HÉLIO SANTIAGO RAMOS JÚNIOR

UMA ONTOLOGIA PARA REPRESENTAÇÃO DO CONHECIMENTO JURÍDICO-PENAL NO CONTEXTO DOS DELITOS INFORMÁTICOS

Florianópolis
2008

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO

HÉLIO SANTIAGO RAMOS JÚNIOR

UMA ONTOLOGIA PARA REPRESENTAÇÃO DO CONHECIMENTO JURÍDICO-PENAL NO CONTEXTO DOS DELITOS INFORMÁTICOS

FLORIANÓPOLIS, SETEMBRO DE 2008.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA E GESTÃO DO CONHECIMENTO

HÉLIO SANTIAGO RAMOS JÚNIOR

UMA ONTOLOGIA PARA REPRESENTAÇÃO DO CONHECIMENTO JURÍDICO-PENAL NO CONTEXTO DOS DELITOS INFORMÁTICOS

Dissertação de mestrado submetida ao Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da Universidade Federal de Santa Catarina como requisito parcial para obtenção do título de mestre em Engenharia e Gestão do Conhecimento.

FLORIANÓPOLIS, SETEMBRO DE 2008.

HÉLIO SANTIAGO RAMOS JÚNIOR

UMA ONTOLOGIA PARA REPRESENTAÇÃO DO CONHECIMENTO JURÍDICO-PENAL NO CONTEXTO DOS DELITOS INFORMÁTICOS

Esta Dissertação foi julgada adequada para a obtenção do Título de "Mestre em Engenharia", Especialidade em Engenharia e Gestão do Conhecimento e aprovada por decisão unânime pelos membros da banca e em sua forma final pelo Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento da UFSC.

Florianópolis, 26 de novembro de 2008.

_____

Prof. Roberto Carlos dos Santos Pacheco, Dr
Coordenador do Curso

Banca Examinadora:

_____

Prof. Aires José Rover, Dr.
(Orientador)

_____

Prof. Orides Mezzaroba, Dr.

_____

Prof. Fernando Álvaro Ostuni Gauthier, Dr.

RESUMO

RAMOS JÚNIOR, Hélio Santiago. **Uma ontologia para representação do conhecimento jurídico-penal no contexto dos delitos informáticos**. Florianópolis, 2008. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) – Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Universidade Federal de Santa Catarina.

O objetivo primordial desta dissertação é propor uma ontologia para representar o conhecimento jurídico-penal sobre delitos informáticos com o intuito de esclarecer ao cidadão acerca da tipicidade destes crimes. O conhecimento compartilhado deste domínio no tocante à aplicabilidade da lei penal brasileira aos crimes informáticos será extraído a partir de uma pesquisa sobre o entendimento jurisprudencial dos tribunais pátrios e de um estudo da doutrina dos principais especialistas sobre a legislação penal vigente aplicável aos delitos informáticos realizado pelo autor da dissertação. Embora o cidadão leigo seja o principal destinatário da ontologia, ela também será útil aos estudantes de Direito, advogados, promotores de justiça e juízes que necessitem obter auxílio na indicação de obras científicas que contenham um determinado assunto dentro do domínio dos crimes informáticos e ainda permitir a consulta acerca do entendimento de um tribunal pátrio acerca de um delito específico cometido através da informática. Além disso, ela pretende explicitar os conceitos utilizados neste domínio quanto à natureza jurídica dos crimes informáticos e identificar as condutas criminosas que podem ser cometidas contra ou através dos sistemas informáticos com a indicação de um verbo que conste no tipo penal de diversas leis penais que sejam potencialmente aplicáveis em se tratando de um delito informático. O procedimento metodológico adotado para construir a ontologia está baseado na metodologia *Ontology Development 101*, proposta por Noy & McGuiness (2000), definindo-se as classes, propriedades, instâncias e, ao final, são formuladas questões de competência as quais a ontologia deverá ser capaz de responder. Destaca-se que esta ontologia apenas considera a legislação penal atualmente vigente no Brasil e que a validação da ontologia foi realizada através de questionário e entrevista com dois especialistas da área. Ao final, conclui-se sobre a importância do uso da ontologia desenvolvida, principalmente por facilitar o acesso do cidadão leigo a conceitos e conhecimento jurídico sobre crimes informáticos.

Palavras-chave:
Crimes informáticos; Ontologias jurídicas; Engenharia do conhecimento.

RESUMEN

RAMOS JÚNIOR, Hélio Santiago. **Una ontología para representación del conocimiento jurídico-penal en el dominio de los delitos informáticos**. Florianópolis, 2008. Tesis de maestría. (Maestría en Ingeniería y Gestión del Conocimiento) – Programa de Post-Grado en Ingeniería y Gestión del Conocimiento, Universidad Federal de Santa Catarina, Brasil.

El objetivo primordial de esta disertación es proponer una ontología para representar el conocimiento en el ámbito jurídico-criminal sobre delitos informáticos con la intención de aclarar al ciudadano acerca de la aplicabilidad de las leyes penales brasileñas vigentes a estos crímenes. El conocimiento compartido de este dominio en lo que se refiere a la aplicabilidad de las leyes penales brasileñas a los delitos informáticos será extraído de una investigación sobre la jurisprudencia de las cortes nacionales y de estudios sobre la doctrina de los especialistas acerca de la legislación criminal del país que sea aplicable a los delitos informáticos, realizados por el autor de la disertación. Aunque el ciudadano sea el principal destinatario de la ontología propuesta, ella también será útil a los estudiantes de Derecho, a los abogados, a los miembros del Ministerio Público y a los jueces que necesitan obtener la indicación de libros y artículos científicos sobre un tema específico del dominio de los delitos informáticos y todavia permitir la consulta referente al entendimiento de los tribunales del país acerca de un delito específico cometido a través de la informática. Por otra parte, la ontología pretende también explicitar los conceptos usados en este dominio cuánto a la naturaleza legal de los delitos informáticos e identificar los comportamientos criminales contra los sistemas informáticos y cometidos a través del uso de la informática con la indicación del verbo que consista en un tipo penal de las diversas leyes penales que sean potencialmente aplicables a estos crímenes. El procedimiento metodológico adoptado para contruir la ontología se basa en el *Ontology Development 101*, propuesto por Noy & McGuiness (2000), definiendo las clases, propiedades, instancias e las cuestiones de competencia formuladas las cuales la ontología deberá ser capaz de aclarar. Es importante decir que esta ontología considera solamente la legislación criminal de Brasil vigente en la actualidad y que la validación de la ontología fue hecha con cuestionario y entrevista con dos especialistas del área. Por fin, se concluye acerca de la importancia del uso de la ontología desarollada, principalmente por facitar el acceso del ciudadano a los conceptos y conocimiento legal sobre delitos informáticos.

Palabras-clave:
Delitos informáticos; Ontologías Jurídicas; Ingeniería del conocimiento.

ABSTRACT

RAMOS JÚNIOR, Hélio Santiago. **Ontology for criminal legal knowledge representation in the cyber crime domain**. Florianópolis, 2008. Dissertation. (Master in Knowledge Engineering and Management) – Post-Graduate Program in Knowledge Engineering and Management (EGC), Universidade Federal de Santa Catarina, Brazil.

The aim of this dissertation is to propose an ontology for criminal legal knowledge representation in the cyber crime domain in order to clarify to the citizens about the Brazilian law enforcement to these criminal behaviors. The shared knowledge of this domain in regards to the applicability of the Brazilian criminal law to the cyber crimes will be extracted from a research about judicial decisions of national courts and a study of the main specialists' doctrine about the criminal law enforcement to the cyber crimes which will be done by the author of this dissertation. Although the lay citizen is the main user of the ontology, it will be useful to the law students, lawyers, attorneys general and judges who need indications of books or scientific papers which approach a specific subject on the cyber crime domain and it still allow to retrieve information about the national jurisprudence about the cyber crime. Moreover, it intends to clarify the concepts used in this domain related to the legal nature of the cyber crimes and it can also identify the criminal behaviors which can be committed against or through the computer science by indicating a verb that is described as a crime in the national criminal law and which is potentially applicable to the cyber crimes. The methodology procedure adopted in order to construct the ontology is the *Ontology Development 101*, which was proposed by Noy & McGuiness (2000), defining the classes, properties, instances and the competence questions which the ontology must be able to answer. It is important to mention that this ontology only considers the Brazilian criminal law currently effective in the legal order and its validation was done by two steps, applying questionnaire and interview with two specialists of the area. Finally, it concludes on the importance of the use of the ontology proposed in this disertation, maily for facilitating the access of the lay citizen to the concepts and legal knowledge on cyber crimes.

Keywords:
Cyber crimes; Legal Ontologies; Knowledge Engineering.

SUMÁRIO

1 INTRODUÇÃO.....1
1.1 Contextualização e problema de pesquisa.....1
1.2 Objetivos.....2
1.3 Justificativa.....4
1.4 Aderência à engenharia e gestão do conhecimento.....5
1.5 Escopo e delimitação do tema.....6
1.6 Metodologia.....7
1.7 Estrutura da dissertação.....7

2 INTELIGÊNCIA ARTIFICIAL E ONTOLOGIAS......8
2.1 Contextualização sobre IA e engenharia do conhecimento.....8
2.2 O uso da IA na detecção de condutas criminosas.....9
2.3 *Web* semântica.....14
2.4 Ontologias.....16
2.5 Recuperação de informação baseada em semântica e apoio à jurisprudência.....17
2.6 Modelo ONTOINFOJUS: acesso à informação na área jurídica.....18
2.7 Ontologias para explicitação de conceitos e valores jurídicos.....19
2.8 Ontologia jurídica com aplicação na área de direito tributário.....19
2.9 Ontologias para cenários de missões complexas em perícia forense.....21
2.10 Projetos internacionais que envolvem o uso de ontologias jurídicas.....22

3 CRIMES INFORMÁTICOS.....39
3.1 Contextualização da origem dos crimes informáticos.....39
3.2 Definição e classificação dos crimes informáticos.....40
3.3 Estudo sobre a aplicabilidade da lei penal aos crimes informáticos.....44
3.4 Projeto de lei substitutivo sobre delitos informáticos.....70

4 ONTOLOGIA JURÍDICA DE DELITOS INFORMÁTICOS.....72
4.1 Domínio da ontologia.....72
4.2 Princípios jurídicos observados.....73
4.3 Reuso das ontologias existentes.....75
4.4 Enumeração dos termos importantes.....76
4.5 Classes e hierarquia de classes.....76
4.6 Localização de obras científicas.....78
4.7 Recuperação de jurisprudências.....83
4.8 Leis penais aplicáveis.....88
4.9 Natureza jurídica dos delitos.....90
4.10 Explicitação dos conceitos jurídicos.....93
4.11 Tipicidade dos crimes informáticos.....95

CONCLUSÃO.....101

REFERÊNCIAS BIBLIOGRÁFICAS.....105

1. INTRODUÇÃO

1.1 Contextualização e problema de pesquisa

Este estudo parte da premissa de que a sociedade necessita ser esclarecida acerca das condutas penais que constituem delitos informáticos uma vez que o cidadão que praticar um ilícito penal será responsabilizado criminalmente e não poderá argumentar o desconhecimento da lei em benefício próprio já que todos são obrigados a conhecê-la.

A questão do desconhecimento da lei penal aplicável aos crimes informáticos é um problema tanto para o cidadão leigo quanto para o profissional do direito, já que no país não existe atualmente uma lei específica para lidar com os delitos informáticos, de maneira que a simples consulta às normas vigentes nem sempre é capaz de sanar todas as dúvidas que existem quando o assunto se refere aos crimes cometidos na Internet.

Os delitos informáticos são um fenômeno recente cuja origem remonta ao uso do computador e da Internet para a prática de condutas criminosas e a necessidade de se conhecer a aplicabilidade da lei a estes crimes se justifica para garantir a segurança jurídica para que todos possam saber com exatidão quais são estes delitos. Para resolver este problema existente, é proposta uma ontologia na *web* semântica, objetivando fazer com que o cidadão em geral possa ter acesso ao conhecimento jurídico-penal adequado, independentemente de possuir ou não formação ou prévio conhecimento nesta área.

Além disso, a relevância desta temática se deve também ao fato de que os delitos informáticos estão experimentando um grande crescimento nos últimos anos, que os criminosos comuns estão migrando suas atividades ilícitas para a Internet e a previsão que se tem, segundo Silva (2006) é que, daqui a 15 anos, os criminosos terão nascido na época da cibernética e da inclusão digital, conseqüentemente, possuindo muito mais conhecimentos e habilidades no uso da informática.

Assim, por se vivenciar justamente este momento histórico chamado ‘sociedade da informação’ é que mais do que antes se faz necessário esclarecer à sociedade acerca dos crimes informáticos, usando ontologias para facilitar o acesso de todo o cidadão ao conhecimento legal acerca das condutas delituosas praticadas com o uso da informática.

O conhecimento jurídico-penal na área dos crimes informáticos é complexo, não basta apenas aos profissionais do direito conhecer a lei, ela deve ser conhecida por toda a sociedade e a engenharia do conhecimento poderá fazer com que isto seja possível.

1.2 Objetivos

Nesta seção, pretende-se deixar bem claro os objetivos do trabalho, subdividindo os mesmos em objetivo geral e objetivos específicos.

1.2.1 Objetivo geral

- Criar uma ontologia para representar o conhecimento jurídico-penal no contexto dos delitos informáticos, objetivando esclarecer ao cidadão acerca da tipicidade destes crimes, incluindo os conceitos jurídicos usados neste domínio.

1.2.2 Objetivos específicos

a) Apresentar uma fundamentação teórica do trabalho a partir da introdução dos conceitos básicos de inteligência artificial, engenharia do conhecimento, web semântica e ontologias para representação do conhecimento;

b) Identificar e comentar os principais projetos sobre ontologias na área do direito, em âmbito nacional e internacional, visando o seu possível reuso no domínio estudado;

c) Realizar um estudo sobre a aplicabilidade da lei penal aos crimes informáticos no país, com base na doutrina e em pesquisa jurisprudencial sobre a matéria, com a finalidade de extrair o conhecimento jurídico adequado a ser modelado na ontologia;

d) Construir uma ontologia para representar o conhecimento jurídico-penal sobre delitos informáticos, localizando obras científicas relativas a este domínio, recuperando jurisprudências da área e esclarecendo conceitos relacionados à tipicidade destes crimes e as condutas criminosas que podem ser cometidas contra ou através da informática.

e) Verificar e validar a ontologia jurídica de delitos informáticos a ser proposta.

1.2.3 Questões de competência

No que concerne à ontologia a ser desenvolvida, é importante, desde já, deixar claro também quais são as questões de competência que ela pretende esclarecer, as quais estão relacionadas com o objetivo geral e com o objetivo específico da letra "d".

É importante destacar que enquanto o objetivo geral visa esclarecer a tipicidade dos crimes informáticos, o objetivo específico da letra 'd' define particularmente os meios que serão utilizados para que este objetivo principal possa ser alcançado.

O esclarecimento sobre a aplicação da lei penal aos delitos informáticos pode ocorrer indiretamente, através da localização de obras científicas ao cidadão que tratem de um determinado crime específico ou mesmo com a recuperação de decisões judiciais que abordem a questão da tipicidade de um crime na Internet, assim como fornecendo ao cidadão os conceitos dos termos jurídicos que são utilizados neste domínio.

Ademais, além de indicar referências doutrinárias e jurisprudências que poderão servir para o cidadão aprofundar um pouco mais o seu conhecimento sobre o assunto e da explicitação dos termos jurídicos usados neste domínio, a ontologia se dispõe a esclarecer diretamente as principais questões sobre as normas penais aplicáveis aos crimes informáticos, que é o foco central deste trabalho de dissertação.

Desta forma, no que concerne aos objetivos da ontologia proposta, ela se destina a responder, dentre outras, exemplificativamente, as seguintes questões de competência:

a) Quais as obras científicas sobre delitos informáticos relacionadas a crimes cometidos contra os direitos da criança e do adolescente?

b) Qual o entendimento do Superior Tribunal de Justiça acerca da competência para julgar crimes de furto cometidos pela Internet?

c) Quais as características dos crimes informáticos cometidos contra a Administração Pública?

d) Quais os conceitos jurídicos das diversas categorias de crimes que existem?

e) Quais os crimes informáticos que podem ser cometidos com o verbo "incitar" descrito no núcleo do tipo penal?

f) Quais as normas penais aplicáveis aos crimes contra a honra das pessoas através da Internet?

1.3 Justificativa

Conforme mencionado, a presente proposta de uma ontologia para representação do conhecimento jurídico-penal no contexto dos delitos informáticos visa esclarecer ao cidadão sobre a tipicidade dos crimes praticados na Internet, justificando-se a realização deste trabalho para tornar acessível o conhecimento jurídico-penal sobre crimes informáticos a todo o indivíduo na sociedade da informação, através da *web* semântica.

A Constituição Federal de 1988 garante em seu artigo 5º, inciso XXXIX, que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, ou seja, é preciso sempre observar o princípio fundamental segundo o qual ao cidadão não pode ser imputado um crime que não esteja definido em lei e que toda pena somente pode ser aplicada se estiver prevista em norma preexistente ao fato criminoso.

Entretanto, como não há uma legislação específica sobre crimes informáticos, muitos tribunais pátrios passaram a aplicar o Código Penal às condutas ilícitas que são cometidas na Internet e o cidadão precisa de um esclarecimento a respeito deste assunto, particularmente quanto à aplicação da lei penal aos crimes cometidos no ciberespaço.

Assim, o estudo exploratório sobre inteligência artificial, *web* semântica e ontologias se apresenta muito pertinente porque fornecerá a base teórica necessária para a representação do conhecimento jurídico-penal no âmbito dos crimes informáticos.

A localização de obras científicas sobre estes delitos será uma funcionalidade que contribuirá bastante para auxiliar no objetivo de esclarecer questões relacionadas aos crimes informáticos já que permitirá ao cidadão encontrar referências bibliográficas que sejam úteis e que abordem exatamente o assunto acerca do qual se está procurando.

Também poderá servir para que se conheça o entendimento de um tribunal sobre um delito informático, cuja resposta poderá ser obtida de modo preciso com ontologias ao recuperar decisões judiciais sobre estes crimes, especificando as suas propriedades.

Uma vez sendo identificadas as características destes delitos, enumerados os termos e definidos seus conceitos formalmente na ontologia, será possível fazer com que este conhecimento possa ser recuperado através da estrutura da *web* semântica para que seja possível esclarecê-los ao cidadão, inclusive quanto à aplicação da lei penal.

No âmbito dos delitos informáticos no Brasil, não existia até então ontologias para representar o conhecimento jurídico-penal neste domínio considerando o sistema legal em sua integridade, abrangendo não só a lei, mas também os princípios jurídicos, a doutrina dos especialistas em crimes informáticos e a jurisprudência acerca do assunto.

1.4 Aderência à engenharia e gestão do conhecimento

O tema abordado nesta dissertação de mestrado está inserido na Engenharia e Gestão do Conhecimento uma vez que o objetivo deste trabalho é propor e elaborar uma ontologia para representação do conhecimento jurídico-penal sobre delitos informáticos.

Por esta razão é que se pretende construir uma ontologia para ajudar a esclarecer questões sobre a tipicidade dos crimes informáticos, o que será possível de se realizar a partir do mapeamento, modelagem e representação do conhecimento jurídico nesta área.

Embora os crimes informáticos sejam objeto de estudo e o autor da dissertação possua formação em direito, o que torna possível o desenvolvimento deste trabalho é justamente o conhecimento adquirido no Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, pois não se trata aqui apenas de dissertar sobre a aplicação da lei penal aos crimes informáticos, mas principalmente de representar este conhecimento.

Desta maneira, o autor pretende dissertar acerca do tema proposto sob a ótica de um engenheiro do conhecimento jurídico, abordando o assunto com enfoque central na engenharia do conhecimento, contando subsidiariamente com o conhecimento jurídico que já possui apenas para guiá-lo e orientá-lo na consecução do objetivo principal do trabalho que é a representação do conhecimento legal acerca dos delitos informáticos.

Assim, o conhecimento do domínio a ser modelado será proveniente do estudo a ser realizado no terceiro capítulo pelo próprio autor da dissertação, que, além de deter razoável conhecimento técnico, possui formação acadêmica na área do Direito. Isto é uma vantagem, porque permitirá uma maior evidência na identificação do conhecimento compartilhado, na formulação das questões de competência e nas respostas quanto à aplicação da lei penal, tendo em vista a teleologia e a complexidade do sistema legal.

Neste sentido, considerando que a construção de ontologias jurídicas ou sistema especialista legal não consiste apenas em mero exercício de programação, mas exige sólida fundamentação jurídica, recomenda-se que, havendo condições técnicas, seja o profissional do Direito o próprio engenheiro do conhecimento. (ROVER, 2000, p. 211)

É evidente que o presente trabalho de dissertação terá contribuições para a área do direito ao representar o conhecimento jurídico-penal para esclarecer a aplicabilidade da lei penal aos crimes informáticos, porém a expectativa é que as contribuições para a engenharia do conhecimento também sejam significativas, com a possibilidade de reuso da ontologia a ser proposta, servindo ainda de suporte para um sistema especialista legal ou para um sistema de raciocínio baseado em casos na recuperação de jurisprudências.

1.5 Escopo e delimitação do tema

Para fins de representação do conhecimento jurídico-penal através da ontologia, serão abrangidos apenas os delitos que estejam tipificados atualmente nas legislações penais brasileiras onde haja um entendimento compartilhado ou predominante na doutrina e na jurisprudência acerca da sua aplicabilidade aos crimes informáticos, pois se considera imprescindível conhecer as diversas condutas criminosas para que as ontologias jurídicas sejam eficazes no esclarecimento de questões relacionadas à tipicidade destes crimes, tendo em conta o sistema jurídico-penal em sua integralidade.

Desta forma, a ontologia será desenvolvida, a princípio, para ter uma aplicação *ex nunc*, ou seja, será válida apenas para esclarecer questões atuais sobre delitos informáticos, não sendo aplicável a casos pretéritos no tempo da lei velha por considerar apenas a lei penal brasileira vigente no momento de sua construção, sendo atualizada daqui para frente. Esta delimitação se torna recomendável para fins de estudo e desenvolvimento da ontologia por simplificá-la sem comprometer a sua validade quanto a sua aplicação a fatos ocorridos a partir da legislação penal em vigor no país.

Por outro lado, é importante ressaltar que sendo aprovada a legislação de delitos informáticos no Brasil, a ontologia será atualizada para abranger as novas modalidades de crimes informáticos que forem inseridas no ordenamento jurídico brasileiro, pois, uma das características das ontologias é que elas devem ser constantemente atualizadas para que o seu resultado seja sempre útil e eficaz.

Assim, embora a ontologia não considere atualmente os projetos de lei sobre os crimes informáticos em tramitação, é possível incorporá-los à ontologia jurídica de delitos informáticos proposta tão logo passem a integrar o sistema jurídico vigente.

Destaca-se também que as questões de competência na ontologia proposta estão adstritas às condutas que são suscetíveis de caracterizar crimes informáticos, já que a ontologia se adstringe a esclarecer a tipicidade destes delitos através da representação do conhecimento jurídico-penal neste domínio. Não obstante, existe a possibilidade de seu reuso para ampliar a sua aplicação e abranger outros delitos, além dos informáticos.

1.6 Metodologia

Utiliza-se, na presente dissertação, o método dedutivo, partindo-se de uma visão geral do assunto para as suas especificidades, identificando os problemas e propondo as respectivas soluções por meio da engenharia do conhecimento.

O procedimento metodológico adotado para construir a ontologia está baseado na metodologia *Ontology Development 101*, proposta por Noy & McGuiness (2000).

Entretanto, no que concerne ao conhecimento do domínio a ser modelado, tal como descrito no objetivo específico da letra 'c', ele será extraído através de um estudo jurídico sobre a doutrina dos especialistas em crimes informáticos e de pesquisa sobre o entendimento jurisprudencial dos magistrados brasileiros sobre estes delitos.

Quanto à metodologia para validação da ontologia, serão entrevistados dois profissionais, ambos pós-graduados e detentores de conhecimento jurídico sobre delitos informáticos para constatar, ao final, se a ontologia proposta consegue responder as questões de competência que foram formuladas no item 1.2.3 desta dissertação.

1.7 Estrutura do trabalho

No segundo capítulo, é apresentada a fundamentação teórica da dissertação com a introdução dos conceitos fundamentais acerca da inteligência artificial, engenharia do conhecimento, *web* semântica e ontologias para representação do conhecimento; sendo identificados e comentados os principais projetos sobre ontologias na área do direito, em âmbito nacional e internacional, que são os objetivos específicos da letra 'a' e 'b'.

O terceiro capítulo, por sua vez, tem a finalidade de identificar o cenário atual dos crimes informáticos a partir do estudo sobre as normas jurídicas que lhes sejam consensualmente aplicáveis, abordando o seu conceito e as suas formas de classificação, onde se analisarão a doutrina e a jurisprudência acerca dos crimes informáticos no país, tecendo, ao final deste capítulo, comentários sobre as propostas legislativas nesta área.

Por fim, no quarto e último capítulo, propõe-se uma ontologia a qual será desenvolvida pelo autor para representar o conhecimento jurídico-penal no contexto dos delitos informáticos, objetivando esclarecer a tipicidade dos crimes informáticos no país e os conceitos jurídicos, além de recuperar doutrina e jurisprudências destes delitos.

2. INTELIGÊNCIA ARTIFICIAL E ONTOLOGIAS

Neste capítulo, estuda-se a inteligência artificial (IA), destacando a aplicação de algumas de suas técnicas pela engenharia do conhecimento para resolver problemas sobre condutas criminosas, com ênfase para o uso de *web* semântica e de ontologias jurídicas, destacando alguns projetos desenvolvidos tanto no país quanto no exterior.

2.1 Contextualização sobre IA e engenharia do conhecimento

A inteligência artificial teve origem a partir das pesquisas realizadas por Alan Turing que propôs um teste o qual tinha o intuito de verificar se um computador poderia ser dotado de inteligência. Trata-se do famoso teste de Turing o qual foi projetado para fornecer uma definição operacional satisfatória de inteligência. Assim, "em vez de propor uma lista longa e talvez controversa de qualificações exigidas para inteligência, ele sugeriu um teste baseado na impossibilidade de distinguir entre entidades inegavelmente inteligentes – os seres humanos". (RUSSELL & NORVIG, 2004, p. 4)

Segundo o teste de Turing, um computador é considerado inteligente se ele consegue agir como se fosse um ser humano, respondendo perguntas de forma racional e lógica, de maneira que a pessoa que formula as questões não seja capaz de identificar se quem as respondeu foi um ser humano ou um computador previamente programado.

Em outras palavras, o teste funciona do seguinte modo: uma pessoa faz perguntas de forma escrita a duas entidades ocultas, sendo uma o ser humano e a outra o computador, sendo-lhe fornecidas as respostas em seguida, também por escrito, sendo a comunicação entre a pessoa realizada indiretamente de maneira que a mesma formulará perguntas, com a finalidade de descobrir qual das duas entidades é o ser humano.

O computador, por sua vez, é programado para se passar por um ser humano enquanto que o ser humano responderá de forma a confirmar a sua condição. Se no final do teste a pessoa que formulou as perguntas não conseguir distinguir dentre as duas entidades quem é o ser humano, então o teste conclui que o computador é inteligente.

A referência a Alan Turing e ao seu teste é importante porque se pode dizer que as suas pesquisas contribuíram para o progresso da ciência não apenas por introduzir uma noção básica de IA, mas, principalmente, porque veio a suscitar o desenvolvimento

de novos estudos envolvendo a IA visando a sua aplicação em áreas do conhecimento específicas para propor soluções inovadoras.

Há uma grande dificuldade por parte dos pesquisadores em definir com precisão o conceito de IA, entretanto é possível conceituá-la como sendo um campo de estudo que procura explicar e emular o comportamento inteligente em termos de processos computacionais. (SCHALKOFF, 1990, p. 2) A inteligência artificial também pode ser entendida como um exercício de busca pelos formalismos apropriados para serem utilizados na representação do conhecimento. (SCHANK, 1990, p. 3)

Já a engenharia do conhecimento está relacionada com o uso da IA para modelar o conhecimento de especialistas humanos em resolver problemas, sendo esta a sua concepção inicial já que se entendia que o papel do engenheiro do conhecimento consistia em adquirir e codificar o conhecimento para que fosse utilizado em seguida para solucionar questões referentes a uma área do conhecimento específica.

Novas abordagens para codificar o conhecimento foram desenvolvidas, o que permitiu uma maior expansão da engenharia do conhecimento que passou a se dedicar não apenas à construção de **sistemas especialistas**, mas também à aplicação de outras técnicas de IA, como, por exemplo, o raciocínio baseado em casos.

Entretanto, os engenheiros do conhecimento de antigamente empregavam as ferramentas adequadas para o caso concreto, sem focalizar nas prioridades e objetivos estratégicos da organização; enquanto que a nova engenharia do conhecimento vem justamente para ressaltar a necessidade de que este profissional tenha uma visão sistêmica do processo para modelar o conhecimento.

2.2 O uso da IA na detecção de condutas criminosas

Dentre algumas aplicações de IA para auxiliar na detecção de crimes, pode-se destacar seu uso na identificação de casos suspeitos de furto de energia elétrica, fraude em telecomunicações, vigilância eletrônica e ainda no combate às invasões cibernéticas.

2.2.1 Furto de energia elétrica

A inteligência artificial pode ajudar a detectar casos de furto de energia elétrica através de detectores inteligentes que sejam capazes de identificar os fraudadores.

Uma notícia publicada em fevereiro de 2008 na *Gazeta On Line* reportou que está sendo implantado no Estado do Espírito Santo um sistema de medição eletrônico que permite controlar o fornecimento de energia diretamente da sede da Escelsa, empresa fornecedora de energia elétrica daquele estado, a qual estaria investindo no uso da IA para melhorar a eficiência do serviço e dificultar a ação de fraudadores.

Neste sentido, a empresa desenvolveu também um programa de IA em parceria com a Universidade Federal do Espírito Santo (UFES) com a finalidade de usar o computador para rastrear locais onde há indícios de fraudes em medidores e de ligações clandestinas e identificar os potenciais infratores.

2.2.2 Fraude nas telecomunicações

O uso da inteligência artificial pode ajudar no combate a qualquer tipo de fraude, não apenas em relação ao furto de energia elétrica, mas também tem aplicações, por exemplo, no âmbito das telecomunicações.

Pesquisadores da Faculdade de Ciências e Tecnologias da Universidade de Coimbra (FCTUC) desenvolveram um sistema denominado *ECA3RL*, o qual utiliza diversas técnicas de IA, como, por exemplo, o **raciocínio baseado em casos** (RBC), que é uma técnica que utiliza raciocínio analógico; a ferramenta adota também processos de análise de informação registrada em casos suspeitos, possuindo como uma de suas principais características o fato da mesma ser capaz de aprender novos processos de detecção e se adaptar à evolução das fraudes.

2.2.3 Monitoramento eletrônico

Outro âmbito de aplicação da inteligência artificial relacionada à prevenção aos crimes tem sido o uso de câmeras de vigilância inteligentes por meio da realização de um sistema de monitoramento eletrônico que adota técnicas de IA e que possui a

capacidade de reconhecer padrões de comportamento perigosos, identificando, sozinho, situações de risco, como tentativa de assalto ou de vandalismo.

Uma das ferramentas utilizadas é o *software AISight*, o qual emite sinais de alerta e pode ser empregado para prevenir acidentes ou crimes, sendo utilizado pelo governo americano para reconhecer atividades suspeitas e prever atentados terroristas.

Em recente notícia publicada em maio de 2008, na *Gazeta do Povo*, divulgou-se que a prefeitura de Curitiba instalou câmeras de vigilância inteligentes no centro da cidade, causando um temor por parte da sociedade de que tal sistema seja utilizado para invasão de privacidade ou para um controle excessivo do governo.

Diante desta realidade, caracterizada pelo constante monitoramento do cidadão por parte do Estado, é pertinente a observação no sentido de que "a sociedade disciplinar, marcada pelo 'vigiar e punir', foi substituída por um novo tipo de sociedade marcada pelo 'monitorar, registrar e reconhecer'". (VIANNA, 2007, p. 83)

2.2.4 Invasões cibernéticas e agentes inteligentes

No ano de 2004, foi apresentado um estudo sobre o uso de agentes inteligentes móveis no combate às invasões cibernéticas durante a I Conferência Internacional de Perícia em Crimes Cibernéticos que ocorreu em Brasília/DF.

O objetivo do trabalho foi esclarecer a sociedade sobre o problema das invasões cibernéticas e propor o uso de agentes inteligentes móveis na defesa digital dos sistemas de informática, evitando a invasão de computadores e ataques de negação de serviço.

Assim, desenvolveu-se uma arquitetura de agentes baseada em linguagem de programação PROLOG para realizar o monitoramento do sistema e o combate de forma automatizada às invasões DoS e DDoS, sem a necessidade da intervenção humana. Entretanto, ressalta o autor que é preciso melhorar a interface e ampliar o escopo de atuação do agente inteligente móvel implantado. (NOGUEIRA, 2004, p. 72)

2.2.5 Redes neurais e sistemas especialistas na detecção de intrusos

Outra aplicação de inteligência artificial voltada para o combate às invasões cibernéticas é um modelo híbrido proposto que usa **redes neurais artificiais** (RNA) e sistemas especialistas para detecção de intrusos em redes de computadores TCP/IP.

