PhD RESEARCH

Request to be included

If you completed a PhD regarding an element of electronic evidence and electronic signatures, or are involved in a research project in this field, and would like to have your details added to our Current Research section or PhD listing, please download and complete a submission form (docx) and send by email to: stephenmason@stephenmason.co.uk

PhDs completed

Name of candidate: Claudia Warken

University at which the PhD is registered and the awarding institution: Universität Heidelberg, Heidelberg (University of Heidelberg, Heidelberg, Germany)

Department or faculty: Juristische Fakultät der Universität Heidelberg (Faculty of Law of the University of Heidelberg)

Title of the degree: Dr. jur.

Title of the thesis:

> Klassifizierung elektronischer Beweismittel für strafprozessuale Zwecke
>
> Classification of electronic evidence for criminal law purposes

Brief description (it will be helpful if you provide this information in both your native language and in English if the degree was not written in English):

Die Arbeit beschreibt die Notwendigkeit der (Neu-) Klassifizierung elektronischer Beweismittel, da die derzeitige Unterscheidung vieler Strafprozessordnungen von Kommunikationsdaten in Bestands-, Verkehrs- und Inhaltsdaten nicht zielführend ist. Es wird gezeigt, dass sich eine Klassifikation ausschließlich nach dem aus den einschlägigen Grundrechten hergeleiteten Kriterium der berechtigten Erwartungshaltung der Vertraulichkeitswahrung des Datensubjekts richten darf. Sie erlaubt eine Unterscheidung in Kernbereichsdaten, geheime Daten, vertrauliche Daten, beschränkt zugängliche Daten und unbeschränkt zugängliche Daten. Diese Klassifikation ist umfassend und technikneutral und daher beständig.

Die Arbeit beinhaltet einen umfassenden Gesetzesentwurf zur entsprechenden Neuregelung am Beispiel der deutschen Strafprozessordnung.

The thesis explains the need of a new classification of electronic evidence as the common distinction between subscriber data, traffic data and communication content data is no longer suitable for both legal and practical reasons. The key criterion for determining the sensitivity of a dataset which derives solely from the specifically affected fundamental rights is the data subject's reasonable expectation of confidentiality. It allows a distinction of electronic data as follows: data of core significance for private life, secret data, shared confidential data, data of limited accessibility, and data of unlimited accessibility. The newly proposed classification is comprehensive and technically neutral – thus, future-proof.

A comprehensive legislative proposal addressing the topic and exemplarily referring to the German Code of Criminal Procedure (Strafprozessordnung) is included.

Supervisor: Professor Dr Gerhard Dannecker

Rapporteurs: Professor Dr Gerhard Dannecker and Professor Dr Kai Cornelius

Date of registration: 7 May 2018

Date of defence: 1 July 2019

Date of award: 15 July 2019

Thesis published at https://archiv.ub.uni-heidelberg.de/volltextserver/26928/

For a longer description in English, see Claudia Warken, 'Classification of Electronic Data for Criminal Law Purposes', *eucrim, The European Criminal Law Association's Forum*, 2018/4, 226 – 234 at https://eucrim.eu/articles/classification-electronic-data-criminal-law-purposes/

Name of candidate: Lene Wacher Lentz

University at which the PhD is registered and the awarding institution: Aalborg Universitet, Denmark

Department or faculty: Juridisk Institut (Department of Law)

Title of the degree: PhD

Title of the thesis:

> Politiets hemmelige efterforskning på internettet
>
> The Police's Secret Investigation on the Internet

Brief description:

Formålet med afhandlingen er at analysere den retlige regulering af politiets hemmelige efterforskning på internettet. To typetilfælde af hemmelig efterforskning er udvalgt: Først det 'tekniske tvangsindgreb', hvor politiet skaffer sig hemmelig teknisk adgang til private datasystemer på internettet, hvilket i retsplejeloven er reguleret af tre regelsæt, hemmelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning. Dernæst det 'menneskelige indgreb', hvor politiet under dække interagerer med borgeren for at skaffe beviser mv., hvilket er omfattet af de tre efterforskningsmetoder, infiltration, lokkedue-situationen og agentvirksomhed. Et gennemgående tema i afhandlingen er, hvornår nye efterforskningsmetoder kræver lovhjemmel. I afhandlingen behandles det straffeprocessuelle legalitetsprincip i et digitalt og menneskeretligt perspektiv.

