CSEIA CENTRO STUDI IN AFFARI EUROPEI E INTERNAZIONALI

QIL

WORKSHOP ON:

New Technologies as Shields and Swords: Challenges for International, European Union and Domestic Law

UNIVERSITY OF PARMA

19-20 JUNE 2017

PALAZZO CENTRALE - AULA MAGNA

SUMMARY

Panel 1
New Technologies and "Borders"

Panel 2
The Age of Big Data: International and European Perspectives

Panel 3
The (Mis)use of New Technologies: Responsibility Issues and the Role of Private Actors

Panel 4
New Technologies in International and Domestic Adjudication

Panel 1
New Technologies and "Borders"

Abstract 1
The Intensification of the contemporary challenges posed to the *jus in bello* by drone programs (UCAV)

Rebecca Mignot-Mahdavi
Ph.D. Candidate in Public International Law
European University Institute

In the past fifteen years, several States have adopted policies which allow them to conduct targeted killings in foreign territories against non-state actors through the use of combat drones. These policies, because of their strategy and the rhetoric accompanying them, but also because of the technology of drones, have had the effect of blurring and expanding the boundaries of the applicable legal frameworks. How do drone programs challenge the *jus in bello*?

The presentation will examine the legal rationalizations for drone programs in terms of *jus in bello*, as discerned from the public statements of US, UK and French officials. Although France does not yet use drones, it offers a valuable illustration of the processes that the presentation wants to understand: i) the individualization of the way war is conducted, and ii) the loss of spatial delineation of war. Indeed, the rationale behind French strikes in Syria suggests that they share with the US and the UK an unbounded vision of war and an individualized targeted killing policy. I argue that drone programs allow such rationales to be fully put into practice and, ergo, intensify them.

In this respect, and because the laws of war were thought to regulate state-centred wars, drone programs tend to deformalize International Humanitarian Law (IHL). The presentation will focus on three main aspects of the *jus in bello* that are being challenged by targeted killings and, I argue, even more so by drone programs: the classification of conflicts, the spatial extent of application of IHL, and the notion of direct participation in hostilities

Abstract 2
Legal challenges related to the use of new technologies in migration control

Philip Hanke
Post-doctoral Research Fellow in Public Law
University of Bern
Daniela Vitiello
Post-doctoral Research Fellow in European Union Law
University of Roma Tre

Disruptive technological changes currently taking place at an accelerating rate across all industries also affect the control of migratory flows. It thus needs to be asked whether and how these and foreseeable advances create new legal and ethical problems while challenging the economics of border protection, particularly in the context of the European Union.
The link between international mobility, border surveillance and the internal security of the Schengen area is now new; rather it has been established and reinforced in EU policy and practice through the last decades and it is not new. However, it has received a formal investiture in the aftermath of the so-called "refugee crisis", leading to the adoption of the European Agenda on Security (COM(2015) 185 final). The Agenda was agreed upon with a view to setting out new approaches on interoperability of information systems and launching the work of the High-Level Expert Group on Information Systems and Interoperability (Decision C/2016/3780). In May 2017, the Expert Group delivered its final report, outlining the roadmap for the improvement of existing systems (*i.e.* SIS, Eurodac, VIS) and the development of new systems (namely, the Entry/Exit System, the European Travel Information and Authorisation System, the European Criminal Records Information System for third-country nationals and the Repository of long-stay visas, residence permits and cards, and local border traffic permits). The Expert Group recommended the attainment of the highest-possible threshold of interoperability by the establishment of common identity repositories, shared biometric matching tools and universal message formats. The proposed solutions seem to address identified gaps in the present information system landscape and provide original solutions to unleash the potential of new technologies for purposes of cross-border surveillance and migration management. However, these solutions pose several legal and political concerns that do not seem to be adequately dealt with in the final report. Indeed, as a matter of definition and legal obligation, the developments of the European Agenda on Security should promote a comprehensive and less-fragmented machinery for EU information systems, *operating in full compliance with fundamental rights, including data protection*. Over and above the rhetorical evocation of fundamental rights clauses and obligations, the key question would be how the Union is going to deal with the trade-off between the search for an efficient and integrated border management and the attainment of the highest possible level of human rights and data protection. Accordingly, the presentation will move on from the description of the normative, institutional and operational design of the Union as an area in which the lion's share of internal security is ensured through new technologies, information system and big data. It will then turn to analyse the main threats arising from the use of new technologies in migration control, regarding both legal threats to individuals and political threats to the well-functioning of intergovernmental cooperation. In particular, specific legal and ethical challenges arise with increasing autonomy of computer systems. Overall, the presentation aims at disentangling the complex interaction among efficiency requirements, protection needs and data reliability in migration control systems the Union is developing, whilst embedding these developments in a wider international context.