Redes neurais artificiais são técnicas de IA que utilizam um modelo baseado na estrutura do cérebro humano onde o sistema é capaz de adquirir conhecimento através da experiência. Enquanto as RNA são comumente usadas neste caso para detectar o comportamento, os sistemas especialistas permitem a detecção com base no conhecimento. Assim, foi criada uma ferramenta de detecção denominada *Newnids* com o objetivo de "perceber o tráfego entrante em uma rede de computadores, que usa tecnologia ETHERNET e está baseada em TCP/IP, submetê-lo ao parecer de uma RNA do tipo MLP [*Multi Layer Perceptron*], cujo resultado será submetido ou não a um Sistema Especialista (ambos formam a *Engine*) o que findará na diagnose se a ação é ou não intrusiva". (BARREIRA, ALVARENGA & JARDIM, 2006, p. 53)

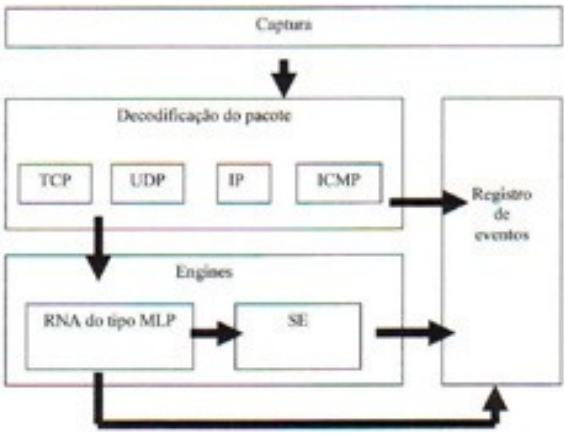

Figura 1. Representação do fluxo de informação através da ferramenta *Newnids*.
(Fonte: BARREIRA, ALVARENGA & JARDIM, 2006, p. 53)

Em síntese, o modelo captura os pacotes e os decodifica com a obtenção dos valores a serem submetidos a *Engine* de detecção por meio da rede neural artificial, e, havendo dúvida quanto à ação intrusiva, ela é submetida ao sistema especialista. Ao final, os autores concluem que "a combinação de técnicas de detecção de intrusão com representação neural e simbólica pode constituir maior qualidade no processo de detecção de intrusão". (BARREIRA, ALVARENGA & JARDIM, 2006, p. 56)

2.2.6 Detecção de intrusão utilizando lógica *Fuzzy* e *Data Mining*

No ano de 2005, pesquisadores da *Universiti Teknologi Malaysia* propuseram um modelo dinâmico para sistemas inteligentes de detecção de intrusão, baseado em uma abordagem específica de IA para a detecção de intrusos. Esta técnica inclui o uso de redes neurais artificiais e da lógica *fuzzy*, traçando o perfil da rede e utilizando técnicas de *data mining* para processar os dados da rede:

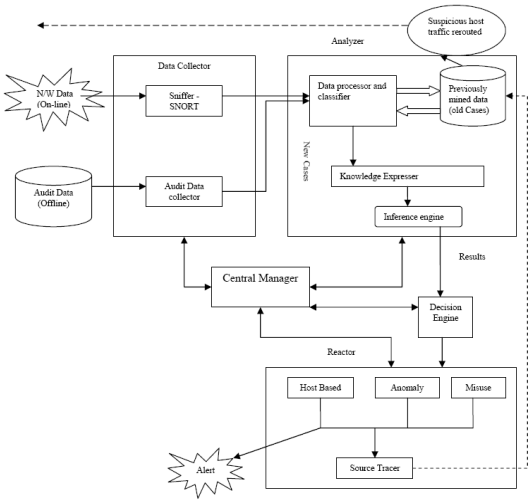

Figura 2. Sistema inteligente de detecção de intrusão proposto.
(Fonte: BASHAH, BHARANIDHARAN & AHMED, 2005, p. 293)

A **lógica *fuzzy*** (difusa) consiste em uma técnica de IA utilizada para a criação de sistemas especialistas que considera a imprecisão e variáveis do ambiente, podendo assim ser utilizada para detecção de intrusão já que os parâmetros para a definição de uma ação intrusiva são geralmente vagos e incertos.

Data mining, por sua vez, é um método de mineração de dados utilizado para extrair as informações mais importantes e úteis que constam em bancos de dados.

Na detecção de intrusão, pode-se escrever uma regra como um sinal de alerta, definindo uma razão para que o alarme seja disparado no sistema, como, por exemplo, estabelecer como um dos motivos a quantidade referente ao número de diferentes destinações de endereços de IP detectados nos últimos dois segundos.

Assim, se o número de diferentes destinações de endereços durante os últimos X segundos for maior que o usual, então se conclui que existe uma situação anormal.

Estas regras úteis são descobertas com o uso de *data mining* através da extração do conhecimento da base de dados, enquanto a lógica *fuzzy* é empregada justamente

para detectar situações anormais e ajudar a criar testes padrões abstratos.

2.3 *Web* semântica

Depois do estudo sobre a inteligência artificial bem como a sua relação com a engenharia do conhecimento e suas aplicações na detecção de condutas criminosas, é importante dissertar sobre um fenômeno denominado de *web* semântica, pois será através dele que agentes de *software* serão capazes de identificar o contexto das informações disponíveis na Internet, tornando-se aptos em ajudar a esclarecer questões relacionadas aos crimes informáticos.

Todo o conteúdo existente na *web* foi originariamente inserido no espaço cibernético de forma que a única preocupação era que tais dados e informações fossem compreendidos apenas pelas pessoas que acessavam a rede, esta é a *web* tradicional.

A *web* semântica, por sua vez, foi idealizada por Tim Berners-Lee o qual propôs uma rede estruturada de forma inteligente de modo que as informações pudessem ser compreendidas por agentes de *software* ao realizarem uma determinada busca na *web*.

Assim, ela aparece como uma evolução da *web* atual com o intuito de utilizar linguagens de programação que permitam dar significado de conteúdo às páginas da *web*, criando condições para que agentes de *software*, através do acesso e interpretação contextualizada dos dados disponibilizados na Internet, possam realizar tarefas complexas para o usuário, permitindo, assim, um tratamento automático deste conteúdo.

Segundo Berners-Lee, Hendler & Lassila (2001) "o problema que a web semântica tem de resolver consiste em proporcionar uma linguagem capaz de dar expressão tanto a dados como a regras para raciocinar sobre dados e que permita ainda a exportação à rede das regras de inferências de qualquer sistema de representação de conhecimento que já exista".

Uma das vantagens apresentada pela *web* semântica é que ela possibilita indexar documentos de modo que as suas propriedades e características possam ser identificadas pelos agentes de *software* no momento da realização de consulta às páginas da *web*, o que facilita consideravelmente a recuperação de informações na rede.

A *web* semântica está estruturada em camadas, conforme ilustra a seguir:

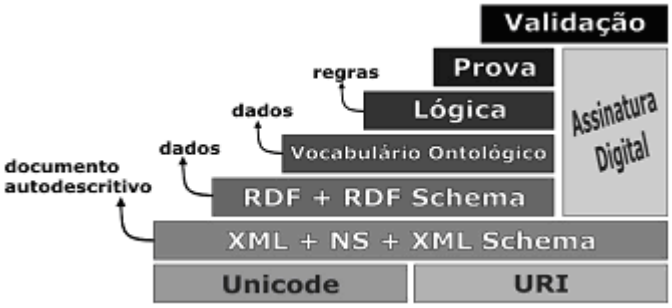

Figura 3. Arquitetura em camadas da *Web* Semântica (W3C).

A primeira camada da *web* semântica é composta por um sistema de codificação denominado *Unicode*, o qual fornece um número único para os diferentes caracteres independentemente do idioma, programa ou plataforma utilizada, o que permite que os dados possam ser transportados por diferentes sistemas sem que sejam corrompidos. Além disso, esta camada inicial também é composta pelo *Uniform Resources Identifier* (URI), que serve para referenciar os recursos existentes na rede.

Estes esquemas de codificação única de caracteres e de identificação dos recursos existentes na rede tornam possível atingir a segunda camada da *web* semântica com a utilização de padrões modernos como a linguagem de marcação XML (*Extensible Markut Language*), a qual, diferentemente da linguagem HTML (*HyperText Markut Language*), é compreensível tanto pelas pessoas quanto pelos computadores, já que permite definir marcadores e a relação estrutural entre eles, contando com o auxílio dos recursos XML *NameSpace* (NS) e XML *Schema* na descrição dos documentos.

A terceira camada da *web* semântica se aproveita da estrutura da camada XML, sendo formada pelo RDF (*Resource Description Framework*) e RDF *Schema*. Trata-se de uma camada de metadados que tem o objetivo de garantir a interoperabilidade entre as aplicações, representando os dados sob a forma de triplas através de descrições de recursos, propriedades e valor. Assim, ela serve não apenas para representar dados e expressar afirmações sobre os recursos utilizando a forma de triplas, mas também visa garantir que os diversos formatos e aplicações que existem possam ser compatíveis.

As ontologias estão representadas na quarta camada da *web* semântica e elas são utilizadas para representar o vocabulário de um determinado domínio, explicitando conceitos dentro desta área em uma linguagem formal que possa ser compartilhada. Desta forma, ela é comumente representada através da linguagem padrão OWL (*Ontology Web Language*) e apresenta maior riqueza semântica em relação as demais.

Por fim, as camadas de lógica, prova e validação que estão apoiadas sobre a estrutura inferior da arquitetura da *web* semântica apresentada, implementam a definição de regras e possibilitam a prova e a validação de inferências realizadas por agentes de *software* que fazem uso dos recursos de toda a estrutura existente para a representação do conhecimento. (BRAGA, RAMOS JÚNIOR & COELHO, 2007, p. 4)

2.4 Ontologias

A palavra ontologia tem a sua origem nas ciências filosóficas, sendo utilizada por Aristóteles para se referir ao estudo do ser, de como as coisas realmente são. Entretanto, a engenharia do conhecimento passou a utilizar este termo dentro de outro contexto de tal sorte que, neste estudo, ela é entendida como "uma especificação formal e explícita de uma conceituação compartilhada". (GRUBER, 1993, p. 199)

De acordo com Staab & Maedche (2007), "a ontologia constitui a base para anotar na Web documentos da comunidade de aquisição do conhecimento com o objetivo de possibilitar o acesso inteligente a estes documentos e inferir o conhecimento implícito das regras e fatos declarados explicitamente na ontologia".

Para que uma especificação seja considerada uma ontologia de verdade, ela deve ser expressa em linguagem formal que seja suscetível de compreensão pelo computador, definindo os conceitos e classificações de forma explícita referente a uma determinada área do conhecimento, devendo haver um consenso quanto a estes conceitos utilizados.

Há diversas vantagens no uso de ontologias, dentre elas, pode-se apontar o auxílio na recuperação de informação na *web*, facilitando a atuação de agentes de *software* inteligentes. Neste caso, a recuperação de informações seria mais eficiente porque a pesquisa realizada pelos agentes de busca leva em conta não apenas o termo ou expressão literal utilizada na pesquisa, mas permite que esta seja otimizada, apresentando informações relacionadas ao assunto pesquisado que não contenham necessariamente em seu teor as mesmas palavras que foram utilizadas na pesquisa. (BRAGA, RAMOS JÚNIOR & COELHO, 2007, p. 5)

Recuperação de informação baseada em semântica e apoio à jurisprudência

No ano de 2007, foi proposta uma arquitetura de aplicação para extração de informação de documentos baseada em semântica com apoio à pesquisa jurisprudencial.

Um dos objetivos desta arquitetura é gerar ontologias e anotações semânticas de forma automática, para organizar e recuperar documentos, fornecendo suporte à jurisprudência por meio de uma consulta mais eficiente com o uso de ontologias, já que estas podem evitar ambigüidades, além de permitir a recuperação do documento jurídico através do conteúdo semântico relacionado às expressões utilizadas na pesquisa.

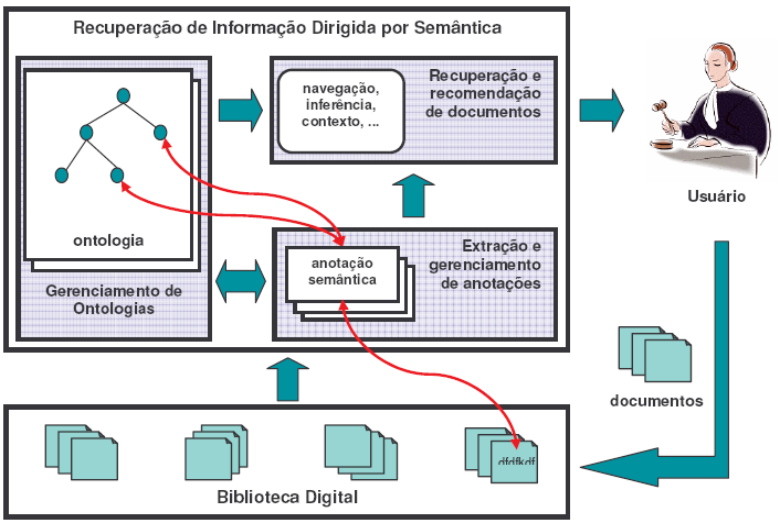

Figura 4. Arquitetura para recuperação de informação baseada em semântica com apoio à jurisprudência. (Fonte: NUNES & FILETO, 2007, p. 5)

Conforme ilustra a figura acima, a arquitetura é composta de uma biblioteca digital que contém os documentos jurídicos (sentenças e acórdãos), os quais possuem diversos formatos, mas apresentam similaridade quanto à organização das informações. Assim, "é possível aplicar técnicas de processamento de linguagens naturais para identificar entidades nomeadas e associá-las a conceitos e instâncias da ontologia jurídica, de modo a definir anotações semânticas para facilitar a recuperação da informação desses documentos" (NUNES & FILETO, 2007, p. 5).

Nesta arquitetura, o gerenciamento de ontologias serve para armazenar uma ou mais ontologias que serão utilizadas para recuperar as informações nos documentos. O módulo de recuperação e recomendação de documento cria a interface com o usuário. Enquanto que o módulo de extração e gerenciamento de anotações realiza o processamento dos documentos jurídicos contidos na biblioteca digital.

Modelo ONTOINFOJUS: acesso à informação na área jurídica

No que concerne ao acesso à informação jurídica, foi desenvolvido, em 2003, um modelo denominado ONTOINFOJUS o qual se destina a solucionar problemas relativos à necessidade de atualização do conhecimento jurídico do advogado.

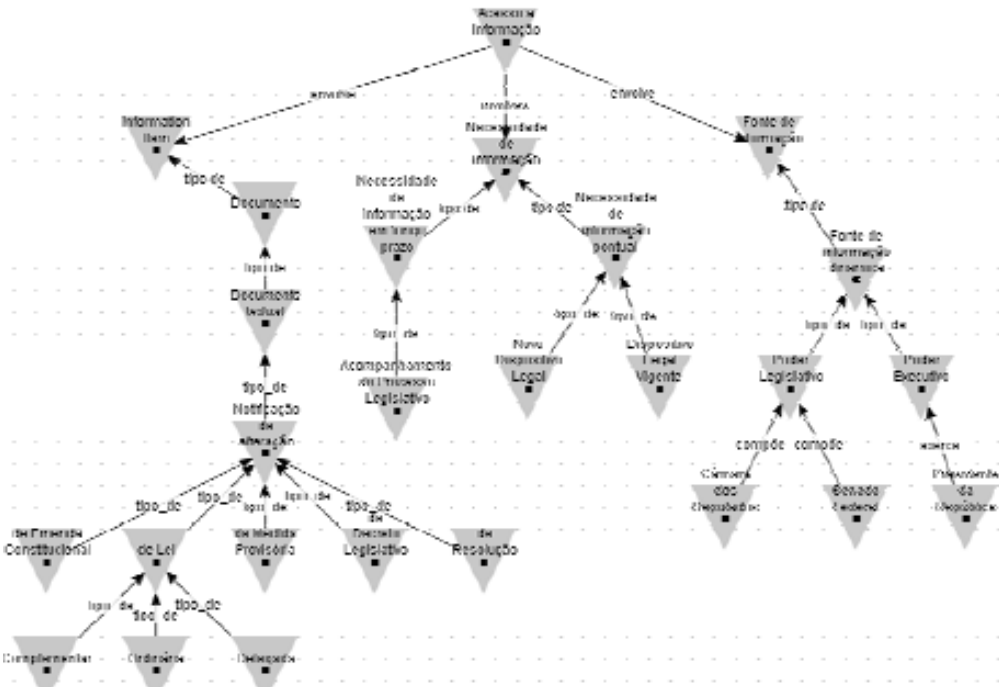

Figura 5. Modelo de conceitos da ONTOINFOJUS.
(Fonte: LINDOSO, SERRA & GIRARDI, 2003, p. 259)

O ONTOINFOJUS é decorrente de duas ontologias, de um lado, a ONTOINFO que descreve formalmente o conhecimento acerca do acesso à informação, e de outro, o ONTOJUS, referente à abordagem do conhecimento jurídico. Ambas resultam da aplicação da técnica GRAMO (*Generic Requirement Analysis Method based on Ontologies*), que consiste em uma técnica baseada em uma ontologia genérica denominada ONTODM que serve de orientação para a modelagem de domínios.

Este modelo de domínio proposto consiste em uma extensão da ontologia de acesso à informação ONTOINFO para abranger as particularidades do conhecimento jurídico modelado na ontologia ONTOJUS, tendo como usuários deste sistema os advogados que necessitem de informação jurídica para se manterem constantemente atualizados quanto à legislação vigente. (LINDOSO, SERRA & GIRARDI, 2003, p. 254)

Ontologia para explicitação de conceitos e valores jurídicos

Durante o VIII Encontro Nacional de Pesquisa em Ciência da Informação, que aconteceu nos dias 28 a 31 de outubro de 2007, em Salvador (BA), foi proposto um método para a construção de um domínio-ontológico do direito positivo brasileiro.

Trata-se da construção de uma ontologia em linguagem OWL mediante o uso do editor de ontologias *Protégé* para o domínio jurídico com o objetivo de explicitar conceitos e valores inseridos nas leis e atos normativos em âmbito nacional.

Em relação à ontologia desenvolvida, ela permite não apenas a navegação livre entre documentos jurídicos e sua visualização por critérios textuais, mas se destina a responder as seguintes questões de competência: "Como um instituto jurídico se estende na legislação? Qual o contexto de validade ou regulamentação superior e inferior de uma dada norma no ordenamento? Quais conceitos e valores são tratados em uma norma ou conjunto de normas, e vice-versa?". (CERQUEIRA & BAX, 2007, p. 5)

Ontologia jurídica com aplicação na área de direito tributário

No ano de 2006, foi proposto um estudo sobre a modelagem do conhecimento legal no contexto do direito tributário direcionado para a recuperação de normas jurídicas pertinentes ao âmbito de atuação da Receita Federal, mais especificamente em relação ao crédito presumido de IPI (imposto sobre produto industrializado).

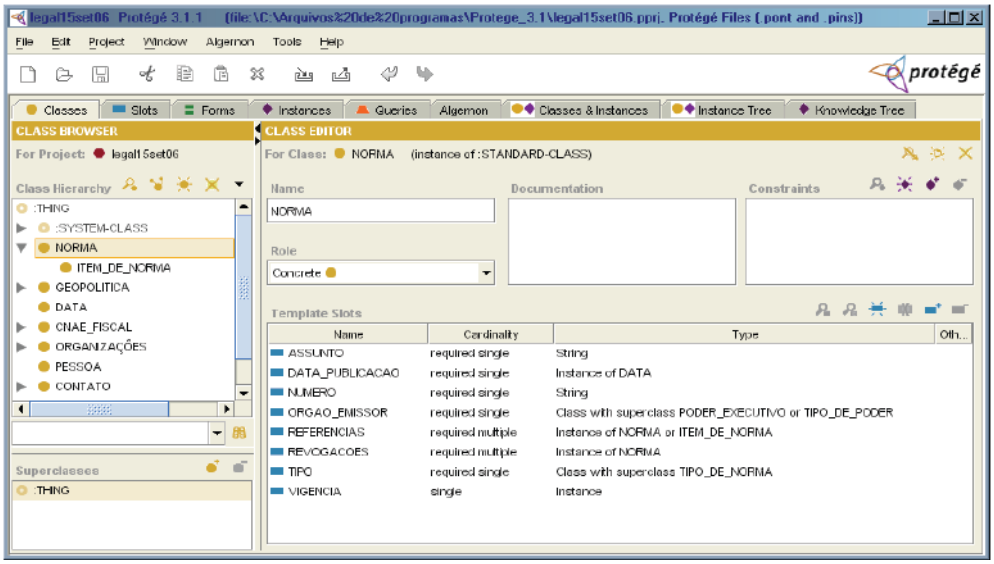

Figura 6. Ontologia legal. (Fonte: MARTINS, 2006, p. 212).

A ontologia em questão foi desenvolvida através do uso do editor de ontologias *Protégé*, com o intuito de demonstrar ser possível a aplicação da engenharia do conhecimento ao sistema jurídico uma vez que facilita o entendimento do cidadão leigo e também torna mais fácil a busca por legislação para apoiar a fundamentação de decisões dos órgãos responsáveis pelo lançamento de tributos e também aqueles responsáveis pelo julgamento de litígios entre contribuintes e a administração pública. (MARTINS, 2006, p. 193)

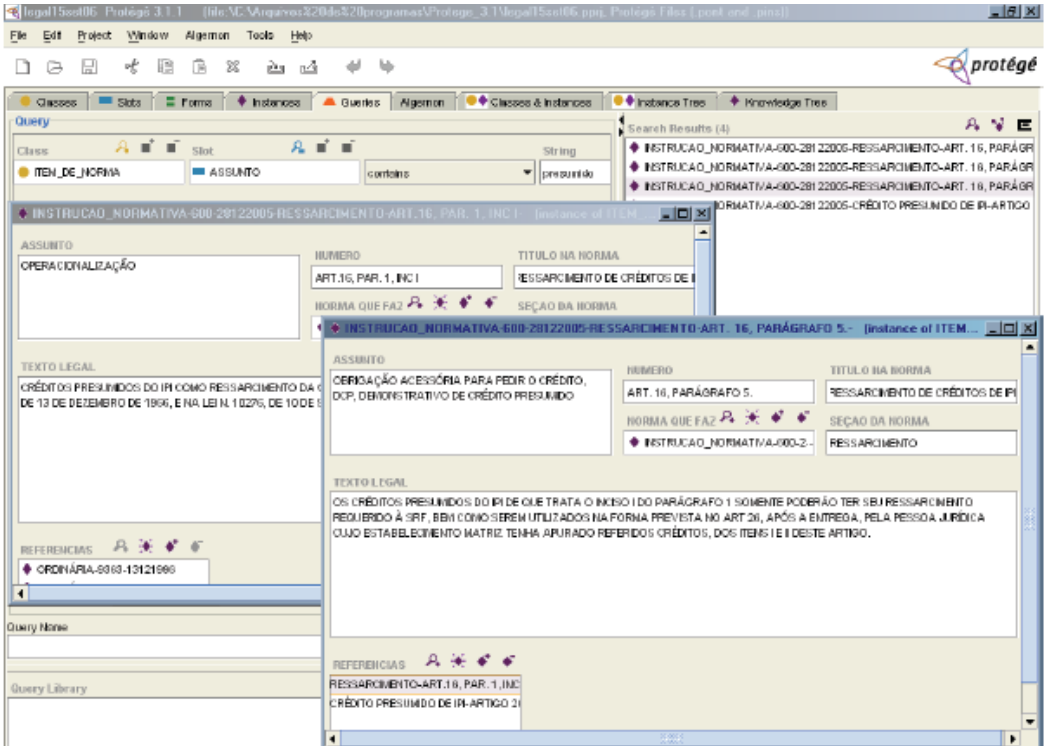

Figura 7. Exemplo de pesquisa semântica – procurar as instâncias da classe <item_de_norma> cujo assunto contém a string <presumido>. (Fonte: MARTINS, 2006, p. 216).

Destacou-se como uma das possíveis vantagens do emprego de ontologias para modelar o conhecimento jurídico o uso de mecanismos de pesquisa com filtragem baseada em conteúdo, tornando mais efetiva a busca de normas dentro de um contexto, conforme se constatou em relação à consulta acerca da legislação aplicável ao IPI.

Ontologias para cenários de missões complexas em perícia forense

No ano de 2007, foi apresentada uma pesquisa científica, realizada por um pesquisador e perito criminal do Departamento de Polícia Federal do Brasil, a qual teve o intuito de investigar o uso de ontologias com agentes computacionais para apoiar cenários de missões complexas na área da perícia forense, para criar as ontologias que ajudem a mapear uma missão para organizações como a polícia ou as forças militares:

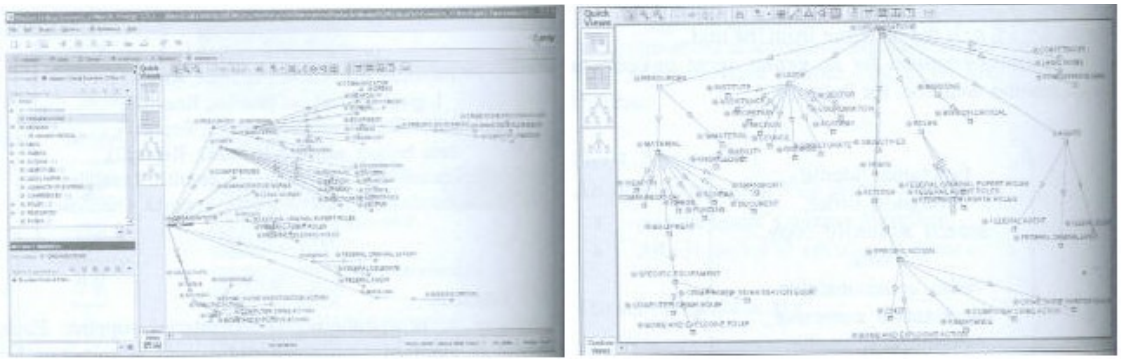

Figura 8. Ontologia para cenários de missões complexas. (Fonte: NOGUEIRA, 2007, p. 52)

Cenários de missões complexas são aqueles nos quais a informação muda constantemente e rapidamente ou aqueles onde há grande quantidade de recursos expendidos, muitas normas e regras a ser observadas, grande número de pessoas envolvidas, como, por exemplo, em se tratando de crimes nos ciberespaço, perícia forense, investigação em computador e em meios digitais. (NOGUEIRA, 2007, p. 48)

Quanto à organização formal, ela consiste na ação de agentes (seres humanos ou programa de computador), planejada e coordenada com a finalidade de construir ou realizar objetivos tangíveis ou intangíveis.

Dentre as questões de competência, a ontologia para cenários de missões complexas em perícia forense é capaz de responder a diversas perguntas, tais como:

a) Quais as missões que existem no processo? b) Quais das missões são complexas? c) Quais os agentes que possuem determinada habilidade? d) Onde podem ser encontrados agentes que tenham simultaneamente duas ou mais habilidades específicas? e) Qual a unidade da organização onde podem ser requisitados recursos materiais para determinada missão?

Projetos internacionais que envolvem o uso de ontologias jurídicas

Nesta seção, são apresentados projetos internacionais sobre ontologias jurídicas e áreas de interesse que poderão servir de apoio para o desenvolvimento da ontologia jurídica de delitos informáticos, que será proposta no quarto e último capítulo.

Estados Unidos

Pesquisadores norte-americanos converteram um sistema especialista legal (SEL) em um sistema baseado em conhecimento usando a linguagem OWL através do *Protégé*, em 2005, cujo sistema originário (SEL) vinha sendo utilizado para esclarecer questões relativas à formação de contratos, com base nas regras derivadas do Código Comercial Uniforme do estado da Pensilvânia que também é aplicável aos contratos eletrônicos, conforme regulamentado pelo *Uniform Electronic Transactions Act*.

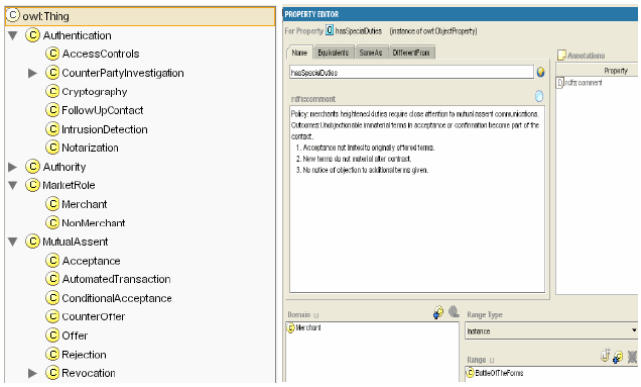

Figura 9. À esquerda, parte do protótipo da ontologia norte-americana, enquanto à direita, observa-se a propriedade <*hasSpecialDuties*> da subclasse <*Merchant*>. (Fonte: BAGBY & MULLEN, 2005, p.4)

Um dos motivos que incentivou os autores a modelarem o *Uniform Commercial Code* (UCC) é que se trata de um código bem organizado, resultado da experiência das melhores práticas acumuladas ao longo dos séculos sobre a atuação comercial, o que o torna uma codificação prática. Além disso, o UCC é organizado de forma modular que facilita a análise e a representação ontológica. (BAGBY & MULLEN, 2005, p. 2)

No artigo que consta no apêndice, tivemos a oportunidade de comentar sobre outro projeto, denominado *Legal Mapping of Cyberspace* que foi desenvolvido pela Universidade de George Mason, nos Estados Unidos, e que tem o intuito de categorizar todos os documentos legais sobre crimes informáticos a partir de uma ontologia geral.

Projeto CYC

Em se tratando de ontologias nos Estados Unidos, não se poderia olvidar também de fazer comentários sobre o projeto CYC, que existe desde o ano de 1984 e é considerado a maior base de conhecimento do senso comum existente na atualidade.

Ramachandran, Reagan & Goosbey (2005) afirmam que a ontologia do CYC faz o uso intensivo de constructos lógicos de ordem superior como um sistema de contexto, predicados de primeira classe dentre outros, que são tidos como a razão da habilidade do CYC em representar o conhecimento do senso comum e a razão de sua eficiência.

Dentre as ontologias desenvolvidas através deste sistema, destaca-se aqui a base de conhecimento detalhada sobre terrorismo que, segundo Deaton *et al* (2005), passará a conter todo o conhecimento relevante sobre grupos terroristas, como, por exemplo, membros, líderes, afiliações, além de descrições completas de especificação de eventos terroristas:

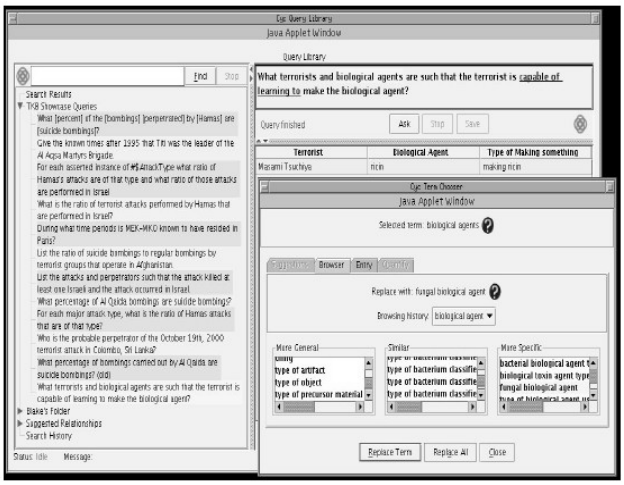

Figura 10. Biblioteca de perguntas da ontologia de terrorismo. (Fonte: DEATON *et al*, 2005)

A base de conhecimento sobre terrorismo agregou ao CYC conhecimento sobre mais de 2.000 terroristas, mais de 700 grupos terroristas e mais de 65 ataques terroristas. Uma biblioteca de perguntas faz a interface para a capacidade de inferência do CYC, através dela, o usuário pode formular perguntas na base de conhecimento sobre terrorismo, usando modelos de perguntas que estão contidos no sistema.

Além disso, conforme ilustrado na figura 10, a partir dos modelos de pergunta, o usuário pode especificá-la, indicando o nome do terrorista e/ou o tipo de agente biológico que ele é capaz de produzir, obtendo uma resposta precisa e objetiva para o problema através da engenharia do conhecimento.

México

No ano de 2005, um pesquisador do Centro de Sistemas Inteligentes do Instituto Tecnológico e de Estudos Superiores de Monterrey (ITESM), no México, propôs o uso de uma ferramenta multi-agente baseada em ontologias para identificar ataques de código, denominada FROID (*First Resource for Outbound Intrusion Detection*).

Embora não se trate especificamente de uma ontologia jurídica, optou-se por fazer comentários acerca deste sistema de detecção de intrusos já que está diretamente relacionado com a adoção de mecanismos que visam combater os crimes informáticos.

Diversos protótipos baseados em agentes de *software* têm sido desenvolvidos, porém nenhuma construção ontológica havia sido implementada realmente para permitir que os agentes pudessem coletar e compartilhar informações em um formato rico semanticamente que permitisse comportamentos mais inteligentes destes agentes.

O sistema FROID foi criado com o objetivo de explorar as possibilidades que um sistema de detecção de intrusão baseado em ontologias pode oferecer. Assim, uma das características do protótipo elaborado é que ele se apresenta como um mecanismo de detecção capaz de identificar ferramentas de ataque remoto em execução.

O sistema segue o paradigma de detecção de intrusão de partida, o qual consiste em uma abordagem coletiva para a monitoração de segurança que visa proteger uma sociedade de nós, garantindo que cada membro monitore o seu próprio tráfego de partida através de sinais da atividade maliciosa.

Pela distribuição da carga de trabalho de monitoramento entre todos os nós membros da rede, ao posicionar um pouco o mecanismo de detecção a um ponto intermediário de bloqueio, a sociedade de nós em conjunto consegue realizar o monitoramento de segurança, certificando-se que nenhum processo do local que funciona em algum dos nós tentou lançar um ataque para o outro.

A ferramenta utiliza uma OWL para definir uma ontologia que representa os componentes do ambiente no qual os agentes habitam, e, através do teste deste sistema, constatou-se que a integração de uma ontologia na ferramenta de detecção de intrusões de partida com agentes de *software* implicou em uma melhora no desempenho devido ao tamanho reduzido da mensagem e uma interpretação acelerada do conhecimento apoiada por estruturas de suporte de inferência. (MANDUJANO, 2005, p. 166)

Austrália

A polícia de New South Wales (NSW), na Austrália, pretende utilizar padrões XML para a troca de informações estratégias com mais de 27 agências estatais e federais, pois considera que o uso da informação e da tecnologia científica é a chave para melhorar as práticas de trabalho e reduzir a criminalidade.

Desta forma, o objetivo a ser alcançado consiste em definir estratégias e formular uma abordagem para criar uma estrutura governamental que forneça suporte às aplicações de negócios da polícia de NSW, permitindo o compartilhamento de informações dentro da organização, e também com agências externas, especialmente com setores da Justiça e modelo de mensagens utilizando padrões XML:

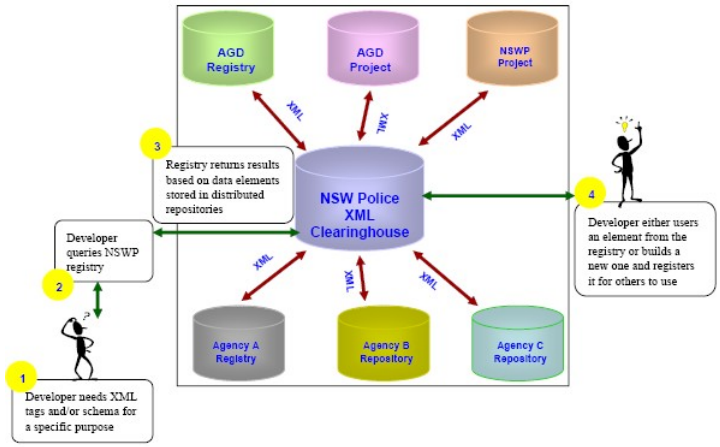

Figura 11. Estratégia de implantação XML da polícia de NSW. (Fonte: KUMAR, 2005, p. 34)

Ram Kumar (2005) aponta como alguns dos principais benefícios do uso do XML pela polícia de NSW a possibilidade de independência da plataforma já que os dados podem ser transportados para qualquer plataforma sem serem corrompidos, a oportunidade de padronizar os dados, a representação e apresentação consistente das informações, a troca de informações padronizadas e serviços reutilizáveis dentre outros.

Já em relação às ontologias jurídicas na Austrália, a pesquisadora Pamela Gray (2007), da *Charles Sturt University*, considera que a engenharia do conhecimento jurídico requer o desenvolvimento de sua própria engenharia e que o uso de ontologia e epistemologia na filosofia é uma fonte rica para o desenvolvimento da engenharia do conhecimento jurídico jurisprudencial. Para ela, um modelo aprofundado da *expertise* legal para a engenharia do conhecimento jurídico deve enfatizar a prática legal e mais ainda o desenvolvimento da engenharia do conhecimento jurídico jurisprudencial.

