Problema: Anuario de Filosofía y Teoría del Derecho
ISSN: 2007-4387
problema.unam@gmail.com
Universidad Nacional Autónoma de México
México

ABEL, Wiebke; SCHAFER, Burkhard
BIG BROWSER MANNING THE THIN BLUE LINE - COMPUTATIONAL LEGAL THEORY MEETS LAW ENFORCEMENT
Problema: Anuario de Filosofía y Teoría del Derecho, núm. 2, 2008, pp. 51-84
Universidad Nacional Autónoma de México
Distrito Federal, México

PROBLEMA

Anuario de Filosofía y Teoría del Derecho 2

BIG BROWSER MANNING THE THIN BLUE LINE - COMPUTATIONAL LEGAL THEORY MEETS LAW ENFORCEMENT[1]

Wiebke ABEL
Burkhard SCHAFER[2]

Resumen:

En este ensayo se analizan algunos tópicos conceptuales y filosóficos de actualidad sobre el procedimiento y las pruebas desde la óptica de una teoría del derecho computacional. En él se presenta un mecanismo específico de investigación, relativo a los "troyanos" operados por la policía durante la investigación de delitos, y analiza si los enfoques formales contemporáneos sobre el razonamiento jurídico pueden ser modificados de tal modo que el código de *sofware* que subyace a este mecanismo puede representar las limitaciones jurídicas relevantes que deberían regir su operación. Los autores sostienen que las teorías formalistas tradicionales del razonamiento jurídico se limitan por lo general al razonamiento dentro de un sistema y, por lo tanto, son incapaces de hacer la noción de "sistema jurídico" suficientemente explícita. Asimismo, se discuten las posibilidades de ampliar estos enfoques e identificar los elementos necesarios de una teoría computacional del razonamiento jurídico en una era de fronteras porosas.

Abstract:

This paper analyses some current jurisprudential and conceptual issues in evidence and procedure from the perspective of a computational legal theory. It introduces a specific investigative device, Trojans operated by police

[1] Research for this paper was supported by ESRC grant RES-000-23-0729 "Evidence, its nature and evaluation" and the AHRC Centre for IT and IP Law SCRIPT.

[2] University of Edinburgh School of Law. Email *b.schafer@ed.ac.uk*.

during crime investigation, and analyses whether current formal approaches to legal reasoning can be modified in such a way that the software code underlying this device can represent the relevant legal constraints that should govern its operation. We will argue that traditional formalist theories of legal reasoning are typically restricted to reasoning within a system, and incapable therefore of making the notion of "legal system" sufficiently explicit. We discuss possibilities to expand on these approaches and identify the necessary elements of a computational theory of legal reasoning in an age of porous borders.

I. INTRODUCTION

This paper analyses some current jurisprudential and conceptual issues in evidence and procedure from the perspective of a computational legal theory.[3] In particular, we will analyse some of the cross-border issues raised by the recent decision of the German Federal Court of Appeal (BGH) to outlaw, for the time being, the use of Trojans by police forces for surveillance purposes.[4] In the first part, we prepare the ground for our analysis by discussing different aspects of the notion of "porous borders" in the law of evidence. In the second part, we introduce our case study, the use of Trojans and similar remote forensic tools (RFS) for investigative purposes and sketch some of the most pertinent legal issues that this technology raises. In the final part, we return to the issue of porous borders, especially the border between normative and descriptive discourses in internet governance. We outline how formalist jurisprudential theories of legal reasoning can inform technological solutions to these problems if they are capable of representing identity criteria for normative systems in a formally rigorous and computational way.

II. ON GEOGRAPHICAL AND CONCEPTUAL BORDERS

When thinking about the future of law in an age of porous borders, what comes first to mind are geographical borders between states. The nature of police procedure and investigation, and the laws of evidence connected with

[3] "Computational legal theory" concerns itself with the representation and modelling of legal norms and concepts on software platforms.

[4] BGH, NJW 2007, 930.

them, have changed under the impact of globalisation and globalised crime just as much as substantive laws and regulations.[5] Increasing roles for international police organisations such as Interpol and Europol, or the debate around the European arrest warrant, demonstrate the steps taken by governments to better co-ordinate their crime fighting efforts.[6] At the same time, worries persist that globalisation could undermine the due process guarantees and civil liberties traditionally connected to the notion of the nation state. "Rendition flights" and the "outsourcing of torture" are but two examples that illustrate the potential of emerging global orders to subvert traditional civil liberty guarantees in the criminal law field. In the same way in which according to some critics globalisation and global competition for markets ensures that only the lowest common denominator in fields such as environmental protection or health and safety laws will prevail, competition between states for political favours could see the transfer of investigative activities to states with the least restraint on police powers.

Sometimes. Geographical constraint will prevent this. Physical crime scenes do not travel well. But digital evidence, generated in cyberspace, will often exists on servers distributed over several countries, and can therefore be accessed and collected from more than one country. In conceptualising the porous border between cyberspace and physical space, the question changes from one of geographical territory to that of "conceptual spaces". Geographical metaphors, while heuristically helpful, quickly reach here the limits of their usefulness.[7] This also reminds us that

[5] See *e. g.* Blum, Jack and Passas, Nikos, "Controlling Cross Border Undercover Investigations", in Field, Stewart and Pelser, Caroline (eds.), *Invading the Private: State, Accountability and the New Investigative Methods in Europe*, Aldershot, Dartmouth 1998.

[6] See *e. g.* Fijnaut, Cyrille, "Transnational Organized Crime and Institutional Reform in the European Union: The Case of Judicial Cooperation", in Williams, Phil and Vlassis, Dimitri (eds.), *Combating Transnational Crime: Concepts, Activities And Responses* 276, London, UK, Routledge, 2001.

[7] One could think in this context of the notion of "safe harbour", in data protection contexts, a problematic metaphorical use of a geographical notion taken

more generally, the real issue will often be one of conceptual borders between abstract legal contexts more than one of geographical borders. It does not matter so much where Guantanamo Bay is located geographically, but where it is located "conceptually", that is within or outside the jurisdiction of US courts and their habeas corpus protection.

The example of evidence collected from cyberspace indicates a second porous border, this time a border between the virtual and the real, digital evidence and concrete physical evidence. In a highly complex process, electronic traces are eventually transformed into hard, tangible printouts.[8] In crossing the border between the digital and the physical, the nature of the evidence changes, raising numerous problems for procedural law. Where, exactly, in this process is "the" evidence located?