Abstract 3
Cross-border surrogacy: the role of the European Court of Human Rights

Mario Gervasi
Ph.D. in International Law and European Union Law
University of Rome "La Sapienza"

As it is well known, surrogacy represents one of the thorniest issues in contemporary family law, raising ethical and moral perplexities in addition to legal questions. The surrogate child may be born from the egg of either the surrogate mother or the female component of the intended parents or a third donor; at the same time, the egg may be fertilised by either the male component of the intended parents or a third donor. Moreover, same-sex couples have recourse to surrogacy.
States all over the world react differently to the possibility for a couple to request a woman to bear – upon payment or free – a child on their behalf. By way of simplification only, surrogate motherhood is forbidden in some countries, whereas it is regulated or accepted in others. In a globalised world, such a lack of uniformity among States induces individuals from countries where surrogacy is banned or strictly regulated to have recourse to surrogacy abroad, namely in those countries where it is permitted. Here the legal problem of the circulation of family status comes into consideration. In other words, the question emerges about the legal condition of the intended parents coming back with a surrogate child born abroad to their country of origin, where surrogate motherhood is forbidden.
The presentation aims at critically exploring the role of the European Court of Human Rights in front of the briefly described problem. The research question arises whether and to what extent the borders between countries allowing and countries banning surrogacy are increasingly vanishing as a consequence of the human rights protection according to the European Convention on Human Rights. To this end, it is necessary to investigate the factors underlying the phenomenon.
Under the lens of the right to respect for private and family life, protection of human rights seemingly tends to safeguard the continuity of family status established abroad. For instance, in the 2014 'twin' judgments on the cases *Mennesson* and *Labassee*, the Strasbourg Court declared that France violated the right of the surrogate children to respect for their private life in denying the registration of the birth certificates issued in the United States of America as well as refusing to acknowledge or establish any legal tie between the children and their respective biological fathers. On the other hand, such approach risks eroding the margin of appreciation and public order of those countries prohibiting surrogate motherhood. So, in the 2017 *Paradiso and Campanelli* case, the Grand Chamber of the European Court of Human Rights held that the Italian removal of a surrogate child from the intended parents was compatible with the European Convention on Human Rights, even though the Chamber had previously found a breach of the applicants' right to respect for their private and family life.

Abstract 4
Questioning the reach of the right to be forgotten beyond European Union's borders

Alberto Miglio
Post-doctoral Research Fellow in European Union law
University of Turin