Índia

No ano de 2006, pesquisadores do Departamento de Ciências da Computação e Engenharia, do Instituto Indiano de Tecnologia (IIT) de Madras, na Índia, apresentaram uma proposta de uso de modelos gráficos para a sumarização de documentos jurídicos:

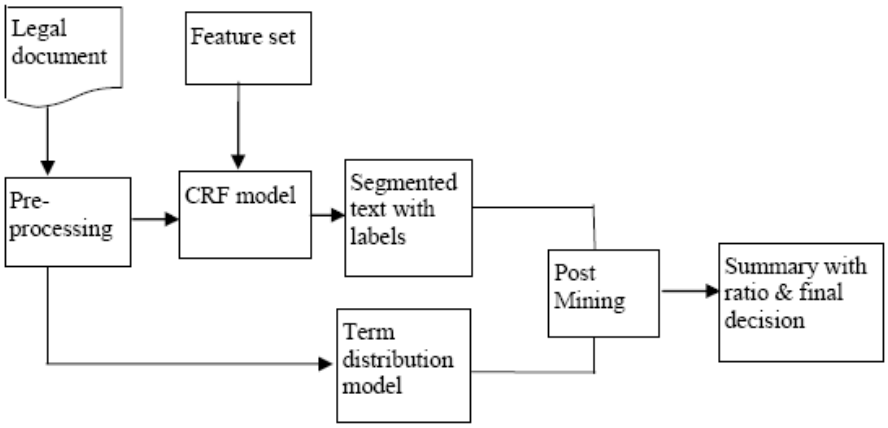

Figura 12. Etapas do processo de sumarização de documentos jurídicos referentes às decisões judiciais. (Fonte: SARAVANAN, RAVINDRAN & RAMAN, 2006, p. 57)

O modelo CRF (*Conditional Random Field*) consiste em uma das técnicas gráficas que foram aplicadas para realizar a tarefa de segmentação do texto na exploração do conjunto de características de um determinado texto, sendo aplicada para segmentar a estrutura de documentos jurídicos, particularmente as sentenças judiciais.

Através deste sistema se objetivou verificar como a extração destes dados pode melhorar o processo de sumarização dos documentos, sendo criada uma estrutura genérica de sumário para descrever as decisões judiciais em diferentes sub-domínios.

Por sua vez, no ano de 2007, eles propuseram uma nova estrutura detalhada com a construção de uma ontologia para recuperação de informações contidas nos documentos jurídicos, especialmente no tocante à jurisprudência, objetivando, através de perguntas formuladas pelo usuário, recuperar as decisões judiciais mais relevantes.

A avaliação deste sistema foi realizada através de perguntas formuladas por especialistas da área jurídica e por pessoas leigas, a partir do qual se constatou que o sistema de formulação de perguntas baseado em ontologias apresentou um resultado mais significativo do que os sistemas de perguntas padrão do Microsoft Windows. (SARAVANAN, RAVINDRAN & RAMAN, 2007, p. 1)

Japão

O Japão também desenvolve projetos de ontologias jurídicas. No ano de 2007, um pesquisador do *Japan Advanced Institute of Science and Technology* propôs um procedimento de detecção de discordância aplicado à legislação japonesa, em particular, foi testado com base no ordenamento regional da Prefeitura de Toyama naquele país.

Na referida pesquisa, expandiu-se a noção de inconsistência para discordância incluindo antônimos, baseando-se em uma ontologia e impossibilitando a sua conexão convencional negativa. Implantou-se um sistema que converte os formatos lógicos do XML para o Prolog, sendo inspecionado todo o código jurídico:

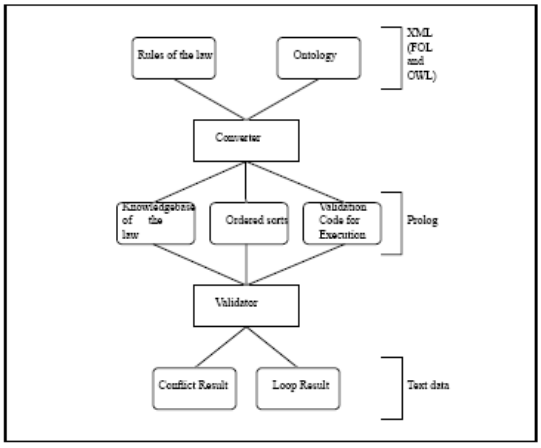

Figura 13. Visão geral do sistema japonês de detecção de discordância.
(Fonte: HAGIWARA, 2007, p. 2)

A discrepância ou a discordância não é apenas uma inconsistência lógica. No código jurídico, os itens léxicos que incluem prefixos negativos não podem coexistir com as palavras positivas originais. Além disso, há antônimos que apresentam conflitos de significado sem prefixos e sua incompatibilidade é perceptível pelo senso comum.

Assim, o primeiro passo foi definir a noção de conflito ou discordância com a representação da oposição de antônimos e das palavras que possuam prefixos negativos.

Entretanto, para definir os conflitos, tornar-se-ia necessário enumerar todas as possíveis combinações de predicados que aparecem no código jurídico. Para evitar este problema foi empregada uma ontologia ordenada em classes e com as suas hierarquias.

A implementação do sistema utiliza dois programas: um programa conversor, escrito em Ruby e que converte arquivos XML para Prolog; e um programa de validação, escrito no Prolog e encarregado de validar o código de saída pelo conversor.

Bélgica

No ano de 2005, Yan Tang e Robert Meersman, pesquisadores do STARLab (*Semantics Technology and Applications Research Laboratory*) do Departamento de Ciências da Computação da *Vrije Universiteit Brussel*, na Bélgica, propuseram o uso de um sistema de análise de casos de privacidade baseado em ontologias para que houvesse uma maior eficiência no processo e no apoio aos sistemas jurídicos.

A ontologia belga de privacidade se propõe a interligar os casos e regulamentos pela captura dos elementos do conhecimento do domínio da privacidade, com o objetivo de melhorar a qualidade, transparência, consistência e eficiência da jurisprudência.

Esta ontologia abrange a semântica na apresentação das leis e os fragmentos de raciocínio de caso, levando em consideração tanto as Diretivas, que são um tipo de legislação da comunidade européia, como também os princípios da privacidade, sendo ambos relacionados aos casos concretos, auxiliando na tarefa de argumentação jurídica.

Além disso, considera-se que a ontologia de privacidade exerce papel importante no mecanismo de interpretação das normas, ao trazer conceitos variados e os aproximar das diretivas orientadoras com conteúdo normativo relacionado à privacidade. (TANG & MEERSMAN, 2005, p. 801)

Dentre a diversidade de aplicações práticas no âmbito da ontologia da lei, destacam-se a criação de sistemas de recuperação de informação jurídica, de sistema de aprendizagem da lei pelas máquinas, de sistemas de extração automática de textos jurídicos, de sistemas de orientação na elaboração de leis, de consultas jurídicas etc.

Entretanto, o desafio na construção destas aplicações consiste justamente em analisar como abstrair fatos de casos automaticamente ou semi-automaticamente; como interligar os fatos às diretrizes e em qual nível de abstração; como usar princípios como orientadores da execução da aplicação e criação de diretivas; como provar a qualidade da aplicação para ver se ela realmente atende às necessidades dentre outras.

Desta forma, com o objetivo de contornar tais desafios, foi apresentada uma estrutura para a ontologia de privacidade que está baseada nas relações entre princípios, diretivas, fatos e casos, utilizando como método de abordagem o ambiente DOGMA (*Developing Ontology-Guided Mediation for Agentes*), conforme ilustra a figura abaixo:

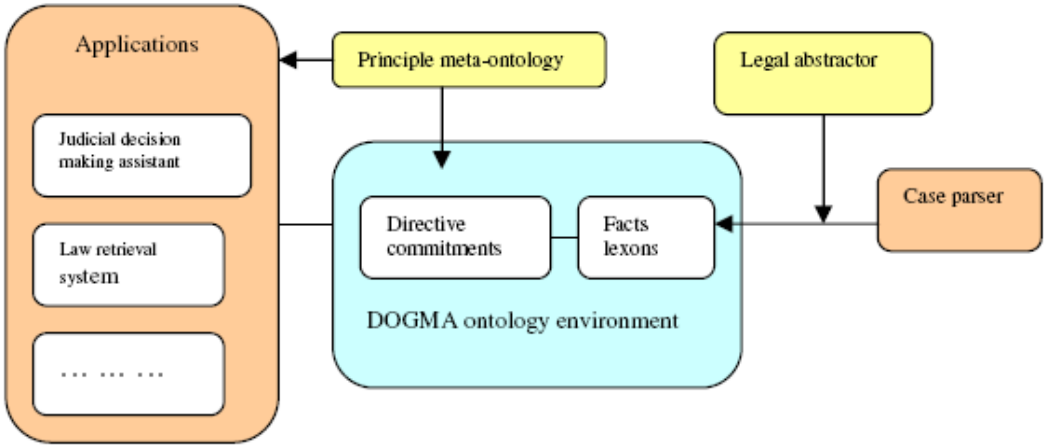

Figura 14. Estrutura da ontologia de privacidade. (Fonte: TANG & MEERSMAN, 2005, p. 802)

O DOGMA é uma abordagem de engenharia de ontologias desenvolvida por pesquisadores do STARLab que consiste em uma base de ontologias dirigida para abarcar relações conceituais intuitivas específicas do contexto e uma camada de compromissos ontológicos relativamente genéricos que integram as regras do domínio. (SPYNS, MEERSMAN & JARRAR, 2002, p. 12)

O ambiente ontológico DOGMA é composto por duas camadas separadas, uma referente aos compromissos diretivos e outra que engloba os fatos léxicos os quais seriam extraídos do caso pela orientação de um abstrator jurídico e consistem em entidades que são representadas em dupla e podem ser armazenados em qualquer sistema de banco de dados. Já os compromissos diretivos são baseados no conhecimento compartilhado de diretivas de privacidades unidas com regras de privacidade.

Além do uso deste ambiente ontológico, a estrutura da ontologia de privacidade é composta ainda por aplicações de privacidade, um abstrator jurídico, uma meta-ontologia de princípios de privacidade e um *case parser*.

No caso, o *case parser* consiste em um motor automático ou semi-automático que realiza a interface entre o usuário e o sistema, com apresentação dos casos reais e a geração de fatos coordenados, o qual, junto com o abstrator jurídico, forma um sistema especialista que está sendo desenvolvido pelos pesquisadores da universidade belga.

Quanto à meta-ontologia de princípios, ela é usada para a orientação na elaboração de diretivas de privacidade e em projetos de aplicações voltadas para este domínio, sendo sua modelagem conceitual representada através de um diagrama UML.

Itália

Na Itália, há projetos que estão sendo desenvolvidos e que visam utilizar ferramentas de apoio às atividades judiciais na área criminal e existe a proposta de utilizar ontologias jurídicas para criar uma estrutura conceitual homogênea para tais projetos e adicionar conhecimento do domínio, servindo de suporte para as ferramentas.

A partir da conceituação deste domínio, pretende-se gerir documentos por meio de metadados; identificar e sugerir uma hipótese de crime para o juiz, fazer a varredura de documentos e marcar semanticamente as leis criminais com o uso da linguagem XML. (ASARO *et al*, 2003, p. 2)

Desta forma, o primeiro passo na construção da ontologia italiana foi esboçar um conceito abstrato de crime já que as várias figuras previstas no Código Penal Italiano, assim como no Código Penal Brasileiro, herdam essa definição básica.

As condições fundamentais para a caracterização do crime no direito penal italiano são: a ausência de situações excludentes do ilícito penal (como, por exemplo, estado de necessidade, que exclui a aplicação da norma penal) e a existência do que os italianos denominam de *suitas* e que no direito penal brasileiro corresponde ao dolo, isto é, a vontade livre e consciente de praticar uma conduta proibida pela lei criminal.

Estando presentes estes dois pressupostos, analisam-se os elementos estruturais do crime que são: o ofensor, o comportamento, o evento, a circunstância e a punição.

O ofensor é a pessoa que age de maneira a praticar uma conduta descrita como crime pela lei penal abstrata; já o comportamento é formado por um elemento material que pode ser uma ação ou uma omissão do agente e do conceito de responsabilidade penal subjetiva (malícia ou negligência) e de responsabilidade penal objetiva.

Ainda, o comportamento pode ser completo ou incompleto. Será completo quando o fato realizado pelo autor corresponder exatamente à previsão legislativa, ou seja, quando houver a efetiva consumação do crime. Por outro lado, será incompleto quando o comportamento não corresponder à previsão legislativa, caracterizando-se, neste caso, a tentativa, quando for inequívoca que a intenção do agente era a de realizar a conduta criminosa.

O evento é o resultado do comportamento criminoso e consiste na ofensa ao interesse protegido pela lei. Deve haver um nexo de causalidade entre o evento e o comportamento do agente para que se possa imputá-lo a prática de um delito.

Já a punição é a sanção ou a pena que a lei penal estabelece para um determinado crime. Junto com a punição e o comportamento, outro elemento deve ser considerado: as circunstâncias. As circunstâncias são fatores e situações que podem agravar ou atenuar a pena de um determinado crime.

A definição conceitual sumária do crime permite identificar algumas constantes uma vez que, conforme mencionado, as várias tipologias de crime herdam esta estrutura conceitual. Os elementos desta estrutura combinam os fatos humanos que podem ser parte de um crime e diagnosticam sua relevância penal:

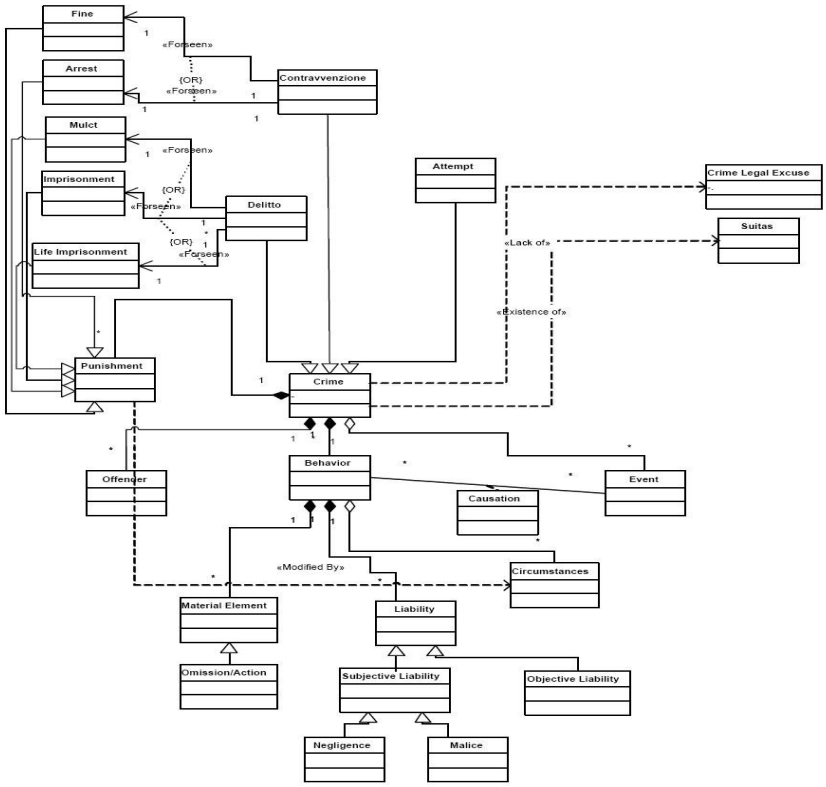

Figura 15. Ontologia italiana de conceito abstrato do crime. (Fonte: ASARO *et al*, 2003, p. 4).

O mapeamento entre fatos humanos e a estrutura abstrata do crime pode conduzir às seguintes conclusões: a) a subsunção do crime, ou seja, os fatos humanos constituem crime tipificado pela lei penal; b) o fato não é um crime, isto é, os fatos não se enquadram na norma ou há uma excludente do ilícito penal; c) o ofensor não cometeu o fato, isto é, o fato não pode ser imputado ao mesmo.

Os autores italianos utilizaram um diagrama UML (*Unified Modelling Language*) para formalizar o conceito ontológico do crime. Este tipo de representação permite a visualização gráfica e conceitual de modo que tanto os profissionais do direito quanto os engenheiros do conhecimento possam trabalhar juntos.

Holanda

No ano de 1994, André Valente e Joost Breuker, pesquisadores da Universidade de Amsterdã, na Holanda, propuseram uma ontologia jurídica baseada em um conjunto de categorias primitivas interconectadas e subcategorias do conhecimento legal, sob uma visão teleológica e funcional do sistema jurídico.

Esta ontologia jurídica funcional está relacionada com os aspectos centrais da teoria jurídica, fazendo distinção entre os tipos de conhecimento usados para resolver os problemas da área, indo além da simples divisão entre regras jurídicas e casos práticos.

Não obstante seja reconhecida a impossibilidade de representar qualquer domínio em toda a sua riqueza de detalhes, a representação do conhecimento pode ser usada para fornecer uma interpretação do mundo, sendo ela resultado do compromisso ontológico assumido, o qual consiste em identificar as abstrações corretas que podem ser utilizadas para resolver problemas.

Em conseqüência, todo e qualquer sistema baseado no conhecimento jurídico contém compromissos ontológicos que limita o que ele pode ou não pode fazer, porém a vantagem do uso de ontologias é o fato de que ela nos permite compreender porque os sistemas funcionam, permitindo a comparação de diferentes representações do conhecimento jurídico nos principais aspectos. (VALENTE & BREUKER, 1994, p. 3)

Assim, o núcleo desta ontologia consiste em um conjunto de categorias de conhecimento suscetível de ajudar na interpretação do conhecimento jurídico bem como na especificação de sua estrutura e de suas inter-relações.

Esta ontologia, denominada *FOLaw*, sigla derivada do inglês (*Functional Ontology of Law*), é composta pelas seguintes classes de tipos ou categorias de conhecimento: conhecimento normativo (*normative knowledge*), conhecimento da responsabilidade (*responsability knowledge*), conhecimento do mundo (*world knowledge*), conhecimento reativo (*reactive knowledge*), conhecimento posicional (*positional knowledge*) e conhecimento criativo (*creative knowledge*):

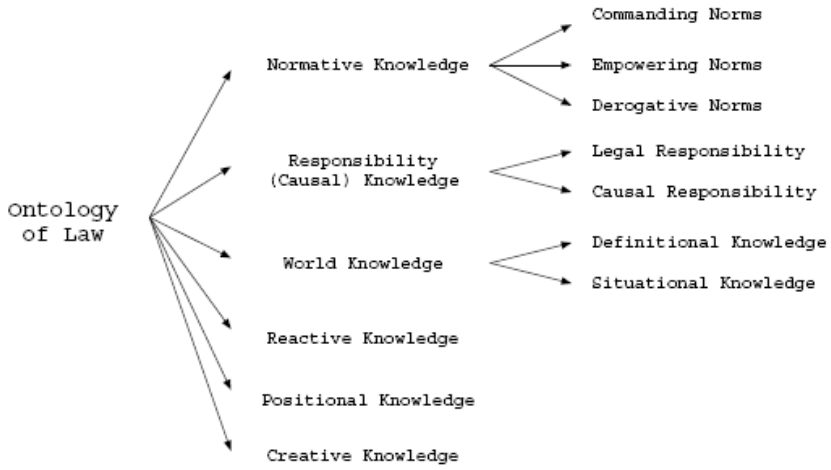

Figura 16. Ontologia jurídica funcional. (Fonte: VALENTE & BREUKER, 1994, p. 5)

O conhecimento normativo (*normative knowledge*) é apresentado como sendo aquele que define um padrão ideal a ser utilizado para comparar com a realidade, ou seja, a norma sempre contém alguma descrição do mundo, na qual algumas possibilidades na realidade são recortadas para que ela seja um mundo ideal.

As normas jurídicas podem ser observadas ou violadas. Elas são observadas quando o comportamento no mundo real não conflita com a sua especificação no mundo ideal. Por sua vez, quando houver conflito, haverá violação à norma jurídica. Desta forma, aplicar a lei significa verificar ou comparar a realidade com o mundo ideal definido na norma jurídica, classificando a realidade seja como complacente com a norma ou não. (VALENTE & BREKER, 1994, p. 6)

O conhecimento normativo é subdividido em três tipos de normas jurídicas: normas imperativas ou de comando (*commanding norms*), normas autorizadoras (*empowering norms*) e normas derrogativas (*derrogative norms*). Em síntese, as normas imperativas impõem um determinado comportamento, as normas autorizadoras permitem um comportamento e as normas derrogativas derrogam outra norma existente.

Já o conhecimento da responsabilidade (*responsability knowledge*) compreende todo o conhecimento jurídico com a função de atribuir ou limitar a responsabilidade de um agente em relação a uma situação ou conjunto de situações.

O conhecimento do mundo (*world knowledge*) consiste no conhecimento usado no direito para descrever o mundo, ou seja, todos os conceitos e termos usados neste domínio são partes de um modelo abstrato estruturado de como o mundo é e como ele opera, sendo denominado de modelo jurídico abstrato.

Por sua vez, o conhecimento reativo (*reactive knowledge*) especifica a reação que deve ser tomada quando houver violação ao sistema jurídico, sendo o Código Penal um exemplo que representa este tipo de conhecimento já que nele está prescrita a punição específica para o caso de se cometer uma conduta criminosa descrita na norma.

Em relação ao conhecimento criativo (*creative knowledge*), ele decorre do ato do legislador que cria alguma entidade concreta que não existia no mundo até então, como, por exemplo, a elaboração de uma lei que cria um novo departamento governamental.

Acrescenta-se, por último, o conhecimento posicional (*positional knowledge*) que consiste em um tipo de conhecimento jurídico que expressa normas como uma indicação sobre o posicionamento jurídico de um agente ou grupo de agentes.

Desta forma, a ontologia jurídica funcional propõe a representação do conhecimento jurídico a partir da especificação das categorias de conhecimento conforme a sua função ou papel desempenhado no sistema jurídico:

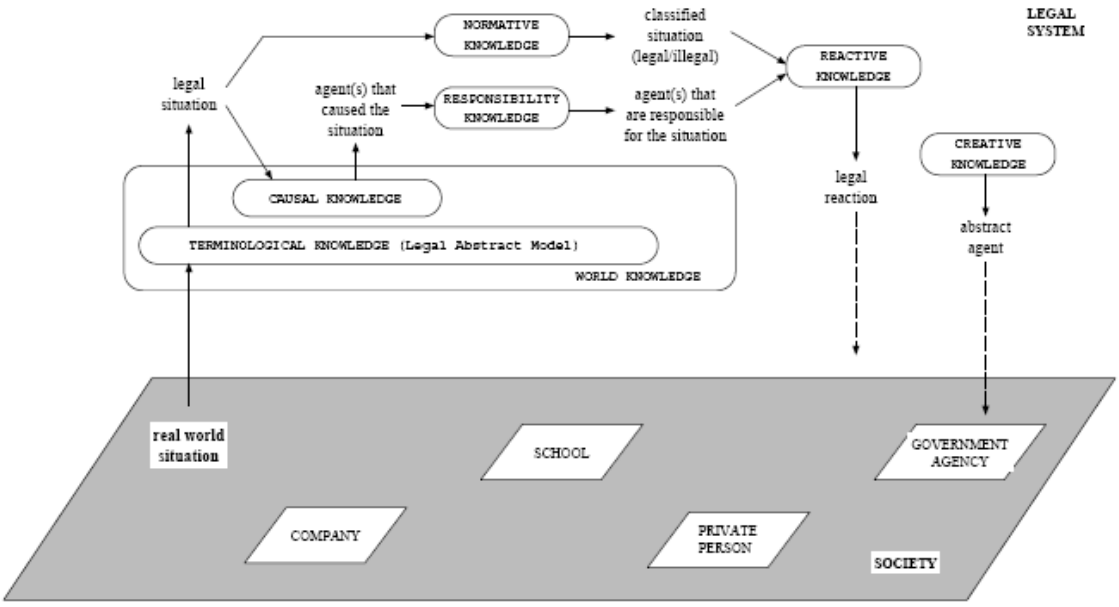

Figura 17. Representação funcional do sistema jurídico considerando o tipo de conhecimento aplicado. (Fonte: VALENTE & BREUKER, 1994, p. 11)

A representação funcional acima exibe a conexão existente entre as categorias de conhecimento jurídico e suas inter-relações para dar efetividade ao funcionamento do sistema jurídico como um todo através de uma visão teleológica com a finalidade de realizar uma determinada função que constitui um meio para atingir os objetivos sociais.

Alemanha

Stephan Walter & Manfred Pinkal (2005), ambos pesquisadores do *Department of Computational Linguistics and Phonetics*, da *Universität des Saarlandes*, propuseram um sistema computacional lingüístico para servir de apoio na construção de ontologias, particularmente voltado para melhorar o processamento de informações de documentos jurídicos alemães, como decisões e veredictos proferidos pelos tribunais na Alemanha.

Eles trabalham no projeto CORTE (*Computational Linguistic Methods for Legal Terminology*), tendo acesso a um corpo normativo de mais de 8 milhões de documentos jurídicos alemães, realizando a descrição detalhada de estruturas lingüísticas e de mecanismos semânticos para o desenvolvimento de ferramentas que automaticamente reconheçam e processem partes de veredictos que contenham conceitos importantes.

Assim, o problema que os pesquisadores se propõem a resolver se refere ao fato de que as definições contidas nos estatutos jurídicos nunca especificam completamente como os conceitos relevantes serão aplicados nos casos de tomada da decisão judicial.

Acontece que as definições nos textos jurídicos são formuladas em linguagem natural e as expressões utilizadas são freqüentemente vagas e ambíguas. Além disso, há situações em que o conceito existente numa norma jurídica apresenta obscuridade.

Outro aspecto é que a realidade é complexa e está constantemente mudando, assim, na época em que um conceito é definido na lei, é praticamente impossível prever toda complexidade e desenvolvimento que pode ocorrer no domínio da regulamentação.

As definições nos veredictos servem, dentre outras coisas, para adaptar o grau de precisão de um conceito para as necessidades do contexto respectivo. Por sua vez, as ontologias jurídicas existentes apenas utilizavam os conceitos da lei, sem especificar como eles eram usados e modificados com os veredictos e tampouco quais os conceitos auxiliares que porventura foram criados e incorporados no domínio pela jurisprudência.

Em uma análise de aproximadamente 150 definições nos veredictos dos tribunais alemães, selecionados randomicamente, eles evidenciaram uma grande variedade de formulações que os juízes alemães empregam quando introduzem ou modificam conceitos, bem como um alto grau de complexidade sintática.

Desta maneira, como nenhum serviço simples de busca por palavras-chave seria suficiente para extrair a informação relevante neste contexto, consideraram necessárias análises lingüísticas aprofundadas dos componentes das sentenças para esta tarefa.

É preciso, portanto, desenvolver uma abordagem para lidar com o problema da ambigüidade sem perda significativa, tendo em vista a necessidade de uma rica estrutura de informação confiável e acessível juntamente a uma complexidade lingüística elevada, que é geralmente encontrada no domínio dos textos jurídicos.

Para analisar gramaticalmente estes documentos, eles construíram um sistema de pesquisa e análise de documentos orientado semanticamente que foi desenvolvido no projeto COLLATE (*Computational Linguistic and Language Technology for Real Life Applications*), financiado pelo Ministério de Educação e Pesquisa da Alemanha.

O mais importante no sistema proposto pelos pesquisadores da universidade alemã é o fato de que o sistema é orientado semanticamente. Ele não só analisa a estrutura gramatical de entrada, mas também fornece uma representação abstrata do seu significado através de uma estrutura dependente parcialmente resolvida (PREDS).

As sentenças recebem idênticas representações, desta forma o seu índice semântico comum se torna acessível para o seu processamento posterior.

A partir da coleção de definições compiladas confiáveis do conhecimento do especialista jurídico, foi planejado um esquema de anotação para marcação das partes funcionais destas definições, o qual será ampliado para codificar a informação a respeito das relações exteriores tais como as funções retórica e argumentativa das definições e da estrutura de citação, e será aplicado na coleção de informações adicionais.

Também estão sendo elaboradas, pelos pesquisadores, análises lingüísticas detalhadas de instâncias de definição para relacioná-las com as análises nos termos funcionais, com o objetivo de desenvolver uma taxonomia de tipos de definições de acordo com as suas funções semânticas e realização sintática.

Segundo os autores, a informação contida no PREDS construído será usada para organizar os resultados de extração coletado dentro da base de conhecimento semi-estruturada, que servirá para segmentar automaticamente e classificar definições extraídas de acordo com a taxonomia proposta, baseada em sugestões lingüísticas.

A base de conhecimento resultante conterá passagens do texto extraído junto com informação adicional rica para permitir ao usuário navegar pelas definições coletadas conforme a sua necessidade, por exemplo, classificado pelo conceito definido, agrupado por tipo de definição ou pesquisa por citações.

Por último, um tópico bastante promissor e ambicioso do projeto é o uso da informação fornecida pelo sistema de extração de definição baseada no PREDS para atualizar e ampliar as ontologias formalizadas existentes.

Projeto FF POIROT

Na União Européia, um projeto denominado FF POIROT se destina a ajudar a prevenir e combater as fraudes financeiras através de ontologias, tendo em vista que se estima que ela perde milhões de euros por ano devido à fraude financeira.

O objetivo do projeto é construir uma ontologia detalhada do Direito Europeu, práticas preventivas e conhecimento do processo de fraude financeira dentro da União Européia. Além disso, ele visa também compilar as várias línguas (holandês, italiano, francês e inglês) em um repositório computacionalmente fácil de gerir, controlar e compartilhar o conhecimento (uma combinação formalmente descrita de conceitos e de seus relacionamentos significativos) para o domínio da fraude financeira. (LEARY, VANDENBERGHE & ZELEZNIKOW, 2003, p. 4)

Projeto *Syllabus*

O projeto *Syllabus* consiste no desenvolvimento de uma ferramenta multilíngüe baseada em ontologias que está sendo desenvolvida para melhorar as aplicações das diretivas européias nos vários países europeus.

A União Européia produz um grande número de diretivas todos os anos, as quais são traduzidas para cada um dos idiomas dos países comunitários, entretanto às vezes os mesmos conceitos utilizados nas diretivas européias também são empregados pela legislação nacional dos países membros em sentido diferente, seja com maior amplitude do conceito ou de forma mais restritiva. Isto pode ser resolvido através de ontologias:

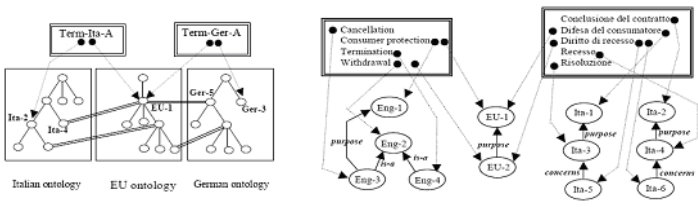

Figura. 18. Interconexão entre termos na ferramenta *Syllabus*. (Fonte: AJANI *et al*, 2006)

Desta forma, a ferramenta multilíngüe baseada em ontologia se destina a contribuir para a transposição precisa do conceito utilizado nas diretivas européias para ser integrado no ordenamento jurídico dos Estados membros. Para tanto, realiza-se através de ontologias uma distinção entre a noção do termo e a noção do conceito, construindo uma classificação sistemática baseada nesta distinção.

Projeto *e-Court*

O projeto *e-Court* é um projeto europeu que envolve a universidade, o governo e parcerias industriais, com a finalidade de desenvolver um sistema integrado de aquisição de sinais de áudio e vídeo dentro das salas de tribunais, o arquivamento de documentos jurídicos, pesquisa documental e consulta sincronizada com áudio, vídeo e texto. A Universidade de Amsterdã é a principal responsável pelo desenvolvimento e utilização de ontologias jurídicas neste sistema. (BREUKER *et al*, 2002, p. 1)

Projeto ESTRELLA

De todos os projetos de ontologias jurídicas estudados, aquele que se apresentou mais complexo, ambicioso e interessante vinculado à Engenharia do Conhecimento Aplicada ao Governo Eletrônico foi o projeto ESTRELLA (*European Project for Standardized Transparent Representations in order to Extend Legal Accessibility*).

Trata-se de um projeto europeu que visa desenvolver e validar uma plataforma aberta baseada em padrões que permitam às administrações públicas desenvolverem e desdobrarem soluções detalhadas de gestão do conhecimento jurídico, sem se tornar dependente de produtos proprietários de vendedores particulares na União Européia.

O projeto ESTRELLA apoiará, de modo integrado, tanto a gestão de documentos jurídicos como os sistemas legais baseados em conhecimento, para fornecer uma solução completa melhorando a qualidade e a eficiência dos processos de determinação da administração pública que exigem a aplicação da legislação complexa e de outras fontes legais.

Além disso, o projeto ESTRELLA irá facilitar um mercado de componentes interoperáveis para sistemas baseados no conhecimento legal, permitindo às administrações públicas e seus usuários escolherem livremente entre ambientes de desenvolvimento de competência, motores de inferência e outras ferramentas.

Portanto, um dos objetivos técnicos principais do projeto ESTRELLA é desenvolver um formato de intercâmbio do conhecimento jurídico (LKIF), construído sobre padrões emergentes baseados em linguagem XML da *web* semântica, incluindo RDF e OWL, e APIs (*Application Programmer Interfaces*) para interagir com os sistemas baseados em conhecimento jurídico.

CRIMES INFORMÁTICOS

Este capítulo tem o objetivo de apresentar uma breve contextualização histórica dos crimes informáticos no país, conceituando e classificando os crimes informáticos, para, em seguida, identificar tais condutas criminosas tipificadas no ordenamento jurídico-penal brasileiro e extrair o conhecimento compartilhado deste domínio, a partir da realização de um estudo doutrinário e de pesquisa jurisprudencial acerca da matéria.

3.1 Contextualização da origem dos crimes informáticos

A origem dos crimes informáticos está relacionada com o surgimento do computador, entretanto esta temática adquire maior relevância a partir do advento da Internet em 1969, a qual foi idealizada na época da Guerra Fria, para fins militares pelo governo norte-americano, objetivando construir uma rede de comunicação que se mantivesse intacta mesmo na hipótese de ataques bélicos a uma de suas bases.

Posteriormente, esta rede se expandiu para algumas universidades com o projeto ARPANET com fins científicos, e, em seguida, houve a sua abertura para os demais países, permitindo assim a integração de todos os computadores do mundo a esta rede, a Internet, tal qual se conhece atualmente.

É justamente com a popularidade da grande rede de computadores que começou a se praticar delitos através do ciberespaço, o qual passou a ser visto como um ambiente livre de toda e qualquer regulamentação jurídica, tornando-se necessário o exame da legislação penal vigente no tocante à possibilidade de sua aplicação aos denominados crimes cibernéticos, ou seja, tanto aos delitos praticados contra o computador quanto aos que utilizam a rede mundial como um meio para a prática de condutas criminosas.

A Internet passou a ser denominada também de ‘ciberespaço’ e a origem desta palavra provém da cibernética, do grego *kubernetes*, que significa ‘piloto do barco’ ou ‘timoneiro’, sendo comum se referir ao ciberespaço, comparando-o a um mar digital.

O mito do ciberespaço como um ambiente virtual fora da lei começou a ser afastado a partir do momento em que os primeiros casos envolvendo crimes praticados através da rede mundial de computadores foram sendo punidos no país, interpretando-se as normas penais em vigor, definindo os critérios acerca da competência e verificando a

possível aplicabilidade da norma penal a destes delitos.