This alerts us to several more borders which in the past were perceived as rock solid, and have recently become fluid and permeable. The most important of these for our purpose is the border between normative and descriptive discourses. Larry Lessig's influential work on "code as code" has alerted us to the potential of cyberspace to replace traditional normative and legal debates with questions of software programming.[9] Where traditional normative legal thinking analysed for instance copyright law as including a set of sanctions for copyright violation, norms that required application of the law by courts to a situation, digital rights management can be seen as a self-applying, descriptive version of the same law that makes violation of the legal norm physically impossible.

Furthermore, technologically enhanced evidence collection requires non-legal expert knowledge. In the law of evi-

from traditional international public law and applied to the conceptual issue of data transfer across borders in cyberspace.

[8] For an analysis that also analyses the "borders" between physical and digital evidence see Carrier, Brian, and Spafford, Eugene, Getting Physical with the Digital Investigation Process *International Journal of Digital Evidence*, 2, 2003, pp. 1-20.

[9] Lessig, Larry, *Code and Other Las of Cyberspace*, New York, USA, Basic Books, 2000.

dence and procedure, the conceptual boundaries between scientific and legal discourse have always been particularly permeable, with the law giving due deference to domain specific expertise. Increasing reliance on self-regulation by professional bodies for forensic practitioners, and an increased role for other institutional set ups outside the formal court system such as the planned Forensic Science Advisory Council in the UK[10] are evidence for a further acceleration of the process by which borders between legal-normative and scientific-descriptive discourses are broken down.

To sum up, the modern law of evidence operates in a precarious environment where not just the permeable borders between nation states form a formidable challenge. Rather, we find porous borders between

— The scientific and the legal.
— The normative and the descriptive.
— The public police and the private data gatherer.
— Cyberspace and the brick and mortar world.
— Jurisdictions and other regulatory spaces.
— Official law and autonomous self-regulation by professional associations and other groups.

In the example that we are now going to discuss, online search of computers through Trojans, we will see how these different types of gaps in legal-normative orders converge. all these different aspects come together, raising some serious questions for adequate due process protection and civil rights safeguards. However, in the third part, we will see that while the malleability of law that comes with porous borders poses a prima facie risk for civil rights, it can equally be used to protect them. In particular we will see how we can utilize the porosity between normative and descriptive discourses to counteract the problem posed to on-

[10] *http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf.*

line searches by porous geographical and jurisdictional borders.

III. The "Federal Trojan"

During a recent investigation of a suspect in a terror investigation, the German prosecution authorities suspected that information crucial to the investigation might be stored on the suspect's computer.[11] Therefore, the attorney general applied to the responsible investigating judge for a warrant to secretly search the suspect's private computer. The application asked for permission to investigate the data stored on the hard disk and the working memory of the computer. To accomplish this, a specifically designed computer program was to be planted on the suspect's computer without raising his suspicion. This program would then copy all data stored on the computer and subsequently transfer it back to the investigating authority for evaluation. In addition to files stored on the computer, prosecutors also sought access to the suspect's email traffic and information about visited websites.[12]

On the 25.11.2006, the investigating judge of the BGH declined the application by the attorney general. The attorney general appealed against this decision to the federal court the BGH, claiming that articles 102, 110 and 94 of the Criminal Code (Strafprozessordnung- StPO) allowed for such a search. The court disagreed, rejecting in its judgement the analogy between a traditional search of physical premises and clandestine searches of a computer, including real time internet traffic, through a remote device. For the time being, the borders between physical world and cyberspace seemed protected, and a "dangerous metaphor" of the type mentioned above appeared to have been re-

[11] Hornung, Gerrit, "Ermächtigungsgrundlage für die «Online-Durchsuchung»?," *Datenschutz und Datensicherheit,* 31, 2007, pp. 575-580.

[12] Leipold, Klaus, *Die Online-Durchsuchung, Neue Juristische Wochenschrift,* 2007, p. 315.

jected. However, the court made it clear that its decision was based merely on the absence of a formal law creating the relevant powers for the investigative authorities. It explicitly did not address whether such law, if enacted, would contravene constitutional and European human rights safeguards. In what follows, we assume that as is likely, appropriate primary legislation has been created and the use of Trojans by the police is at least in principle legally permitted.

To prepare the ground for the formal analysis in the later part of this paper, we will now try to give some indication of how the technology is likely to work. Few details are available at the moment about the precise nature of the proposed remote forensic software. Indeed, it has been doubted if such a search is at present feasible at all. The focus of this paper is on the use of software that shares crucial features with well known malware, in particular viruses and Trojans, pieces of software code which are designed to carry out functions on a user's computer without the user knowing of the presence of the software or its function, which ranges from disruption of ordinary functions for the quasi-recreational purposes of the code writer, or for gathering and transmitting information about the computer's user. Both can be used to steal personal data from targets, *e. g.*, banking information including the keystrokes used to enter personal identification numbers, and hence are equally suitable for data collection by police authorities. As with their criminal counterparts, police Trojans require the unwitting cooperation of the target. This can happen through opening an email, for instance an email that purports to come from a bona fide state agency such as the local council or the department for pensions. For obvious reasons, police investigators would have little problem generating emails that spam filters and similar software could not distinguish from genuine information coming from other public authorities – indeed, these public authorities may well be the source of the email which carries the

Trojan as a payload on behalf of the police. Unlike their criminal software counterpart, it would not even be necessary for police to fake sender addresses and other identifying data embedded in an email.

Alternatively, the Trojan could be embedded in a website that the suspect is likely to visit, or could be part of software downloads from such websites. The police could set up for instance websites that look as if they contain material helpful for would-be terrorists, and infect the computers of visitors. The problem with this approach is that it would be highly indiscriminate, attacking every visitor and not just people named in the warrant. Alternatively, a combination of the two methods could be used, directing the suspect through an email to a website that requires log in, for instance a website that allows submission of tax returns – the suspect could be identified through his login information, and he and only he then directed to an infected site that, apart from this infection, is identical to a genuine tax office website.

We claimed above that the use of Trojans for the collection of evidence by the police poses radical questions about the nature of evidence in an age of porous borders. This becomes apparent when we look at the debate around the legality of such attacks under German and international law, either with or without explicit legislation. In what follows, we will show how all of the different categories of "border crossing" that we identified above impact on the answer to this question.

The first set of problems we face concerns conceptual borders. The German Constitution distinguishes between the protection of the home (Art. 13 Constitution) and the protection of telecommunication (Art. 10). Both predate the internet, as do most of the rules of criminal procedure that followed from them. As so often is the case with internet regulation, the task becomes to find the best conceptual match between the new technology and the prototypes envisaged by the older legislation. Art 10 would apply if the

measure was a form of surveillance of communication, in particular if we could compare it to the surveillance of telephone calls and letters. Art. 13 would apply if the next best match of the measure is the physical search of dwellings. The proposed law clearly tries to conceptualise the online search through remote forensic tools as a search of dwellings, protected by Art. 13, not as a surveillance method, regulated by Art. 10. The reason for this is simple: Hidden surveillance requires a much higher level of scrutiny under the constitution than the search of a home in the presence of the owner.