The purpose of the dissertation is to analyse the legal regulation of the police's secret investigation on the internet. Two cases of secret investigation have been chosen for this dissertation. The first case is the 'technical coercive method', which entails that the police gain secret technical access to private data systems, platforms, etc. on the internet, which in the Danish Code of Criminal Procedure is regulated by three sets of rules; (1) covert search, (2) interception of communication and (3) computer surveillance. The second case is the 'human intervention', which entails that the police whilst undercover interacts with the citizen in order to obtain evidence, etc., which is comprised of three methods of investigation, (1) infiltration, (2) decoy situations and (3) undercover agents. A recurring theme in the dissertation is when does new methods of investigation require legal regulations. The principle of legality of criminal procedure is considered in a digital and human rights perspective.

Supervisor: Professor Birgit Feldtmann, Aalborg University

Date of Registration: 1 August 2016

Date of submission of the PhD thesis: 26 July 2019

Date of award: 22 October 2019

Name of candidate: Sofie Royer

Contact: sofie.royer@kuleuven.be

University at which the PhD is registered and the awarding institution: KU Leuven – University of Leuven

Department or faculty: Instituut voor strafrecht (Institute of Criminal Law)

Title of the degree: PhD

Title of the thesis:

> Strafrechtelijk beslag: digiproof en (multi)functioneel?

Criminal seizure: digiproof and (multi)functional?

Brief description:

De traditionele Belgische regels inzake beslag zijn geschreven in de 19de eeuw en sloegen op fysieke voorwerpen, vaak bewijsstukken en wapens. Het strafrecht en de wereld waarin het functioneert, zijn echter zeer snel geëvolueerd. Enerzijds is er nog een belangrijke bijkomende functie van het beslag gekomen, het waarborgen dat geld of goederen beschikbaar zouden blijven voor het uiteindelijk na een soms jarenlange procedure uit te spreken sancties, m.n. verschillende varianten van verbeurdverklaring. Anderzijds stelt de combinatie van globalisering en digitalisering zowel de wetgever als de rechtspractici voor nieuwe uitdagingen. Een aantal waarborgen bij klassiek beslag, zoals de aanduiding en beschrijving van specifieke voorwerpen, het wegnemen en inventariseren, vallen niet onverkort door te trekken naar digitale sporen of bewijselementen. De wetgever heeft in 2000 weliswaar in een specifieke onderzoeksmaatregel (databeslag) voorzien, maar die volstaat niet, nu er steeds meer grensoverschrijdend dataverkeer bestaat, met een belangrijke rol voor de privésector, nu verdachten soms digitale munteenheden gebruiken en er steeds meer continue wisselwerking bestaat tussen fysieke dragers en gegevensverkeer (internet of things). Het opzet van het onderzoek is het vinden van een coherent regime voor de fysieke en de digitale wereld, nu die in elkaar overvloeien. Het is complementair aan en bouwt voort op een doctoraat over de zoeking, waarvan het een soort spin-off is.

The traditional Belgian regulation on criminal seizure was written in the 19th century and covered physical objects, mainly evidence and guns. Criminal law and the world in which it operates have been evolving very quickly. On the one hand, criminal seizure has obtained an important additional function: the guarantee that money or objects would still be available after years of procedure for the sentence to be imposed, in particular the different kinds of confiscation. On the other hand, the combination of globalization and digitalization creates new challenges for lawmakers and legal practitioners. Several guarantees of the traditional seizure, such as designation and description of the specific objects, the removal and inventory, cannot be extended to digital traces and digital evidence. In 2000 the legislator created a specific measure of inquiry (seizure of data). However, this attempt was not sufficient, considering the increasing transboundary data traffic, in which private companies play an important role, since suspects sometimes use digital monetary units and there is a continuous interaction between physical supports and data traffic (internet of things). This research intends to establish a consistent legal framework for the physical and digital world, as they are strongly connected. This research is complementary to and continues on a PhD on criminal searches, of which it is a kind of spin-off.

Supervisors: Professor Dr M. Panzavolta and Professor Dr F. Verbruggen

Date of registration: September 2015

Date of submission: October 2019

Date of defence: 29 January 2020

Date of award: 29 January 2020

Name of candidate: Armando Dias Ramos

University at which the PhD is registered and the awarding institution: Universidade Autónoma de Lisboa (Lisbon Autonomous University)

Department or faculty: Law

Title of the degree: PhD

Title of the thesis:

O agente encoberto digital: vissicitudes na recolha de prova em processo penal

The digital undercover agent: the collection of evidence

Brief description:

A lei portuguesa sobre o cybercrime (Art. 19.º da Lei n.º 109/2009, de 15 de setembro) remete, com as devidas adaptações, para o regime do agente encoberto (Lei n.º 101/2001, de 25 de

Agosto). Essa legislação é de 2001 e a meu ver é desatualizada da realidade tecnológica. Na minha investigação pretende-se provar tal desadequação e afirmar que é necessário mudar as leis de forma a que o agente encoberto possa efetuar uma investigação dentro da lei com salvaguarda dos direitos, liberdades e garantias dos investigados.

