/17/technology/17cyber.html?_r=2

64. Kirk, J.: Rede de espionagem política online atingiu computadores de 103 países
IDG News Service, 30 de Março de 2009.
http://idgnow.uol.com.br/seguranca/2009/03/30/rede-de-espionagem-politica-online-atingiu-computadores-de-103-paises/

65. Higgins, K.: Security Expert Calls For New Model For 'Demonetizing' Cybercrime, Botnets
DarkReading, April 23, 2009.
http://www.darkreading.com/security/government/showArticle.jhtml?articleID=217100239

66. Schneier, B.: Who Should be in Charge of Cybersecurity?
The Wall Street Journal, March 31, 2009.
http://online.wsj.com/article/SB123844579753370907.html

67. Security Darkreading: New UK Cybersecurity Centre Open Doors
Darkreading, September 23, 2009.

http://www.darkreading.com/security/government/showArticle.jhtml?articleID=220101007

68. IDG Now: Paraná torna ilegal uso de software para redes de compartilhamento. IDG Now, 16 de Setembro de 2009. http://www.iplay.com.br/Jogos/Noticias/?Parana_torna_ilegal_uso_de_software_para_redes_de_compartilhamento+520&Grupo=2

69. Virilio, P.: Cibermundo, a Política do Pior Ed. Teorema, Lisboa, 2000

70. REFERENCIA A ACRESCENTAR - TEORIA DA INFORMAÇÃO

71. Daily Botnet Statistics, http://botnet-tracker.blogspot.com

72. Manfredo A Oliveira: "Reviravolta Linguístico-Pragmática na Filosofia Contemporânea", Coleção Filosofia, 40, Loyola, 1996

73. Gilles Deleuze: "Pourparlers" (Ed. Minuit, 1990) p. 93 apud Muniz Sodré Cabral: "As Estratégias Sensíveis" (Ed. Vozes)

74. Pete Herzog: "What They Don't Teach You in "Thinking Like the Enemy" Classes". Trad.: Pedro A. D. Rezende, em http://www.cic.unb.br/~pedro/trabs/peteherzog.html

75. Wikipedia: Efeito Dunnig-Kruger http://pt.wikipedia.org/wiki/Efeito_Dunning-Kruger

76. Fley, B. & Florian, M.: "Trust and the Economy of Symbolic Goods: A Contribution to the Scalability of Open Multi-agent Systems", em: Fisher, K., et al, ed.: "Socionics. Scalability of Complex Social Systems" Springer Verlag, 2005 http://cs5128.userapi.com/u11728334/docs/5e19428be862/Klaus_Fischer_Socionics_Scalability_of_Complex.pdf

77. Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., Shmatikov, V.: "The Most Dangerous Code in the World: Validating SSL Certificates in non-Browser Software" https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html

78. Wikipedia: Cyberwarfare http://en.wikipedia.org/wiki/Cyberwarfare

79. John Austin, "Sense and Sensibilia", Oxford, 1962 (op. cit. [72]:)

Exercícios

1. Compare o caso da aviação citado na seção "Cenários, Enredos e Papéis" (1.3) com o caso dos medicamentos em nossa sociedade atual (conforme você o percebe)*, no que se refere à prioridade do interesse coletivo em práticas normativas (conforme discorrido na seção 1.3).
2. Quando se compara um canal que habilita o uso de um mecanismo criptográfico e um canal no qual se quer usá-lo (seção 2.2), em relação à confiabilidade (ser ou não confiável para habilitar esse uso) e serem ou não distintos esses dois canais, para quais das quatro possíveis combinações este uso da Criptografia seria ineficaz, desnecessário ou inviável?
3. A primeira sentença do segundo parágrafo da seção "Habilitando à Criptografia" (2.3) descreve como, exatamente, um canal de confiança pode ser demandado para habilitar o uso da Criptografia. Liste as possíveis combinações de garantias que podem ser demandadas desse canal quando os conectivos "e/ou", "vice-versa" e "e talvez" desta sentença têm seus sentidos desdobrados. Ou seja, escreva as frases correspondentes nas quais essas abreviações não são usadas, e onde cada frase descreve uma situação específica de possível demanda (independentemente da possível demanda na frase construída fazer ou não sentido para os usos da Criptografia que você já conhece).
4. A primeira nota de rodapé da seção "Uma Hipótese Semiológica" (3.2) cita várias definições concretas de Confiança deriváveis da definição abstrata de Gerck. Indique, dentre estas, em Inglês e em sua tradução ao Português, a que lhe parece mais obscura, a que lhe parece mais intuitiva, e a que lhe parece mais pertinente ao processo de segurança em informática.
5. O quinto parágrafo da seção "Modelando Confiança para Políticas de Segurança" (4.2) faz referência a possíveis localizações do segundo agente principal numa comunicação. Dois sentidos de localização – tempo e espaço – foram inicialmente abordados na seção 2.3. Agora, levando em conta os tipos de arquitetura de sistemas informáticos aqui abordados, para o sentido de localização no espaço classifique algumas situações práticas (duas ou três) nas quais é possível haver um canal de confiança entre os dois interlocutores, e situações nas quais não é possível haver um tal canal (caso você encontre alguma). Nos casos em que é possível, justifique por que considera o "canal de confiança" indicado confiável para interlocutores que precisam habilitar, através do mesmo, o uso de algum mecanismo criptográfico entre eles.
6. Na figura 5 (seção 5.1), o diagrama para modelagem de sistemas de significação bipolares apresenta cinco agentes (**A, B, D, X, Y**), cada um com algum interesse relacionado à situação sob foco. No quadro "premissas mínimas" há duas listas com relações de alinhamento ou conflito de interesses entre agentes envolvidos. Essas listas querem indicar exemplos de como esses interesses poderiam se polarizar em dois grupos, onde em cada grupo os interesses se alinham, mas conflitam com algum interesse no outro grupo (grupos conformes). As duas listas parciais são: **A ~ B, A ⊥ D, ...** e **A ~ Y, B ~ X, ...** Encontre as formas em que esses cinco agentes podem ser alocados em dois grupos conformes, compatíveis com uma das duas listas parciais apresentadas. Ou seja, liste as formas de completar estas listas parciais, ou melhor, de alocar os agentes