Police and prosecution service try to support this analysis through certain procedural safeguards: The Trojan may for instance only look for files whose extension indicates that they are not used currently for communication purposes. It would operate for a limited time only, and the police could also not ask for repeated permissions to search a suspect's drive, as this would come too close to a continuous surveillance.

However, the surveillance-search dichotomy sits uneasily with features of internet based communication. The conceptual borders that the constitution draws become precarious at a time when it is one feature of most homes that they are "constantly communicating" through permanent connection to the internet. This also blurs the differences between the different legal ontologies that these two articles induce. Art 10 essentially protects a *process*, whereas Art. 13 protects objects. In the pre-internet world, a letter was either in the process of being delivered by the post, protected by Art. 10, or a object sitting at home, on a desk, and protected by Art. 13. What, and even more importantly, where, are my emails? What happens if I draft an email on a web based account that automatically saves drafts every couple of seconds in a hidden folder? Digital evidence is crucially linked to the process that makes it visible to the human eye – electronic documents are not mere objects, but objects continuously created through processes on the

computer on which they reside. The border between object and process thus becomes contested, and the legal conceptualisation that is based on this dichotomy inadequate.

Nor does a purposive interpretation of the relevant legislation provide us with a clear answer. The value protected by Art. 13 is personal privacy. It has been questioned however if this term projects well into cyberspace. Should the very act of logging onto the web be understood as some form of public activity, akin to going to the market? Or is it conceptually similar to merely opening a window that allows you to observe the outside world from within your home? Where, again, is cyberspace and what are its borders? Research indicates that engaging with modern information technologies has profoundly changed the way we perceive the borders between the private and the public. Putting information *e. g.* on Facebook is often perceived by the poster as a private activity, restricted to a network of friends, an understanding not shared for the time being by official legal discourses.[13] But even if we accepted for the time being that a remote search of a computer at a suspect's home falls within the scope of Art. 13, at least some of the suggested methods to install a remote forensic tool could not guarantee that this is where the device eventually ends up: If the Trojan is delivered through an email attachment or a download, then it is perfectly possible that it will reside on a laptop that is taken out of the house, or worse, the email is opened in a public place such as an internet café.

In addition to the possibility that the Trojan crosses the borders between legal-conceptual spaces, it can also cross the border between nation states. We will discuss an example based on this idea in more detail below. Obviously, a suspect may carry the Trojan on a mobile device such as a laptop from one country to another, and may also during

[13] Berkovsky, Shlomo *et al.*, "Examining users' attitude towards privacy preserving collaborative filtering", *Proceedings of DM.UM'07*, 2007, *http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/berkovsky.pdf*.

the journey move into spaces governed in part by international law such as extraterritorial waters. Since different jurisdiction draw the border between legal –conceptual spaces differently, the number of permutations multiplies: When taking a laptop with a Federal Trojan to the UK, the device may be active in an area that according to UK law is part of the public sphere, but according to German law would still constitute private space.

Police searches of computers, just like the traditional search of a dwelling, are sovereign acts, intimately linked to the notion of the state and its territory. That the investigator is located in Germany does not change the fact that the remote device carries out investigative actions which are effective primarily outside the territory of the Federal Republic. Even within the EU, extraterritorial deployment of police officers for instance in the context of international football competitions, has met fierce resistance and required complex bi-national negotiations which reduced the foreign police force to mere observers without powers of arrest.[14] Without the consent of the country where the investigative action takes effect, such a search would be a violation of international law, and arguably even a crime under public international law.

Assuming the consent of the nation on whose territory the investigative action takes place, a different set of legal issues arises. The consent may exist in the form of bilateral or multilateral treaties that describe in general terms the scope of any such concession. The interpretation of these treaties is governed by international public law. Alternatively, consent can be granted in the form of ad-hoc, one off permissions. In both cases, the permission can establish constraint on the operation of the Trojan that go beyond those that govern its use under national law. Also, in both cases a formal request through diplomatic channels will normally be required. Only exceptionally, and only when a

[14] See O'Neill, Megan, *Policing Football: Social Interaction and Negotiated Disorder*, Houndmills, UK, Palgrave Macmillan, 2005.

bilateral treaty is in place, can this request come directly from the investigative authority to its foreign counterpart. Since one reason for the use of Trojans is that they are less subject to time and resource constraints than police officers seizing hardware, at least in the future it may be possible that the Trojan itself initiates the required requests, if it finds that the computer it is accessing is outside the national territory of the authority it belongs to. This issue in itself would raise several interesting philosophical and legal issues on the status of autonomous software devices.[15] Where existing treaties on police cooperation permit requests for assistance directly from investigating authorities, it will become questionable if automated requests (and possibly even replies) would also be covered by the treaties. To the extend that they refer to officers holding a certain rank within an institution, it may even be necessary to assign to the forensic tool a formal rank within the police organisation.

The first set of issues again assumes that the Trojan itself initiates the process of asking for permission to operate outside the territory of its home jurisdiction.

First, such a request will normally only be granted if reciprocal requests are also likely to succeed. Second, the crime under instigation has to be a criminal offence in both jurisdictions. Third, only the crime specified in the assistance request may be investigated – this can obviously create problems if also evidence of other crimes is on the computer or even worse, evidence of other activities of the suspect which are not crimes under the jurisdiction of the country where the computer is located.

The second condition creates a particularly interesting problem for legal reasoning. They require of the lawyer making the assessment at least a partial engagement with comparative law. With other words, he has to move beyond

[15] See Schafer, Burkhard, "The taming of the Sleuth—problems and potential of autonomous agents in crime investigation and prosecution", *International Review of Law, Computers and Technology* 20 2006 63-76 with further references.

reasoning within his legal system. In prosecuting for instance an alleged murder, he needs to know

a) If murder is a criminal offence of the legal system from which assistance is required (the "target system")
b) If the specific alleged acts of the accused constitute a crime under the legal rules of the target system
and
c) If that crime, as understood in the target system, is close enough to the concept of "murder" in the home jurisdiction.