The Portuguese law on cybercrime (art. 19.º da Lei n.º 109/2009, 15 September) refers, once the necessary changes have been made, to the regime of the undercover agent (Lei n.º 101/2001, august 25th). This legislation dates from 2001, and my view no longer reflects the technological reality. My research aims to prove such a mismatch and argue that it is necessary to change the laws so that the undercover agent may conduct an investigation within the law to safeguard the rights, freedoms and guarantees of those people that are investigated.

Supervisor: PhD teacher André Ventura

Date of registration: May 2015

Date of defence: 25 October 2018

Publication: Armando Dias Ramos, *A Prova Digital em Processo Penal: O Correio Eletrónico* (2nd edn, 2017, Chiado Books)

Name of candidate: Nikolaos Trigkas, LLB, MBA

University at which the PhD is registered and the awarding institution: University of Aberdeen

Department or faculty: Faculty of Law

Title of the degree: PhD in Law

Title of the thesis:

> Challenging the Presumption of Reliability of Social Networking Website Evidence under U.S. Jurisdiction

Brief description:

Since the dawn of the current century cyber technology has gradually left its mark on the practice of law and electronically stored information (ESI) has become litigants' best ally or worst problem. The centre of the debate can be shifted to the jurisdiction of the U.S., where leading cases involving electronic evidence have been decided. The evidentiary treatment of ESI constitutes a dynamic field of law, yet existing federal rules have failed to keep pace with the technological revolution creating potential for inconsistent and incoherent rulings.

As ESI emerges before the court at a high rate of incidence, it is vital to prevent fundamental juridical principles from being compromised because of the legal community's loose approach to virtual data admissibility. This paper serves a twofold purpose; firstly, it challenges the (rebuttable) presumption of social networking website (SNW) credibility that has been adopted by the prevailing opinion on SNW content authenticity. Secondly, it is a call for consistency of judicial decisions pertaining to SNW evidence authentication, which can be achieved through standardization of computer forensics procedures.

Supervisor: Dr Abbe Brown

First internal examiner: Dr Philip Glover

First and second external examiner: Stephen Mason

Second internal examiner: Professor John Paterson

Date of registration: 1 September 2014

Date of submission: November 2017

Date of viva: 15 February 2018

Date of award: April 2019

Name of candidate: Dominikos Arvanitis

Contact: arvanitis.dom@dsa.gr

University at which the PhD is registered and the awarding institution: Panteion University of Social and Political Sciences (Athens)

Department or faculty: Department of International, European and Area Studies

Title of degree: PhD in International, European and Area Studies (with specialisation in the area of international criminal law)

Title of PhD thesis:

Cooperation in criminal matters in the European Union and Human Rights: the instrument of European Investigation Order

Brief description:

The European Investigation Order (EIO) was established by Directive 2014/41/EU, and shall be transposed into Member States' national legislations by 22 May 2017 (with the exception of Denmark and Ireland). The necessity for this instrument occurred because the – then existing – framework for gathering evidence was too fragmented and complicated and needed to be replaced by a comprehensive single instrument. The EIO is to be issued for the purpose of having one or several specific investigative measures carried out in the Member State executing the EIO (executing state). This instrument does not only concern the gathering of new evidence but also allows the issuing state to request evidence that the executing authorities already have in their possession. This tool can be compared to the European Arrest Warrant, since it is also based on the principle of mutual recognition of judgements and judicial decisions (article 82§1 TFEU). Most probably, many issues concerning human rights and their violation will be raised by the enforcement of such an instrument.

In the PhD thesis in preparation, firstly we analyse the traditional instruments of cooperation in criminal matters deriving from the Council of Europe's legal framework, as well as the European Union legal framework concerning mutual legal assistance in criminal matters. Then follows an in-depth study of the EIO as a tool to perform investigations and to obtain evidence (namely any investigative measure, including the gathering of digital evidence etc.). Finally we examine this system from a human rights perspective. Indeed it appears of primary importance (to try) to assess whether the enforcement of such an instrument will violate human rights.

Supervisor: Assistant Professor Olga Tsolka

Date of registration: 16 July 2014

Defence: October 2019

Date of award: 27 November 2019

Thesis available at (in Greek): https://www.sakkoulas.com/product/18989-i-evropaiki-entoli-erevnas/

Name of candidate: Juhana Riekkinen

University at which the PhD is registered and the awarding institution: Lapin Yliopisto (University of Lapland)

Department or faculty: Oikeustieteiden tiedekunta (Faculty of Law)

Title of the degree: Oikeustieteen tohtori (OTT) (Doctor of Laws (LL.D.))