em dois grupos, incluindo os requisitos de uma das listas parciais, sem incluir contradições.

7. Na figura 5 (seção 5.1), o diagrama para modelagem de sistemas de significação multipolares apresenta cinco agentes (**A, B, D, X, Y**), cada um com algum interesse relacionado à situação sob foco. No quadro "premissas mínimas" há duas listas com possíveis relações de alinhamento ou conflito de interesses entre agentes envolvidos. Essas listas indicam como esses interesses poderiam se polarizar em três ou mais grupos, onde dentro de cada grupo os interesses se alinham, mas conflitam com algum interesse em cada outro grupo (grupos conformes). As duas listas parciais são: **A ⊥ B, A ⊥ D, ...** e **A ⊥ Y, B ⊥ X, ...** Encontre as formas em que esses cinco agentes podem ser alocados em tres grupos conformes, compatíveis com uma das duas listas parciais apresentadas. Ou seja, liste as formas de completar estas listas parciais, ou melhor, de alocar os agentes em três grupos, incluindo os requisitos de uma das listas parciais, sem incluir contradições.

Comentários sobre a questão 1:

Considerando que a venda de fármacos é regulamentada, os interesses que podem merecer atenção na resposta são:
- Como se compara, grosso modo, o controle da produção e da comercialização de fármacos e serviços correlatos quando se considera países (caso conheça o cenário em mais de um) e finalidades do produto (alta e baixa tecnologia, drogas que já foram lícitas mas não são mais, ou são com restrições – como o álcool e o fumo –, etc.)?
- Como as variações nesta regulamentação se comparam com as variações na regulamentação do transporte aéreo?
- Com se comparam a proporção de fornecedores e usuários que boicotam essas normas (raizeiros, curandeiros, aborteiros, dieteiros, drogas sintéticas, etc.), quando comparado ao transporte aéreo (voos clandestinos, inadequação do serviços de controle, etc.)?
- Como o Estado prioriza o combate à violação dessas normas, comparando as de fármacos às do transporte aéreo?

Não precisa fazer pesquisa, não precisa citar fontes, não precisa de fatos ou estatísticas concretas. Basta a intuição e a percepção oriundas da observação leiga e da cultura geral. O objetivo da pergunta é permitir que quem responda busque uma comparação *subjetiva* entre duas práticas sociais (transporte aéreo e serviços de saúde) nas quais o conceito de risco e sua aferição são difíceis de serem banalizados ou separados de sentimentos íntimos. A questão tem a ver com o teatro da segurança, que por sua vez tem a ver com a segurança de quem se informa e se comunica. Tem isso a ver num mundo em que o desafio de identificar reais interesses de interlocutores e mediadores virtuais se assemelha cada vez mais ao de identificar reais efeitos de substâncias ingeríveis, injetáveis, inaláveis ou absorvíveis, inclusive pelos ouvidos.

Comentários sobre as questões 6 e 7

Se quiser uma analogia, pense no que faria um administrador de redes para encontrar as possibilidades de alocar serviços numa rede corporativa segmentada, a partir de uma lista parcial de requisitos, lista que depois poderá vir a ser alterada ou contraposta.