The third condition prevents emergence of a situation where the actions of the suspect constitute offences in both countries in principle, but the respective legal conceptualisations of the actions are so radically different to make them incommensurable. If the actions of the accused constitute "criminal tax evasion" in the home jurisdiction, but only a misdemeanour of failing to comply with reporting requirements in the target jurisdiction, the specificity requirement for cross-border assistance would stand in the way of such a request being granted.[16]

It is not sufficient for the Trojan to collect data from the suspect's computer. It has to collect this data in such a way that the information can be admitted in trial against the suspect. While this question is superficially the exclusive domain of the home jurisdiction, the procedural rules of the target system and the rules of international law both play a role in making this assessment.

A short example best illustrates the issues that can arise. Assume that under the law of the home jurisdiction, information contained in a personal diary is protected by privacy laws that would result in the inadmissibility of any information gained from them. Assume further that the target jurisdiction does not contain such a provision. If the Trojan

[16] See *http://www.europe-solidaire.org/spip.php?article9468 for an example of this kind*.

copies information it finds in a folder labelled “diary”, containing a word document whose content is in the form of a personal diary, it complies with the relevant law of the jurisdiction where the computer is physically located. However, the evidence would not normally be admissible in the courts of the home jurisdiction. An exception however may exist if both countries are member states of the EU. In this case, the convention on mutual assistance in criminal matters *may* require the home jurisdiction to accept evidence collected in accordance with the standards applicable in the target jurisdiction.[17] Even in this case, the home jurisdiction may well have non-negotiable public order limitations on admissibility that prevent for instance the police from circumventing domestic laws – in our case for instance, activating the Trojan only after the suspect left the country, even if an investigation while still on domestic territory would have been possible.

The converse situation poses slightly different issues. In this case, the Trojan performs actions which would result in the inadmissibility of evidence were it to be used in a court in the target country. Despite this, the evidence would normally be admissible in the courts of the home country, the courts for which the evidence is intended. Nonetheless, a problem may arise under international law: The permission to operate an extraterritorial search at all will only be granted if the investigative actions do not violate the ordre public of the target state granting the permission.[18] Especially gross violations of a person’s privacy may well constitute such a violation of ordre public, even if the target of the investigation is not a citizen of the state granting the privacy protection. If the Trojan proceeds nonetheless in copying the protected files, it may well operate outside the scope of the permission to carry out investigative

[17] See *http://conventions.coe.int/Treaty/en/Treaties/Html/030.htm*.

[18] A more traditional example: State A may grant foreign police officers that right to question one of their nationals held in country A. But this does not give them the right to torture the suspect, even if their country has no admissibility bar on evidence obtained under torture.

actions in the first place, and as a result (also) violate international law. Whether violations of international law constitute an obstacle to admissibility is in turn a question that refers to both international and domestic rules.

This means that in making the decision whether or not to copy the information in the diary folder, the Trojan would need to reason across three different contexts:

a) Is the investigative action permissible under the law of the home jurisdiction?
b) Is the investigative action permissible under the law of the target jurisdiction?
c) Is there a "higher order" international context that exceptionally overrides the consequences of the answers to a) and b)?

Let us illustrate these ideas through an example. Our suspect starts his journey in Germany, the Trojan resides on his laptop. Assume Parliament has enacted the enabling law required by the Constitutional Court when ruling for the first time on the issue of remote online searches. Assume furthermore that the future law regulating online searches as sui genesis investigative activities prescribes, as it is likely, a maximum time that the Trojan can remain active. The purpose of this restriction is the need to differentiate online searches from continuous surveillance activities, which are governed by more restrictive procedural safeguards. The Trojan now starts making copies of the material it finds on the laptop's hard drive, sending them back to the human investigator. Copies of the diary are inadmissible, and ideally would not be communicated to the police in the first place. The other material, by hypothesis, is admissible under German law assuming the Trojan did not remain active for longer than permitted. If the suspect uses wireless internet access, potential problems under international law occur once he gets near the Dutch–German border, where it may not always be possible to determine if the computer is still on German soil. On arrival in the UK, and

assuming permission has been granted by the UK authorities, (at least) two issues arise: Under UK law, also the diary would be permissible in evidence. Since both the UK and Germany are as EU member states bound by the convention on mutual legal assistance, this seems to render the diary evidence admissible also under German law. This however would conflict with constitutional core guarantees, which would potentially constitute an exception from the convention. What however if the Trojan remained active for marginally longer, or reported marginally more often than permissible under German law? Since this provision too does not have a counterpart in UK law, this does not violate the *lex loci* of the investigative action. In this case though, the European Convention seems to apply, and the apparent violation of German law can not be used to suppress the evidence.

Conversely, none of the evidence collected by the Trojan would be admissible under UK law, as it violates the rules on digital evidence under PACE, the Police and Criminal Evidence Act 1984. Since the Trojan only produces a copy of the evidence, and furthermore is situated on a "live" computer interfering with its proper working, the "best evidence" rule is violated and the exceptions established under PACE do not apply. PACE regulates the actions of the police in England and Wales, particularly in relations to such issues as searches and powers of entry. However, this violation of police procedure under the *lex loci* is harmless as far as the use of the evidence in a German court is concerned. In Germany, the courts are willing to accept expert evidence as to the reliability of the digital data on a case by case basis, drawing the border between scientific expertise and legal regulation differently from the UK. However, the resulting violation of UK procedure is not of a nature that threatens the validity of the permission given (hypothetically) to the German police to carry out the online search. When our suspect travels to the US, the European

convention on mutual assistance does not apply any longer, and the diary becomes again inadmissible.

IV. Federal Trojans and Computational Jurisprudence

As we have seen above, the use of remote forensic tools as investigative aids raises some pertinent legal issues, several of which are connected to the porosity of borders in the internet age. Trojans used by the police have the potential of increasing the efficiency of investigative actions, but also pose new threats to personal privacy and other core liberties. The response by the German Constitutional court so far has followed traditional regulatory modes to control this new technology. The inevitable outcome of this approach is the need for post-investigation scrutiny, first by the investigative judge and ultimately by the courts. Potentially more promising is regulation by software code, enabling the Trojan to perform autonomously parts of the legal reasoning described above, and make it "understand" the rights and limitations that apply to its investigative actions.

To realise their full potential in the fight against crime, Trojans should ideally be able to address these concerns "by design", ensuring *e. g.* that a Trojan that collects unsupervised suspicious data does not waste police resources by collecting information that due to its nature would be inadmissible in court, does not expose the police to litigation for civil rights violation and at the same time utilises all those additional powers granted to the police but not available to commercial agents, such as the penetration of firewalls or other manipulation of a computer system that would constitute a violation of the law if committed by a private person. For a specific type of software programs, autonomous agents, this idea has already been intensively studied. Trojans can be seen as a particularly simple form of autonomous agent, and for our purpose, everything that applies to the (software) code based regulation of agents also applies

to Trojans. The need to imbue autonomous agents with explicit legal knowledge was first recognised in commercial applications.[19] Hohfeld's formal system of rights and duties in particular has been proposed as a framework for agent communication languages.[20]

Other attempts at computational implementation of Hohfeld's theory have been developed in the wider AI and law community, but not for use with autonomous agents in mind. Layman Allan's language "A-Hohfeld" and Sergot's analysis of normative positions[21] have been the most developed approaches so far. Their intended use as interpretative tool for text analysis and analysis of bureaucratic organisations respectively however make a transfer of these ideas to agent communication languages however less straightforward. Hohfeld's own original work was primarily concerned with private law concepts, and it is at least not obvious that his framework can be transported to a criminal law setting.