Title of the thesis:

Sähköiset todisteet rikosprosessissa. Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen.

Electronic Evidence in Criminal Procedure. On the Effect of ICT and the Development towards the Network Society on the Life-cycle of Evidence.

Brief description:

Suomen esitutkinta-, pakkokeino- ja todistelulainsäädäntöä on uudistettu merkittävästi 2000-luvulla. Monin paikoin todistusoikeuden juuret ovat kuitenkin edelleen ajassa ennen nykyisenkaltaista tietotekniikkaa. Alun perin silminnäkijöitä, fyysisiä esineitä ja paperisia asiakirjoja silmällä pitäen luodut normit ovat haasteiden edessä uudessa digitaalisessa ja verkottuneessa ympäristössä, jossa todisteet ovat enenevästi elektronis-digitaalisen, tietojärjestelmissä käsiteltävän datan muodossa.

Väitöskirjassa pyritään selvittämään, kuinka nykyinen suomalainen todistusoikeus soveltuu verkkoyhteiskunnassa esille nousevien todisteluun liittyvien ongelmatilanteiden ratkaisemiseen. Lisäksi tavoitteena on hahmottaa, millaista todistusoikeutta verkkoyhteiskunnassa tarvittaisiin. Väitöstutkimus keskittyy rikosprosessiin, joskin monet käsitellyistä kysymyksistä ja tuloksista ovat merkityksellisiä

myös siviiliprosessin ja hallintolainkäytön näkökulmasta.

Väitöstutkimus hyödyntää metodinaan oikeusinformatiikan tukemaa lainoppia. Se käsittelee useita oikeudellisia ja käytännöllisiä ongelmakenttiä, jotka liittyvät sähköisten todisteiden elinkaaren eri vaiheisiin, kuten tällaisen aineiston syntyyn, hankintaan, säilyttämiseen, esittämiseen ja arviointiin. Soveltuvia säännöksiä ja ilmiöitä arvioidaan myös prosessioikeuden yleisten oppien – erityisesti rikosprosessioikeuden tavoite- ja arvoperiaatteiden – valossa.

In the 21st century, significant law reforms concerning pre-trial criminal investigations, coercive measures, and evidence in the courtroom proceedings have been carried out in Finland. However, in many respects the roots of the current law of evidence can still be traced to a time well before modern ICT. The legal regulation of evidence that was originally created with eyewitnesses, physical objects, and paper documents in mind is facing challenges in the new digital and networked environment, in which relevant evidence exists increasingly in electronic and digital form as data in computer systems.

The dissertation has the aim of ascertaining how current Finnish law adapts to solving the problems of evidence in the network society. A further aim is to determine what kind of law of evidence is needed in the network society. The research focuses on the criminal procedure, although many questions and results hold relevance in relation to civil or administrative proceedings, as well.

Combining legal dogmatics with legal informatics, the dissertation addresses numerous legal and practical issues having to do with different phases in the life-cycle of electronic evidence, such as creation, collection, preservation, presentation, and evaluation of computer data with evidentiary value. The applicable legal provisions and the relevant phenomena are assessed against the backdrop of the established general principles, goals, and values of procedural law.

Supervisors: Professor Tuula Linna and Professor emeritus Ahti Saarenpää

Reviewer and opponent: Professor emeritus Asko Lehtonen

Reviewer: Supreme Court Justice Jussi Tapani

Date of registration: 5 February 2014

Date of defence: 10 May 2019

Date of award: 5 June 2019

Thesis published: Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa. Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen* (Helsinki: Alma Talent 2019), XXII, pp 597 ISBN 978-952-14-3858-5

Name of candidate: Charlotte Conings

University: Catholic University of Leuven, Belgium

Department or faculty: Faculteit Rechtsgeleerdheid, Instituut voor Strafrecht (Law Faculty, Institute of Criminal law)

Title of degree: PhD

Title of the thesis:

Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld

A coherent criminal procedure regime for search in the physical and digital world

Brief description:

De procedureregels die burgers beschermen tegen zoekingen naar strafrechtelijk relevante informatie, zijn erg versnipperd: huiszoeking, netwerkzoeking, fouillering, telefoon- en informaticatap, bijzondere opsporingsmethoden... Elke vorm van zoeking kent een apart regime met specifieke voorwaarden. Dit is geen typisch Belgisch probleem, de meeste Europese staten kampen er mee. De versnipperde Europese aanpak vloeit immers voor een deel voort uit de strengheid waarmee het EHRM het legaliteitsbeginsel van art.8, 2 heeft ingevuld. In de Verenigde Staten lijkt het 4de amendement bij de Federale Grondwet daarentegen een meer overkoepelend beschermingsmechanisme tegen onverantwoorde zoekingen en beslagen in te houden. De uiteenlopende regelgeving met betrekking tot de zoeking in Europa maakt de

bewijsvergaring inefficiënt. Vooral de digitalisering van bewijs doet ons inzien dat de bestaande regelgeving complex, onduidelijk, achterhaald en inconsistent is. Het onderzoek tracht te komen tot een vereenvoudigde regeling voor efficiëntere bewijsvergaring zowel in nationale als in internationale context, die aangepast is aan de digitale realiteit en bestand tegen toekomstige technologische evoluties.

The Belgian criminal procedure regime for searches is very fragmented. It contains specific regulations for house search, for frisking, for strip search, for wire- or data tapping, for visual observation, for infiltration etc. This approach forms part of a bigger legal picture in two different ways. First of all, the fragmentation into detailed sub regimes is an often criticized characteristic of the Belgian Code of Criminal Procedure as such. On the other hand, the fragmented approach is not typical to Belgium but is also known in other parts of Europe. To a certain extent this can be attributed to the severe interpretation of the legality principle of art. 8, §2 ECHR by the European Court of Human Rights.

However, such fragmented criminal procedure regime for searches causes numerous problems and renders evidence gathering inefficient, not only in a national but also in an international context. Especially digitalization of different types of evidence exposes the complex, unclear, outdated and inconsistent character of the existing legal framework.

This research aims at creating a simplified and clearer comprehensive regulation for searches aimed at gathering criminal evidence, which can make national and international evidence practice more efficient. It should be fit for use in a digitalized society and at the same time be resistant or adjustable to future technological evolutions to the largest extent possible. We will look for a general legal framework for search with certain specific regimes which are necessary to strike a balance between efficient law enforcement and other countervailing legal interests like the right to privacy, due process and human dignity.

Supervisors: Professor dr. Frank Verbruggen and Professor dr. Raf Verstraeten

Date of registration: 1 September 2012

Date of defence: 12 December 2016

Date of award: 12 December 2016

Thesis published: Charlotte Conings, *Klassiek en digital speuren naar strafrechtelijk bewijs (*Antwerpen, Intersentia, 2017), ISBN 9789400008144

Name of candidate: Giuseppe Vaciago

University: Università degli Studi di Milano-Bicocca (University of Milan – Bicocca)

Department or faculty: Facoltà di Giurisprudenza (Faculty of Law)

Title of the thesis:

Digital forensics, procedura penale Italiana e diritti fondamentali dell'individuo nell'era delle nuove tecnologie

Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age

Brief description:

Il mondo digitale interagisce con la giustizia in molteplici segmenti: sempre più numerosi sono i casi in cui esso è sede di reati (dal furto di identità, fino ad arrivare al cyberterrorismo) e non lontani sono i tempi in cui esso sostituirà il tradizionale modo di intendere il processo (questo sta già accadendo nel processo civile e presto accadrà anche nel processo penale). Come Sherlock Holmes nel XIX secolo si serviva costantemente dei suoi apparecchi per l'analisi chimica, oggi nel XXI secolo, egli non mancherebbe di effettuare un'accurata analisi di computer, di telefoni cellulari e di ogni tipo di apparecchiatura digitale.

La presente opera si prefigge due compiti: il primo è quello di offrire al lettore un'analisi della prova digitale e dell'articolato sistema di regole e procedure per la sua raccolta, interpretazione e conservazione. La casistica giurisprudenziale, non solo italiana, ha dimostrato come l'errata

acquisizione o valutazione della prova digitale possa falsare l'esito di un procedimento e come il digital divide sofferto dalla maggior parte degli operatori del diritto (magistrati, avvocati e forze di polizia) possa squilibrare le risultanze processuali a favore della parte digitalmente più forte.

This paper focuses specifically on digital forensics and the rules and procedures regulating the seizure, chain of custody and probative value of digital evidence, with particular emphasis of three distinct aspects. Firstly, the extremely complex nature of digital evidence; Secondly, the dire need for an adequate level of computer literacy amongst judges, lawyers and prosecutors. The last, but no less crucial aspect involves the potentially prejudicial effects of invasive digital forensic techniques (such as the remote monitoring of data stored on hard drives) on the suspects fundamental freedoms (the right to privacy and the inviolability of personal correspondence) and due process rights (including the privilege against self- incrimination and the right to an adversarial hearing on the probative value of the electronic data proffered as evidence).