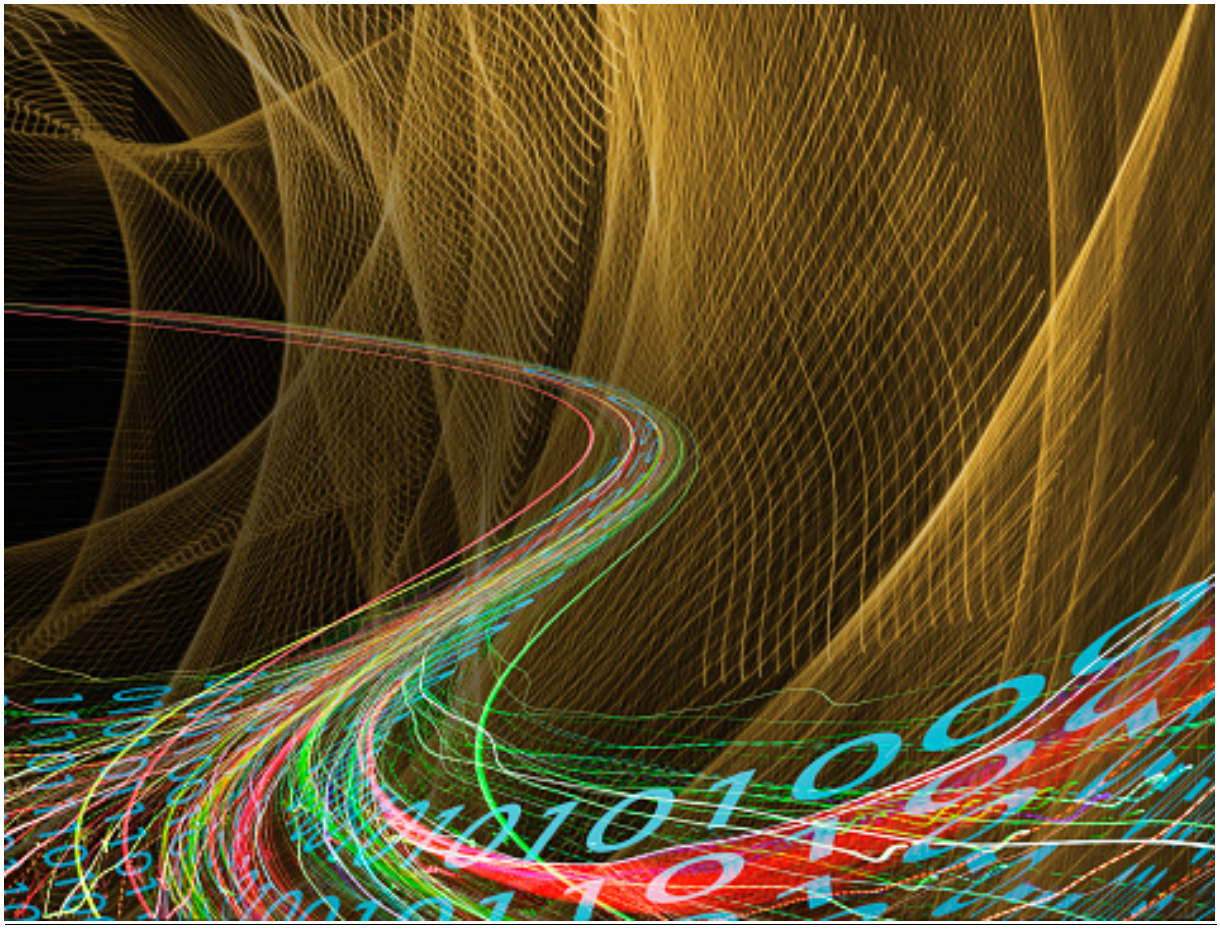
In the landmark *Google Spain* judgment, the Court of Justice of the European Union recognized the existence of an individual right to delisting of certain search results. By broadly interpreting Article 4(1) of Directive 95/46, the Court concluded that Google's search engine activities, although taking place outside the EU territory, were carried out "in the context of the activities" of its subsidiary Google Spain and thus fell within the scope of the directive. The scope of application of the 2016 General Data Protection Regulation, which will replace the Directive from 25 May 2018 and contains a specific provision on the "right to be forgotten", is similarly broad.

Google Spain has often been criticized as an exercise of extraterritorial jurisdiction. The presentation will suggest that this qualification is questionable, and that the application of data protection rules to certain data processing activities carried out in third countries might better be viewed, according to a distinction suggested by Joanne Scott, as a case of territorial extension rather than as an example of true extraterritoriality.

Yet, it is beyond doubt that a broad interpretation of the geographical scope of the right to be forgotten may generate regulatory conflicts. In this context, a key question that has already surfaced before national data protection authorities and national courts is whether EU data protection law allows for geographically selective delisting or whether it obliges search engines to delist search results globally.

The terms of the problem are not new and remind of a similar debate on the regulation of Internet content that took place in the early 2000s in the wake of the *Yahoo!* case. However, while in *Yahoo!* limiting access on the basis of the geographical location of servers offered a practical solution that permitted the coexistence of diverging State policies in the global space, similar variable geometries do not seem compatible with the insistence of the Court of Justice on the effectiveness of fundamental rights protection.