However, there has been an intensive debate in analytical jurisprudence following Hohfeld's paper and further positions and correlations have been identified.[22] Due to their intended use in jurisprudence, they don't take computational characteristics at their heart, but offer the advantage of considerably extending the expressive power of the resulting formalisms, thus providing expressive power which may well be necessary to represent the legal concepts iden-

[19] Hahn, Cristian *et al.*, "Framework for the Design of Self-Regulation of Open Agent-based Electronic Marketplaces", *Proceedings of the 1st International Symposium on Normative Multiagent Systems* (NorMAS2005), 2005 at *http://72.14.207.104/search?q=cache:nBJUrfaGX1UJ:www.aisb.org.uk/publications/proceedings/aisb05/8_Normas_Final.pdf+Hahn+Fley+Florian+Agents&hl=en*.

[20] Krogh, Christian and Herrestad, Henning, Hohfeld in cyberspace and other applications of normative reasoning in agent technology, *Artificial Intelligence and Law* 7 1999, pp. 81-96.

[21] Sergot, Mark, "Normative Positions", in McNamara, Paul and Prakken, Henry (eds.), *Norms, Logics and Information System*, Amsterdam, Netherlands, IOS Press, 1999, pp. 289-308.

[22] See in particular Lindahl, Lars, *Position and Change: A Study in Law and Logic*, Dordrecht, Netherlands, D. Reidel Publishing, 1977; Ross, Arne, *Directives and Norms*. London, UK, Routledge, 1968.

tified here as necessary for "law compliant" collection of evidence. The next task then would be to develop a fully formalised representation of the relevant legal relations, and to show how they can be used by computational agents.

As a first, very cursory step, the following example demonstrates the intended use of Hohfeld-type languages for addressing the problems we have identified above. If our Trojan finds itself on the intranet run by a law firm, for instance because the suspect connected his computer to the machine of his lawyer, it should "understand" that the information on this side is protected by "*immunity*", which triggers a corresponding "*disability*" by the agent to collect information unless there is also a superseding *power* to change the relation between lawyer and police, for instance if the jurisdiction in question allows exceptional violations of the client privilege if certain formal conditions are met. The Hohfeldian terms are represented formally as if-then rules. The documentation of these conditions would be part of the "header" of the program that the agent executes, ensuring continuous documentation of all the procedural steps that have been undertaken. In our example, the Trojan would stop analysing data once it "knows" it is outside German territory (for instance because the suspect accesses the internet from a foreign telephone line). Crossing a border triggers by default an immunity of the suspect.

However, this relation between software and suspect can be changed by the exercise of sovereign power by the target state which permits (exceptionally) out-of-border searches. Consequently, the Trojan needs to be able to perform "defeasible" reasoning: applying a general rule first, but capable of revising the result of the rule application if exceptions are triggered.

Giovanni Sartor has shown how these legal relations can be expressed formally in a system that combines action logic with a minimal deontic logic using a formalisation of basic legal concepts inspired by Hohfeld's work, but in-

tended for agent communication.[23] We show very briefly how his definitions, intended primarily for private law interactions, can be made useful for our context.

We have seen how the movements of the suspect over time, and the corresponding procedural actions by the investigators, affect the legal status of the evidence. This can be expressed in a simple action logic with temporal parameters. This gives us two operators, "Does $_{(x,t)}$" and "Brings-about $_{(x,t2)}$". The first can be used to express *e. g.* that at time t, Peter moves the laptop to the UK, and a similarly structured "Does $_{(y,t2)}$" can be used to express the idea that the Trojan performs at t_2 the investigative action to copy the computer's content. The second type of sentence can be used to express the idea that the German police officer Schmidt brings about the permission to investigate Peter in the UK, through the appropriate application for assistance. In a problematic setting, the order of these events is either reversed, or the "brings about X" part is missing altogether. Appropriate axiomatisations for both the temporal and the action logic dimension can be found in the work of Horty.[24]

We can apply to both actions the usual basic deontic modalities, to obtain obligations and permissions:

Obl Does_j [acts on a reasonable suspicion]
(it is obligatory that j acts on a reasonable suspicion)

Would for instance express the criminal law principle that the police has a positive duty to investigate all crimes that come to their attention, something German law knows as the "Legalitätsprinzip" (principle of mandatory prosecution). Extraterritorial use of the Trojan has the potential of violating this principle, simply by bringing offences to the knowledge of the authorities they are not supposed to know

[23] Sartori, Giovanni, "Fundamental Legal Concepts: A Formal and Teleological Characterisation", *Artificial Intelligence and Law*, 14, 2006, pp. 101-142.

[24] Horty, John, *Agency and Deontic Logic*, Oxford, UK, Oxford University Pres, 2001.

about under international law, and has the potential to give a disincentive to search too widely across datasets.[25] To express the contradictory principle, the "principle of opportunity" (Opportunitätsprinzip), we would need the deontic operator of "Facultativity". An action A is facultative when both A and A's omission are permitted. This can be used to express the idea that the Trojan may apply the set of investigative norms relevant for the German courts in collecting the evidence, or omit to carry out these investigative actions if they violate the lex loci, the procedural norms of the target state. In this way, we can formally represent the informal reasoning above that violation of local procedural norms is on the one hand normally harmless as far as admissibility in domestic courts is concerned, but that it is advisable to comply with the procedural norms of the target state wherever possible to observe international legal norms. This way, the apparent and problematic inconsistency between the two norms is remodeled as a facultative choice between legal contexts or orders, changing in the process the norms deontic status.

By contrast, a "bring about" sentence within the scope of the Obligation modality can express the idea that a Trojan may "have to forget" data that it obtained during an investigation, for instance if it made initially a copy of the diary and the laptop has left the scope of the European convention before it can be transmitted back to the "handler" of the Trojan.

Obl Brings_j [k's personal data are cancelled]

(it is obligatory that j brings it about that k's personal data are cancelled)

This allows us to deal at least partly with the changing status of the evidence over time.