* Autor

Pedro Antonio Dourado de Rezende
Professor concursado no Departamento de Ciência da Computação da Universidade de Brasília, Brasil. *Advanced to Candidacy* a PhD pela Universidade da California em Berkeley, onde teve sua pretensa tese de doutorado recusada em 1983. Membro do Conselho do Instituto Brasileiro de Política e Direito de Informática, ex-membro do Conselho da Fundação Software Livre América Latina, e do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-BR), entre junho de 2003 e fevereiro de 2006, como representante da Sociedade Civil.
`http://www.cic.unb.br/~rezende/sd.php`

Histórico deste Documento

Nota: Este artigo registra uma pesquisa acadêmica em andamento, conduzida sob o princípio científico da validação pela crítica fundamentada (*pier review*) e pelo norte filosófico que aponta o conhecimento como bem comum, razão do seu versionamento, seguindo o modelo FOSS de desenvolvimento (*publish early, publish often*).

v1.0 - 11/06/2008: Publicada no portal do autor e nas notas da 1ª turma do Curso de Especialização em Gestão da Segurança da Informação e Comunicações (CEGSIC) da UnB.

v1.1 - 21/06/2008: Republicada no portal do autor após 1ª apresentação no Curso CEGSIC. Acrescenta: referência à lei ou princípio de Kerckhoffs, ao final da seção 5.2; ref. [35] com citações desta em notas de rodapé, ao final da seção 5.3; at. comentários finais (cap.VI).

v1.2 - 29/07/2008: Republicada no portal do autor. Acrescenta: esclarecimentos sobre o referencial inicial do modelos de confiança em significação, na figura 5 e na seção 4.3; definição de virtual, segundo Giles Deleuze, na seção 1.1; revisão textual (não dos conceitos).

v1.3 - 05/08/2008: Republicada no portal do autor. Acrescenta: esclarecimentos sobre a natureza dos conflitos de interesse na modelagem proposta: à luz da definição semiológica de Confiança (Gerk), em notas de rodapé da seção 3.2 e na seção 4.2; à luz dos conceitos abordados, nas demais notas das seções 4.2, 4.3.

v1.4 - 10/10/2008: Republicada no portal do autor. Acrescenta: comentários sobre a tradução da definição de Informação, de Shannon, na seção 3.1 e nota de rodapé. Revisão textual (não de conceitos), especialmente nas seções 3.3 (com notas sobre a crise de 2008), 4.2, 4.3, 6.
v1.4.1 - 21/10/2008: Revisão textual, parágrafo acrescentado ao final do cap. III
v1.4.2 - 01/11/2008: Revisão t., hipótese de trabalho redetalhada na seção 3.2, at. ref. [7].
v1.4.3 - 08/12/2008: Revisão t., fig. 0 incluída; atualização notas de rodapé, refs. [36]-[48].
v1.4.4 - 03/03/2009: Revisão t. para a 2ª turma do curso CEGSIC. Notas 24 e 25 incluídas.

v1.5 - 09/04/2009: Republicada no portal do autor. Revisão do texto e refs. a partir de criticas céticas na 2ª turma CEGSIC, com notas 3, 15, 16, 34, 36 e refs. [50], [51] incluídas, nota 30 e foco da pesquisa redetalhadas, mormente nas seções 2.1 e 5.0. (v1.4.5 entre 2/4 e 5/4)

v1.6 - 31/05/2009: Republicada no portal do autor. Seção 5.0 revisada para incluir análise comparativa com outras modelagens de confiança em contextos computacionais, e também no cap. VI; nota de rodapé 36 atualizada, nota 50 e refs. [52]-[57] incluídas.
v1.6.1 - 09/06/2009: Mais sobre conflitos de interesse: Nota 8 revisada, ref. [58] incluída.
v1.6.2 - 16/08/2009: Revisão textual na seção 1.1. Seção 5.0 revisada para incluir análise comparativa com outras modelagens de confiança em contextos computacionais, e também

no cap. VI; nota de rodapé 36 atualizada, nota 50 e refs. [52]-[57] incluídas.
v1.6.3 - 15/10/2009: Revisão textual, mormente nas seções 2.1, 4.2, 5.0 e na nota 24 acrescentando fundamentação na Teoria da Ação Comunicativa de Habermas; figura 0' e refs. [59]-[69] incluídas (em várias sub-versões entre 12/09 e 06/10).
v1.6.5 - 16/04/2011: Revisão textual extensa, mormente na descrição da Semiose (fig 0 e 0') (em sub-versões entre 16/04 e 01/09)

v1.7 – 23/11/2012: Republicada no portal do autor. Extensa revisão. Inclui detalhes do papel da confiança em semioses (seção 2.1), do paradoxo Sausurreano (seção 4.2), do efeito Dunning-Kruger em PSIs (seção 4.3), e novas citações: à Teoria dos Atos de Fala, de Austin, (seção 4.2), e a outras conceituações de confiança (seção 5.0); notas (*, 22, 36, 52) e refs. [70]-[79].

Direitos de Autor