Os crimes informáticos surgem no ordenamento jurídico a partir da entrada em vigor da legislação que os tipificou. Na hipótese de não existir lei definindo um comportamento como crime, por exemplo, em relação à conduta de acesso indevido a sistemas computacionais, não seria juridicamente correto dizer que se trata de um crime informático, pois esta conduta ainda não está prevista como delito pela norma penal vigente na atualidade, não obstante haver projeto de lei objetivando criminalizá-la.

Muito embora tais condutas ilícitas praticadas contra os sistemas de informática sejam reprováveis pela sociedade do ponto de vista ético, a responsabilidade penal somente ocorrerá quando existir lei que expressamente estabeleça que determinado fato constitua um crime e determine qual a pena lhe seja aplicável, não podendo esta retroagir para punir os que a praticaram quando o comportamento ilícito não estava criminalizado, tudo isso em homenagem à segurança jurídica e à legalidade penal.

Assim, de acordo com o art. 5º, inciso XXXIX, da Constituição Federal de 1988 (CF/88), "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", ou seja, deve-se observar o princípio constitucional segundo o qual ao cidadão não pode ser imputado um crime que não esteja definido em lei e que toda pena somente pode ser aplicada se estiver prevista em norma preexistente ao fato criminoso. Por esta razão é que "não se admite o emprego de analogia para normas incriminadoras, uma vez que não se pode violar o princípio da reserva legal" (CAPEZ, 2004. p. 38).

3.2 Definição e classificação dos crimes informáticos

Embora não exista, no ordenamento jurídico pátrio, uma definição legal de crimes informáticos, de modo geral, pode-se dizer que a doutrina penal e os tribunais brasileiros vêm adotando o conceito de crimes informáticos como "ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão". (TRUZZI & DAOUN, 2007, p. 116)

Definido assim o conceito de crimes informáticos, parte-se para o estudo sobre as suas diversas formas de classificação, bem como para a tentativa de classificá-los a partir de uma adaptação da sistemática utilizada pela doutrina penal tradicional.

Quanto ao seu objetivo material, eles podem ser classificados, segundo Luiz Flávio Gomes, em crimes contra o computador ou crimes por meio do computador. Na

mesma linha é a classificação adotada por Ivette Senise Ferreira (2000) que os classificam em atos ilícitos dirigidos contra um sistema de informática ou cometidos por intermédio de tal sistema.

Além da divisão bipartidária ora apresentada, os crimes informáticos podem ser classificados como puros, mistos ou comuns. Neste sentido, os crimes informáticos puros são aqueles praticados com o intuito de atingir o computador, o sistema de informática ou os dados e as informações neles utilizadas; os crimes informáticos mistos, por sua vez, são aqueles nos quais o agente não visa o sistema de informática e seus componentes, mas a informática é instrumento indispensável para consumação da ação criminosa; e os crimes informáticos comuns, onde o agente não visa o sistema de informática e seus componentes, mas usa a informática como instrumento (não essencial, poderia ser outro o meio) de realização da ação. (CASTRO, 2003a, p. 42)

Em seu parecer sobre o Projeto de Lei do Senado nº 76/00, Alexandre Atheniense já havia defendido esta classificação terciária dos crimes informáticos em puros, mistos ou comuns, classificando ainda os crimes informáticos impuros como "aqueles que podem ser cometidos também fora do universo do computador, encontrando já definição no sistema punitivo atual"; ou seja, como sinônimos de 'crimes informáticos comuns'.

Entretanto, entende-se que a terminologia 'crimes informáticos impuros' seja mais apropriada do que 'crimes informáticos comuns', tendo em vista que a doutrina penal tradicional usa a expressão 'crimes comuns' para se referir aos delitos que podem ser praticados por qualquer pessoa, em contraposição aos 'crimes próprios', que exigem determinada qualidade ou condição pessoal do agente para consumação do delito.

Há também uma divisão quaternária a qual classifica os delitos informáticos em impróprios, próprios, mistos e mediatos ou indiretos.

De acordo com esta classificação, os delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados); já os delitos informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados); os delitos informáticos mistos são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. Acrescenta-se, nesta classificação, o delito informático mediato ou indireto que é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para

possibilitar a sua consumação. (VIANNA, 2003, p. 13-26)

No entanto, uma vez que o direito penal informático não é um ramo autônomo do direito penal, e pela mesma razão pela qual se ponderou não ser adequada a utilização da expressão 'crimes informáticos comuns', prefere-se utilizar a expressão 'crimes informáticos puros' para se referir aos 'crimes informáticos próprios', evitando-se, assim, a sua eventual confusão em relação aos 'crimes próprios quanto ao sujeito', praticados através da informática, já que estes possuem significado diferente daqueles.

Em relação aos delitos informáticos mistos, entende-se que estes não podem ser considerados como 'crimes complexos', eis que não se vislumbra atualmente no ordenamento jurídico-penal vigente nenhum crime informático que possa ser representado a partir da fusão de mais de um tipo penal envolvendo o uso da informática. Salienta-se, por exemplo, que o crime de acesso indevido a sistemas informatizado do processo eleitoral constitui, por si mesmo, um único delito, conforme será estudado adiante. Assim, "não constituem crime complexo os delitos formados por um crime acrescido de elementos que isoladamente são penalmente indiferentes". (CAPEZ, 2004, p. 247)

Quanto aos delitos informáticos mediatos ou indiretos, estes ainda não existem no sistema penal brasileiro em razão da falta de tipificação do delito-meio informático que seria fundamental para viabilizar esta classificação. Acontece que a simples prática de acesso indevido objetivando cometer furto, por exemplo, envolve apenas o delito-fim que é o crime de furto uma vez que a conduta de acesso indevido não é considerada delito-meio eis que ainda não estar prevista como crime pela lei penal.

Não obstante à infinita possibilidade de classificação dos delitos informáticos, levando-se em consideração o conceito de crimes informáticos adotado neste trabalho, adota-se, para fins de estudo, uma classificação tripartite relativa ao objetivo material.

Assim, os crimes informáticos puros são definidos como aqueles que visam atingir a incolumidade dos dados e do sistema informatizado como um todo, inclusive no que concerne ao processamento destes dados e de sua transmissão. Por sua vez, os crimes informáticos impuros são considerados aqueles nos quais o agente não visa atingir o sistema de informática propriamente dito, mas a informática é utilizada como um meio alternativo para a consumação de um delito, não sendo a informática um elemento essencial para tanto; enfim, os crimes informáticos mistos são delitos praticados necessariamente por meio da informática e que, além da incolumidade dos dados e sistemas, a norma visa proteger outro bem jurídico tutelável pela lei penal.

Quanto à intenção do sujeito, os crimes informáticos são, em regra, dolosos, admitindo-se, em poucos casos, a modalidade culposa. São crimes dolosos quando o indivíduo quis o resultado ou assumiu o risco de produzi-lo; e culposos quando embora o sujeito não tenha a intenção de cometer o crime, der-lhe causa ao resultado por ato de imprudência, negligência ou imperícia.

De acordo com a ação do agente, os crimes informáticos podem ser categorizados em comissivos ou omissivos. Em sua maioria são comissivos eis que decorrem de uma ação do sujeito objetivando a prática da conduta delituosa. Por sua vez, serão omissivos quando a omissão for o meio através do qual se produz o resultado.

Em relação à consumação do delito, podem ser classificados em crimes informáticos instantâneos, permanentes ou instantâneos de efeitos permanentes. Crimes informáticos instantâneos são aqueles que se consumam com a ocorrência do resultado, enquanto que os crimes informáticos permanentes são aqueles cuja consumação ocorre ao longo do tempo conforme a vontade e a ação do agente.

Por sua vez, os crimes informáticos instantâneos de efeitos permanentes são aqueles que se consumam com a prática do comportamento descrito na norma penal, mas os seus efeitos perduram ao longo do tempo. Assim, no que tange à diferença entre o crime permanente e o instantâneo de efeitos permanentes, ensina a doutrina que "no primeiro há a manutenção da conduta criminosa, por vontade do próprio agente, ao passo que no segundo perduram, independentemente da sua vontade, apenas as conseqüências produzidas por um delito já acabado". (CAPEZ, 2004, p. 246)

Quanto ao bem jurídico tutelado, pode-se classificá-los como crimes informáticos de dano ou de perigo. Crimes informáticos de dano, que não se confundem com o dano informático o qual será objeto de estudo mais adiante, são aqueles em que, para que haja a sua consumação, é necessário que ocorra uma efetiva lesão ao bem jurídico tutelado pela norma penal. Já os crimes informáticos de perigo não exigem dano efetivo ao bem jurídico, sendo suficiente que o bem jurídico objeto de proteção pela lei penal tenha sido exposto a perigo.

Os crimes informáticos podem ser classificados também em materiais, formais ou de mera conduta. Os crimes informáticos materiais são aqueles que para a sua consumação exigem a ocorrência do resultado descrito na norma penal. Já os crimes informáticos formais descrevem um resultado o qual não precisa acontecer para que haja a consumação do delito. E, por último, os crimes informáticos de mera conduta que são aqueles que não prevêem nenhum resultado, bastando a simples prática do

comportamento proibitivo pela lei penal para que seja consumado o crime.

No que concerne ao número de sujeitos necessários para a consumação do crime, os delitos informáticos podem ser unissubjetivos ou plurissubjetivos. Serão unissubjetivos quando puderem ser praticados por apenas um agente sem a necessidade de participação de terceiros, enquanto que os plurissubjetivos são aqueles que não podem ser praticados individualmente, exigindo-se a participação de terceiros.

Os crimes informáticos podem ser unissubsistentes ou plurissubsistentes. São crimes informáticos unissubsistentes quando a conduta do agente consistir em um único ato, sendo plurissubsistentes nos demais casos em que sejam necessários mais de um ato para que ocorra a consumação do delito.

Por último, há também os crimes informáticos de menor potencial ofensivo que são considerados aqueles cuja penalidade máxima não seja superior a dois anos, cumulada ou não com multa, que são de competência do Juizado Especial Criminal.

3.3 Estudo sobre a aplicabilidade da lei penal aos crimes informáticos

Uma vez estabelecido o conceito de crime informático bem como realizada a análise quanto as suas possíveis formas de classificação, faz-se necessário analisar a possibilidade de aplicação da lei penal brasileira às condutas ilícitas cometidas contra ou através dos sistemas de informática, uma vez que a representação do conhecimento jurídico-penal no contexto dos crimes informáticos terá como suporte o presente estudo.

3.3.1 Crimes contra a vida

O uso da informática pode ser utilizado para a prática de crimes contra a vida, nestes casos, o componente informático ou a Internet se constitui apenas no meio através do qual se comete o delito, desta forma, podem ser considerados crimes informáticos impuros: o homicídio (art. 121 do CP); e o induzimento, instigação ou auxílio a suicídio (art. 122 do CP); conforme serão comentado a seguir.

Homicídio

O crime de homicídio consiste na conduta de matar alguém, nos termos do *caput* do art. 121 do Código Penal (CP), sendo a pena de reclusão, de seis a vinte anos.

A prática do crime de homicídio por meio do computador é admissível, por exemplo, quando o criminoso pratica o acesso indevido a sistemas de informações, invadindo computadores de determinada instituição e alterando dados em seu sistema informatizado, induzindo alguém ou a própria vítima em erro, fazendo com que esta se comporte de maneira a pôr em risco a sua própria vida ou a de outrem.

Embora seja de difícil ocorrência, trata-se de um delito informático possível de acontecer tendo em vista o crescente processo de informatização pelo qual passa a sociedade contemporânea, conforme exemplo ilustrado pela doutrina: "Tício invade os computadores do CTI de um grande hospital e altera a lista de remédios a ser ministrada em Mévio. Uma enfermeira, induzida a erro pela falsa receita, acaba matando Mévio com a superdosagem de medicação". (VIANNA, 2002a, p. 22)

Muito embora o Código Penal seja de 1940, a lei penal é, em regra, aplicável a toda conduta criminosa na qual a Internet seja o meio para a prática do crime. No caso em questão, trata-se apenas de um novo meio de execução de conduta já tipificada, toma-se o exemplo clássico da invenção da pólvora que não implicou na necessidade de mudança da lei para redefinir o crime de homicídio pela morte mediante arma de fogo.

Induzimento, instigação ou auxílio a suicídio

O artigo 122 do Código Penal tipifica como criminosa a conduta de induzir ou instigar alguém a se suicidar ou prestar-lhe auxílio para que o faça. Se o suicídio se consuma, a pena é de reclusão, de dois a seis anos; caso da tentativa de suicídio resulte lesão corporal de natureza grave, aplica-se pena de reclusão de um a três anos.

Trata-se de um delito que pode ser praticado através da rede mundial de computadores, como por meio da troca de mensagens eletrônicas ou através de comunidades virtuais de relacionamentos como o *Orkut*, onde o agente induz ou instiga a vítima a cometer o suicídio.

No caso em questão, consiste em um crime informático impuro, porque o agente não visa o sistema de informática e a Internet é apenas o meio para a prática do delito;

material, porque para haja a sua consumação é necessária a ocorrência do resultado (morte ou lesão corporal de natureza grave), sendo inadmissível a tentativa; é obrigatoriamente um crime comissivo, porque somente se consuma mediante a ação do agente; e é crime doloso, pois não existe modalidade culposa.

3.3.2 Crimes contra a honra

Os crimes contra a honra são três: calúnia, difamação e injúria. A diferença entre eles é que na calúnia há a imputação falsa a terceiro de uma conduta criminosa; na difamação, o fato imputado é uma alegação ou afirmação ofensiva à reputação da pessoa, independentemente do fato ser verdadeiro ou falso, desde que este não seja crime; enquanto que na injúria não há a imputação de um fato, mas sim a manifestação depreciativa, com expressões vagas e imprecisas sobre qualidade negativa do ofendido.

Todos estes delitos podem ser praticados através da informática, sendo o bem jurídico ofendido a honra objetiva (no caso de calúnia e difamação, onde se atinge a reputação) ou subjetiva (na hipótese de crime de injúria, onde se ofende a dignidade e o decoro) do agente.

O grande problema envolvendo os crimes contra a honra na Internet é a dificuldade de identificar o autor das ofensas haja vista o mesmo se aproveitar do anonimato para a prática destes delitos. Assim, reporta-se a um recurso de apelação criminal nº 71001070184, julgado em 2007, pelo Tribunal de Justiça do Rio Grande do Sul (TJRS), que manteve a sentença do juízo de primeiro grau que absolveu o réu dos crimes de difamação e injúria perpetrados pela Internet por ausência de provas; ou ainda ao acórdão nº 71001329036 deste mesmo tribunal que confirmou a sentença absolutória em razão de não haver certeza quanto à autoria das ofensas cometidas através de uma comunidade virtual de relacionamentos denominada *Orkut*.

A Carta Magna garante a liberdade de expressão em seu artigo 5º, IV, porém é proibido o anonimato justamente para evitar manifestações abusivas que violem a integridade das pessoas e o próprio ordenamento jurídico, pois, sendo anônimas, não se poderá responsabilizar o agente que cometer abusos no exercício deste direito.

Além dos crimes contra a honra previstos no CP, há também os crimes de calúnia, difamação e injúria, previstos pela Lei nº 5.250, de 9 de fevereiro de 1967, a qual regula a liberdade de manifestação do pensamento e de informação, conhecida

como Lei de Imprensa, cujas normas penais seriam aplicáveis em se tratando de crime praticado mediante a exploração ou utilização dos meios de informação e divulgação tipificados na referida lei.

De modo geral, quando o ofensor utilizasse a rede mundial de computadores para praticar um crime contra a honra (calúnia, difamação ou injúria) incidiria o Código Penal, como nas hipóteses de vir a cometer o delito através do envio de mensagens eletrônicas para grupos de discussão; através da postagem de recados ofensivos à honra de outra pessoa em comunidades virtuais; ou ainda por meio da publicação em páginas virtuais que não estejam vinculadas a atividades publicitárias e jornalísticas.

Por outro lado, quando o crime de calúnia, difamação ou injúria fosse praticado pela imprensa, através de jornais, periódicos ou serviços noticiosos na rede, incidiriam as normas penais da Lei 5.250/67, conforme decidiu o Tribunal de Alçada Criminal de São Paulo, ao julgar o *habeas corpus* nº 416.372-2, em 2002.

É imperioso destacar que se discute atualmente no país a constitucionalidade da Lei de Imprensa no Supremo Tribunal Federal (STF) em virtude de uma ação de descumprimento de preceito fundamental (ADPF nº 130-DF), proposta pelo partido político PDT, argumentando que esta lei teria conteúdo autoritário, sendo recentemente suspendidos os efeitos de diversos artigos, incluindo os acima mencionados, e os processos em trâmite no Poder Judiciário sobre o assunto até que seja julgada esta ação.

Desta forma, se o STF julgar a Lei de Imprensa como sendo inconstitucional, o Código Penal será aplicável às hipóteses previstas na Lei de Imprensa, as quais também estão tipificadas naquele e estenderia o seu alcance para os casos em que a prática do delito contra a honra estiver vinculada a atividades de publicidade e jornalismo, sendo cometido através de jornais, revistas ou serviços noticiosos na Internet.

Calúnia

O crime de calúnia está previsto no art. 138 do Código Penal, com pena de detenção de seis meses a dois anos, e multa. Esta pena é aplicável não apenas a quem imputa a alguém falsamente a autoria de um crime, como também incorre neste crime o terceiro que, sabendo ser falsa a imputação, a propala e divulga.

O crime de calúnia do art. 138 do CP admite a retratação, ou seja, se o ofensor, antes da sentença, se retratar cabalmente do delito, ficará isento de pena; ao contrário da

retratação do crime de calúnia do art. 20 da Lei de Imprensa, que deve ser feita antes de iniciado o procedimento judicial para excluir a ação penal. Acerca da retratação, o Superior Tribunal de Justiça, julgando o recurso especial nº 320958/RN, em 2007, decidiu que a retratação tem que ser completa e inequívoca, exigindo-se a publicidade desta, mormente nos casos em que a calúnia tenha sido praticada através da Internet.

Difamação

O crime de difamação consiste na imputação a outrem de fato ofensivo à sua reputação; estando previsto no art. 139 do CP, com pena de detenção de três meses a um ano, e multa. Assim como na calúnia, a difamação admite a possibilidade de retratação do ofensor; entretanto, para que haja isenção da pena se faz necessário que o ofensor se retrate de forma cabal, desdizendo todos os fatos imputados ofensivos à reputação da vítima, antes de proferida a sentença.

Neste crime, somente se admite a exceção da verdade se o ofendido for funcionário público e a ofensa estiver relacionada ao exercício de suas funções.

Uma vez praticado por meio da rede mundial de computadores, caracteriza-se como um crime informático impuro já que o bem jurídico ofendido no caso do art. 139 do CP é a reputação do sujeito e não visa o sistema de informática propriamente dito.

É crime comum quanto ao sujeito; necessariamente comissivo que exige uma ação do agente; formal, que independe do resultado; doloso, sendo imprescindível o ânimo de ofender a reputação alheia, não admitindo a forma culposa; e instantâneo, que se consuma no momento em que a imputação chega ao conhecimento de um terceiro.

Injúria

O crime previsto no art. 140 do CP consiste em "injuriar alguém, ofendendo-lhe a dignidade ou o decoro", com pena de detenção, de um a seis meses, ou multa.

Há situações nas quais o juiz pode deixar de aplicar a pena, quais sejam: quando o ofendido, de forma reprovável, provocou diretamente a injúria; ou no caso de retorsão imediata, que consista em outra injúria. Não há crime de injúria contra os mortos.

Na hipótese do ofensor utilizar elementos referentes à raça, cor, etnia, religião ou

origem para injuriar alguém, a pena é de reclusão de um a três anos, e multa.

Em 2004, o STJ denegou o *habeas corpus* nº 37493/SP, o qual visava o trancamento da ação penal em virtude do registro de mensagens eletrônicas injuriosas na Internet, afastando a alegação de atipicidade da conduta.

Tanto na difamação quanto na injúria, há hipóteses em que não constituem crime, como, por exemplo, a opinião desfavorável da crítica literária, artística ou científica, salvo quando inequívoca a intenção de injuriar ou difamar.

Em se tratando do mesmo fato imputado, o crime de difamação absorve a injúria; ou seja, neste caso, o ofensor responde apenas pelo primeiro. Entretanto, sendo distintos os fatos, responderá por difamação e também por injúria.

3.3.3 Crimes contra a liberdade pessoal

Os crimes contra a liberdade pessoal que podem ser praticados através da informática são o crime de constrangimento ilegal e o crime de ameaça.

Constrangimento ilegal

O crime de constrangimento ilegal está inserido no art. 146 do CP e consiste na conduta de "constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda", sendo a pena aplicável a este crime de detenção de três meses a um ano, ou multa.

Trata-se de um tipo penal que pode vir a ser praticado, através da informática, apenas mediante grave ameaça, pois "claro que a partir das características da atividade tecnológica, certamente a violência como forma de constrangimento não seria passível de execução a partir da informática". (OLIVEIRA, 2002, p. 71)

O constrangimento ilegal pode acontecer mediante o envio de uma mensagem eletrônica ou qualquer outro meio através do qual o agente faz uma grave ameaça à vítima, reduzindo-lhe a sua capacidade de resistência e obrigando-a a não fazer o que a lei permite ou a fazer o que ela não manda.

Ameaça

Constitui crime, tipificado no art. 147 do CP, "ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto ou grave", cuja pena é de detenção de um a seis meses, ou multa.

O crime de ameaça pode acontecer através do uso da informática, como, por exemplo, por meio do envio de mensagens eletrônicas ou recados virtuais com o intuito de intimidar a vítima, ameaçando-lhe causar mal injusto ou grave.

Trata-se, neste caso, de um crime informático impuro, onde a Internet é apenas o meio utilizado para a prática da conduta delituosa: "A ameaça por escrito ou qualquer outro meio simbólico abre a possibilidade de execução do crime pela utilização de computadores, em especial de e-mails, nos quais contenham escritos ou representações gráficas que configurem a ameaça". (OLIVEIRA, 2002, p. 71)

Portanto, a ameaça, mesmo que praticada através do uso da Internet, seja através do correio eletrônico ou outro meio informático, caracteriza o crime previsto no art. 147 do CP, pois esta norma penal admite esta possibilidade ao se referir ao crime de ameaça cometido por meio de palavra, escrito ou gesto, ou qualquer outro meio simbólico.

3.3.4 Crimes de violação de e-mail e interceptação de comunicação de dados

O art. 151 do Código Penal trata do crime de violação de correspondência, definindo como típica a conduta de "devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem", atribuindo-lhe pena de detenção de um a seis meses, ou multa.

De início, surgiu uma discussão na doutrina acerca da eventual incidência do mencionado artigo na hipótese de se tratar de violação de *e-mail* no tocante a sua equiparação à correspondência para fins de aplicação da lei penal.

Entretanto, predominou o entendimento de que o *e-mail* não pode ser considerado uma correspondência fechada, a teor do art. 151 do CP uma vez que é vedado o uso de analogia no direito penal. Portanto, embora seja semelhante à correspondência, não pode o *e-mail* ser equiparado a esta para fins penais.

Em se tratando de interceptação de comunicação de dados, o art. 10 da Lei nº

9.296/96 estabelece que "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial com objetivos não autorizados em lei", com pena de reclusão de dois a quatro anos, e multa.

O Tribunal de Justiça de Santa Catarina, ao julgar a apelação criminal nº 2007.006842-9, entendeu que configura o crime de interceptação de comunicação a conduta de quem invade provedor de Internet, apropriando-se dos *logins* e senhas de seus usuários. Entretanto, considera-se este posicionamento equivocado, porque o art. 10 da Lei nº 9.296/96 pune apenas a interceptação de comunicações de dados e não o acesso indevido a sistemas computacionais, ainda que disto resulte a obtenção dos nomes de usuários e senhas que permitam a violação ao direito à privacidade. Neste sentido, "só haverá o crime do art. 10 da Lei 9.296, quando, e somente quando, o autor impedir que a mensagem chegue intacta a seu destinatário". (VIANNA, 2002b, p. 410).

3.3.5 Crimes contra a inviolabilidade dos segredos

Quanto à inviolabilidade dos segredos, os crimes de divulgação de segredo e de violação de segredo profissional podem ser cometidos através da Internet.

Divulgação de segredo

O crime de divulgação de segredo está previsto no art. 153, *caput* do CP, e consiste em "divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem", sendo a pena de detenção de um a seis meses, ou multa.

Há também o §1º-A deste artigo que foi inserido pela Lei nº 9.983/2000, estabelecendo pena mais severa no caso de divulgação de informações sigilosas ou reservadas oriundas dos sistemas de informações ou bancos de dados da Administração Pública; circunstância na qual a pena será de detenção de um a quatro anos, e multa.

Quando a divulgação de segredo é praticada através da Internet, por meio do envio de mensagens eletrônicas, por exemplo, caracteriza-se como um crime informático impuro; trata-se de delito formal que para sua consumação basta que o

agente divulgue um segredo que seja apto a causar dano, independente da ocorrência do resultado; é comissivo, pois exige uma ação do sujeito; e instantâneo, porque basta a sua divulgação para a caracterização do delito.

Em relação ao sujeito, o crime de divulgação de segredo contido no *caput* do art. 153 do CP é delito próprio eis que somente pode praticar o crime quem for destinatário ou detentor do documento particular ou da correspondência confidencial; por sua vez, o crime de divulgação do segredo do §1º-A do mesmo artigo é crime comum, ou seja, pode ser praticado por qualquer pessoa, mesmo que não seja funcionário público, inclusive por *hackers* que obtenham acesso indevido a estas informações mediante a invasão de computadores alheios e as divulguem pela rede de computadores.

O delito do *caput* do art. 153 do CP poderá ser aplicável para as hipóteses de divulgação, sem justa causa, de conteúdo de documento eletrônico, ainda que seja encaminhado por *e-mail*, desde que se utilize mecanismo de proteção que seja hábil a garantir a confidencialidade do seu conteúdo e, para que haja sua consumação, o conteúdo do documento eletrônico deve ser suscetível de ocasionar dano a alguém.

Por sua vez, o crime previsto no §1º-A do art. 153 do CP protege apenas a inviolabilidade de informações sigilosas ou reservadas, seja no âmbito da administração pública ou na esfera privada, não sendo aplicável, por exemplo, na hipótese de um *hacker* acessar indevidamente conteúdo de informações sigilosas, sendo imprescindível que ele realize a divulgação deste conteúdo sigiloso para haver a consumação do delito.

Violação de segredo profissional

Além dos crimes de divulgação de segredo acima referidos, o Código Penal também tipifica como crime a violação de segredo profissional, conforme consta em seu art. 154: "revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem", sendo a pena para este delito de detenção de três meses a um ano, ou multa.

O crime de violação de segredo profissional também é um delito próprio quanto ao sujeito uma vez que somente pode praticá-lo a pessoa que tem ciência do mesmo em razão de função, de ministério, de ofício ou da profissão exercida; trata-se aqui também de crime formal que não depende do resultado para a sua consumação; é um crime de menor potencial ofensivo e pode ser cometido através da rede mundial de

computadores, como, por exemplo, a partir da revelação do segredo profissional através do envio de mensagens eletrônicas a terceiros, revelando-os segredos de sua profissão que sejam suscetíveis de ocasionar dano a alguém, conforme a exigência do tipo penal.

Em relação à jurisprudência, lembra a doutrina que já há caso na Justiça brasileira em que "o conteúdo de *e-mail* monitorado foi utilizado como prova para demissão de um funcionário por justa causa, no caso de flagrante violação de sigilo profissional". (PINHEIRO, 2007, p. 157)

3.3.6 Crimes contra o patrimônio

Examinando os crimes contra o patrimônio, observa-se que podem ser cometidos através da informática os crimes de furto, extorsão, dano e estelionato.

Furto

O crime de furto está tipificado no art. 155 do CP e consiste na conduta de "subtrair, para si ou para outrem, coisa alheia móvel", sendo a pena aplicada para quem incorre neste delito, de reclusão, de um a quatro anos, e multa.

No crime de furto, o agente apenas subtrai para si ou para outrem coisa alheia móvel, diferentemente do crime de roubo no qual há o emprego de violência ou grave ameaça dirigida à pessoa, além da subtração da coisa para si ou para outrem.

Trata-se de um crime que pode ser praticado em sua modalidade informática, na qual o agente pratica o acesso indevido a um sistema informático, invadindo computadores de instituições bancárias e desviando dinheiro para outra conta.

Para que ocorra o crime de furto é necessário que haja a efetiva subtração de coisa alheia móvel, ainda que seja energia elétrica ou qualquer outra que tenha valor econômico; tanto a doutrina quanto a jurisprudência já se manifestaram no sentido da possibilidade de aplicação desta norma penal aos furtos através dos meios informáticos.

Neste sentido, o Judiciário tem condenado *hackers* que praticam o acesso indevido a contas bancárias para transferir valores para outras contas, denegando-lhes, inclusive, ordens de *habeas corpus* que são comumente pleiteadas aos tribunais.

Extorsão

O crime de extorsão está previsto no art. 158 do CP e consiste na conduta de "constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa", sendo a pena de reclusão, de quatro a dez anos, e multa.

Trata-se de um delito que pode ser praticado, por exemplo, mediante o envio de mensagens eletrônicas na qual o indivíduo busca constranger alguém, utilizando-se de grave ameaça com o intuito de obter vantagem econômica indevida.

O Superior Tribunal de Justiça, ao julgar o conflito de competência nº 40569/SP, em 2004, decidiu que o juízo competente, em se tratando de crime de extorsão praticado através de *e-mail*, é o foro do local de onde as mensagens foram recebidas pela vítima.

O Tribunal de Justiça do Paraná, julgando a apelação criminal nº 315.642-7, manteve a condenação de um indivíduo pela prática do crime de extorsão mediante grave ameaça praticado através da veiculação de informações vexatórias em *site* da Internet com o objetivo de intimidar a vítima para obter vantagem econômica indevida.

A extorsão pela Internet se caracteriza como um crime comum quanto ao sujeito, doloso e que não admite modalidade culposa, pois exige o dolo específico que é a intenção de obter vantagem econômica indevida mediante constrangimento, podendo ser cometido através de uma grave ameaça lançada à vítima pela rede de computadores.

Dano

O Código Penal estabelece em seu art. 163, como crime de dano, a conduta de "destruir, inutilizar ou deteriorar coisa alheia", sendo a pena de detenção, de um a seis meses, ou multa. Este delito passa a ser qualificado, por exemplo, quando for cometido por motivo egoístico ou com prejuízo considerável para a vítima, hipótese na qual a pena aplicável será de detenção, de seis meses a três anos, e multa.

Há uma resistência por parte da doutrina mais conservadora em admitir a possibilidade de aplicação do art. 163 do CP ao dano informático. Assim, argumenta-se que "se os dados armazenados, processados ou transmitidos por sistemas informáticos forem considerados coisas móveis, este conceito deixará de corresponder a objetos tangíveis para incluir objetos intangíveis. Ele passará da materialidade à imaterialidade,

do âmbito da propriedade para o âmbito do valor. Essa tendência expande excessivamente o conceito de 'coisas móveis'". (ALBUQUERQUE, 2006, p. 45)

Não obstante, admite-se a potencial incidência desta norma penal em se tratando de crime de dano praticado através da rede mundial de computadores desde que a coisa destruída, inutilizada ou deteriorada tenha valor patrimonial.

O crime de dano pode ser cometido mediante o uso da informática, como, por exemplo, através do envio de vírus por *e-mail* com o intuito de inutilizar o computador do destinatário. Deste modo, "caso sejam danificados as placas e circuitos internos, qualquer elemento físico externo, ou ainda, caso se introduza programas maliciosos, inclusive vírus, com o objetivo de modificar a funcionalidade do computador, em tese, poderá haver o enquadramento no crime de dano". (RODRIGUES, 2006, p. 90)

Mesmo sendo um delito material, a consumação do crime poderá ocorrer não somente quando houver um efetivo dano físico ao computador, mas também quando forem destruídos, inutilizados ou deteriorados dados informáticos que possuam concomitantemente valor patrimonial e de utilidade.

Portanto, uma vez que o tipo penal está inserido nos crimes contra o patrimônio, o alcance desta norma será limitado a proteger os dados informáticos com relevância patrimonial, não abrangendo dados que possuam apenas valor afetivo ou de utilidade.

Estelionato

O estelionato é um crime que está tipificado no art. 171 do CP, consistindo na conduta de "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", com pena de reclusão, de um a cinco anos, e multa.

É pacífico, tanto na doutrina quanto na jurisprudência, o entendimento no sentido da aplicabilidade do crime de estelionato aos golpes e fraudes praticados através da informática, como, por exemplo, através do envio de mensagens eletrônicas fraudulentas ou por meio da clonagem de páginas na Internet, visando induzir a vítima a erro para obter vantagem econômica indevida.

Neste sentido, o Tribunal de Justiça de Minas Gerais, ao julgar a apelação criminal nº 1.0024.02.875258-2, manteve a decisão de primeira instância que condenou um estelionatário por utilizar *site* gratuito na Internet com nome de fantasia de

determinada empresa, sem a sua autorização, para induzir as pessoas em erro e obter vantagem econômica indevida mediante falsa promessa de emprego no exterior.

Assim, também comete o crime de estelionato o agente que cria página na Internet ou faz anúncios por intermédio de *sites* como o Mercado Livre, por exemplo, simulando a venda de produtos com o objetivo de induzir a vítima em erro ao efetuar o pagamento antecipado da suposta mercadoria na ilusão de que está efetuando a sua compra e que irá recebê-la posteriormente, quando, na realidade, trata-se de um golpe utilizado pelo agente para obter vantagem econômica indevida, aproveitando-se da boa-fé das pessoas para enganá-las e acarretar prejuízo ao patrimônio destas.

3.3.7 Crimes contra a propriedade intelectual

Dentre os crimes contra a propriedade intelectual que podem ser cometidos através da informática estão o crime de violação de direito autoral previsto no art. 184 do CP e o crime de violação de direito de autor de programa de computador, sendo este último previsto em lei específica (art. 12 da Lei nº 9.609, de 18 de fevereiro de 1988).

Violação de direito autoral

O art. 184 do Código Penal tutela a proteção do direito autoral e os que lhe são conexos, sendo a pena de detenção, de três meses a um ano, ou multa.

O crime de violação de direito autoral previsto no art. 184 do CP é norma penal em branco, ou seja, a lei penal não define o que seja direito autoral tampouco o que seriam direitos conexos aos do autor, conseqüentemente ela precisa ser interpretada de acordo com a Lei nº 9.610/98, que é a lei de direitos autorais vigente no país.

Trata-se de crime comum, podendo ser praticado por qualquer pessoa que viole direito autoral de outrem. Podem ser vítimas do crime de violação de direito autoral, o autor ou o terceiro titular do direito autoral e ainda o titular de direito conexo tal como o artista intérprete ou executante, o produtor fonográfico e a empresa de radiodifusão.

A violação de direito autoral pode ser cometida através do ciberespaço, por exemplo, quando o agente publica obra intelectual na Internet sem citar o nome do autor e sem possuir expressa autorização para sua reprodução ou para modificar o conteúdo da obra intelectual.