[25] Klose, Arno, "Vertrauensschutz kontra Legalitätsprinzip. Schutz personenbezogener Daten in der Jugendhilfe – rechtliche Grenzen der Kooperation von Polizei und Jugendbehörden. Koflikte, Schnittstellen, Kooperation zwischen Jugendhilfe und Polizei", in Bystrich, Herbert *et al.* (eds.), *Jugend – Hilfe – Polizei. BISp-Jahrbuch*, Nürnberg, Germany, Institut für soziale und kulturelle Arbeit, 2004, pp. 113-128.

When one is obliged not to perform a certain action we can say that one is forbidden from doing that action. This can express absolute investigative prohibitions, for instance carrying out investigative actions abroad without the explicit permission of the target state.

Forb $Does_j$ [transmit information gathered while laptop abroad]
(it is forbidden that the Trojan transmits copies of the suspect's computer while the machine is abroad)

As discussed, this is a defeasible norm that can be overridden once the permission has been granted.[26]
We can contrast this with a situation where the target country gives explicit permission to use his material "as if" it was legally obtained.

Perm $Brings_{UK}$ [$Perm_{Trojan}$ carry-out- investigative-action X in accordance with German law]
(it is permitted that the UK allows that the Trojan can act in accordance with German law (and not, for instance PACE as relevant UK legislation)

In this case, the UK grants a license which changes the normative position of the Trojan. This type of activity is particularly important for our context – a warrant by the right authority is the typical example for such a change of legal position. .
Hohfeld, and following him Sartor thought these types of interaction important and distinct enough to merit their own category, that of "privilege" (Hohfeld) or "potestative right" (Sartor). To give a full analysis here would go beyond the scope of this exploratory essay, so a short indication will have to suffice. We give here only one example that

[26] Sartori, Giovanni *et al.*, "Norm Modifications in Defeasible Logic", in Moens, Marie-Francine (ed.), *Proceedings of Jurix 2006*, Amsterdam, Netherlands, IOS, 2006, pp. 13-22.

re-uses an example from Roman private law discussed by Sartor:A previously ownerless animal, through capture, becomes owneed by its captor. That is, the captor has a privilege to perform a certain act (he may or may not capture the animal); but once he performs this act, the legal relation between the animal and anybody else changes. Whereas everyone initially has the same privilege, once it is substantiated by one person, this privilege changes into a no-right.

Formally expressed:

for any (x,y) when [animal y does not belong to anybody]
then Potestative Right (x)
[x becomes the owner of y] via [capturing y]

(for any person x and animal y, if y does not belong to anybody, then x has
the potestative-right of becoming the owner of the animal, by capturing y)

"Potestative right", an aspect of the Hohfeldian privilege, is in turn defined in terms of modal logic, enabling the desired inference. In our context, this simple formalism would already capture some of the issues expressed above. First, we can use it to "tell" the agent that unless certain conditions are met, it has no-right collecting certain data. Together with a suitable meta-rule that enshrines aspects of the legality principle, in particular the idea that an agent can only act if it has an explicit legal basis to do so, from this if follows that it is prohibited from collecting the data Once a suitable antecedent is however met, *e. g.*, [x displayed suspicious behaviour y], this allows the agent to switch the legal status of x and to start investigative actions.

So far, the reasoning that the Trojan/autonomous agents performs remains *within* the normative order of the legal system from which it originates. This is in line with most currently available approaches to modeling legal reasoning in

the Law and Artificial Intelligence community. It is also in line with most of the approaches developed in legal reasoning and formalist jurisprudence. Since in these approaches, reasoning takes place *within* a legal system, the notion of system itself remains implicit – we notice borders only when we have to cross them. In this approach, inconsistencies are an anomaly, and have to be reconciled before formalization takes place, for instance through imposition of hierarchies of norms or rule-exception structures.

However, as we have seen for our application, this may well be insufficient. Here, we have to reason explicitly about different legal contexts, and that they are only internally consistent, but mutually inconsistent is not so much an aberration but an expected and inevitable aspect of the problem. We therefore need not only formal representations of norms, we have to have formal representations of the concept of legal system itself, and an inference engine that allows to draw conclusion in the presence of "global" inconsistencies. While the individual elements of such a formal representation of multi-jurisdiction legal reasoning exist in principle, they have so far not been brought together in one system that could be implemented computationally.

The first element is a formal representation of the notion of "legal system". To be adequate for our purposes, the formal representation of a legal system should enable us to express formally a number of related concepts:

— The idea that norms are part of such a system.
— The idea that certain norms are part of one system but not another.
— The idea that some rules are part of more than one system. Systems can overlap, for instance through the process of borrowing, or by incorporating the same international convention.
— The idea that legal systems can have discreet and mutually incompatible sub-parts (the devolved laws in federally organized jurisdictions).

— The idea that several legal systems can group together for a supranational "legal context", for instance the European Union, or the group of all legal systems that accept a certain international law.

Our Trojan operates not just in a multi-jurisdiction, but also in a multi-language environment. Formal ontologies are therefore an obvious choice to represent laws and legal systems, and to express the idea that laws formulated in different languages can conceptualize the same underlying reality. Ontology modeling has been used in several projects that address computational representation of legal norms in multi-language contexts, and can be considered an increasingly mature technology.[27] One such project, the POIROT project on ontology-based prosecution of financial fraud, shares with the issues discussed here not only the issue of multi-jurisdiction prosecution of crime, but also developed as part of its remit agent technology for the gathering of crime intelligence which differs from the approach discussed here only in its more overt nature. The POIROT methodology also shows that there is a natural convergence between comparative methodology and ontology oriented modeling in the legal domain.[28]

However, to model the legal reasoning described in informal terms above, a "richer" representation of the relation between norms, legal systems and supra-national legal contexts is necessary. In the existing approaches, comparative legal knowledge informs the formalization, but it is not normally possible to reason within the formalism about legal comparison – comparative law is part of the knowledge acquisition process, but not explicit part the legal representation itself.

[27] See for instance the ESTRELLA project, *http://www.estrellaproject.org/index.php/Main_Page*.

[28] Schafer, Burkhard *et al.*, "Towards a Financial Fraud Ontology: A Legal Modelling Approach", *Artificial Intelligence and Law*, 12, 2006, pp. 419-446.