Supervisor: Professor Andrea Rosseti

External marker: Giovanni Sartor

Date of registration: 21 March 2011

Date of submission: 24 January 2011

Publication of thesis: January 2012

URL: https://boa.unimib.it/handle/10281/20472?mode=full.9

Name of candidate: Allison Stanfield

University: Queensland University of Technology

Faculty: Faculty of Law

Title of the degree: PhD

Title of the thesis: The Authentication of Digital Evidence

Brief description:

An analysis of whether the existing rules of evidence sufficiently protects the integrity of electronic evidence in contemporary times.

Supervisors: Professor Bill Duncan and Professor Sharon Christensen

External markers: Judge David Harvey (New Zealand) and Stephen Mason

Date of registration: 2011

Date of submission: November 2015

Date of award: July 2016

Name of candidate: Jonas Ekfeldt

University: Stockholms universitet (Stockholm University)

Faculty: Juridiska fakulteten (Faculty of Law)

Title of the degree: LL.D., Dr. iur., Doctor of Laws

Title of the thesis:

Värdering av informationstekniskt bevismaterial

Legal evaluation of digital evidence

Brief description:

Avhandlingsprojektet har som huvudsyfte att identifiera problemområden som framträder vid viss nationellt rättsligt påbjuden hantering och värdering av informationstekniskt bevismaterial. Informationstekniskt bevismaterial ges i avhandlingen en vidsträckt generisk definition, rättsligt och tekniskt anknuten, innefattande vad som i allmänna ordalag ofta beskrivs som 'digitala bevis', 'elektroniska bevis' och 'it-forensiska bevis'. I avhandlingen görs även bevisrättsliga analyser av aktuellt förekommande civila och polisiära s.k. 'it-forensiska analysprotokoll'.

The dissertation project has as its primary aim to identify problem areas that appear during certain legally imposed handling and evaluation of digital evidence, from a national perspective. Digital evidence is given an extensive generic definition, legally and technically based, encompassing what is generally also described as 'electronic evidence' and 'IT (forensic) evidence'. The thesis also

includes evidence law analyses of currently occurring 'IT forensic analysis reports' from civilian and police sources.

Supervisors: Professor Cecilia Magnusson Sjöberg and Professor Em. Christian Diesen

External marker: not applicable

Date of registration: 2011

Date of submission: Autumn 2015

Date of award: 1 April 2016

Name of candidate: Khaled Ali Aljneibi, LLB, LLM (Dubai)

University at which the PhD is registered and the awarding institution: Bangor University

Department or faculty: Law

Title of the degree: PhD

Title of the thesis:

> The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform

Brief description:

Due to the crucial role that electronic evidence is now playing in the digital age, it constitutes a new form of evidence for prosecutors to rely on in criminal cases. However, research into the use of electronic evidence in the United Arab Emirates (UAE) is still in its initial phase. There have been no detailed discussions on the procedural aspects associated with electronic evidence when investigating crimes, or the problems and challenges faced by law enforcers when handling electronic evidence. In addition, there has also been no detailed explanation of the ideal investigation process, such as the processes involved in computer search and seizure, and forensic investigation. As a result, the understanding and awareness of how to regulate and combat criminal cases that rely on electronic evidence is incomplete. In such situations, offenders usually take advantage of this lack of prescription in law. Because the understanding and awareness levels associated with electronic evidence is not perfect in the UAE, the UAE needs to promulgate new rules for handling electronic evidence as its laws are currently focused on traditional eyewitness accounts and the collection of physical evidence. Thus, it is very important that issues related to the existing approaches pertaining to electronic evidence in criminal procedures are identified, and that reform proposals are developed, so that new rules for handling electronic evidence can be adopted to effectively combat crime, by making full use of it.

This thesis examines the problems and challenges currently affecting the regulation electronic evidence in the UAE, and contributes to the body of academic literature in this area. Such a contribution is appropriate in the UAE context, where the law currently lacks sufficient academic input, especially concerning electronic evidence. The thesis makes actual recommendation as to how the substantive law may be reformed in the form of draft articles and includes an analysis as to how the process of prosecution and evidence collection can be facilitated. In particular it suggests that the electronic evidence process should be regulated in order to facilitate effective investigation and make full use of electronic evidence. This will ensure that electronic evidence is used in a transparent manner to preserve the integrity of criminal procedure, thereby safeguarding the accused, whilst at the same time facilitating prosecution and trial proceedings.