Violação de direito de autor de programa de computador

Em se tratando de violação ao direito de autor de programa de computador, aplica-se o art. 12 da Lei nº 9.609/98, que tipifica como crime "violar direito de autor de programa de computador", com pena de detenção de seis meses a dois anos ou multa, não sendo aplicável o art. 184 do Código Penal, em razão do princípio da especialidade.

Neste sentido, o Tribunal de Justiça de Minas Gerais, ao julgar a apelação criminal nº 1.0145.02.005603-5/001, reconheceu a impossibilidade de aplicação do art. 184 do CP em relação à violação de direito de autor de programa de computador, considerando aplicável, em virtude da especialidade, a norma do art. 12 da Lei 9.609/98.

A violação de direito de autor de programa de computador pode ocorrer mediante o uso da informática, quando um *cracker* utiliza os seus conhecimentos técnicos e altera o programa de computador para modificar sua funcionalidade.

Também pode ocorrer através da Internet, quando um usuário disponibiliza página virtual que permite realizar o *download* de *softwares* proprietários, fornecendo número de série ou senha de acesso que permite ao internauta utilizar os programas sem que tenha que adquirir sua respectiva licença.

3.3.8 Crime contra o sentimento religioso

A doutrina admite a possibilidade de prática de crime contra o sentimento religioso através da informática no tocante ao disposto no art. 208 do CP, o qual prevê o crime de escárnio por motivo de religião: "escarnecer de alguém publicamente, por motivo de crença ou função religiosa; impedir ou perturbar cerimônia ou prática de culto religioso; vilipendiar publicamente ato ou objeto de culto religioso", sendo a pena de detenção, de um mês a um ano, ou multa.

Trata-se de um delito de ação múltipla que pode ser cometido tanto pelo escárnio por motivo de religião, pelo impedimento ou perturbação da cerimônia ou prática de culto religioso ou pelo vilipêndio público de ato ou objeto de culto religioso.

Dentre estas modalidades, é possível a prática do crime de escárnio por motivo de religião pela Internet, por exemplo, este pode ser cometido em listas de grupos de discussão por *e-mail* ou em comunidades virtuais como o *Orkut*, onde o agente escarnece de alguém em razão de sua crença religiosa.

3.3.9 Crimes contra os costumes

Em relação aos crimes contra os costumes previstos no Código Penal, há três tipos penais que, *a priori*, podem ser cometidos através da Internet: o favorecimento da prostituição que atenta contra a moralidade pública sexual; o ato obsceno e o escrito ou objeto obsceno, os quais tutelam o pudor público.

Favorecimento da prostituição

O crime de favorecimento da prostituição está previsto no art. 228 do CP e consiste na conduta de "induzir ou atrair alguém à prostituição, facilitá-la ou impedir que alguém a abandone", com pena de reclusão, de dois a cinco anos.

Trata-se de um crime de ação múltipla que contempla as condutas de induzir ou atrair à prostituição, facilitar a sua prática ou impedir que alguém a abandone. Apenas as duas primeiras condutas podem ser praticadas pela Internet.

Em relação à conduta de induzir, o crime ocorre, por exemplo, quando o agente mantém conversa com a vítima através da Internet, convencendo-a a se prostituir.

Quanto à modalidade de facilitar, o delito pode acontecer quando o indivíduo publica página virtual na Internet, intermediando e facilitando a prática da prostituição.

Ato obsceno

O delito tipificado no art. 233 do CP consiste em "praticar ato obsceno em lugar público, ou aberto ou exposto ao público", com pena de detenção, de três meses a um ano, ou multa. É considerado um crime formal que se consuma com a prática do ato obsceno em lugar público ou aberto ou exposto ao público, independentemente de não ter sido presenciado por ninguém ou não tenha ofendido o pudor de quem o presenciou.

O crime de ato obsceno pode ser praticado através da Internet, considerando-se a rede mundial de computadores como um lugar aberto ao público. Neste sentido, "algumas pessoas chegam a instalar câmeras dentro de suas casas e transmitem, em tempo real, cenas de sexo. (...). Tal conduta constitui ato obsceno, uma vez que qualquer pessoa pode acessar a página e ver as cenas". (CASTRO, 2003b, p. 36-37)

Escrito ou objeto obsceno

O crime de escrito ou objeto obsceno está tipificado no art. 234 do CP e consiste em "fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno", sendo a pena aplicável de seis meses a dois anos, ou multa.

O crime de objeto obsceno, embora esteja previsto em lei com cominação de pena, não deverá ser aplicável a estas condutas que forem praticadas na Internet, pois consiste em um delito que é tolerado pelo poder público por não mais ofender o pudor público como na época em que foi tipificado.

Assim, "trata-se de um tipo penal alheio à realidade mundial, cego diante do panorama que se apresenta. Caso fosse aplicado, 90% dos proprietários de bancas de revistas estariam atrás das grades. É reflexo da moralidade exigida na década de 40, desprovido de qualquer interesse jurídico-penal". (OLIVEIRA, 2002, p. 82)

3.3.10 Crimes contra a paz pública

Os crimes contra a paz pública que podem ser cometidos através da Internet são: a incitação ao crime, a apologia de crime ou criminoso e a formação de quadrilha.

Incitação ao crime

A incitação ao crime está prevista como delito no art. 286 do CP e consiste na conduta de "incitar, publicamente, a prática de crime", sendo a pena de detenção, de três a seis meses, ou multa. Assim, trata-se de crime de menor potencial ofensivo, que pode ser praticado por qualquer pessoa e que tem como sujeito passivo a coletividade.

É um delito formal que se consuma com a incitação pública da prática de um crime determinado, sendo desnecessário que alguém cometa o crime objeto da incitação para que haja a sua perfeita caracterização, é crime doloso que não admite a modalidade culposa e pode ser cometido através da rede mundial de computadores.

O Superior Tribunal de Justiça, ao julgar o conflito de competência nº 62949/PR, decidiu que em se tratando de divulgação na Internet de técnica de cultivo de planta destinada à preparação de substância entorpecente por hospedeiro estrangeiro e tendo a

ação de incitar sido desenvolvida dentro do território nacional, é competente a justiça estadual, e não a federal, para julgar o feito.

Apologia de crime ou criminoso

A apologia de crime ou criminoso está prevista no art. 287 do CP e consiste em fazer, publicamente, apologia de fato criminoso ou de autor de crime, sendo a pena aplicável para este delito de detenção, de três a seis meses, ou multa.

Trata-se de um delito formal, de menor potencial ofensivo, comum quanto ao sujeito, sendo vítima a coletividade, consistindo em um crime doloso, que não admite a modalidade culposa e que pode ser cometido através da Internet.

Neste sentido, "como na incitação ao crime, aqui também é necessária a publicidade. Desta forma, este crime pode ser praticado através de *sites*, *homepages* ou nas salas de conversas. A utilização de *e-mail* não é possível, pois falta a publicidade exigida no tipo penal." (CASTRO, 2003b, p. 40)

Formação de Quadrilha

O art. 288 do CP tipifica o crime de formação de quadrilha que consiste em "associarem-se mais de três pessoas, em quadrilha ou bando, para o fim de cometer crimes", sendo a pena de reclusão, de um a três anos. Trata-se de crime que não é contemplado pelos benefícios da lei dos juizados especiais eis que a pena cominada é superior a dois anos; sendo a pena duplicada se a quadrilha ou bando é armado.

O crime de formação de quadrilha pode ser cometido através da Internet, pois a associação de mais de três pessoas para a prática de crimes informáticos pode ser realizada através do próprio ambiente virtual, sendo desnecessária a presença física, basta que estes estejam reunidos com o propósito de se associarem para cometer crimes informáticos de forma reiterada.

Em 2007, o Tribunal de Justiça de Santa Catarina denegou o pedido de *habeas corpus* nº 2006.046877-4, mantendo a prisão preventiva de um dos pacientes acusados por formação de quadrilha e pela prática de crimes na Internet, envolvendo onze denunciados, baseando-se a sentença na necessária prisão do acusado para a garantia da ordem pública já que este havia reiterado a prática dos mesmos delitos inclusive após a obtenção de outro *habeas corpus* que foi concedido e que o havia posto em liberdade.

3.3.11 Crimes contra a fé pública

No que se refere aos crimes contra a fé pública, tem-se o crime de falsa identidade, o qual pode cometido através da informática.

Este crime está previsto no art. 307 do CP e consiste na conduta de "atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem", com pena de detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Trata-se de delito formal, o termo "para" contido no tipo penal foi utilizado para determinar o dolo do agente, ou seja, para que a conduta de atribuir a si ou a terceiro uma falsa identidade seja punida é necessário que o agente tenha a intenção de obter vantagem para si ou para outrem ou que tenha a intenção de causar danos a terceiros.

É um crime de menor potencial ofensivo, sendo cabíveis os benefícios da transação penal e da suspensão condicional do processo, desde que o fato não constitua elemento de crime mais grave com pena máxima superior a dois anos.

A falsa identidade pode ser cometida através da Internet, quando, por exemplo, o agente registra uma conta gratuita de *e-mail* com dados pessoais de outra pessoa como se fossem suas informações e, a seguir, manda mensagem eletrônica para outra pessoa se identificando com a falsa identidade, ou ainda quando o agente se cadastra em comunidades virtuais como o *Orkut* utilizando o nome e a foto de determinada pessoa com o objetivo de, em ambos os casos, obter vantagem indevida para si ou para outrem ou para causar dano.

3.3.12 Crimes contra a Administração Pública

Dentre os crimes contra a Administração Pública que podem ser cometidos através da informática, destacam-se a inserção de dados falsos em sistemas de informações, a modificação não autorizada de sistemas de informação ou programa de informática e o crime de concussão.

Inserção de dados falsos em sistemas de informações

De acordo com o art. 313-A do Código Penal, considera-se crime de inserção de dados falsos em sistemas de informações a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano". A pena atribuída a este crime é de reclusão, de dois a doze anos, e multa.

Quando o funcionário autorizado insere dados falsos no sistema de informações da Administração Pública com a consciência de que tais dados são falsos e com a vontade de realizar esta ação para obter vantagem para si ou para outrem ou para causar dano, o crime se consuma a partir do momento em que os dados falsos foram inseridos no sistema de informações, independentemente da obtenção de vantagem ou do dano causado em decorrência da prática do crime. (RAMOS JÚNIOR, 2007, p. 65)

Em 2004, o Tribunal de Justiça de Santa Catarina negou provimento a recurso de apelação criminal nº 2004.028935-4, interposto por uma funcionária pública e por seu comparsa, mantendo a sentença de condenação de ambos, proferida na primeira instância, por violação ao art. 313-A do Código Penal.

Neste julgado, uma funcionária pública, autorizada a lidar com o sistema do CIRETRAN, e seu namorado foram condenados pelo crime de inserção de dados falsos em sistemas de informações. Ela teria inserido dados falsos no sistema a pedido de seu namorado, digitando no sistema um código de autenticação de pagamento de seguro, entretanto com valor correspondente às taxas de licenciamentos, sem essas estarem recolhidas, com o fim de obter vantagem indevida para si e para o seu comparsa, o qual também foi condenado em virtude de haver participado e instigado a prática do crime.

Modificação ou alteração não autorizada de sistema de informações

O crime de modificação ou alteração não autorizada de sistemas de informações está tipificado no art. 313-B do Código Penal e consiste na conduta de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação da autoridade competente", com pena de detenção de três meses a dois anos, e multa.

Cumpre mencionar que o art. 327, *caput*, do Código Penal estabelece que, para efeitos penais, considera-se funcionário público quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública; sendo que o §1º deste artigo determina que se equipara a funcionário público quem exerce cargo, emprego ou função pública, em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.

Diferentemente do artigo anterior (art. 313-A) que exige que o funcionário público seja autorizado pela Administração Pública para operar o sistema, o crime do art. 313-B pode ser praticado por qualquer funcionário desde que a modificação ou alteração do sistema de informações ou do programa de computador não tenha sido autorizada nem solicitada pela autoridade competente. (RAMOS JÚNIOR, 2007, p. 66)

Em 2006, o Tribunal Regional Federal da 4ª Região (TRF4) negou provimento a recurso de apelação criminal nº 2005.71.00.016873-9/RS, interposto por um estagiário do Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul (UFRGS) condenado pelo crime de modificação ou alteração de sistemas de informações, reconhecendo se tratar de um crime de mera conduta e que independe de prejuízo para a sua consumação.

Concussão

O crime de concussão está previsto no art. 316 do CP, e consiste na conduta de "exigir, para si ou para outrem, direta ou indiretamente, ainda que fora da função ou antes de assumi-la, mas em razão dela, vantagem indevida", com pena de reclusão de dois a oito anos, e multa.

Em 2007, o Superior Tribunal de Justiça denegou o pedido de *habeas corpus* nº 83188/PA de um investigador da política militar acusado de concussão e por fazer parte de um grupo criminoso voltado para a prática de ilícitos contra a Caixa Econômica Federal e outras instituições bancárias, que realizava transferências de valores de correntistas por meio da Internet.

3.3.13 Crimes contra a criança e o adolescente

A Lei nº 8.069, de 13 de julho de 1990, dispõe sobre o Estatuto da Criança e do Adolescente (ECA) e tipifica os crimes praticados contra a criança e o adolescente, dentre os quais, cita-se o crime de pornografia infantil.

Em sua redação original, o art. 241 do ECA dispunha que constitui crime: "fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente", com pena de reclusão de um a quatro anos.

Este artigo foi alterado pela Lei nº 10.764/2003 que lhe deu nova redação, aumentando a aplicabilidade desta norma penal: "apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente", sendo a pena de dois a seis anos, e multa.

Também se estabeleceu que na mesma pena incorre quem: agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo; assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo; assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do *caput* deste artigo.

Mesmo antes da entrada em vigor da nova redação do art. 241 do ECA, o Supremo Tribunal Federal já tinha se pronunciado acerca da tipicidade desta conduta criminosa ainda que praticada através da Internet, com o julgamento do *habeas corpus* nº 76.689/PB, em razão da publicação de cena de sexo infanto-juvenil na rede.

3.3.14 Crimes contra a segurança nacional

A Lei nº 7.170, de 14 de dezembro de 1983 define os crimes contra a segurança nacional e a ordem política e social, dentre os quais podem ser praticados pela Internet os delitos previstos nos artigos 22 e 23 desta lei.

Propaganda ofensiva à segurança nacional e a ordem política e social

Constitui crime previsto no art. 22 da Lei nº 7.170/83, a conduta de fazer, em público, propaganda: "I - de processos violentos ou ilegais para alteração da ordem política ou social; II - de discriminação racial, de luta pela violência entre as classes sociais, de perseguição religiosa; III - de guerra; IV - de qualquer dos crimes previstos nesta lei", sendo a pena de detenção de um a quatro anos.

A pena deste crime é aumentada de um terço quando a propaganda for feita em local de trabalho ou por meio de rádio ou televisão. Tal penalidade também é aplicada a quem distribui ou redistribui: a) fundos destinados a realizar a propaganda de que trata este artigo; b) ostensiva ou clandestinamente boletins ou panfletos contendo a mesma propaganda. Por sua vez, estabelece a Lei nº 7.170/83 que não constitui propaganda criminosa a exposição, a crítica ou o debate de quaisquer doutrinas.

Trata-se de um crime que pode ser praticado através da Internet, devendo a propaganda ser realizada em ambiente público para que haja a consumação do delito, não se admitindo a sua prática pelo envio de correspondência eletrônica individualizada.

Salienta a doutrina que "em relação à discriminação racial não se aplica esta lei e, sim a Lei nº 7.716/89, pois além de ser especial é posterior. Assim, diante de uma propaganda na Internet sobre racismo deve ser aplicada a lei contra o preconceito de raça e cor". (CASTRO, 2003b, p. 56)

Incitação à subversão da ordem política ou social

Outro crime previsto na lei que define os crimes contra a segurança nacional, é o crime de incitação contido no art. 23 que pune as condutas de incitar: "I - à subversão da ordem política ou social; II - à animosidade entre as Forças Armadas ou entre estas e as classes sociais ou as instituições civis; III - à luta com violência entre as classes sociais; IV - à prática de qualquer dos crimes previstos nesta lei", sendo cominada também pena de reclusão de um a quatro anos.

Assim como a incitação ao crime, prevista no art. 286 do CP, pode ser praticada através da Internet, da mesma forma, tem-se que a incitação aos crimes previstos na Lei nº 7.170/83 pode ser cometida por meio da rede de computadores. Caso a incitação esteja relacionada a atos de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, será aplicável o art. 20 da Lei nº 7.716/89.

3.3.15 Crimes contra a propriedade industrial

A Lei nº 9.279, de 14 de maio de 1996 dispõe sobre os crimes contra a propriedade industrial, dentre eles, os crimes de concorrência desleal, tipificados no art. 195 desta lei, dentre os quais, por exemplo, a conduta criminosa descrita no inciso primeiro, cometendo o delito quem "publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem", sendo a pena de detenção, de três meses a um ano, ou multa.

Desta forma, uma vez que o tipo penal permite a publicação, por qualquer meio, de informação falsa em detrimento do concorrente, o crime de concorrência desleal, no que tange a esta norma, pode ser praticado por meio da publicação de falsa afirmação em *sites* da Internet que tenham a finalidade de obter vantagem em detrimento do concorrente.

O mesmo se pode dizer, por exemplo, quanto ao inciso II no que tange à conduta de quem "presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem", tal divulgação pode ocorrer por meio da Internet, inclusive por *e-mail*.

3.3.16 Crimes de tráfico ilícito de entorpecentes e indução ao uso de drogas

A Lei nº 11.343, de 23 de agosto de 2006, instituiu o Sistema Nacional de Políticas Públicas sobre Drogas – SISNAD, e, dentre outras coisas, tipificou como crime, em seu art. 33, a conduta de "importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar", sendo a pena de reclusão de cinco a quinze anos e pagamento de quinhentos a mil e quinhentos dias-multa.

Trata-se de um crime que pode ser cometido por meio da rede mundial de computadores, principalmente no que concerne à conduta de "oferecer", na hipótese do traficante enviar mensagens eletrônicas oferecendo drogas a terceiros, ou ainda, através de sua oferta ou comercialização através de páginas da Internet.

Há ainda o parágrafo segundo deste artigo o qual prevê como crime a conduta de

“induzir, instigar ou auxiliar alguém ao uso indevido de droga”, com pena de detenção, de um a três anos, e multa de cem a trezentos dias-multa.

De igual modo, quanto a esta norma penal específica, admite-se a possibilidade de sua consumação através da Internet, sendo, neste caso, um crime informático impuro.

3.3.17 Crimes de lavagem de dinheiro

A Lei nº 9.613, de 03 de março de 1998, dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores, os quais estão previstos no art. 1º desta lei.

Constitui crime de lavagem de dinheiro a conduta de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de crime de tráfico ilícito de substâncias entorpecentes; de terrorismo; de contrabando; de extorsão mediante seqüestro; contra a Administração Pública; contra o sistema financeiro nacional; praticado por organização criminosa ou praticado por particular contra a administração pública estrangeira; sendo a pena de reclusão de três a dez anos e multa.

Os crimes de lavagem de dinheiro podem ser praticados por qualquer pessoa, independente de ser ou não o mesmo autor dos crimes anteriores previstos no artigo primeiro. Além disso, são crimes de mera conduta, sendo suficiente que o indivíduo pratique a conduta descrita na norma penal para que haja a sua consumação; podendo ser cometidos através da Internet. Assim, “a informática pode ser utilizada para ocultar a procedência e a localização do dinheiro através de sucessivas transferências feitas em *Home Bank*, ou seja, na Internet”. (CASTRO, 2003b, p. 60)

3.3.18 Crimes eleitorais

Há diversas leis vigentes que definem crimes eleitorais. Dentre elas, destacam-se o Código Eleitoral (Lei nº 4.737/65), a Lei nº 6.996/82 e a Lei nº 9.504/97.

O art. 299 do Código Eleitoral tipifica como crime a compra e venda de votos: “dar, oferecer, prometer, solicitar ou receber, para si ou para outrem, dinheiro, dádiva, ou qualquer outra vantagem, para obter ou dar voto e para conseguir ou prometer abstenção, ainda que a oferta não seja aceita”, com pena de reclusão até quatro anos e

pagamento de cinco a quinze dias-multa.

Trata-se de um delito que pode ser cometido através da rede mundial de computadores, como, por exemplo, mediante a oferta encaminhada por mensagem eletrônica ao eleitor, oferecendo a este dinheiro pelo voto em um determinado candidato. Além do sujeito que faz a oferta, também responde pelo crime o eleitor que solicita qualquer vantagem em troca de seu voto, ainda que esta não seja aceita.

Quanto à conduta de alterar resultados no processamento eletrônico das cédulas eleitorais, a Lei nº 6.996/82 dispõe sobre a utilização de processamento eletrônico de dados nos serviços eleitorais, e prevê em seu art. 15 que "incorrerá nas penas do art. 315 do Código Eleitoral quem, no processamento eletrônico das cédulas, alterar resultados, qualquer que seja o método utilizado", cominando a este crime, assim, pena de reclusão até cinco anos e pagamento de 5 a 15 dias-multa.

A Lei nº 9.100/95, em seu art. 67, VII, passou a dispor sobre o crime de acesso indevido ao sistema informático eleitoral para alterar o resultado das eleições, nos seguintes termos: "obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos", a pena cominada era de reclusão, de um a dois anos, e multa.

Entretanto, a Lei nº 9.504/97 revogou tacitamente este artigo, em parte, em seu art. 72, inciso primeiro, ao tipificar a conduta de "obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos", com pena de reclusão de cinco a dez anos, sendo o art. 67, inc. VII da Lei nº 9.100/95 aplicável então somente aos casos de tentativa previstos na norma. (VIANNA, 2003, p. 23-24)

Também constitui crime eleitoral, segundo o art. 72, inciso segundo, da Lei nº 9.504/97, a conduta de "desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral", sendo aplicável a este a mesma pena do inciso primeiro.

3.3.19 Crimes contra as relações de consumo

A Lei nº 8.078, de 11 de setembro de 1990, mais conhecida como Código de

Defesa do Consumidor (CDC), tipifica alguns crimes contra a relação de consumo os quais podem ser cometidos através da Internet, conforme serão examinados.

O art. 63 do CDC define como crime a conduta de "omitir dizeres ou sinais ostensivos sobre a nocividade ou periculosidade de produtos, nas embalagens, nos invólucros, recipientes ou publicidade", sendo a pena de detenção de seis meses a dois anos e multa. Trata-se de um delito que pode ser cometido pela Internet, por exemplo, através da promoção de publicidade de um produto em página virtual, omitindo informação sobre a sua nocividade.

Além da omissão de informação sobre a nocividade do produto, o art. 66 do CDC também pode ser aplicável para responsabilizar penalmente o fornecedor que, em página virtual de sua empresa, faz afirmação falsa ou enganosa ou omite informação relevante sobre a natureza, característica, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia de produtos ou serviços, sendo a pena de detenção de três meses a um ano e multa.

Também incorre nesta mesma pena quem patrocinar a oferta.

Em relação à promoção de publicidade enganosa ou abusiva na Internet, o sujeito poderá incorrer no crime do art. 67 do CDC, com pena de detenção de três meses a um ano e multa.

No caso da publicidade ser suscetível de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança, poderá incidir o art. 68 do CDC que prescreve pena de detenção de seis meses a dois anos e multa.

Nada impede que a Internet seja também utilizada como um meio para realizar cobranças de dívidas de modo abusivo, sendo aplicável, nesta hipótese, o art. 71 do CDC que considera crime o comportamento de "utilizar, na cobrança de dívidas, de ameaça, coação, constrangimento físico ou moral, afirmações falsas, incorretas ou enganosas ou de qualquer outro procedimento que exponha o consumidor, injustificadamente, a ridículo ou interfira com seu trabalho, descanso e lazer", com pena de detenção de três meses a um ano e multa.

Quanto às informações do consumidor que constem em bancos de dados informáticos, admite-se a incidência do art. 72 do CDC que define como crime a conduta de "impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, bancos de dados, fichas e registros", com pena de detenção de seis meses a um ano ou multa.

3.4 Projeto de lei substitutivo sobre delitos informáticos

O Senador Eduardo Azeredo propôs um projeto de lei (PL) substitutivo ao PL nº 89/2003, de iniciativa do Deputado Luiz Piauhylino, ao projeto de Lei nº 137/2000, de autoria do Senador Leomar Quintanilha, e ao PL nº 76/2000, de autoria do Senador Renan Calheiros, todos sobre crimes informáticos.

Considera-se importante examinar algumas das propostas legislativas relacionadas com os crimes cibernéticos, pois, conforme foi possível observar ao longo deste estudo, as normas penais em vigor nem sempre conseguem tutelar de forma adequada os bens jurídicos que se dispôs a proteger, bem como novos bem jurídicos passam a necessitar de proteção especial nesta era da informação.

Em relação aos crimes contra a honra, o projeto agrega o art. 141-A no capítulo V, do título I, da parte especial do Código Penal, que estabelece que "as penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado".

Já em relação aos crimes contra o patrimônio, será inserido o inciso V no §4º do art. 155 do CP, para definir como furto qualificado o crime cometido "mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares".

Por sua vez, também há a pretensão de tipificar como crime a difusão de código malicioso, que será típico, salvo quando for cometido para fins de defesa digital.

Além disso, o projeto irá garantir de vez a tutela penal do dano informático ao equipará-lo a 'coisa' para fins penais.

No que concerne à defesa digital, para efeitos penais, ela é definida como a manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação.

O projeto pretende ampliar o âmbito da incidência dos artigos 265 e 266 do CP, tipificando o atentado contra a segurança de serviços de informação e a interrupção ou

perturbação destes serviços e dos já definidos no tipo penal.

A falsificação de cartão de crédito ou dispositivo eletrônico similar será acrescida no parágrafo único do art. 298 do CP, equiparando o cartão de crédito a documento particular. Será tipificado, no art. 298-A do CP, o crime de falsificação de telefone celular ou meio de acesso à rede de computadores, com pena de reclusão de um a cinco anos e multa.

Especificamente no que concerne aos crimes contra a rede de computadores, dispositivo de comunicação ou sistema informático, o projeto substitutivo insere novos tipos penais no capítulo VI-A no título I, parte especial do Código Penal, que passa a considerar como crime: a) o acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado; b) a obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica, digital ou similar; e c) a divulgação ou utilização indevida de informações contidas em bancos de dados.

O crime de acesso não autorizado à rede de computadores será acrescido no art. 154-A, com pena de reclusão de dois a quatro anos e multa. Caracteriza-se como um crime de mera conduta, sendo suficiente que o sujeito pratique o acesso ao computador sem autorização para haja consumação do delito. Entretanto há previsão no §4º deste artigo de que não haverá crime quando o agente acessa a título de defesa digital, excetuando o desvio de finalidade ou o excesso.

Já o art. 154-B a ser inserido no CP, define como crime a conduta de "obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida", com pena de detenção de dois a quatro anos e multa.

Sendo aprovado o projeto substitutivo, também passará a constituir crime, a ser agregado no art. 154-D do CP, a divulgação ou utilização de informações contidas em banco de dados com finalidade distinta da que motivou o seu registro, incluindo informações referentes a dados pessoais; a pena prevista será de detenção de um a dois anos e multa.

Esta análise realizada neste capítulo acerca da aplicação da lei penal aos crimes praticados contra os sistemas informáticos ou através da informática é fundamental para o desenvolvimento da ontologia jurídica de delitos informáticos a ser proposta a seguir e que deverá levar em conta as peculiaridades do sistema jurídico penal brasileiro para que o resultado apresentado seja útil e coerente com a legislação nacional vigente.

4 ONTOLOGIA JURÍDICA DE DELITOS INFORMÁTICOS

Neste capítulo, propõe-se uma ontologia para representar o conhecimento jurídico-penal na área dos delitos informáticos, objetivando principalmente auxiliar a esclarecer a tipicidade das condutas criminosas a partir da legislação penal aplicável, considerando as ontologias já existentes, o estudo sobre a aplicabilidade da lei penal e o uso da metodologia *Ontology Development 101* na construção da ontologia proposta.

4.1 Domínio da ontologia

O domínio que a presente ontologia irá cobrir se refere a questões legais pertinentes ao contexto dos delitos informáticos que constituem um assunto importante na atualidade, pois consiste em uma área que necessita de definições e classificações a respeito das condutas puníveis e das normas penais que sejam aplicáveis.

Conforme estudado, as ontologias servem para anotar semanticamente o conteúdo disponível, o que permite que agentes de *software* compreendam a semântica embutida nas páginas da *web*, viabilizando o intercâmbio de informações.

A ontologia jurídica de delitos informáticos pretende esclarecer conceitos para este domínio com o objetivo classificar, organizar e orientar a busca por informações sobre crimes informáticos, auxiliando no esclarecimento da tipicidade de condutas criminosas e suas características e na recuperação de obras e jurisprudências nesta área.

No âmbito dos delitos informáticos, a perspectivas é que as ontologias ajudem não apenas a esclarecer as condutas criminosas, mas também contribuam para: a) apoiar a tomada de decisão judicial; b) facilitar o uso de agentes inteligentes; c) promover a interoperabilidade entre os sistemas de segurança pública no que se refere aos delitos informáticos; d) possibilidade de cooperação internacional na busca por evidências de crimes informáticos em mais de um país; e) ajudar a identificar a inserção e alteração não autorizada de dados nos sistemas de informações das organizações públicas; f) facilitar a busca por notícias e recuperação de legislação e jurisprudência sobre crimes na Internet; g) auxiliar na construção de um observatório de crimes informáticos etc.

4.2 Princípios jurídicos observados

Uma vez que a ontologia proposta envolve o conhecimento jurídico-penal, há de se considerar alguns princípios que são considerados fontes do direito. Devido a sua importância, muitos deles estão consagrados na Constituição Federal ou em leis infraconstitucionais, enquanto outros estão implícitos e decorrem do sistema instituído.

No direito penal, destacam-se, por exemplo, os seguintes princípios: legalidade, anterioridade, insignificância, taxatividade, especialidade, transcedentalidade e irretroatividade da lei penal etc, conforme ilustra a figura 19:

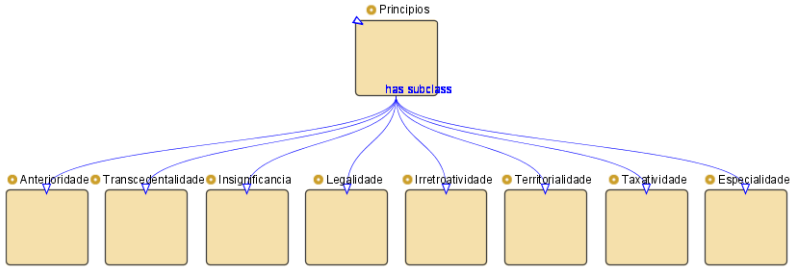

Figura 19. Representação dos princípios de direito na ontologia. (Fonte: o autor)

O princípio da **legalidade** penal está previsto no artigo 1º do Código Penal que estabelece que "não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal", sendo os demais princípios, na maioria, dele decorrentes, como o princípio da **anterioridade** da lei penal que preconiza justamente que para que haja um crime é necessário que a lei já esteja em vigor na data em que o fato foi praticado.

Desta forma, as ontologias jurídicas foram desenvolvidas, a princípio, para terem uma aplicação *ex nunc*, ou seja, ela será válida apenas para esclarecer questões atuais sobre delitos informáticos, não sendo aplicável a casos pretéritos no tempo da lei velha por considerar apenas a legislação penal vigente no momento de sua construção, sendo atualizada daqui para frente. Esta delimitação se torna recomendável para fins de estudo e desenvolvimento da ontologia por simplificá-la sem comprometer a sua validade quanto a sua aplicação a fatos ocorridos a partir da legislação penal em vigor.

No que se refere ao princípio da **irretroatividade da lei penal**, ensina a doutrina que "um dos efeitos decorrentes da anterioridade da lei penal é a irretroatividade, pela qual a lei penal é editada para o futuro e não para o passado". (CAPEZ, 2004, p. 48)

A ontologia foi desenvolvida em consonância com o princípio da legalidade penal, o qual foi considerado ao dissertar no terceiro capítulo sobre a aplicabilidade das leis penais aos crimes informáticos, com base na doutrina e na jurisprudência.

Em relação ao princípio da **insignificância**, também conhecido como princípio da bagatela, este recomenda que muito embora o crime tenha sido cometido, a norma penal não deveria ser aplicada quando se tratar de delitos de lesão mínima, como no caso de furto de objeto insignificante, ou seja, de pequeníssima relevância material.

Trata-se de um princípio cuja aplicação no âmbito dos delitos informáticos deve ser analisada com muita cautela, pois, *a priori*, a subtração de centavos da conta bancária de um cliente por meio da Internet pode parecer insignificante, porém, se o criminoso realiza esta mesma operação com milhares de clientes de uma instituição bancária, em seu conjunto, observa-se que, ao final, o valor obtido pelo agente será expressivo, não podendo, nesta hipótese, ser admitida a aplicação deste princípio.

Portanto, uma vez que o objetivo central da ontologia proposta é auxiliar no esclarecimento e na identificação da tipicidade dos delitos informáticos, este princípio será desconsiderado já que, em um primeiro momento, verifica-se que a tipicidade se faz presente ainda que posteriormente o juiz possa concluir que a lei penal não deva ser aplicável em razão da ausência de gravidade ou relevância material do bem protegido.

O princípio da **taxatividade** serve para garantir segurança jurídica ao cidadão, preconizando que a lei penal deve definir de forma objetiva quais são as condutas que constituem crime e qual pena lhe é aplicável, não admitindo o uso de analogia ou interpretação extensiva para alcançar comportamento não tipificado na lei.

Há questões de antinomia das leis penais que precisam ser resolvidas, ou seja, somente existe uma lei penal que é aplicável para um determinado caso e a ontologia proposta deve ser capaz de identificar a lei aplicável para uma situação específica. Assim, um dos critérios adotados para solucionar tal questão é utilizar o princípio da **especialidade** segundo o qual lei especial prevalece sobre lei geral, em igual hierarquia.

Em relação ao princípio da especialidade, a expectativa é que as ontologias sejam capazes de ajudar os agentes de *software* a compreenderem a diferença entre uma lei geral e uma lei especial tendo em vista os bens jurídicos que são por ela protegidos.

O princípio da **transcedentalidade** ou da alteridade orienta que a lei penal somente pune lesões a interesses jurídicos alheios, ou seja, que transcenda a esfera individual do autor e seja capaz de atingir o interesse de outra pessoa. Assim, por orientação deste princípio, verifica-se que, para que haja a consumação de um crime, torna-se necessário que o sujeito ativo do delito seja obrigatoriamente diferente do sujeito passivo.

4.3 Reuso das ontologias existentes

Depois de definir o domínio, o escopo e observados os princípios do direito, o próximo passo é verificar a possibilidade de reuso das ontologias existentes conforme foram apresentadas no segundo capítulo desta dissertação, enfatizando especialmente aqueles projetos que estejam relacionados com o domínio dos delitos informáticos, porém, antes de verificar a possibilidade de reuso das ontologias de crimes que existem na atualidade, é preciso que se tenha em conta o foco de cada uma destas ontologias.

Há diferentes tipos de ontologias, conforme a sua destinação e aplicabilidade, já que elas podem ser construídas para resolver os mais variados problemas.