By contrast, we have shown elsewhere how borrowing from "semantic" approaches to the theory of science allows the formal representation of the ontological assumption and key concepts of comparative law directly, as set theoretically structured objects. "Structural" descriptions of this type seem to be particularly suited to express the interdependence between contexts that we identified above as a crucial reasoning task for our problem. It is not sufficient to carry out analysis within one system. Rather, the procedural and evidential laws of different countries, just like the rules of international private law, often refer to each other. To determine if evidence discovered in the UK is admissible in German courts requires a parallel, and hypothetical, analysis of the problem in different contexts. Did the investigative action violate UK law on privacy protection, and was the violation of a nature that had it taken place in Germany, inadmissibility of the evidence would have resulted? Alternatively, can the UK decision be recognized for the purpose of German procedural law? To express an analysis of this type, and the comparative legal approximations that it presupposes – is the common law notion of "reasonable expectation of privacy" a suitable equivalent to the German "Privatsphäre" - requires formal equivalents not just of laws and legal systems, but also of the theoretical relations that can exist between them. Those relations, as we have seen, in our case are often in turn part of the international legal order.

It is beyond the scope of this paper to supply a formal analysis of a reasonably sizeable part of the laws of evidence in the vocabulary of these set-theoretical representations of theories and theory-relations. We describe only very briefly some of our key findings: The formal equivalent to "real" systems are set-theoretical structures, the *models* of a theory. They have the form of a list:

$<D_1,....D_k; R_1,....R_k>$

The D_i introduce a theory's "ontology", the objects it assumes. The R_i are relations over the D_i. In a mathematical example, D_1 could be *e. g.* three lines and D_2 a circle on a blackboard, R_1 the relation "is parallel to" and R_2 the relation "is tangential to", the first defined between members of D_1, the second on D_1 x D_2. In our legal example, D_1 could be the set {John, Police-officer- }, D_2 the set {computer}. The Relation R_1 could be the privilege relation defined above "Police officer has-privilege-to seize the computer of John", defined over D_1 x D_2.

Models M so conceived decide the identity of a theory. They are assumed to satisfy the basic laws of the theory. In structuralism, *any* means to describe these models will do. Rather than requiring an explicit set of axioms, these conditions are summarised in informal set theory, by the introduction of a "second order" set-theoretical predicate. To introduce these predicates, a refinement of the notion of model is necessary. We have said above that our models satisfy the (unspecified) axioms or basic laws of our theory. Some of these laws will have a special form: They make use of only one of the relations introduced above. A model that contains only laws of this form is called a "potential" model M_p. They provide the conceptual frame of a theory, but are not sufficient to make "empirical" claims. Intuitively, they describe all those structures for which the question: "are they a model of our theory" makes sense - without answering it. It makes sense to ask for a system that contains two humans whether it is an "arrest situation". It does not make sense to ask this question for a system consisting of two rocks.

"Actual" models on the other hand are models which satisfy at least one "cluster law", that is a law which links at least two relations in a way that the content cannot be expressed by a translation using only one. An example from law would be: If Peter seizes John's computer without a warrant, then John has the right to ask for the evidence to be suppressed in court. This sentence uses the relation:

"seizes without warrant" and the relation: "ask for evidence to be suppressed", and neither of them can be replaced by the other. Obviously, $M \grave{I} M_p$.

The tuple $<M_p\ M>$ is called a "model element". They are the smallest elements necessary to formulate a statement about the world: M_p provides the conceptual frame, a larger class of possible models, and M the class of structures that actually satisfy the claims of the theory.

With this, we have already the components necessary to formulate the set-theoretical predicates mentioned above. Let us look at an example. We can define the predicate "x is a German law theory on privacy in criminal procedure (GCP)" so that x is a model of the theory GCP iff there are $D_1,....D_k$: $R_1,...R_k$ so that

$x = <D_1,...D_k; R_1,...R_k>$ and
1. B_1 $(D_1,....D_k; R_1,...R_k>$
.....
s. B_s $(D_{1,},....D_k: R_1,...R_k)$

The first clause introduces the underlying ontology of privacy law – all those real life configurations for which it makes sense to query whether a "suppression relation" is present. The B(D,...R) symbolise the basic laws of the theory, e.g. the relation between privacy and inadmissibility mentioned above. Such a scheme defines the class of all entities for which "x" can be substituted. This set is then the set of all models for GCT.

Set-theoretical predicates are then used as the formal representatives of comparative legal categories. We start with simple categories of the form: "x is a German privacy law theory" and extend them systematically to more complex and general predicates as "x is a privacy law theory of the European Convention on mutual assistance" on the one hand, "x is a German evidence theory" on the other hand. This means that "models" or "applications" *are* used directly in our definition. This reflects Zweigert and Kötz' idea that applications or problems, and not textbook definitions are

the common denominator of legal systems in one and the same family.

Legal systems and supranational legal contexts are seen as "co-ordinated theory elements", and this leads us to the next distinguishing feature of our approach. One consequence of this approach, in both law and natural sciences, is that universal laws lose their privileged status. Rather than treating sentences of the form: If someone carries out an illegal search, the evidence becomes inadmissible" as building blocks of a theory, here models of the form: "the event that someone illegally searches another's computer has the property that it is an evidence law event" form the basis of law. Application and rule become one, and the notion of the legal case as a "story"[29] is directly and formally expressed.

One of the basic assumptions of structuralism is that "mini-theories" which are based on single model elements, never stand alone. Models of different model elements are mutually connected. Intuitively, these links between different models can have two forms: They can be links between models of the same theory, or they can link models of different theories. Applied in a legal context, this expresses the idea of "systemhood" of law.

Links between models of the same theory are called constraints. The most important are identity links, which are functions that assign the same value to the same objects in two models. In classical mechanics, a particle will have the same mass in all models in which it appears. If we transfer a billiard ball from its table to our laboratory, its mass remains the same. In law, the protection that a German suspect receives through the constitution is the same whether she is in Berlin or Munich. "My laptop being remotely searched while in Berlin" and "my laptop being remotely searched while in Munich" are two (partial) models of the "admissibility of remote searches" theory. Since the "terri-

[29] See Jackson, Bernard, *Making sense in the law*, London, UK, Deborah Charles Publication, 1996.

tory" and "citizenship" functions assign the same value to my privacy protection in both models, I will get the same protection. Formally, constraints are relations over the power set of partial models of a theory element. More precisely, a constraint C for M_p is a non-empty subclass of $Po(M_p)$. The triple $<M_p, M, C>$ will also be called the (formal) *core K* of a theory.[30] Intuitively, identity functions such as territory and citizenship allow us to represent the different "contexts" discussed above. Extraterritorial searches are situations where the range of an identity function is limited – I'm not quite the same person (legally) when travelling abroad.

This leads to the final element of our theory, links between models of different theories or "bridges".[31] Again, they are relations over the products of their partial models, but of a more complex form. The more links there are between two theories and the denser the complex they build, the more similar they are.[32] This allows us to express formally the idea that within the EU, the closer integration of states changes the meaning of certain national evidence laws, but as soon a relation to a non-EU state is concerned, the original meaning reasserts itself.