Supervisors: Dr Yvonne McDermott and Professor Dermot Cahill

External markers: Professor Gavin Dingwal and Mr Griffiths Aled

Date of registration: 1 May 2010

Date of submission: May 2014

Date of award: 1 June 2014

Name of candidate: Gita Radhakrishna

University at which the PhD is registered and the awarding institution: Universiti Multimedia (Multimedia University), Malaysia

Department or faculty: Faculty of Business (formerly known as the Faculty of Business and Law)

Title of the degree: PhD

Title of the thesis:

> Comparative Study of the Admissibility and Discovery of Electronic Evidence in Malaysian Civil Courts

Supervisors: Professor Myint Zan and Associate Professor Dr Dennis Khong Wye Keen

External markers: Assistant Professor Daniel Seng, Faculty of Law, National University of Singapore; Professor Eugene Clarke, School of Business, Griffith University, Gold Coast, Queensland; Professor Nazura Abdul Manap, Faculty of Law, University Kebansaan Malaysia

Date of registration: 12 February 2010

Date of submission: 29 December 2016

Date of award: 9 February 2018

Name of candidate: Maria Astrup Hjort

University: Universitet i Oslo (University of Oslo)

Department or faculty: Det juridiske fakultet (The Faculty of Law, Department of Public and International Law)

Title of the degree: PhD

Title of the thesis:

> Tilgang til bevis i sivile saker – med særlig vekt på digitale bevis
>
> Access to evidence in civil proceedings – with particular emphasis on digital evidence

Brief description:

Avhandlingen tar utgangspunkt i et scenarium der en part vet eller tror at det eksisterer materiale som kan brukes som bevis i en kommende eller verserende rettssak, og at parten ikke selv har hånd om dette beviset. Hovedproblemstillingen er i hvilke tilfeller og på hvilke betingelser parten kan få tilgang til beviset. Problemstillingen fordrer en rettsdogmatisk analyse av de tre fremgangsmåtene for tilgang til realbevis; å få bevis stilt til rådighet, bevisopptak og bevissikring.

En type bevis som det ofte er utfordrende å få tilgang til, er digitalt lagrede bevis. Mens fysiske gjenstander stort sett er klart definert og avgrenset, er digitalt lagret informasjon dynamiske størrelser i stadig endring som gjerne er lagret sammen med en mengde annen informasjon uten relevans for saken. I tillegg er digitalt lagret informasjon lett å kopiere, manipulere og slette. Disse trekkene utfordrer spørsmålet om tilgang, både praktisk og rettslig. Digitale bevis er derfor godt egnet til å belyse spørsmål knyttet til bevistilgangsinstituttet. Det er imidlertid vanskelig å behandle alle bevistilgangsspørsmål med utgangspunkt i digitale bevis, og noen spørsmål behandles derfor for realbevis generelt. Hovedvekten vil likevel - såfremt det er mulig – være på digitale bevis.

Avhandlingen har et komparativt tilsnitt, der svensk, dansk og engelsk rett er med på å belyse norsk rett.

The thesis is based on a scenario where a party knows or believes that there exists material that can be used as evidence in an upcoming or pending case and where the party is not in possession of this evidence. The main question is in what circumstances and on what conditions the party can get access to the evidence. The problem requires a dogmatic analysis of the three procedures for access to real evidence according to Norwegian law; the obligation to make evidence available, taking of evidence and securing of evidence.

One type of evidence that it is often challenging to get access to is digitally stored evidence. While physical objects are generally clearly defined and delineated, digitally stored information is dynamic and often stored together with a plethora of other information, irrelevant to the case. In addition, digitally stored information is easy to copy, manipulate, and delete. These features are challenging the issue of access, both practically and legally. Digital evidence is therefore well suited to shed light on issues related to the provisions on access to evidence. It is however

difficult to treat all questions related to access to evidence based on digital evidence, and some questions are therefore discussed based on real evidence in general. The emphasis will anyway – if possible – be on digital evidence.

The thesis has a comparative perspective, where Swedish, Danish and English law shed light on Norwegian law.

Supervisors: Professor Inge Lorange Backer and Professor Magne Strandberg

Date of registration: 1 February 2007

Date of submission: 13 March 2015

Date of defence: 6 May 2015

Name of candidate: Danidou Yianna

University at which the PhD is registered and the awarding institution: University of Edinburgh

Department or faculty: College of Humanities and Social Science, School of Law

Title of the degree: PhD

Title of the thesis:

> Trusted Computing or trust in computing? Legislating for trust networks

Brief description:

The thesis aims to address several issues emerging in the new digital world. Using Trusted Computing as the paradigmatic example of regulation though code, it tries to address the cyber security problem that occurs, where the freedom of the user to reconfigure her machine is restricted in exchange for greater, yet not perfect, security. Trusted Computing is a technology that while it aims to protect the user, and the integrity of her machine and her privacy against third party users, it discloses more of her information to trusted third parties, exposing her to security risks in case of compromising occurring to that third party. It also intends to create a decentralized, bottom up solution to security where security follows along the arcs of an emergent "network of trust", and if that was viable, to achieve a form of code based regulation. Through the analysis attempted in the thesis, we laid the groundwork for a refined assessment, considering the problems that Trusted Computing Initiative (TCI) faces and that are based in the intentional, systematic but sometimes misunderstood and miscommunicated difference (which as we reveal results directly in certain design choices for TC) between the conception of trust in informatics ("techno-trust") and the common sociological concept of it. To reap the benefits of TCI and create the dynamic "network of trust", we need the sociological concept of trust sharing the fundamental characteristics of transitivity and holism which are absent from techno-trust.

This gives rise to our next visited problems which are: if TC shifts the power from the customer to the TC provider, who takes on roles previously reserved for the nation state, and how in a democratic state can users trust those that make the rules? The answer lies partly in constitutional and human rights law and we consider those functions of TC that makes the TCI provider comparable to a state, and ask what minimal legal guarantees need to be in place to accept, trustingly, this shift of power. Secondly, traditional liberal contract law reduces complex social relations to binary exchange relations, which are not transitive and disrupt rather than create networks. Contract law, as we argue, plays a central role for the way in which the TC provider interacts with his customers and the thesis contributes in considering a contract law that does not result in atomism, rather "brings in" potentially affected third parties and results in holistic networks. In the same vein, the thesis looks mainly at specific ways in which law can correct or redefine the implicit and democratically invalidated shift of power from customer to TC providers while enhancing the social environment and its social trust within which TC must operate.

Supervisor: Professor Burkhard Schafer

External marker: Dr Andres Guadamuz

Date of registration: 1 March 2007

Date of viva: 2 May 2016

Date of award: 24 November 2016

Name of candidate: Aashish Srivastava

University at which the PhD is registered and the awarding institution: Monash University

Department or faculty: Business Law and Taxation

Title of the degree: PhD

Title of the thesis:

> Is the Pen Mightier than the Electronic Signature? The Australian Businesses' Perspective

Brief description:

Using a qualitative approach, the thesis conducts a comprehensive empirical investigation to identify factors that have contributed to the low acceptance of electronic signatures, in particular, the digital signature in the Australian business community.

Supervisors: Professor Paul von Nessen and Mr Paul Sugden

Date of registration: November 2004

Date of submission: November 2008

Date of award: April 2009

Thesis published: Aashish Srivastava, *Electronic Signatures for B2B Contracts Evidence from Australia* (Springer India, 2013)

Name of candidate: George Dimitrov

University at which the PhD was registered and the awarding institution: Katholieke Universiteit Leuven

Department or faculty: Interdisciplinair Centrum voor Recht und Informatica

Title of the degree: PhD in Laws

Title of the thesis: Liability of Certification Service Providers

Supervisor: Professor Dr Jos Dumortier

Thesis published: George Dimitrov, *Liability of Certification Services Providers* (VDM Verlag Dr. Müller, 2008)

Name of candidate: Adrian McCullagh

University at which the PhD is registered and the awarding institution: Queensland University of Technology

Department or faculty: Information Security Research Centre, Faculty of Information Technology

Title of the degree: PhD

Title of the thesis: The Incorporation of Trust Strategies in Digital Signature Regimes

Brief description: The aim of this research is to document the differences between a traditional signature and an electronic signature including in particular one form of electronic signature known as a "digital signature". It will be established that it is a fallacy for legislators to insist upon functional equivalence between electronic/digital signatures and traditional signatures from a legal perspective. Many jurisdictions have not only advocated functional equivalence but in so doing have also approached the legal recognition of signing digital documents from a technology neutral language perspective in their respective electronic signature legislative regimes, whilst at the same time attempting to create some magical certainty for commerce to rely on. In short, there is, as this thesis will show, a clear contradiction concerning technology neutral language in electronic signature regimes and the certainty that commerce requires. Technology neutral language regimes provide no guidance to either the judiciary or commerce in their dealings with enforceable contracts that are evidenced electronically and where the "signature" is in dispute. There are, as will be established in this thesis, too many fundamental differences for functional equivalence to be achieved. This thesis does not attempt to define an electronic signature, as any definition would most likely overtime become outdated as technology advances such concept, but this thesis does describe a set of elements which if technologically achievable would closely correspond to the traditional concept of a signature as commercially and legally understood.

Supervisors: Professor William Caelli and Professor Peter Little

External markers: Professor Alan Tyree and Professor Bob Blackley Snr, University of Texas A&M

Date of submission: July 2001

Date of award: 3 February 2001