Desta forma, a primeira categoria é representada pelas ontologias de pouca significância (*lightweight ontologies*) e consistem em um conjunto de termos hierarquicamente organizados, sendo destinadas principalmente a auxiliar na recuperação de informação; outro tipo de ontologias serve para descrever categorias fundamentais aplicáveis a todos os domínios, sendo, por isso, denominadas de ontologias de topo (*top ontologies*); há ontologias que cuidam de desenvolver conceitos básicos para um domínio específico (*core* ou *domain ontologies*); e, por último, existem as ontologias de aplicação (*application ontologies*) que são utilizadas para detalhar e especificar os conceitos necessários para a execução de uma determinada tarefa. (BENCH-CAPON, 2007, p. 72-73)

Um exemplo de ontologia de domínio é a ontologia jurídica funcional proposta por André Valente e Joost Breuker (1994), que é definida a partir do tipo de conhecimento jurídico empregado e, por isso, pode ser usada como referência para qualquer área do direito, apresentando a conexão existente entre as diversas categorias de conhecimento jurídico e suas inter-relações para dar efetividade ao funcionamento do sistema jurídico como um todo através de uma visão teleológica.

A ontologia italiana de crime é também tida como uma ontologia de domínio, pois o conceito abstrato de delito somente é válido, em regra, dentro do domínio do direito penal italiano, entretanto ela pode servir de modelo para a ontologia brasileira de delitos informáticos, já que tanto o direito penal italiano quanto o direito penal brasileiro herdam as mesmas definições básicas quanto ao conceito abstrato de crime.

Um tipo de ontologia de aplicação pode ser exemplificado através da ontologia mexicana apresentada no capítulo anterior, já que ela se destina a apoiar a ferramenta FROID na detecção de intrusão e ataques cibernéticos.

4.4 Enumeração dos termos importantes

Nesta etapa, cuida-se de identificar os termos e expressões que são utilizados no âmbito do conhecimento jurídico-penal voltado para os delitos informáticos, ou seja, são enumerados termos que fazem parte do domínio da presente ontologia, tais como: crime, tipicidade, antijuridicidade, autoria, culpabilidade, materialidade, lei penal, tipo penal, artigo, pena, conduta, bem jurídico, princípios, pessoas, sujeito ativo, sujeito passivo, tentativa, consumação, dolo, culpa, doutrina, jurisprudência dentre outros.

Tratou-se, assim, de listar diversos termos do domínio que serão abordados na ontologia seja para formular declarações ou para esclarecer conceitos ao usuário.

Para tanto, questionou-se quais são os termos empregados, sobre as propriedades que estes termos possuem e o que se pretende dizer a respeito dos termos jurídicos.

A relevância desta fase na construção da ontologia jurídica de delitos informáticos é que a enumeração dos termos importantes utilizados no domínio irá ajudar consideravelmente no próximo passo que consistirá em definir as classes e a hierarquia de classes e também a estabelecer as propriedades dos conceitos empregados.

4.5 Classes e hierarquia de classes

A abordagem utilizada para o desenvolvimento da hierarquia de classes na ontologia jurídica de delitos informáticos foi no sentido *top-down*, ou seja, foram definidas, em primeiro lugar, as classes de maior nível hierárquico que possuem os conceitos mais gerais do domínio, partindo-se para a sua subseqüente especificação.

Assim está representada a hierarquia de classes na ontologia jurídica proposta:

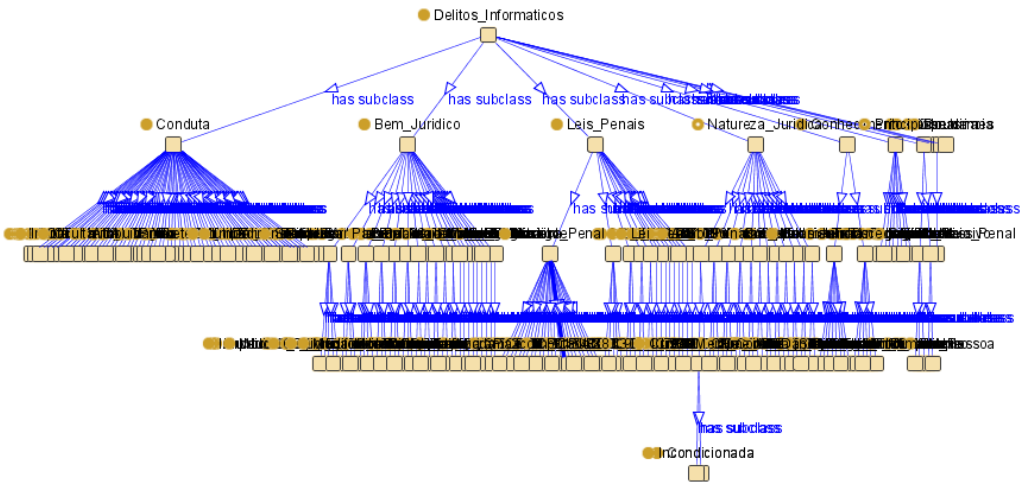

Figura 20. Taxonomia da hierarquia de classes na ontologia proposta. (Fonte: o autor)

Conforme é possível observar, as classes que compõem a ontologia jurídica de delitos informáticos são as seguintes: Cibercrimes, Princípios, Natureza Jurídica, Leis Penais, Pessoas, Bem Jurídico, Jurisprudência, Doutrina e Conhecimento:

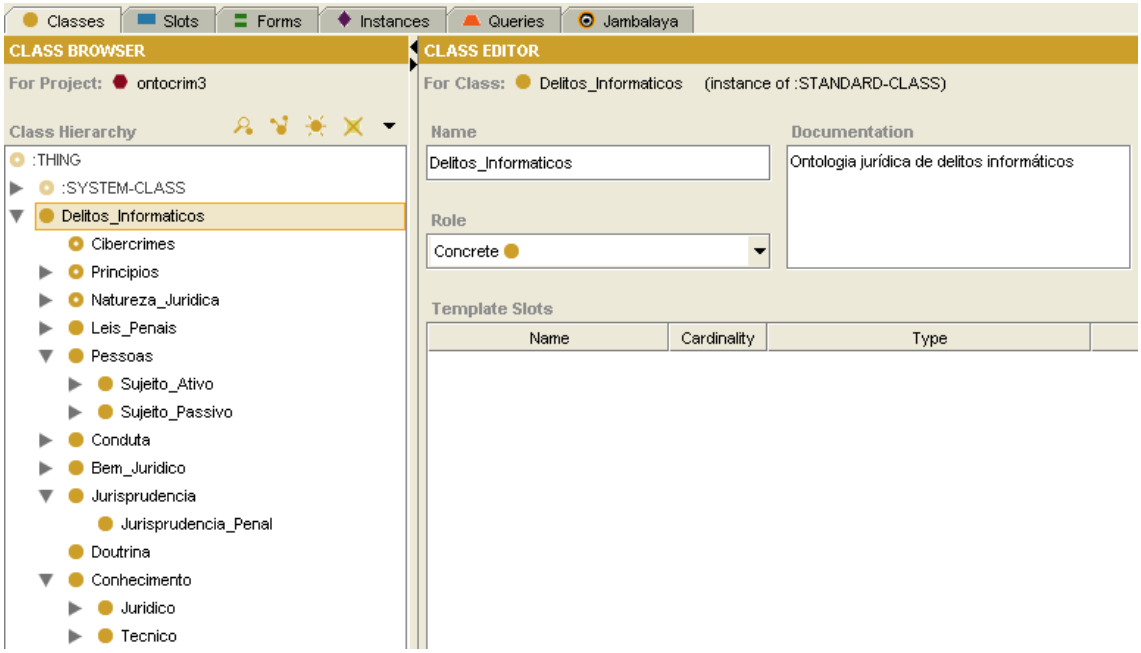

Figura 21. Exibição das classes da ontologia proposta visualizada no editor *Protégé*. (Fonte: o autor)

A classe <Cibercrimes> está relacionada com o conceito ontológico e abstrato de delito informático, enquanto que a classe <Principios>, como o próprio nome sugere, representa os princípios jurídicos que influenciam na identificação da tipicidade e da caracterização ou não de um delito informático.

Já a classe <Natureza_Juridica> permite a análise de aspectos relacionados à natureza jurídica dos delitos, bem como a especificação de seus respectivos conceitos.

As leis penais aplicáveis aos crimes informáticos estão representadas pela classe <Leis_Penais>, enquanto que a classe <Pessoas> servirá para ajudar a esclarecer a posição das pessoas em relação ao crime, quem pode ser vítima ou autor do crime.

Para identificar quais as condutas criminosas que podem ser praticadas através de determinada ação do sujeito, considerou-se importante a inserção da classe <Conduta>, permitindo, assim, a associação entre o verbo contido na norma e o delito.

A classe <Bem_Juridico> representa os interesses jurídicos tutelados pela lei penal e que podem ser ofendidos por condutas criminosas que utilizem a informática.

A <Jurisprudencia> é a classe que se refere às decisões judiciais dos tribunais

brasileiros, sendo utilizada aqui para recuperar julgados sobre delitos informáticos.

Em relação à classe <Doutrina>, ela foi agregada com o intuito de indexar referências ou obras científicas relacionadas aos delitos informáticos, permitindo a sua relação com a classe <Conhecimento>, a qual servirá para definir e mapear as diversas áreas e subáreas do conhecimento que possuam produções científicas de interesse do domínio dos delitos informáticos, embora a ênfase maior seja para o domínio jurídico.

4.6 Localização de obras científicas

Em relação às obras científicas, a ontologia jurídica de delitos informáticos exerce um papel muito importante porque pode ajudar a recuperar com precisão as referências bibliográficas úteis para resolver determinado problema ou sanar uma dúvida acerca destes delitos, seja no âmbito jurídico, técnico ou sociológico, ajudando tanto o cidadão leigo quanto ao profissional que atua nesta área a encontrar indicação útil de obras científicas neste domínio com precisão sobre o assunto de seu interesse.

Existe uma relativa escassez de obras tanto jurídicas quanto técnicas relativas ao domínio dos delitos informáticos, de forma que muitos profissionais e cidadãos comuns que necessitam de esclarecimento jurídico ou técnico sobre crimes informáticos não sabem onde encontrar as obras científicas úteis para atender sua necessidade específica.

Trata-se de uma questão que pode ser resolvida através da *web* semântica, com o uso de ontologias que permitam aos computadores processarem as informações estruturadas em uma linguagem padrão que seja compreensível pelas máquinas e que lhe permitam entender as relações que estão explícitas através da ontologia.

Enquanto um profissional do direito necessita de informações sobre crimes informáticos com conteúdo jurídico, como, por exemplo, acerca dos crimes contra a honra na Internet, um perito criminal, por sua vez, precisa de informações e conhecimento técnicos para conduzir o seu trabalho com maior presteza e segurança.

Assim, a ontologia jurídica se propõe a localizar obras científicas sobre crimes informáticos que possam ser úteis para o cidadão, atendendo às suas reais necessidades, seja ele cidadão leigo, profissional do direito, perito criminal etc.

Para atender às diversas necessidades de informação a respeito do domínio dos delitos informáticos, agregou-se à ontologia jurídica a classe <Doutrina>, com as respectivas subclasses <Livro>, <Artigo>, <Anais>, <Revista> e <Dissertacao>,

podendo-se incorporar novas subclasses para incluir outras categorias de obra científica.

Em relação às **propriedades** da classe <Doutrina>, ela apresenta os seguintes *slots*: <ano_publicacao>, que representa o ano em que a obra científica foi publicada; <assunto> que especifica o conteúdo abordado na obra científica; <autor> que determina quem é o autor da obra científica; <idioma> que informa qual é a língua em que a obra científica foi escrita; e <titulo> que corresponde ao título da obra científica, podendo se referir a título de livro, artigo, anais, revista, dissertação dentre outros.

Na figura 22 a seguir, é possível visualizar as propriedades da classe <Doutrina> que foram inseridas e configuradas através do editor de ontologias *Protégé*:

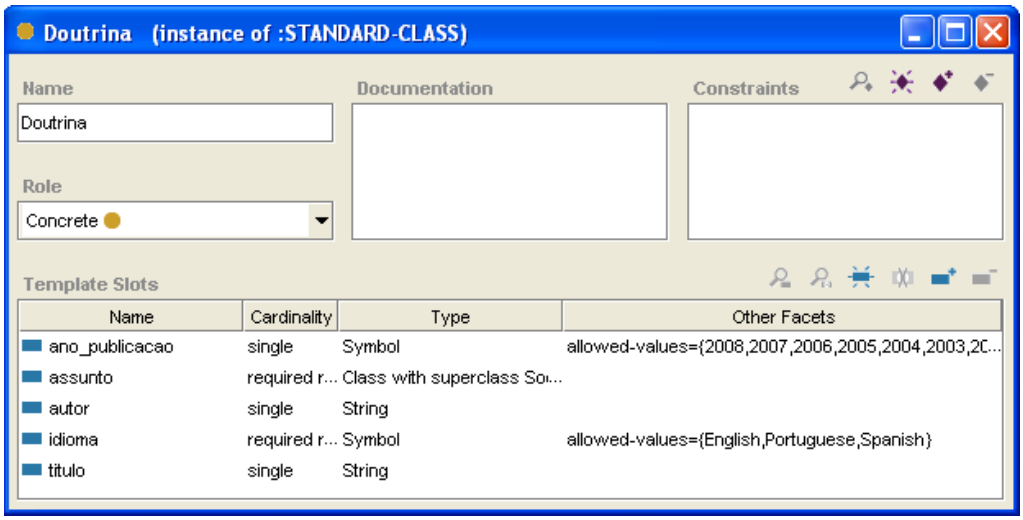

Figura 22. Propriedades da classe <Doutrina> na ontologia proposta. (Fonte: o autor)

Há de se observar, no entanto, que um artigo publicado em um livro possui dois títulos, um que se refere ao título do artigo e outro que se refere ao título do livro. Não obstante, as ontologias podem ajudar os agentes de *software* a entenderem se um determinado título se refere ao artigo ou ao livro em que este artigo foi publicado.

Para que isto seja possível, incorporou-se à subclasse <Artigo>, além de suas propriedades herdadas da classe <Doutrina>, o *slot* <origem_publicacao> para permitir não apenas identificar se o título se refere a um livro ou a um artigo, mas principalmente para recuperar referências de artigos de interesse publicados em um livro específico. Desta forma, definiu-se esta propriedade como sendo instâncias da subclasse <Livro>, <Anais> e <Revista>, podendo outras subclasses ser incorporadas posteriormente.

Com o objetivo de ampliar o escopo para atender às diversas necessidades de informação, incorporou-se à ontologia jurídica a classe <Conhecimento> não somente

para que fosse possível definir qual a área de conhecimento das obras científicas como também para permitir a sua posterior recuperação através da delimitação do assunto que esteja sendo abordado em uma determinada obra científica sobre crimes informáticos.

A classe <Conhecimento> representa as áreas do conhecimento que mantêm relações com os delitos informáticos, sendo a mesma elaborada a partir do material bibliográfico pesquisado pelo autor ao longo da elaboração desta dissertação cujo conteúdo estivesse direta ou indiretamente relacionado com os crimes informáticos. Desta sorte, esta classe possui como subclasse <Sociologico>, <Juridico> e <Tecnico>:

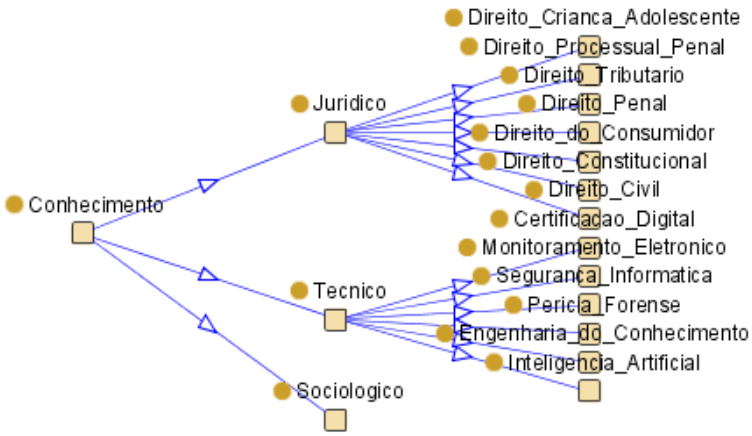

Figura 23. Hierarquia da classe <Conhecimento> na ontologia proposta. (Fonte: o autor)

Enfatiza-se aqui que as áreas de conhecimento cobertas pela ontologia jurídica se referem precisamente aos campos de estudos que possuem obras científicas abordando a questão dos crimes informáticos, embora a ênfase seja mais para a representação do conhecimento jurídico-penal, esta ampliação será útil para mapear a produção científica de diversas áreas do conhecimento referentes ao tema central deste domínio que trata dos crimes informáticos, permitindo o reuso da ontologia proposta.

Assim, a abordagem utilizada para desenvolver esta hierarquia de classe referente à classe <Conhecimento> foi o método da combinação, ou seja, primeiro se definiu as subclasses principais <Juridico> e <Tecnico>, sendo as suas respectivas subclasses agregadas na medida em que as instâncias de doutrina foram inseridas. Ao constatar que alguns artigos sobre crimes informáticos não se referiam a aspectos jurídicos e tampouco a aspectos técnicos, tornou-se necessária a inclusão da classe <Sociologico> para referenciar as obras científicas que focalizam os aspectos sociais.

Desta forma, foram inseridas aproximadamente 100 (cem) instâncias de obras científicas na classe <Doutrina> e suas respectivas fontes, sejam livros, anais, revistas

ou dissertação, sendo a maioria artigos tanto de conteúdo jurídico assim como de conteúdo técnico e sociológico, conforme ilustra a figura abaixo:

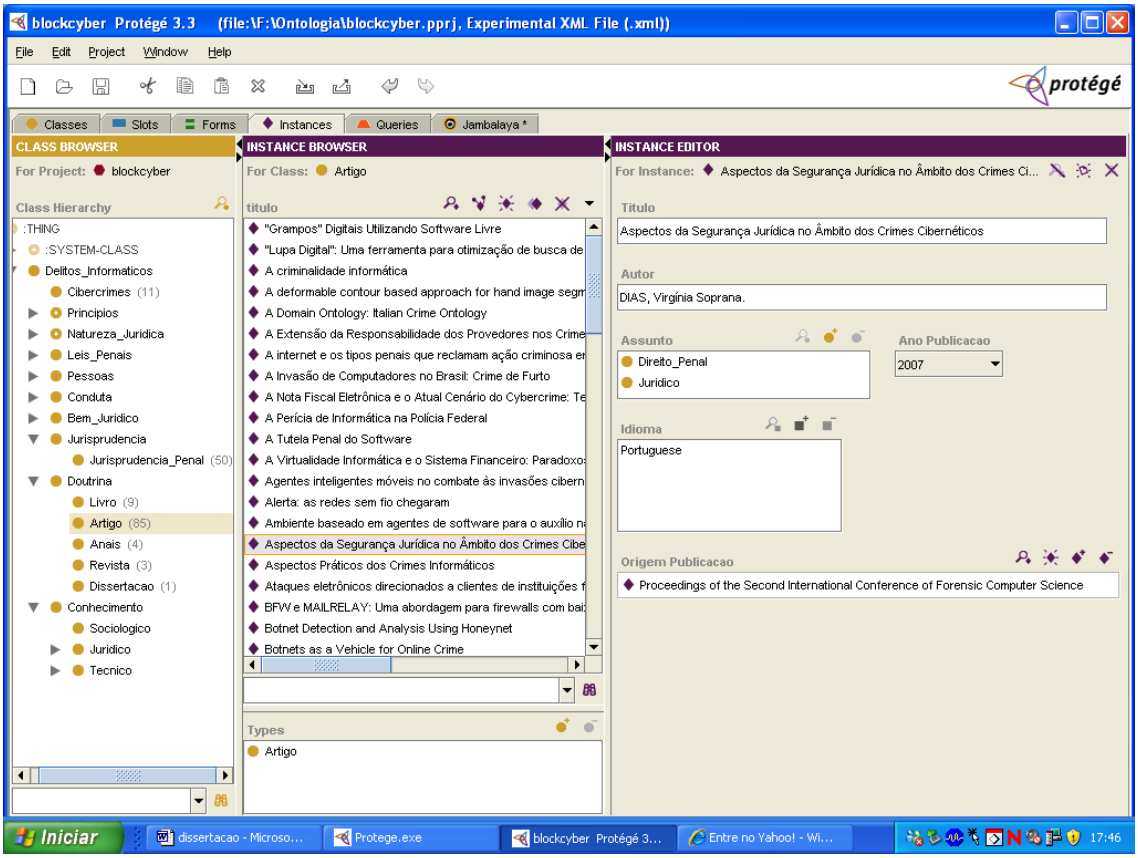

Figura 24. Instâncias de artigos científicos na ontologia proposta. (Fonte: o autor)

Em seguida, cuidou-se de definir as questões de competência da ontologia quanto à localização de obras científicas sobre delitos informáticos, objetivando, assim, ajudar o cidadão comum a encontrar referências de obras científicas úteis para esclarecer uma dúvida específica sobre um determinado delito informático.

Assim, por exemplo, caso um usuário necessite de indicação de obras científicas que contenham doutrina sobre crimes informáticos que ofendem o direito da criança e do adolescente, a ontologia consegue recuperar as obras que lhe sejam potencialmente úteis por se referirem especificamente a este assunto, independente do título da obra.

Desta maneira, ao formular a pergunta: “Quais as obras científicas sobre delitos informáticos relacionadas a crimes cometidos contra os direitos da criança e do adolescente?”, a ontologia apresenta como resposta três artigos científicos, um no idioma espanhol e os outros dois em português, todos envolvendo doutrina relativa aos crimes informáticos cometidos contra os direitos da criança e o adolescente:

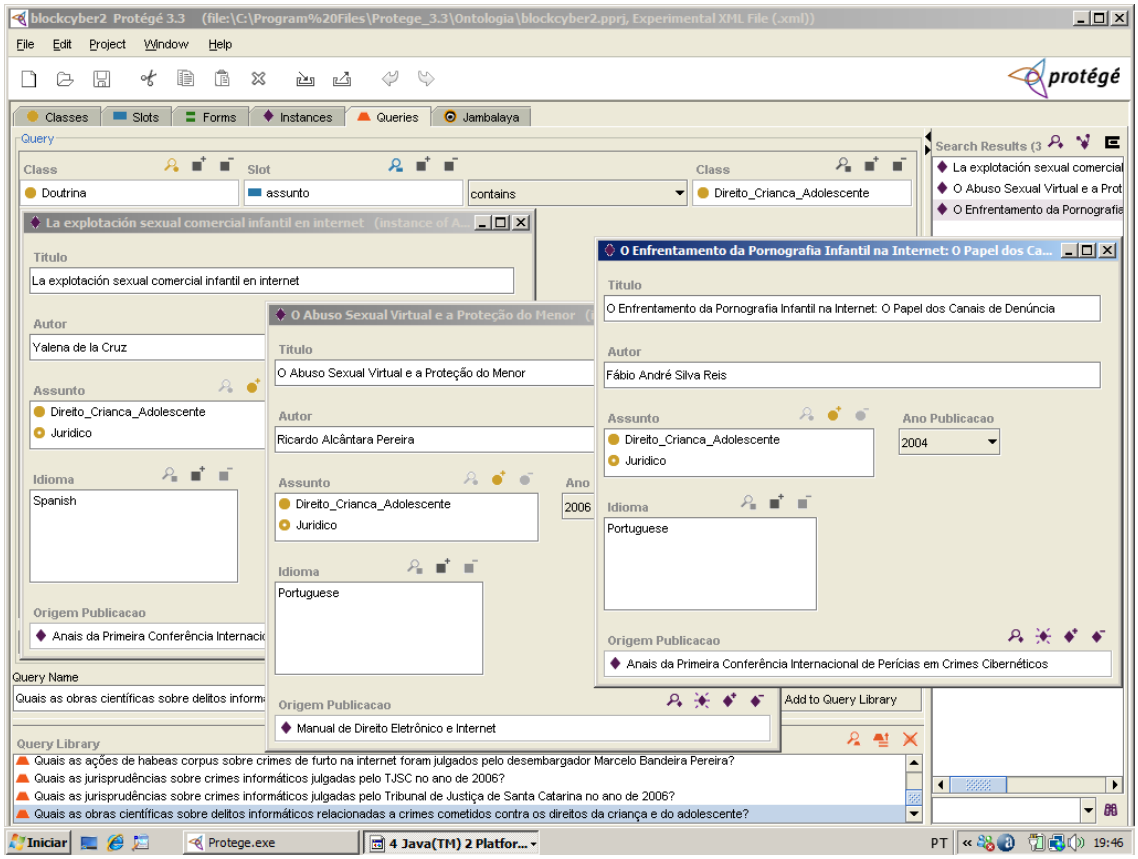

Figura 25. Base de conhecimento de doutrinas sobre delitos informáticos na ontologia. (Fonte: o autor)

Destaca-se, porém, que se o usuário não domina o idioma espanhol tampouco o idioma inglês não será útil que o sistema lhe indique referências doutrinárias nestas línguas. Assim, é possível especificar em qual idioma a pesquisa deverá ser realizada.

Outras questões de competência que a ontologia jurídica de delitos informáticos é capaz de responder são as seguintes:

5 Quais as obras científicas cujo título inicia (ou termina) com uma determinada palavra ou expressão? Exemplo: “Crimes Informáticos”;

6 Quais as obras científicas que foram publicadas no ano X? Exemplo: “2007”.

7 Quais os artigos sobre crimes informáticos que foram publicados em um determinado livro? Exemplo: “Manual de Direito Eletrônico e Internet”;

8 Quais as obras científicas sobre crimes informáticos escritas pelo autor X? Exemplo: “Túlio Lima Vianna”.

9 Quais as obras científicas sobre crimes informáticos que abordam um determinado assunto? Exemplo: “Segurança Informática”.

4.7 Recuperação de jurisprudências

As jurisprudências consistem em decisões já proferidas pelos tribunais e que muitas vezes são utilizadas para apoiar e orientar os juízes no momento de proferirem as suas decisões sobre uma matéria específica a qual já tenha sido apreciada pelo tribunal.

Embora a jurisprudência seja considerada uma fonte formal do direito, não basta ao juiz dizer que decide de uma determinada maneira porque outro juiz assim já decidiu, ele precisa fundamentar as suas decisões para que elas tenham validade jurídica.

Assim, a Constituição Federal estabelece em seu art. 93, inc. IX, que todas as decisões dos órgãos do Poder Judiciário serão fundamentadas sob pena de nulidade.

No entanto, nada obsta ao juiz utilizar os mesmos fundamentos que foram expostos por outro julgador para servir de base para a sustentação da sua decisão.

Através da pesquisa jurisprudencial realizada durante o terceiro capítulo desta dissertação, foi possível constatar que existem algumas decisões judiciais teratológicas dos tribunais pátrios quanto o assunto envolve os crimes informáticos, pois na ânsia de praticar a justiça, às vezes os juízes põem em risco a legalidade e a segurança jurídica.

Há de se considerar ainda a necessidade de atualização do conhecimento jurídico-penal no âmbito dos delitos informáticos por parte dos próprios membros do Poder Judiciário, já que alguns provêm de uma época onde a Internet sequer existia.

Os tribunais possuem a tradição de disponibilizar na rede os seus julgados para que possam ser consultados por todos os interessados, porém, os mecanismos de busca empregados são feitos de forma sintática, através de palavras-chave, trazendo conteúdo que muitas vezes não interessa ao cidadão que necessita de uma informação precisa e contextualizada.

Existe também outro problema que é o excesso de documentos jurídicos que constam no banco de dados dos tribunais e que podem atrapalhar consideravelmente e até mesmo impedir o usuário do sistema de encontrar a informação desejada.

Para solucionar todas estas questões é que aparece como alternativa o uso da *web* semântica com a utilização de padrões de linguagem XML e ontologias jurídicas, pois os documentos contendo as decisões judiciais envolvendo delitos informáticos também podem ser marcados com propriedades que permitam a sua recuperação de forma mais eficiente através do emprego de ontologias.

No âmbito da IA e direito, uma técnica que é bastante útil na recuperação de jurisprudências é o raciocínio baseado em casos. Acerca dos sistemas de raciocínio

baseado em casos, pode-se dizer que eles "imitam o ato humano de recordar um episódio prévio para resolver um determinado problema devido à forte semelhança entre eles. No processo de recordar uma situação semelhante quando comparado a uma nova, sistemas de RBC simulam o raciocínio analógico". (WEBER, 2000, p. 216)

Já se comentou que, "no atual estágio da Web Semântica, existe a possibilidade de se obter uma maior eficácia na recuperação de informações jurídicas e na construção de um sistema de conhecimento jurídico a partir do uso de ontologias juntamente com as técnicas de RBC". (BRAGA, RAMOS JÚNIOR & COELHO, 2007, p. 7)

Acontece que o simples uso da técnica de RBC não é suficiente para abranger toda a complexidade do domínio dos delitos informáticos já que este técnica utiliza o raciocínio analógico e o uso da analogia no direito penal é vedado e somente é admissível a interpretação analógica quando assim expressamente permitir o tipo penal.

Desta forma, as ontologias podem servir para apoiar um sistema de raciocínio baseado em casos para torná-lo mais eficiente, aumentando a similaridade ao considerar as propriedades dos crimes informáticos, o que reduziria a possibilidade de erro e evitaria cometer o que os juristas denominam de analogia *in malam parte*, isto é, o uso da analogia para prejudicar a parte, aplicando a norma penal a uma conduta atípica.

É importante mencionar que nesta dissertação não se pretende desenvolver um sistema de raciocínio baseado em casos apoiado por ontologias jurídicas, entretanto, uma vez que os crimes informáticos estão sendo representados ontologicamente a partir de sua natureza jurídica, poderão servir de suporte ao desenvolvimento de tal sistema.

Enfatiza-se então que não se tem por objetivo aqui recuperar jurisprudências sobre crimes informáticos através de raciocínio analógico ou grau de semelhança, mas sim representar formalmente estas jurisprudências através da ontologia jurídica para permitir a posterior recuperação do seu conteúdo a partir de suas propriedades.

Depois de criar a classe <Jurisprudencia>, cuidou-se então de definir as suas **propriedades**, quais sejam: o nome do tribunal, o tipo do processo, o número do processo, o nome do relator, a ementa, o resultado da decisão e a data do julgado. Em síntese, o nome do tribunal identifica qual foi o tribunal que proferiu a decisão (exemplos: TJSC, TJMG, STJ, etc), o tipo do processo define qual o nome da ação ajuizada ou do recurso interposto (exemplos: *Habeas Corpus*, Agravo de Instrumento, Apelação Criminal etc), o número do processo corresponde ao número fornecido pelo tribunal que permite a identificação do processo e o seu acompanhamento processual (exemplo: 2006.022998-3 etc), o nome do relator identifica quem foi o magistrado que

atuou como relator no processo (exemplos: Juíza Ângela M. Silveira, Desembargador Marco A. Bellizze, Ministro Gilson Dipp); a ementa corresponde a um sumário onde é descrito sucintamente o conteúdo da decisão judicial (exemplo: APELAÇÃO CRIMINAL DEFENSIVA. DELITO DE INTERCEPTAÇÃO DE COMUNICAÇÕES DE INFORMÁTICA – ARTIGO 10, CAPUT, DA LEI Nº 9.296/1996. PROVA MANIFESTAMENTE INSUFICIENTE. ABSOLVIÇÃO QUE SE IMPÕE); o resultado indica qual foi o pronunciamento final da decisão judicial proferida acerca da ação ou do recurso, e, finalmente, a data do julgado aponta quando a decisão foi julgada, não se confundindo com a data de sua publicação.

Em relação à subclasse <Jurisprudencia_Penal>, além de possuir os atributos acima descritos, ela se diferencia dos demais tipos de jurisprudência porque ela se refere em geral a um ou mais crimes que violam os bens jurídicos tutelados pela lei penal. Desta forma, agregou-se a esta subclasse as propriedades <crime> e <bem_juridico>:

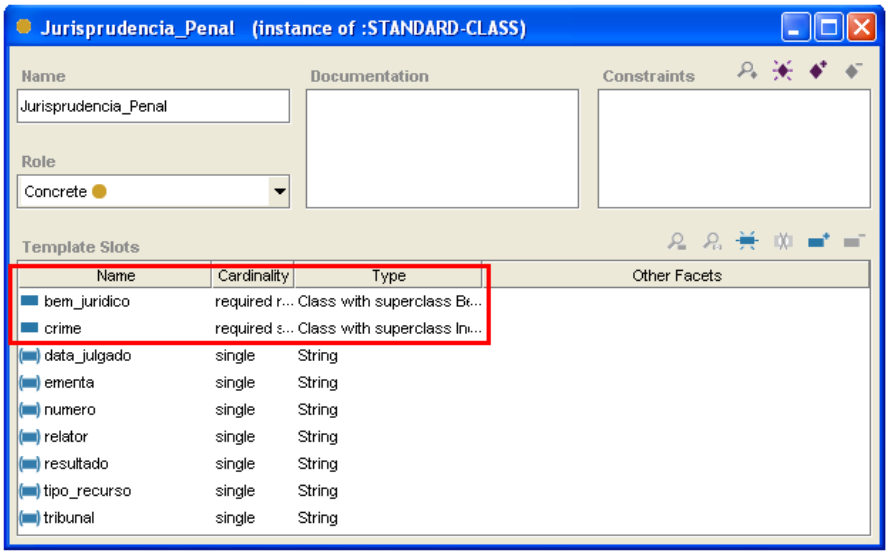

Figura 26. Propriedades da subclasse <*Jurisprudencia_Penal*>, com destaque em vermelho para as suas peculiaridades representadas pelos *slots* <*bem_juridico*> e <*crime*> na ontologia. (Fonte: o autor)

Uma das finalidades da ontologia jurídica é recuperar documentos jurídicos referentes às decisões judiciais sobre crimes informáticos dentro do contexto do conhecimento jurídico-penal. Portanto, a inclusão dos *slots* <crime> e <bem_juridico> na subclasse <Jurisprudencia_Penal> é de grande importância porque permitirá recuperar os documentos jurídicos relativos às jurisprudências sobre um crime específico e a respeito de decisões judiciais que ofendem os bens jurídicos tutelados.