The concept of bridges between theory clusters also allows us to represent the idea that the more technical aspects of say PACE are at the periphery of UK evidence law, whereas the hearsay or the best evidence rule are forming its core. Legal systems are structured objects, with the individual constituent part more or less densely linked to other

[30] This expression is chosen intentionally to emphasise that this approach can be understood as a formal version of the common core approach in comparative law, see Bussani, Mauro, "Current trends in European comparative law: the common core approach", 21 *Hastings Int'l & Comp. L. Rev.*, 1999 p. 785.

[31] Moulines, Carlos Ulisses and Polanski, Marek Bridges, "Constraints, and Links", in Balzer, Wolfgang and Moulines, Carlos Ulisses (eds.), *Structuralist Theory of Science. Focal Issues, New Results*, Berlin, Germany, Springer, 1996, pp. 219-232.

[32] Moulines, Carlos Ulisses, "Towards a Typology of Intertheoretical Relations", in Echeverría, Javier *et al.* (eds.), *The Space of Mathematics*, Berlin, Germany, Springer 1992 pp. 403-411.

parts. The more links a sub-theory has to other theories, the more important it is for the identity and core value commitments of that legal system. We have seen above that this may be necessary to assess if the violation of a *lex loci* rule results also in inadmissibility at the home courts.

In conclusion, while formal theories of legal reasoning have so far largely avoided analysis of multi-jurisdiction reasoning, there are external to jurisprudence some formal theoretical approaches whose vocabulary and expressive power enables them to model legal reasoning across contexts. Developing suitable formal representations of legal reasoning using these theories has the potential not only to provide us with tools to carry law into cyberspace, it can also change the way we think about the nature of legal reasoning and the formal modelling of valid legal argumentation.

V. Bibliography

BERKOVSKY, Shlomo *et al.*, "Examining users' attitude towards privacy preserving collaborative filtering", in *Proceedings of DM.UM'07*, 2007, *http://vasarely.wiwi.huerlin.de/DM.UM07/Proceedings/berkovsky.pdf*.

BLUM, Jack and PASSAS, Nikos, "Controlling Cross Border Undercover Investigations", in FIELD, Stewart and PELSER, Caroline (eds.), *Invading the Private: State, Accountability and the New Investigative Methods in Europe*, Dartmouth, UK, Aldershot, 1998.

BUSSANI, Mauro, *Current trends in European comparative law: the common core approach 21 Hastings Int'l & Comp. L. Rev.*, 1999.

CARRIER, Brian and SPAFFORD, Eugene, "Getting Physical with the Digital Investigation Process", *International Journal of Digital Evidence* 2 2003.

FINJAUT, Cyrille, "Transnational Organized Crime and Institutional Reform in the European Union: The Case of

Judicial Cooperation", in WILLIAMS, Phil and VLASSIS, Dimitri (eds.), *Combating Transnational Crime: Concepts, Activities And Responses,* London, UK, Routledge 2001.

HAHN, Cristian *et al.*, "Framework for the Design of Self-Regulation of Open Agent-based Electronic Marketplaces", *Proceedings of the 1st International Symposium on Normative Multiagent Systems (NorMAS2005)* 2005 at *http://72.14.207.104/search?q=cache:nBJUrfaGX1UJ:www.aisb.org.uk/publications/proceedings/aisb05/8_Normas_Final.pdf+Hahn+Fley+Florian+Agents&hl=en*.

HORNUNG, Gerrit, Ermächtigungsgrundlage für die "Online-Durchsuchung"?, *Datenschutz und Datensicherheit* 31 2007.

HORTY, John, *Agency and Deontic Logic,* Oxford, UK, Oxford University Pres, 2001.

JACKSON, Bernard, *Making sense in the law*. London, UK, Deborah Charles Publication, 1996.

KLOSE, Arno, "Vertrauensschutz kontra Legalitätsprinzip. Schutz personenbezogener Daten in der Jugendhilfe – rechtliche Grenzen der Kooperation von Polizei und Jugendbehörden. Koflikte, Schnittstellen, Kooperation zwischen Jugendhilfe und Polizei", in BYSTRICH, Herbert *et al.* (eds.), *Jugend – Hilfe – Polizei. BISp-Jahrbuch* Nürnberg, Germany, Institut für soziale und kulturelle Arbeit, 2004.

KROGH, Christian and HERRESTAD, Henning, "Hohfeld in cyberspace and other applications of normative reasoning in agent technology", *Artificial Intelligence and Law* 7 1999.

LEIPOLD, Klaus, "Die Online-Durchsuchung", *Neue Juristische Wochenschrift* , 2007.

LESSIG, Larry, *Code and Other Las of Cyberspace*, New York, USA, Basic Books, 2000.

LINDAHL, Lars, *Position and Change: A Study in Law and Logic*, Dordrecht, Netherlands, D. Reidel Publishing, 1977.

MOULINES, Carlos Ulisses and POLANSKI, Marek, Bridges, "Constraints, and Links", in BALZER, Wolfgang and MOULINES, Carlos Ulisses (eds.), *Structuralist Theory of Science. Focal Issues, New Results*, Berlin, Germany, Springer, 1996.

MOULINES, Carlos Ulisses, "Towards a Typology of Intertheoretical Relations, in ECHEVERRÍA, Javier *et al.* (eds.), *The Space of Mathematicsm*, Berlin, Germany, Springer 1992.

O'NEILL, Megan, *Policing Football: Social Interaction and Negotiated Disorder*, Houndmills, UK, Palgrave Macmillan, 2005.

ROSS, Arne, *Directives and Norms*, London, UK, Routledge, 1968.

SARTORI, Giovanni, "Fundamental Legal Concepts: A Formal and Teleological Characterisation", *Artificial Intelligence and Law* 14 2006.

——— *et al.*, "Norm Modifications in Defeasible Logic", in MOENS, Marie-Francine (ed.), *Proceedings of Jurix 2006*, Amsterdam, Netherlands, IOS, 2006.

SCHAFER, Burkhard, "The taming of the Sleuth-problems and potential of autonomous agents in crime investigation and prosecution", *International Review of Law, Computers and Technology*, 20, 2006.

——— *et al.*, "Towards a Financial Fraud Ontology: A Legal Modelling Approach", *Artificial Intelligence and Law*, 12, 2006.

SERGOT, Mark, "Normative Positions", in MCNAMARA, Paul and PRAKKEN, Henry (eds.), *Norms, Logics and Information System*, Amsterdam, Netherlands, IOS Press, 1999.