Depois de definir e configurar as propriedades da classe <Jurisprudencia> e da

subclasse <Jurisprudencia_Penal>, realizou-se uma pesquisa jurisprudencial em vários tribunais brasileiros, colhendo-se precisamente 50 (cinqüenta) decisões judiciais sobre crimes informáticos para testar a recuperação de jurisprudências que foram inseridas como instâncias através do editor de ontologias *Protégé*, conforme ilustra a figura 27:

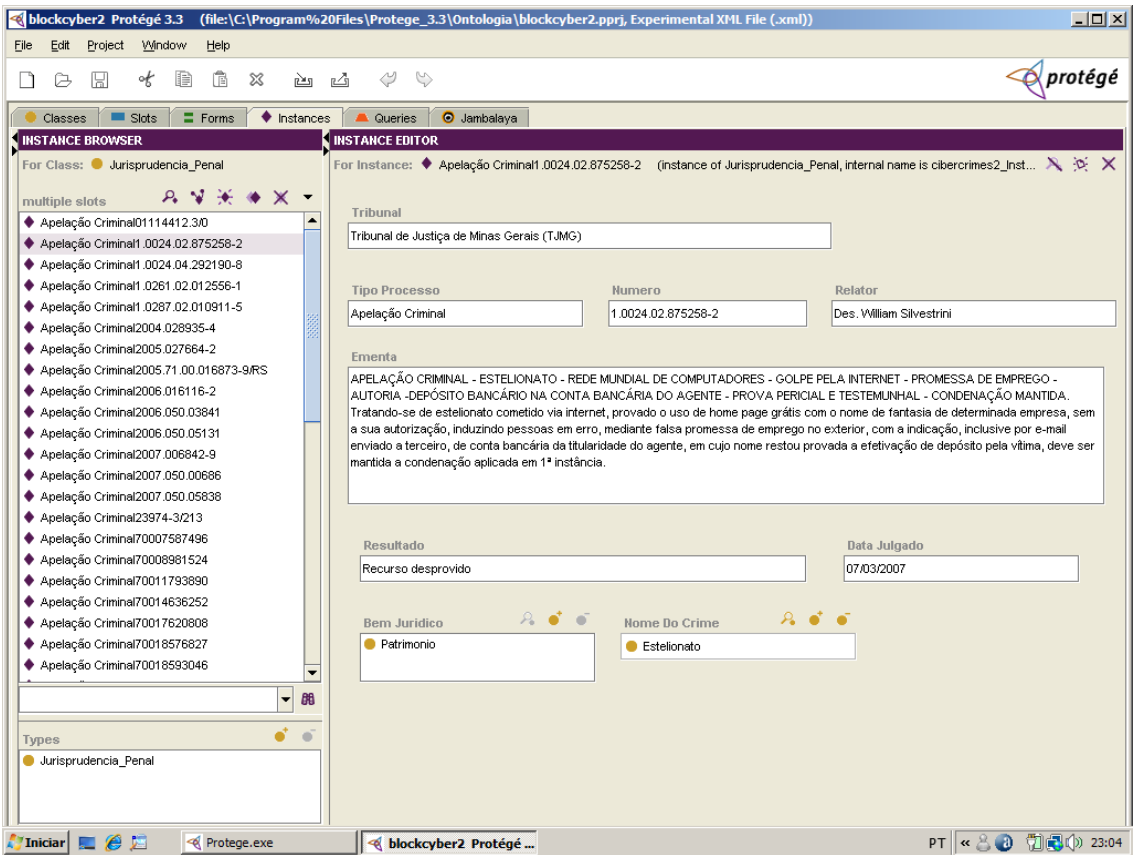

Figura 27. Instâncias de jurisprudências na ontologia jurídica de delitos informáticos. (Fonte: o autor)

O passo seguinte consistiu em formular algumas questões de competência a serem respondidas pela ontologia com o objetivo de ajudar tanto os juízes e desembargadores a recuperar com precisão e eficiência os julgados sobre crimes informáticos dos tribunais pátrios como também os promotores de justiça a promover uma ação penal contra um delito informático, e, igualmente, os advogados e demais profissionais que necessitem de esclarecimento sobre a jurisprudência neste domínio, inclusive ao cidadão leigo que queira conhecer se já houve algum pronunciamento judicial sobre determinado crime informático e qual entendimento dos tribunais pátrios.

A figura a seguir exibe uma ilustração de uma das questões de competências respondida pela ontologia acerca do entendimento do Superior Tribunal de Justiça acerca da competência para julgar crimes de furto cometidos pela Internet, onde são

recuperados três julgados daquele tribunal acerca desta questão específica, sendo apresentados a seguir outros exemplos de questões que a ontologia consegue esclarecer:

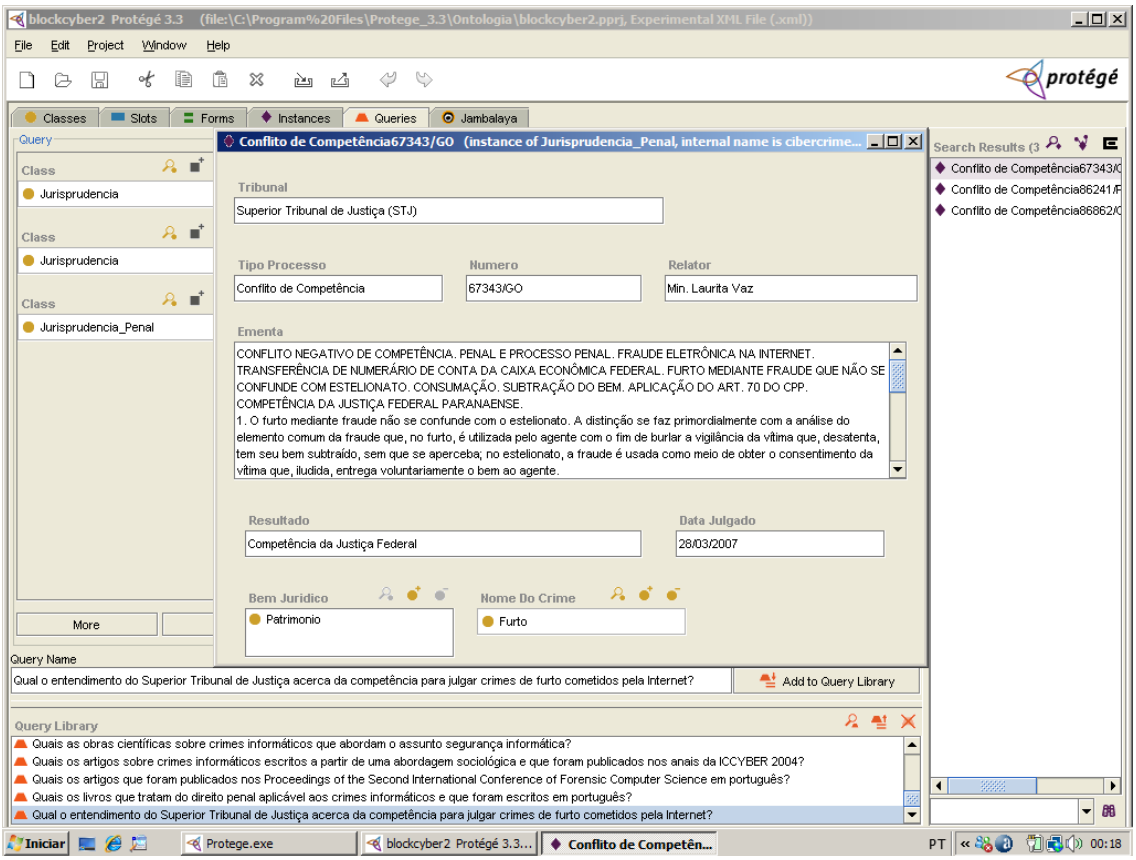

Figura 28. Resposta à questão de competência: "Qual o entendimento do Superior Tribunal de Justiça acerca da competência para julgar crimes de furto cometidos pela Internet?". (Fonte: o autor)

1) Quais as jurisprudências sobre crimes informáticos contra o bem jurídico A? Por exemplo: Crimes informáticos contra a honra das pessoas na Internet;

2) Quais as jurisprudências sobre o crime informático B? Exemplo: "O crime de inserção de dados falsos em sistemas de informações (art. 313-A do Código Penal)";

3) Quais os tipos de processo C sobre o crime informático B que foram julgados no tribunal D tendo como relator E? Exemplo: "Ações de *Habeas Corpus* sobre crime de furto na Internet que foram julgados no TJRS pelo relator desembargador Marcelo Pereira Bandeira".

4) Qual o entendimento do relator E do tribunal D sobre o crime informático B? Exemplo: "Entendimento do relator desembargador William Silvestrini do TJMG sobre o crime de estelionato praticado através da Internet".

5) Quais as jurisprudências sobre o crime informático B, julgadas tribunal D no ano F? Exemplo: "Jurisprudências sobre calúnia julgadas pelo TJSC no ano de 2006".

4.8 Leis penais aplicáveis

A tarefa de identificar as leis penais aplicáveis aos crimes informáticos foi executada através do estudo realizado no terceiro capítulo da dissertação, considerando apenas a legislação penal vigente no país para fins de estudo e construção da ontologia.

Por outro lado, é importante ressaltar que sendo aprovada a legislação de delitos informáticos no Brasil, a ontologia será atualizada para abranger as novas modalidades de crimes informáticos que forem inseridas no ordenamento jurídico brasileiro, pois, uma das características das ontologias é que além do conhecimento do domínio ser compartilhado, elas devem se manter atualizadas para que sejam sempre útil e eficaz.

Assim, por exemplo, foram definidas como subclasses de Leis penais aplicáveis aos crimes informáticos: Código Penal (Decreto-lei nº 2.848, de 07 de dezembro de 1940 e suas alterações), Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990, com suas alterações); a Lei nº 9.296, de 24 de julho de 1996 (Lei de Interceptação das Comunicações) e a Lei nº 9.609, de 19 de fevereiro de 1998 (Lei do *Software*) dentre outras legislações penais aplicáveis:

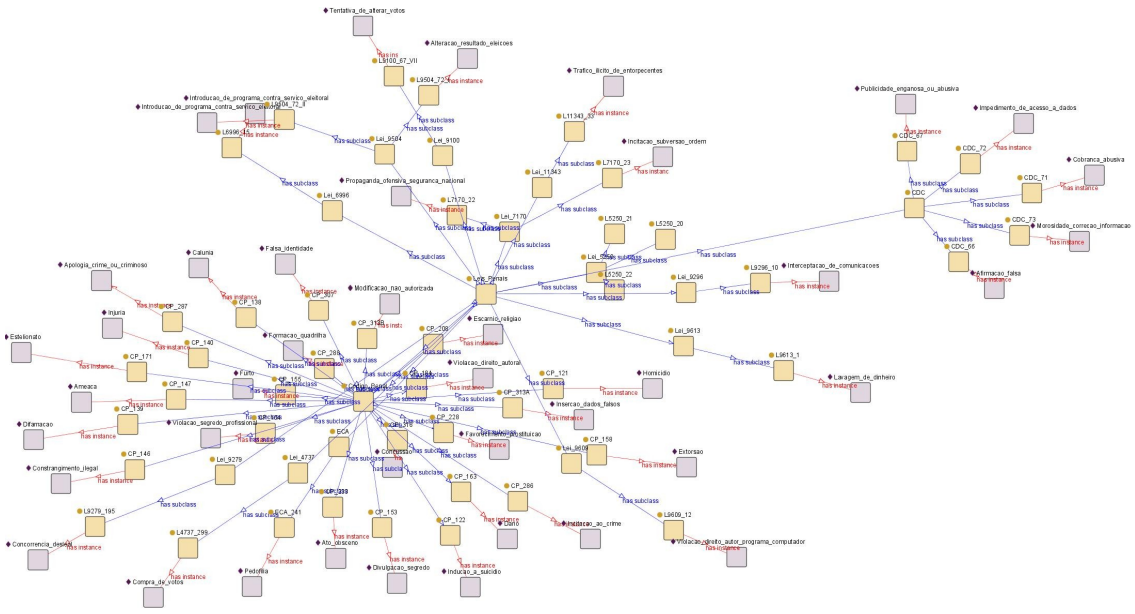

Figura 29. Leis penais aplicáveis aos delitos informáticos na ontologia proposta. (Fonte: o autor)

No que tange às **propriedades** desta classe e de suas respectivas subclasses, é oportuno destacar que todas estas apresentam como característica o fato de possuírem, no mínimo, uma conduta típica descrita na lei que é denominada tipo penal e uma

respectiva pena, a qual se aplica quando um comportamento proibido em lei é praticado.

Para que as ontologias jurídicas obtenham êxito na identificação da lei penal aplicável, é importante também definir qual o âmbito de sua aplicação. Isso poderá ser feito ao estabelecer quais os bens jurídicos que são tutelados por determinada lei.

A vantagem de definir o âmbito de aplicação das leis penais é importante porque auxilia o cidadão leigo a tomar conhecimento sobre quais as legislações penais vigentes sobre determinado assunto que esteja relacionado aos crimes informáticos, como, por exemplo, a legislação penal aplicável aos crimes contra a honra ou contra o patrimônio.

Isto parece uma tarefa muito fácil para um profissional do direito, mas pode ser bastante complicado para o cidadão que não detém conhecimento na área jurídica.

Quando o cidadão leigo procura por informação sobre um determinado crime, é comum recorrer imediatamente ao Código Penal já que nele está contida grande parte dos crimes tipificados no ordenamento jurídico nacional. Entretanto, há outras leis penais que prescrevem condutas criminosas e determinam as suas respectivas penas.

No caso de se deparar com um crime de violação de direito de autor de programa de computador, por exemplo, o indivíduo, ao consultar o Código Penal, poderá se enganar ao supor que o art. 184 do CP seja aplicável ao caso, por se tratar justamente de um crime de violação de direito de autor cujo tipo penal é "violar direito autoral".

Ocorre que, conforme já estudado no terceiro capítulo da dissertação, existe uma lei especial que regulamenta especificamente o crime de violação de direito de autor de programa de computador, previsto no art. 12 da Lei nº 9.609/98. É evidente que se o cidadão não conhece esta lei, irá deduzir que o art. 184 do CP possa ser aplicado. Além disso, mesmo que a conheça, poderá ter dúvidas sobre qual das duas leis se aplica.

Esta ambigüidade pode ser resolvida mediante o uso da *web* semântica que possa orientar os agentes de *software* na aplicação das regras da especialidade, bem como a partir do uso de ontologias para determinar qual o objeto do direito autoral que está sendo tutelado e assim conduzir o cidadão a obter a resposta jurídica apropriada.

Outro problema é o desconhecimento da lei, que é inescusável. Quanto aos crimes contra a propriedade intelectual, por exemplo, argumenta-se que as condutas típicas de "violar direito autoral" e "violar direito de autor de programa de computador" possuem um tipo penal demasiadamente vago, caracterizando-se como normas penais em branco, ou seja, cujo conceito jurídico de violar direito de autor precisa ser complementado pela lei civil que tutela a propriedade intelectual (Lei nº 9.610/98).

No que concerne a esse assunto, observa-se que a complexidade destes tipos

penais é muito bem apontada por Túlio Lima Vianna (2006, p. 942) ao comentar que "a sua leitura implica em uma jornada da norma penal em branco à lei civil que a complementa, mas que, muita vez, remeteria o intérprete a uma licença com características contratuais na qual o autor dispensaria a tutela legal dos seus direitos patrimoniais, isto é, conduziria a uma interpretação extremamente complexa até mesmo para profissionais do Direito, e praticamente impossível para o cidadão leigo, a quem a função de garantia dos tipos penais deveria contemplar".

Neste sentido, o TJMG, ao julgar a apelação criminal nº 1.0172.04.910501-5/001, reconheceu que a expressão "violar direitos autorais" é bastante vaga e até mesmo especialistas em Direito Penal não poderiam precisar o seu âmbito de significação, quanto mais um vendedor ambulante sem educação jurídica, sendo escusável o desconhecimento da lei se esta não for suficientemente clara para permitir que qualquer um do povo possa compreender ainda que potencialmente seu significado.

Portanto, tendo em vista que o desconhecimento da lei é, em regra, inescusável, enfatiza-se a importância da construção de ontologias jurídicas para esclarecer questões legais e para que todos possam conhecer as condutas criminosas cometidas com o uso da informática, fazendo com que qualquer cidadão possa ter acesso ao conhecimento jurídico adequado.

4.9 Natureza jurídica dos delitos

Conforme visto no terceiro capítulo desta dissertação, os crimes informáticos podem ser classificados: quanto ao sujeito (crime comum ou próprio), culpabilidade (crime culposo ou doloso), comportamento (crime comissivo ou omissivo), lesividade (crime de perigo ou de dano), subjetividade (crime unissubjetivo ou purissubjetivo), tentativa (admite ou não admite), consumação (crime material, formal ou de mera conduta), subsistência (crime unissubsistente ou plurissubsistente), efeitos (crime instantâneo, permanente ou instantâneo de efeito permanente), ação penal (pública ou privada, e, sendo pública, se é ação é condicionada ou incondicionada), potencial ofensivo (crime de menor potencial ofensivo ou de maior gravidade) e, finalmente, quanto ao elemento informático (se o crime informático é puro, impuro ou misto).

A hierarquia de classes na classe <Natureza_Juridica> foi realizada a partir de uma abordagem *top-down*, podendo ser visualizada na imagem apresentada a seguir:

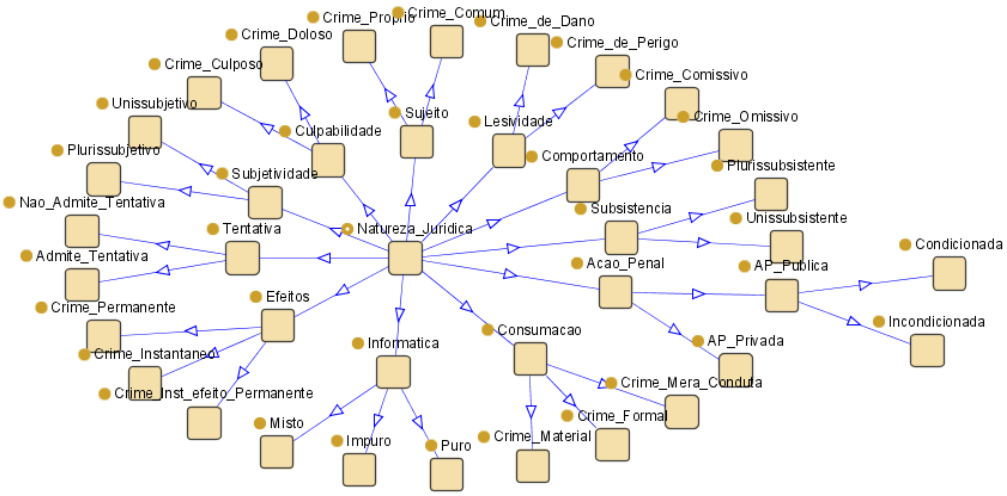

Figura 30. Classificação dos crimes pela natureza jurídica na ontologia proposta. (Fonte: o autor)

Através da ontologia proposta, torna-se possível identificar as características dos crimes informáticos e esclarecer ao cidadão o significado dos termos jurídicos.

A importância desta classificação é que, por exemplo, a identificação dos crimes próprios e comuns quanto ao sujeito permitem determinar quais pessoas podem ser sujeitos ativos do crime, ou seja, se qualquer indivíduo pode ser autor do delito ou se o tipo penal exige determinada qualidade ou condição especial do sujeito.

Assim, criou-se a classe <Pessoas> para definir quais as pessoas que podem ser sujeitos ativos dos delitos e quais podem ser vítimas de determinado crime informático.

Utiliza-se como exemplo os crimes informáticos contra a Administração Pública: a inserção de dados falsos em sistemas de informações (art. 313A do CP); a modificação de tais sistemas (art. 313B do CP) e o crime de concussão (art. 316 do CP).

Uma das questões importantes que a ontologia poderá esclarecer neste domínio é, por exemplo, o conceito de funcionário público para fins penais, o qual deverá ser representado em conformidade com o disposto no art. 327 do Código Penal.

Esta norma penal, por sua vez, estabelece que, para efeitos penais, considera-se funcionário público quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública; sendo que o §1º deste artigo determina que se equipara a funcionário público quem exerce cargo, emprego ou função pública, em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública. Esta equiparação é importante porque delimita com exatidão quem se enquadra ou não no

conceito de funcionário público para fins de responsabilidade criminal.

Recorda-se que em 2006, um *hacker* identificado como *Lady Diana*, invadiu o sistema de informática do governo do Rio Grande do Norte e modificou as páginas iniciais de diversos órgãos vinculados ao Poder Executivo. Em seguida, argumentou-se na mídia que a conduta deste indivíduo estaria tipificada no art. 313-B do Código Penal. Entretanto, conforme já se havia comentado, tratou-se de uma informação equivocada, porque o artigo 313-B do Código Penal é um crime próprio e o *hacker* não poderia ser equiparado a funcionário público para fins penais. (RAMOS JÚNIOR, 2007, 67-68)

Acontece que muito se divulgam, na mídia, as condutas típicas aplicáveis aos crimes informáticos, porém, sem esclarecer realmente à sociedade as características e o âmbito de aplicação destes delitos, podendo ocasionar uma ilusão de segurança jurídica.

Quanto aos diversos conceitos e categorias de crimes que existem, o que se verifica é que muitos conceitos jurídicos não constam expressamente na lei, eles são resultado da construção doutrinária (como, por exemplo, a classificação dos crimes informáticos em puro, impuro ou misto) ou mesmo do entendimento jurisprudencial.

Assim, as ontologias jurídicas podem ser utilizadas para orientar o profissional do direito e ao cidadão em geral, por exemplo, quanto às características dos crimes informáticos cometidos contra a Administração Pública, conforme ilustra a figura 31:

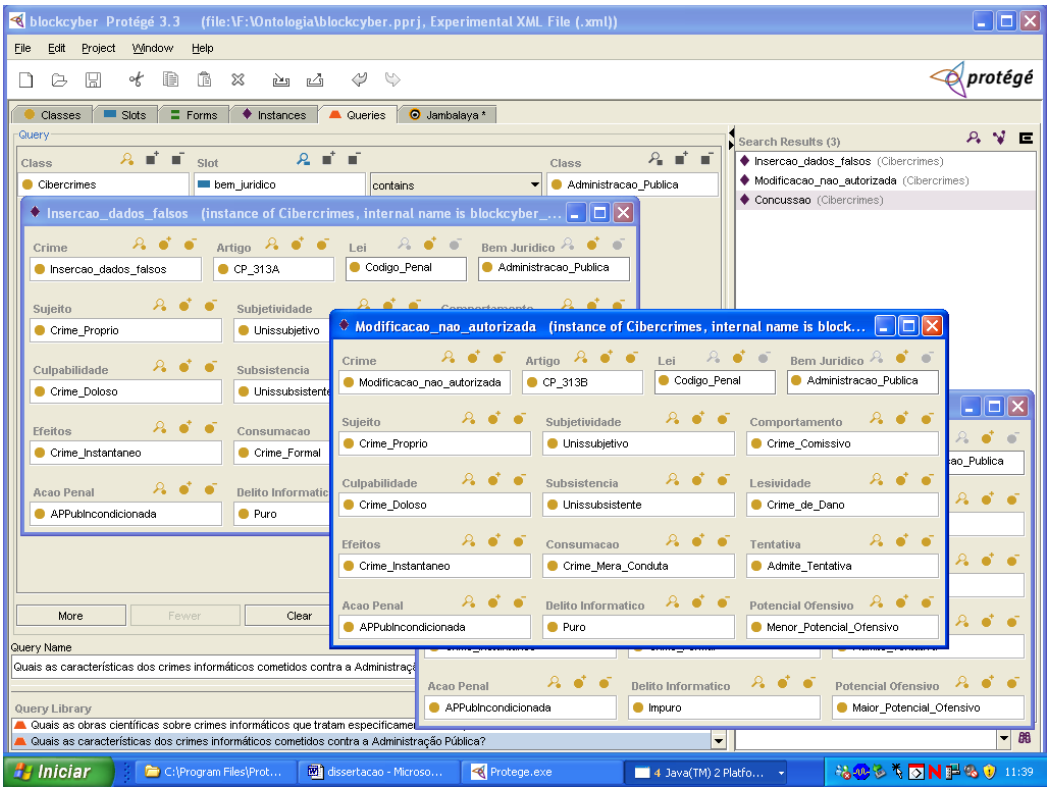

Figura 31. Resposta da ontologia jurídica de delitos informáticos à questão de competência: "Quais as características dos crimes informáticos cometidos contra a Administração Pública?". (Fonte: o autor)

A partir da pergunta objetiva sobre as características dos crimes informáticos cometidos contra a Administração Pública, a ontologia é capaz de explicitar todos os aspectos sobre a natureza jurídica de cada um destes delitos. Por exemplo, em relação à consumação do crime, ela esclarece se o crime é material, formal ou de mera conduta.

Desta forma, a ontologia também se presta para fins didáticos, pois o estudante de direito também poderá consultá-la para sanar as suas dúvidas sobre estes crimes. Assim, a ontologia lhe orientará a concluir, por exemplo, que sendo o crime de inserção de dados falsos em sistemas de informações previsto no art. 313-A do CP um crime formal, isto significa que este delito se consuma independentemente do agente ter conseguido ou não o resultado pretendido (obtenção de vantagem ou dano).

Por outro lado, esta informação apenas é útil para o estudante ou profissional do direito e para aquelas pessoas que já conhecem o significado do conceito jurídico utilizado. Quanto aos que não conhecem os termos empregados neste domínio, a ontologia jurídica irá explicitá-los, fornecendo as suas respectivas definições.

4.10Explicitação dos conceitos jurídicos

O extenso corpo normativo existente torna difícil até mesmo para o profissional do direito conhecer todas as leis e se manter atualizado sobre todos os assuntos jurídicos gerais. Esta dificuldade é bem maior para um cidadão leigo.

Conforme já estudado no primeiro capítulo da dissertação, há projetos de ontologias jurídicas que também estão direcionados para resolver questões semelhantes.

De um lado, o modelo ONTOINFOJUS propõe uma ontologia para atualização do conhecimento legal do advogado; por outro, a ontologia desenvolvida por Cerqueira e Bax (2007) explicita conceitos e valores jurídicos relativos às leis e atos normativos.

Embora os projetos sejam interessantes, optou-se por desenvolver um esquema próprio para a representação do conhecimento jurídico-penal no contexto dos delitos informáticos tendo em vista as particularidades e características deste domínio.

Quanto à atualização do conhecimento legal do advogado, verifica-se que, em se tratando de delitos informáticos, enquanto não é aprovado o projeto de lei, o profissional do direito tem de lidar com a legislação velha e atual vigente, até então não se havia feita nenhuma interpretação da lei com o uso de ontologias para resolver o

problema da aplicabilidade da lei penal neste domínio, sendo esta questão importante e diferencial da ontologia jurídica de delitos informáticos em relação aos demais projetos.

Por sua vez, no que se refere aos conceitos e valores jurídicos, embora algumas das definições empregadas neste domínio estejam presentes na lei e em atos normativos, observa-se que a grande maioria decorre de construção doutrinária e jurisprudencial.

A ontologia jurídica de delitos informáticos pretende esclarecer os diversos conceitos jurídicos que são utilizados tanto na doutrina quanto na jurisprudência, porém não se ignora o fato de que pode acontecer de haver um determinado conceito onde haja interpretação divergente entre os tribunais ou mesmo entre os doutrinadores, entretanto esta questão é resolvida com uma nota explicativa apresentada quando for necessário.

Desta forma, são explicitados na ontologia os conceitos jurídicos que são utilizados no domínio dos delitos informáticos e que foram apresentados no terceiro capítulo da dissertação, tornando-os acessíveis aos usuários e compreensíveis tanto por estes quanto pelos agentes de *software*:

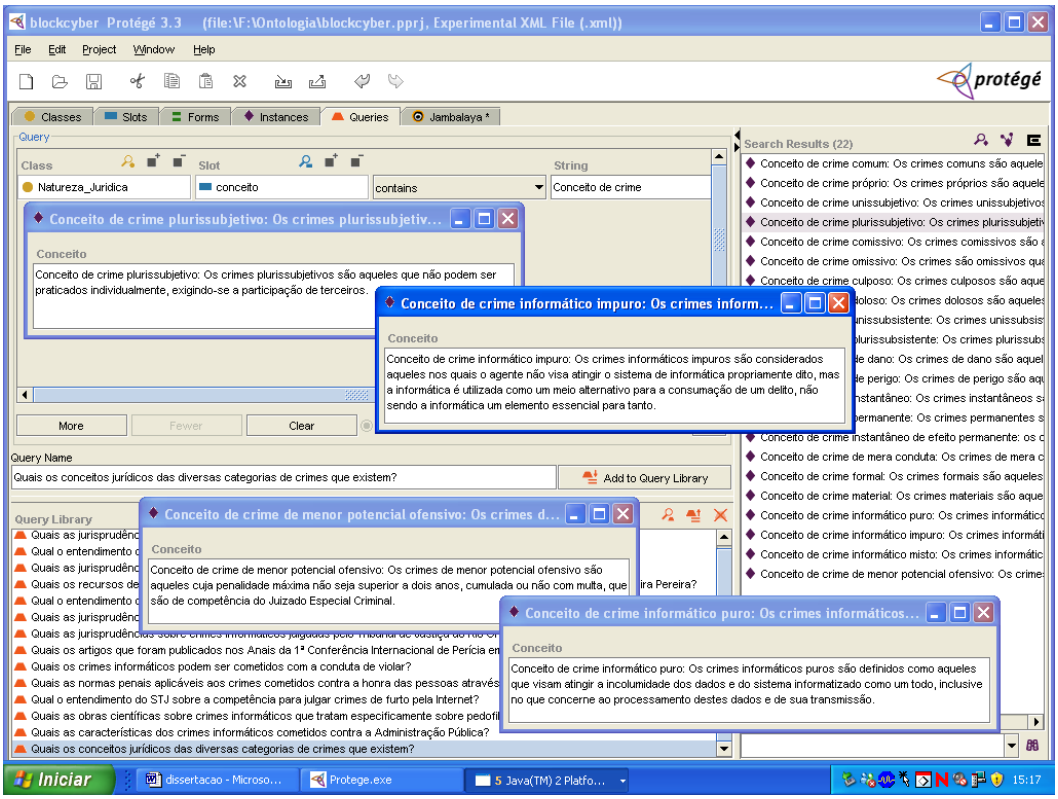

Figura 32. Resposta da ontologia jurídica de delitos informáticos à questão de competência: "Quais os conceitos jurídicos das diversas categorias de crimes que existem?" (Fonte: o autor)

Conforme acima ilustrado, a ontologia jurídica de delitos informáticos é capaz de explicitar quais os conceitos jurídicos das diversas categorias de crimes que existem

e que são utilizados na ontologia proposta, tornando estes conceitos disponíveis.

4.11 Tipicidade dos crimes informáticos e validação da ontologia

A ontologia jurídica de delitos informáticos também permite identificar o crime pelo verbo contido nos diversos tipos penais que prescrevem condutas criminosas que podem ser consideradas crimes informáticos, os quais foram incorporados na base de conhecimento a partir do estudo sobre a aplicabilidade das leis penais a estes delitos.

A relevância desta função decorre do fato de que até então nenhum sistema baseado em conhecimento foi desenvolvido para esclarecer quais os crimes informáticos podem ser cometidos a partir dos verbos utilizados no Código Penal e nas demais leis penais brasileiras para tipificar os delitos e tampouco havia sido proposta qualquer ontologia voltada para o domínio dos delitos informáticos, objetivando resolver os principais problemas existentes quando o assunto se refere a estes crimes específicos.

No entanto, as questões de competência formuladas para resolver tais problemas estão adstritas às condutas que são suscetíveis de caracterizar crimes informáticos, já que a ontologia proposta se adstringe ao conhecimento jurídico-penal neste domínio. Porém, de igual modo, poderá ser reutilizada para ampliar o seu escopo de aplicação.

Após serem definidas e configuradas as propriedades da classe <Conduta>, quais sejam, <verbo>, <fato_tipico>, <lei_penal> e <artigo>, inseriu-se as instâncias de condutas cometidas a partir de verbos contidos nos tipos penais de crimes informáticos já identificados com base no estudo jurídico realizado no terceiro capítulo desta dissertação, partindo-se, em seguida, para a formulação das questões de competência:

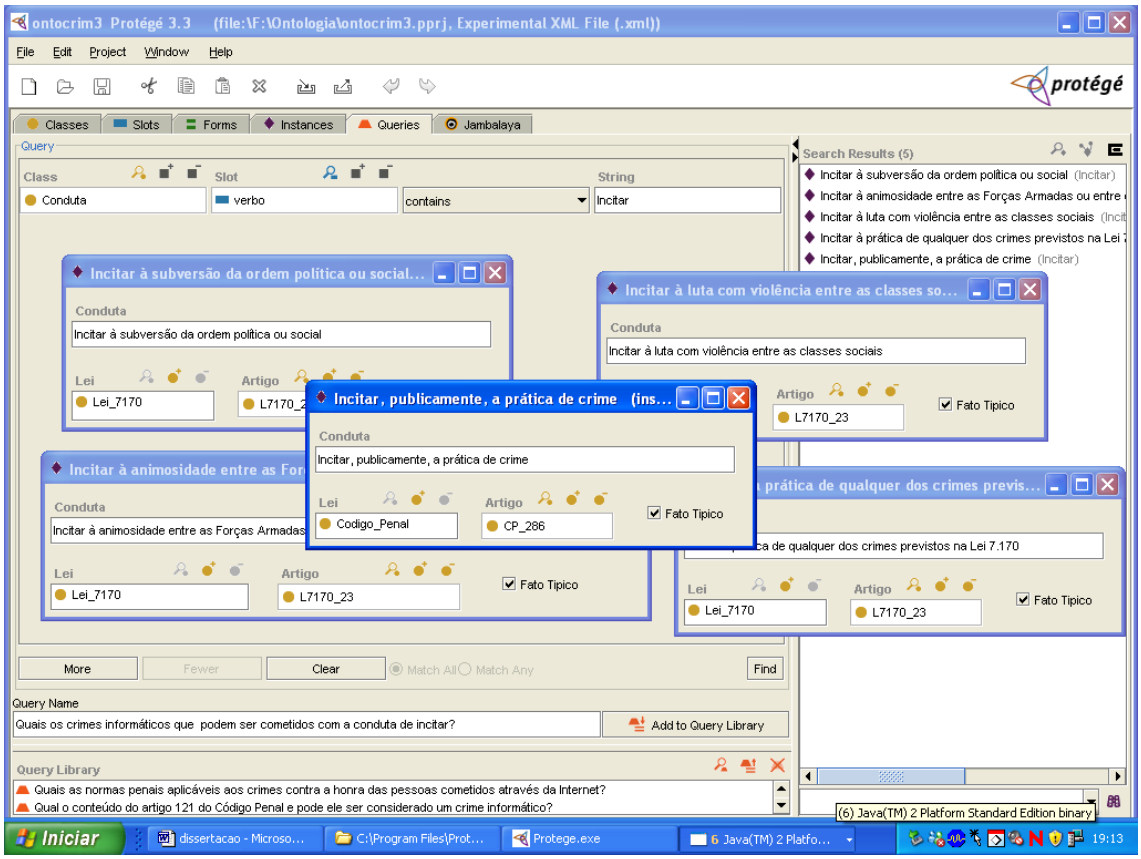

Figura 33. Identificação do crime pelo verbo contido no tipo penal na ontologia jurídica. (Fonte: o autor)

Na figura 33, destaca-se a resposta da ontologia jurídica de delitos informáticos para a seguinte questão de competência: "Quais os crimes informáticos que possuem o verbo "incitar" contido no núcleo do tipo penal?". A ontologia apresenta cinco instâncias de condutas que podem ser cometidas com o verbo incitar, abrangendo em sua resposta tanto o artigo 286 do Código Penal que contém no tipo penal o verbo "Incitar", quanto àqueles previstos no *caput* e incisos do art. 23 da Lei nº 7.170 e que também possui no tipo penal este verbo, contribuindo para esclarecer o usuário qual a lei penal aplicável.

Para fins de maior ilustração, toma-se outro exemplo. Ao se indagar quais os crimes informáticos podem ser cometidos através da conduta de "violar", a ontologia fornece como resposta exatamente os crimes informáticos que possuem este verbo contido no tipo penal, quais sejam: o art. 12 da Lei nº 9.609/98 (violação de direito de autor de programa de computador); o art. 184 do Código Penal (violação de direito autoral); e o art. 154 do CP (violação de segredo profissional):

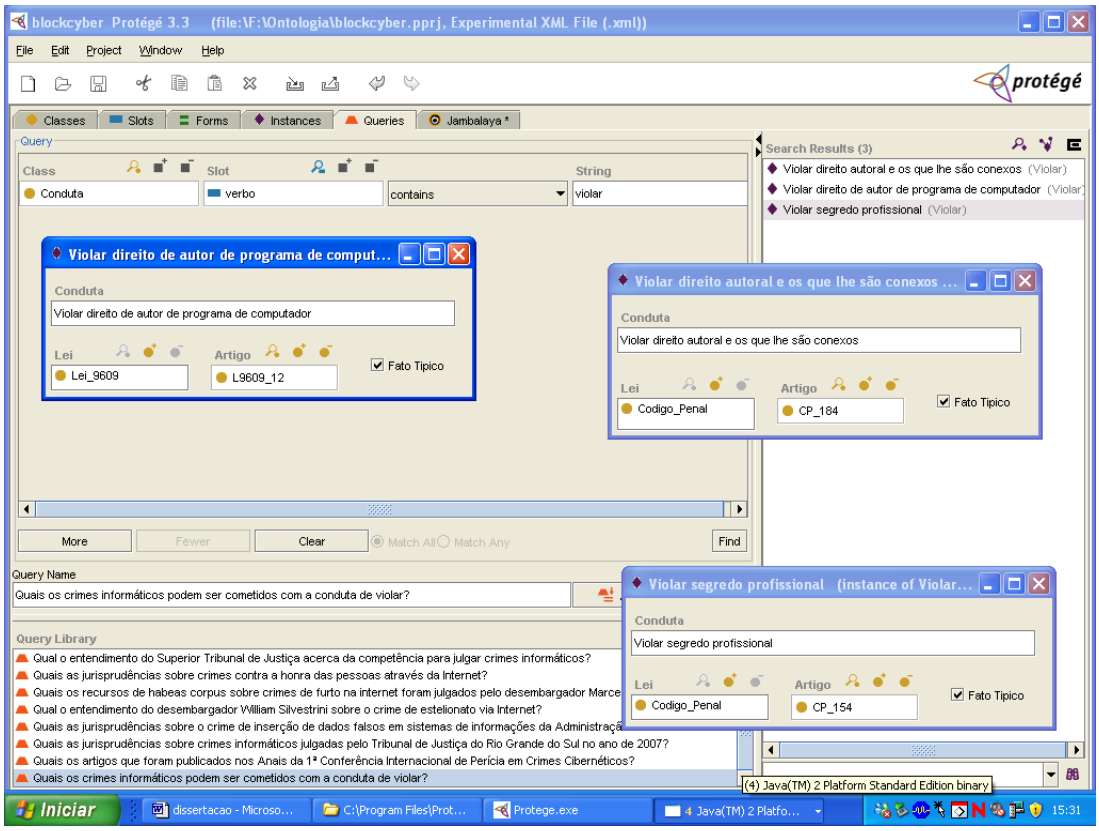

Figura 34. Resposta da ontologia jurídica de delitos informáticos à questão de competência: "Quais os crimes informáticos podem ser cometidos com a conduta de violar?". (Fonte: o autor)

Desta forma, a partir da consulta aos possíveis delitos informáticos cometidos a partir da indicação de um verbo no infinitivo, a ontologia jurídica é capaz de apontar quais são as condutas típicas que podem ser cometidas com este verbo específico, inclusive, poderá ser ampliada para abranger os seus sinônimos e as condutas atípicas, já que, a princípio, todas as condutas agregadas à base de conhecimento são típicas já que decorrem diretamente dos verbos contidos no tipo penal de crimes informáticos.

Além disso, tomando-se como exemplo os crimes contra a honra na Internet, por exemplo, a ontologia jurídica poderá auxiliar na identificação da tipicidade destes delitos a partir do momento em que sejam especificadas de forma que os agentes de *software* consigam entender o significado daquilo que esteja sendo atribuído a alguém.

A partir da definição do fato ou da alegação que esteja sendo imputada a um determinado indivíduo e através da criação de relações entre os seus significados dentro do contexto respectivo, tornar-se-á possível identificar qual o crime que foi cometido.

Entretanto esta não é uma tarefa simples, pois uma mesma palavra pode constituir crime de calúnia ou de injúria, dependendo do contexto em que for empregada. Por exemplo, quando um indivíduo chama o outro de 'ladrão', pode

caracterizar o crime de calúnia se o ofensor estiver se referindo a um fato perfeitamente identificado, ou então pode se tratar de crime de injúria, caso ele esteja apenas atribuindo à vítima uma qualidade negativa.

O primeiro passo consiste em definir se o bem jurídico ofendido é a honra das pessoas, hipótese em que a ontologia será capaz de delimitar quais as normas penais que são potencialmente aplicáveis para o caso em questão, excluindo do âmbito de sua aplicação ao caso concreto, por exemplo, os crimes contra o patrimônio e todos os demais que não possuam nenhuma relação ontológica com o bem jurídico <Honra>:

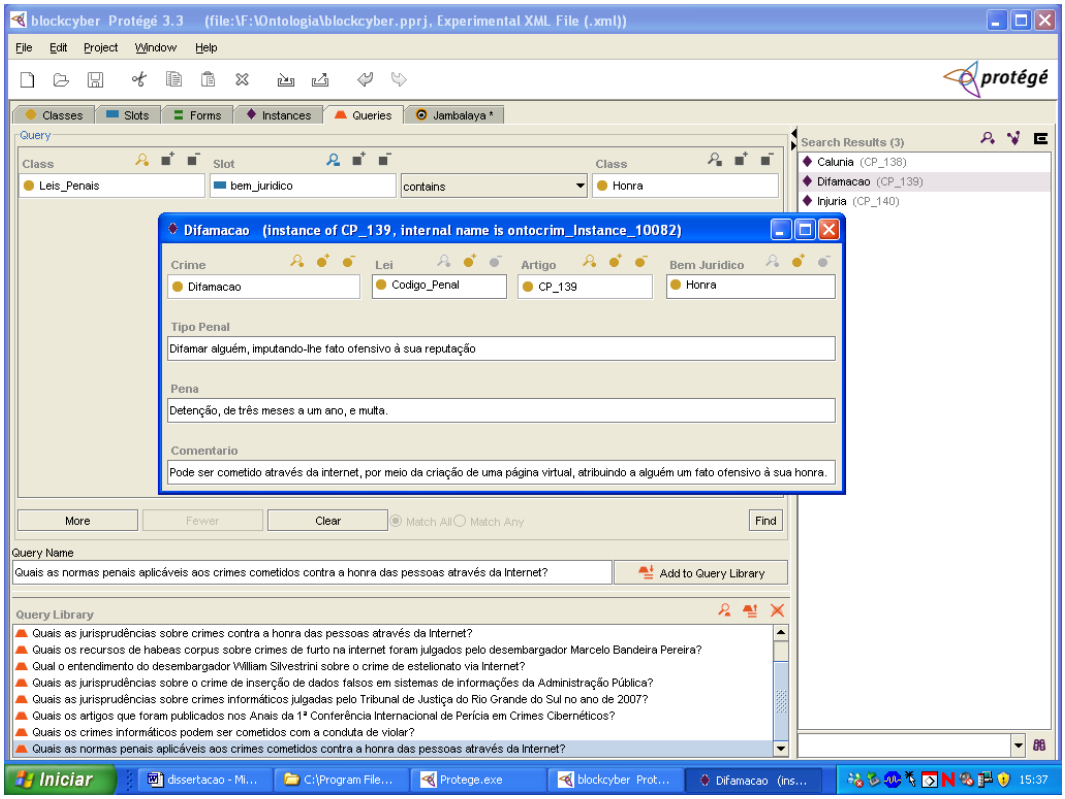

Figura 35. Normas penais aplicáveis aos crimes contra a honra das pessoas na Internet. (Fonte: o autor)

Conforme ilustrado na figura 35, a ontologia é capaz de responder, dentre outras, a seguinte questão de competência: “Quais as normas penais aplicáveis aos crimes contra a honra das pessoas através da Internet?”.

Ela apresenta como resposta as instâncias que correspondem exatamente aos crimes de calúnia, difamação e injúria do Código Penal Brasileiro, os quais são normas penais que tutelam a honra das pessoas. Além disso, a ontologia identifica a lei aplicável, o artigo correspondente, descreve o tipo penal e pena, e ainda traz um exemplo didático para auxiliar no esclarecimento do usuário acerca do assunto.

No estágio atual de desenvolvimento da ontologia jurídica, ela é capaz de esclarecer qual o crime contra a honra foi cometido, desde que o usuário especifique se o fato imputado é crime, se é uma afirmação ofensiva ou uma alegação vaga sobre qualidade negativa do ofendido, sendo fornecida a lei penal aplicável ao caso concreto.

Tratando-se do crime de calúnia, a necessidade atual de que o próprio usuário informe se o fato imputado é crime se deve em razão de que há infinitas condutas criminosas no ordenamento jurídico penal, e a ontologia desenvolvida contém na sua base de conhecimento apenas os tipos penais que caracterizam delitos informáticos, sendo esta delimitação fundamental para viabilizar o estudo e a construção da ontologia, porém ela poderá servir de suporte para o desenvolvimento de um sistema especialista.

Em relação ao crime de pornografia infantil do art. 241 do Estatuto da Criança e do Adolescente (ECA), o usuário precisa informar se a fotografia ou a imagem publicada, divulgada ou comercializada através da Internet contém ou não pornografia ou cenas de sexo explícito envolvendo criança ou adolescente, hipótese em que a ontologia poderá conduzir os agentes de *software* a identificarem a tipicidade do crime.

Quanto ao crime de interceptação de comunicações de informática, será preciso que o usuário informe se houve autorização judicial para realizar a interceptação da comunicação, e, em caso positivo, a ontologia permitirá ao agente de *software* entender que se trata do crime de interceptação previsto no art. 10 da Lei nº 9.296/96, e, em caso negativo, a conduta será atípica, pois, neste caso, o sujeito possui a autorização judicial.

Outro exemplo é em relação aos crimes contra a propriedade intelectual, uma vez que o usuário informe qual é o objeto do direito autoral que foi violado ou esta informação possa ser extraída pelo agente de *software*, a ontologia jurídica poderá ajudar a esclarecer qual a norma penal aplicável, tratando-se de programa de computador ela apontará para o art. 12 da Lei nº 9.609/98, e, sendo outra obra intelectual diversa de programa de computador, conduzirá a resposta ao art. 184 do CP.

Além das questões de competências já apresentadas ao longo deste capítulo, a ontologia também é capaz de responder a outras perguntas, conforme ilustra a figura 36:

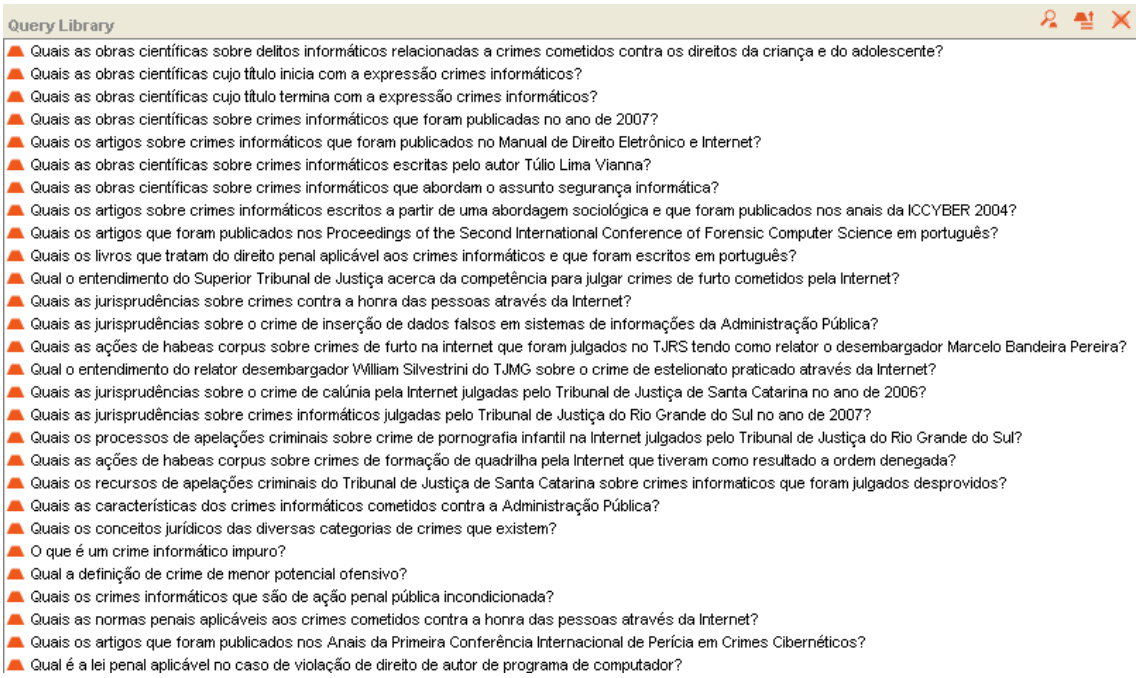

Figura 36. Biblioteca com as questões de competência da ontologia. (Fonte: o autor)

A ontologia desenvolvida possui extensão OWL (*Ontology Web Language*), efetuou-se a verificação formal da linguagem e a validação ocorreu em duas etapas, através de um questionário aplicado a um Doutor em Ciências da Informação e também com formação em Direito e com experiência na área dos crimes informáticos acerca das questões de competência do item 1.2.3 do primeiro capítulo, indagando-o se a ontologia proposta consegue ou não esclarecê-las, sendo acolhidas as sugestões e reformuladas algumas destas perguntas, e, na segunda etapa, realizou-se uma entrevista presencialmente para apresentar todas as funcionalidades da ontologia a um Mestre em Ciências Penais com dissertação defendida nesta área, o qual constatou que a ontologia consegue responder às questões de competência formuladas.

CONCLUSÃO

A finalidade precípua desta dissertação de mestrado foi propor uma ontologia para representar o conhecimento jurídico-penal no contexto dos delitos informáticos, objetivando esclarecer ao cidadão acerca da tipicidade destes crimes, incluindo os conceitos jurídicos usados neste domínio, conforme apresentado no terceiro capítulo.

Para que este objetivo pudesse ser alcançado, foi fundamental a realização de um estudo teórico sobre a inteligência artificial, sua relação com a engenharia do conhecimento e o uso da *web* semântica e de ontologias na sociedade da informação.

No segundo capítulo, vimos então o conceito de inteligência artificial, o papel da nova engenharia do conhecimento e exemplos de aplicação das técnicas de IA para detectar condutas criminosas, não apenas para identificação de casos suspeitos de furto de energia elétrica e fraude nas telecomunicações, mas também para fins de vigilância eletrônica e, principalmente, para evitar ataques e intrusão aos sistemas computacionais.

Foi feita uma abordagem acerca das alternativas de proteção contra invasões cibernéticas que utilizam as técnicas de inteligência artificial para este fim, tais como agentes inteligentes e sistemas híbridos com redes neurais e sistemas especialistas etc.

Em seguida, iniciou-se o estudo sobre a *web* semântica, definindo o seu conceito e a sua relevância na sociedade da informação ao permitir que agentes de *software* sejam capazes de realizar tarefas complexas para o usuário, explicando as camadas que servem de estrutura para esta rede inteligente a qual foi idealizada por Berners-Lee.

Depois de conceituar e esclarecer o sentido do termo 'ontologia' que é usado na engenharia do conhecimento, sendo definida como uma das camadas da *web* semântica, destacou-se a vantagem da ontologia na recuperação de informações na Internet, sendo apresentados projetos nacionais e internacionais que as utilizam, com ênfase especial para aqueles direcionados para o direito e/ou referentes aos delitos informáticos, tendo em vista a pretensão de propor uma ontologia jurídica para este domínio específico.

O terceiro capítulo tratou de abordar os crimes informáticos, dissertando sobre a aplicabilidade da lei penal vigente no país a estes delitos, com base na doutrina dos especialistas nesta área e em pesquisa jurisprudencial sobre o tema, com a finalidade de extrair o conhecimento jurídico compartilhado apropriado a ser modelado na ontologia.

Assim, percebeu-se a existência de algumas controvérsias entre os próprios especialistas que atuam nesta área uma vez que não há ainda um consenso quanto à forma de classificar os crimes informáticos. Isto se constatou também em relação ao

crime de dano, por exemplo, quanto à questão da sua tipicidade ou não em relação ao dano informático e à dificuldade em se admitir a equiparação dos dados intangíveis à coisa, para fins de incidência e aplicação do art. 163 do Código Penal que é de 1940.

Ora, se estas dúvidas existem para um profissional do direito que atua nesta área, quanto mais para um cidadão leigo, justificando-se a importâncias do uso de ontologias para que se possa conhecer os conceitos consensuais que são utilizados neste domínio e também aqueles conflitantes, indicando a existência de controvérsia, mas apontando, de maneira didática, ambas as visões e informando qual o entendimento que é majoritário.

Para construir a ontologia, utilizou-se a metodologia *Ontology Development 101*, proposta por Noy e McGuiness (2000) que estabelece os passos que devem ser seguidos para o seu desenvolvimento, os quais foram observados, sendo a ontologia descrita no quarto capítulo que trata da sua elaboração para o domínio dos delitos informáticos.

Trata-se de uma ontologia de domínio destinada a esclarecer questões atuais relacionadas com a tipicidade dos crimes informáticos no país a partir da lei penal em vigor, desconsiderando a legislação penal revogada e projetos de lei em tramitação.

Conforme se observou, ela é capaz de esclarecer questões referentes aos crimes informáticos no país a partir da lei penal vigente, como, por exemplo, identificar quais as normas penais aplicáveis aos crimes contra a honra das pessoas na Internet.

Embora ela não considere atualmente os projetos de lei sobre os crimes informáticos em tramitação, é possível incorporá-los à ontologia jurídica de delitos informáticos desenvolvida tão logo passem a integrar o sistema jurídico vigente.

Foi possível constatar que o uso da ontologia pode contribuir para facilitar o acesso do cidadão leigo a conceitos e conhecimento jurídico sobre crimes informáticos.

Além de esclarecer a tipicidade sobre estes delitos, também poderá servir de base para o reuso e desenvolvimento de outras ontologias para este domínio.

Buscou-se desenvolvê-la de modo simples e prático para representar o conhecimento jurídico sobre os delitos informáticos, sendo esta uma tarefa constante.

Trata-se, entretanto, de um domínio que carece de definições e conceitos, servindo a presente ontologia jurídica para orientar tanto os profissionais do direito quanto os cidadãos leigos que necessitam de esclarecimentos acerca da matéria.

Ela contribui ainda para auxiliar na formação do entendimento dos juízes para que evitar decisões judiciais conflitantes sobre crimes informáticos e, principalmente, para que haja segurança jurídica de forma que o cidadão leigo possa saber com precisão quais as condutas ilícitas praticadas através da informática que estão criminalizadas.

Deste modo, como resultado do trabalho científico desenvolvido na dissertação, aponta-se inicialmente para contribuições em duas áreas distintas do conhecimento.

Para a área da Engenharia do Conhecimento, apresenta-se uma ontologia para ajudar a esclarecer questões jurídicas sobre crimes informáticos, graças à representação do conhecimento jurídico-penal no domínio dos delitos informáticos em um nível de especificação que ainda não havia sido explorado nesta área, abrangendo tanto a questão dos conceitos jurídicos utilizados neste domínio quanto às características e à identificação da tipicidade dos delitos informáticos no Brasil.

Além disso, a ontologia jurídica de delitos informáticos poderá ser reutilizada como uma ontologia de aplicação para apoiar sistemas de raciocínio baseado em casos para uma melhor recuperação de jurisprudências sobre crimes informáticos já que ela permitirá obter um maior grau de similaridade entre os julgados a partir da relação existente entre o bem jurídico tutelado, o crime respectivo e características peculiares.

Do mesmo modo, outra contribuição para a Engenharia do Conhecimento é que a ontologia poderá ser utilizada também para apoiar um sistema especialista com o objetivo de determinar com maior objetividade se uma determinada conduta constitui um crime informático, tendo como suporte a estrutura ontológica criada neste domínio.

Esta dissertação permitiu ainda um estudo acerca de alguns projetos de ontologias jurídicas existentes tanto em âmbito nacional quanto internacional, o que certamente irá contribuir para compreender a sua importância, servindo para demonstrar as diversas possibilidades e perspectivas do uso de ontologias jurídicas em nosso país.

No campo do Direito, a primeira contribuição está no segundo capítulo, ao construir uma ponte entre a inteligência artificial e o direito, duas disciplinas bastante diferentes, e abordar a *web* semântica, trazendo uma visão geral do uso de ontologias no país e no exterior, fornecendo uma dimensão real de sua aplicação na área jurídica.

A segunda contribuição para o mundo da lei se evidencia no terceiro capítulo com a realização de um estudo aprofundado sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil, fundamentado na doutrina e jurisprudência, bem como nos comentários acerca do projeto de lei sobre estes delitos, visando esclarecer algumas questões controvertidas existentes sobre a temática.

Porém, a contribuição mais significativa está certamente no quarto e último capítulo, haja vista a proposta do uso da ontologia desenvolvida para representação do conhecimento jurídico-penal no contexto dos delitos informáticos que se destina a esclarecer questões relacionadas à tipicidade destes crimes, às condutas típicas previstas

na lei penal e aos conceitos jurídicos utilizados neste domínio, permitindo ainda a recuperação de decisões judiciais sobre o assunto e de obras científicas sobre o tema.

Enfim, considerando que o uso da inteligência artificial e da *web* semântica no direito ainda é muito incipiente no país, a relevância desta dissertação está no fato de que abre novas perspectivas para a sua aplicação, caminhando este trabalho científico neste sentido ao propor uma ontologia que irá promover o esclarecimento de questões importantes sobre os delitos informáticos, facilitando consideravelmente o acesso do cidadão leigo a estes conceitos jurídicos, apoiando-se na estrutura da *web* semântica.

REFERÊNCIAS

AJANI, Gianmaria. *et al*. “A Development Tool For Multilingual Ontology-based Conceptual Dictionaries”. In: *Proceedings of 5th International Conference on Language Resources and Evaluation*, LREC 2006, Genova, May 2006. Disponível em: <http://www.di.unito.it/~guido/PS/FV-lrec06.pdf>. Acesso em: 30 abr. 2008.

ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo: Juarez de Oliveira, 2006. 241 p.

ASARO, Carmelo *et al*. “A Domain Ontology: Italian Crime Ontology”. In: *Workshop on Legal Ontologies & Web Based Legal Information Management*. ICAIL, 2003. 7 p.

ATHENIENSE, Alexandre. *Parecer sobre o Projeto de Lei do Senado nº 76/2000*. Disponível em: <http://www.oab.org.br>. Acesso em: 25 jan. 2008.

BAGBY, John W.; MULLEN, TRACY. “Legal Ontology of Contract Formation: Application to eCommerce”. In: *Proceedings of the AAAI Workshop on Contexts and Ontologies*. Pittsburg, PA. Julho, 2005.

BARREIRA, André Calazans; ALVARENGA, Rogério; JARDIM, Jerônimo. “Modelo híbrido baseado em redes neurais e sistemas especialistas para detecção de intrusos em redes de computadores TCP/IP”. In: *Proceedings of the International Conference of Forensic Computer Science*. Brasília: Departamento de Polícia Federal, 2006. 124 p.

BASHAH, Norbik; BHARANIDHARAN, Shanmugam; AHMED, Abdul Manan. "Hybrid Intelligent Intrusion Detection System". In: *Proceedings of World Academy of Science, Engineering and Technology*. v. 6. Junho, 2005. 291-294 p.

BENCH-CAPON, Trevor. "Ontologies and Legal Knowledge-Based Systems Development". In: *Jaap 60 Jaar Symposium*: Intelligent Systems. Universiteit Maastricht, Holanda. Outubro, 2007. pp. 69-77.

BERNERS-LEE, T.; HENDLER, J.; LASSILA, O. “The Semantic Web”. In: *Scientific*

American, Maio 2001.

BRAGA, Marcus de Melo; RAMOS JÚNIOR, Hélio Santiago; COELHO, Tatianna de Faria. "Aplicações de Ontologias na Recuperação de Informações Jurídicas na Web Semântica". In: *Anales 36 JAIIO. Jornadas Argentinas de Informática. Simpósio Informática y Derecho*. Mar del Plata, 2007. Buenos Aires: SADIO, 2007. 8 p.

BREUKER, Joost; ELHAG, Abdullatif; PETKOV, Emil; WINKELS, Radboud. "IT Support for the Judiciary: Use of Ontologies in the e-Court Project". In: *Proceedings of the 10th International Conference On Conceptual Structures:* Integration and Interfaces. Borovets, Bulgaria. Julho, 2002.

CAPEZ, Fernando. *Curso de Direito Penal*: parte geral. v.1. 7.ed. São Paulo: Saraiva, 2004. 563 p.

CASTRO, Aldemário Araújo. "A internet e os tipos penais que reclamam ação criminosa em público". In: *Revista de Direito Eletrônico*. Petrópolis: IBDE, v. 1, n. 3, 2003a. pp. 41-51. ISSN – 1679-1045. Disponível em: <http://www.ibde.org.br/index_arquivos/rede3.pdf>. Acesso em: 29 mai. 2007.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2.ed. rev., ampl. e atual. Rio de Janeiro: Lumen Juris, 2003b. 230 p.

CERQUEIRA, Roberto Figueiredo Palleta de; BAX, Marcello Peixoto. "Método de modelagem domínio-ontológica do direito positivo brasileiro". In: *Anais do VIII Encontro Nacional de Pesquisa em Ciência da Informação*. Salvador/BA, 2007. 16 p.

DEATON, Chris *et al*. "The Comprehensive Terrorism Knowledge Base in Cyc". In: *Proceedings of the 2005 International Conference on Intelligence Analysis*, McLean, Virginia, Maio 2005.

FERREIRA, Ivete Senise. "A criminalidade informática". In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Org.). *Direito e Internet*: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

GOMES, Luiz Flávio. “Atualidades criminais”. In: *Instituto Brasileiro de Ciências Criminais*. Disponível em: <http://www.direitocriminal.com.br>. Acesso em: 12 jan. 2008.

GRAY, Pamela N. “The Ontology of Legal Possibilities and Legal Potentialities”. In: *Proceedings of the 2nd Workshop on Legal Ontologies and Artificial Intelligence Techniques*. Stanford University, Stanford, CA, USA. Junho, 2007. pp.7-23.

GRUBER, T. “A translation approach to portable ontology specifications”. In: *Knowledge Acquisition*, v. 5, p. 199-220, 1993. Disponível em: <ftp://ftp.ksl.stanford.edu/pub/KSL_Reports/KSL-92-71.ps.gz>. Acesso em: 27 jul. 2007.

HAGIWARA, Shingo. *Discordance Detection in Regional Ordinance*: Ontology-based Verification. Disponível em: <http://www.jaist.ac.jp/jinzai/Report18/ReportHagiwara.pdf>. Acesso em: 15 mai. 2008.

JORGE, Marco *et al*. “ECA3RL: Fraud Detection in Mobile Communications”. In: *Cognitive & Media Systems: Winter Meeting*. Coimbra, Portugal. Fevereiro 2008.

KUMAR, Ram. “XML Standards Based Information Exchance Strategy of NSW Police”. In: *OASIS Open Standards*. Sydney, Australia. Outubro, 2005. 39 p.

LEARY, Richard M.; VANDENBERGHE, Wim; ZELEZNIKOW, John. “Towards a Financial Fraud Ontology: a Legal Modelling Approach”. In: *Workshop on Legal Ontologies & Web based legal information management*. ICAIL, 2003.

LINDOSO, Alisson Neres; SERRA, Ivo da Cunha; GIRARDI, Rosário. “ONTOINFOJUS: um Modelo de Domínio baseado em Ontologias para o Acesso à Informação na Área Jurídica”. In: *Anais do V Encontro de Estudantes de Informática do Tocantins*. Palmas, TO. Outubro, 2003. pp. 251-260.

MANDUJANO, Salvador. "Identifying Attack Code through an Ontology-Based

Multiagent Tool: FROID". In: *Proceedings of World Academy of Science, Engineering and Technology*. v. 6. Junho, 2005. pp. 163-166.

MARTINS, Maria Cleci Coti. "Ontologia legal: Estudo sobre a modelagem do conhecimento legal no contexto do direito tributário". In: *Prêmio Schontag 2006*. Disponível em: <http://www.receita.fazenda.gov.br>. Acesso em: 10 abr. 2008.

NOGUEIRA, José Helano Matos. "Agentes inteligentes móveis no combate às invasões cibernéticas". In: *Anais da 1ª Conferência Internacional de Perícias em Crimes Cibernéticos*. Brasília: Departamento de Polícia Federal, 2004. pp. 69-72.

NOGUEIRA, José Helano Matos. "Ontology for Complex Mission Scenarios in Forensic Computing". In: *Proceedings of the Second International Conference of Forensic Computer Science*. Guarujá: ABEAT, 2007. pp. 48-55.

NOY, Natalya; MCGUINNESS, D. L. *Ontology Development 101*: a guide to creating your first ontology. CA: Stanford University, 2000.

NUNES, Anselmo Maciel; FILETO, Renato. "Uma Arquitetura para Recuperação de Informação Baseada em Semântica e sua Aplicação no Apoio a Jurisprudência". In: *Anais da III Escola Regional de Banco de Dados*. Caxias do Sul, RS: Universidade de Passo Fundo, 2007. 10 p.

OLIVEIRA, Felipe Cardoso Moreira de. *Criminalidade Informática*. Dissertação. Mestrado em Ciências Criminais. Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre: PUC/RS, 2002. 160 p.

PINHEIRO, Patrícia Peck. *Direito Digital*. 2.ed. Sâo Paulo: Saraiva, 2007. 407 p.

RAMACHANDRAN, Deepak; REAGAN, Pace; GOOLSBEY, Keith. "First-Orderized ResearchCyc: Expressivity and Efficiency in Common-Sense Ontology". In: *AAAI Workshop on Contexts and Ontologies*: Theory, Practice and Applications. Pittsburgh, Pennsylvania, Julho, 2005.

RAMOS JÚNIOR, Hélio Santiago. “Crimes contra a Segurança dos Sistemas de Informações da Administração Pública”. In: *Proceedings of the Second International Conference of Forensic Computer Science*. Guarujá (SP), ABEAT, 2007. pp. 64-69.

RAMOS JÚNIOR, Hélio Santiago *et al*. “O uso de web semântica e ontologias no domínio jurídico: Perspectivas de sua aplicação no âmbito dos crimes cibernéticos”. In: *Anais da IV Conferência Sul-Americana em Ciência e Tecnologia Aplicada ao Governo Eletrônico*. Florianópolis: Editora Digital Ijuris, 2007. pp. 315-324.

RODRIGUES, Jorilson da Silva. “Aspectos Práticos dos Crimes Informáticos”. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha (Org.). *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006. pp. 85-98.

ROVER, Aires José. *Informática no direito*: inteligência artificial. Curitiba: Juruá, 2001. 270 p.

RUSSELL, Stuart; NORVIG, Peter. *Inteligência artificial*. 2.ed. Rio de Janeiro: Elsevier, 2004. 1021 p.

SARAVANAN, M.; RAVINDRAN, B.; RAMAN, S. . “Improving legal document Summarization using graphical models”. In: ENGERS, T. M. van. *Legal Knowledge and Information Systems*, JURIX 2006: The Nineteenth Annual Conference, Paris, 2006, IOS Press, pp.51-60.

SARAVANAN, M.; RAVINDRAN, B.; RAMAN, S. "Using Legal Ontology for Query Enhancement in Generating a Document Summary". In: LODDER, A. R.; MOMMERS, L. (Org.). *Legal Knowledge and Information Systems*. JURIX 2007: The Twentieth Annual Conference. v. 165, IOS Press. December 2007.

SCHALKOFF, Robert J. *Artificial Intelligence*: An Engineering Approach. New York, USA: Mc Graw-Hill Publishing Company, 1990. 646 p.

SCHANK, Roger C. “What is AI, anyway?”. In: PARTRIDGE, Derek; WILKS,

Yorick. *The foundations of artificial intelligence:* a sourcebook. New York, U.S.A: Cambridge University Press, 1990. pp. 3-13.

SILVA, Paulo Quintiliano da. "Crimes cibernéticos e seus efeitos internacionais". In: *Proceedings of the International Conference of Forensic Computer Science*. Brasília: Departamento de Polícia Federal, 2006. pp. 10-14.

SPYNS, Peter. MEERSMANN, Robert; JARRAR, Mustafa. "Data Modelling Versus Ontology Engineering". In: *SIGMOD Records*. v. 31, n. 4, dez 2002. pp. 12-17.

STAAB, S.; MAEDCHE, A. *Knowledge Portals – Ontologies at Work*. Disponível em: <http://www.aifb.uni-karlsruhe.de>. Acesso em: 14 mai. 2007.

TANG, Yan; MEERSMAN, Robert. "Judicial Support System: Ideas for a Privacy Ontology-Based Case Analyzer". In: *OTM 05 PHD Symposium*, LNCS, Springer Verlag 2005. pp. 800-807.

THE Protégé Ontology Editor and Knowledge Acquisition System. Disponível em: <http://protege.stanford.edu>. Acesso em: 14 mai. 2007.

TRUZZI, Gisele; DAOUN, Alexandre. "Crimes informáticos: o direito penal na era da informação". In: *Proceedings of the Second International Conference of Forensic Computer Science*. Guarujá (SP), ABEAT, 2007. pp. 115-120.

VALENTE, André; BREUKER, Joost. "A Functional Ontology of Law". In: BARGELLINI, G.; BINAZZI, S. (Org.). *Towards a Global Expert System in Law*. Padua: CEDAM Publishers, 1994. pp. 201-212.

VIANNA, Túlio Lima. "Dos crimes por computador". In: *Revista dos Tribunais*. Ano. 91. v. 801. jul. 2002. São Paulo: RT, 2002a. pp. 405-421.

VIANNA, Túlio Lima. "Dos crimes pela internet". In: REINALDO FILHO, Demócrito (Org.). *Direito da Informática*: temas polêmicos. Bauru: Edipro, 2002b, p. 211-224.

VIANNA, Túlio Lima. *Fundamentos do Direito Penal Informático*: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003. 170 p.

VIANNA, Túlio Lima. "A ideologia da propriedade intelectual: a inconstitucionalidade da tutela penal dos direitos patrimoniais do autor". In: *Anuario de Derecho Constitucional Latinoamericano*. Tomo II. Uruguay: Fundación Konrad-Adenauer, 2006. pp. 934-948.

VIANNA, Túlio Lima. *Transparência pública, opacidade privada*: O Direito como instrumento de limitação do poder na sociedade de controle. Rio de Janeiro: Revan, 2007. 230 p.

WEBER, Rosina. "Inteligência artificial: técnicas e metodologias para a manipulação do conhecimento textual". In: ROVER, Aires José. (Org.). *Direito, Sociedade e Informática*: Limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000. pp. 213-222.