Panel 2
The Age of Big Data: International and European Perspectives



Abstract 1
Processing and transfer of personal data 'reshaped': recent evolutions within the European Union

Stefano Saluzzo
Post-doctoral Research Fellow in European Union Law
Valle D'Aosta University

Transfers of data between States are mainly regulated by national legislations. States have enacted unilateral measures to create a regime applicable in the case of data flows from one territory to another, often focused on the protection of personal data within the territory of destination.
The European Union, since Directive 95/46, has adopted a sophisticated mechanism to address the issue of data flowing from the territory of one of the Member States into a third country. The system is based on a decision by which the Commission evaluates whether the third country of destination ensures an adequate standard of protection to European data. Beside this, data flows also find a legal basis in the so-called corporate binding rules and standard contract clauses.
The *Schrems* judgment, rendered by the Court of justice in October 2016, has reshaped the landscape of EU rules on data transfers, by acknowledging that the level of protection afforded to European data by the third country's legal order must be "essentially equivalent" to that of the European Union. This standard of course also includes the protection granted by the Charter of fundamental rights. Moreover, a case is still pending before the Court in which the national judge has raised the question whether this standard must also be applied to data flows having their legal basis in contractual clauses.
First of all, the presentation will try to offer an overview of the general legal framework of EU law regulating data transfers from the European Union to third countries, taking into account the recent case-law of the Court of justice.
It will then provide an attempt to reconstruct the standard applicable to third countries necessary to allow them to receive data collected on the territory of the EU. In this context, a brief account will be given on the potential extraterritorial effect that such measures may produce within the legal order of other countries. The analysis will be conducted in particular by looking at the example of the recently adopted Privacy Shield in the United States.
In the last part, the focus will shift on the developments enshrined in the General Data Protection Regulation, adopted in 2016, that will substitute Directive 95/46. The Regulation provides for certain norms in relation to data transfers that partly differ from those of the Directive and that need to be analysed in the light both of the recent case-law of the Court of justice and of the relevance the Charter of Fundamental Rights has acquired in the field of data protection. The analysis will conclude on enforcement mechanisms provided within the Regulation and especially on the role of national authorities.

Abstract 2
Asylum seekers and irregular migrants' data: some reflections on the potential use and misuse of the EURODAC database

Serena Bolognese
Ph.D. Candidate in International Law
University of Modena and Reggio Emilia

When the EURODAC database was established in accordance with EC Regulation No. 2725/2000, its purpose was to determine the EU Member State responsible to examine an application for international protection based on the criteria set out in the Dublin Convention. In a nutshell, the EURODAC database worked as the "electronic heart" of the common European asylum system.
While preserving EURODAC's original function, Regulation No. 603/2013, adopted within the framework of the EU area of freedom, security and justice, assigned new tasks to the database. In particular, the 2013 EURODAC regulation permits for the first time access of EURODAC data to EUROPOL for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences. Furthermore, according to the recent European Commission (hereinafter "EC") proposal on the recast of the EURODAC regulation ((COM) 2016 272), information and sensitive data of asylum seekers and irregular migrants may be transferred to third States.
Considering the aforementioned amendments, and other EC proposals of recast, the purpose of the presentation is to highlight potential use and misuse of the EURODAC database. The structure of the analysis is three-headed. Firstly, the presentation questions the human rights compliance of the 2013 EURODAC regulation and of the EC recast proposal, devoting attention to the rights of asylum seekers and migrants. In particular, the analysis will be focused on the interference of data transmission with the fundamental rights to privacy and data protection as enshrined in the EU Charter of Fundamental Rights. It also addresses the compliance of fingerprints mechanisms with the right to personal integrity and the right to human dignity. Indeed, the new EURODAC regulation was emended in order to make the obligation on States to put in place fingerprints mechanisms stricter. Alongside with this obligation, specific sanctions could be applied for those individuals who do not provide fingerprints and facial images, including accelerated procedure, or even the use of detention or physical coercion. Furthermore, it will be analysed if the transfer of data stored in EURODAC to third countries – both countries of origin and third countries – would expose the concerned asylum seekers to specific risks and jeopardize the right to asylum. Since the application of the safe country concept under the Procedure Directive 2013/32/UE has already favoured pushing back policies towards countries considered safe, exchanging information and biometrical data with third countries might turn the EURODAC database into an instrument to facilitate border control rather than to ensure the access to fair and efficient asylum procedures. Secondly, the presentation focuses on the access of EURODAC data to EUROPOL. Whereas the importance of strengthening police cooperation in the EU is out of doubt, it could be asked whether the principle of proportionality in data access is effectively ensured, as requested by the CJEU in relation to law enforcement access to data.
While, for all above, the expansion of the EURODAC mandate presents controversial aspects, a third point worth addressing concerns the potential beneficial use of EURODAC database, especially if fingerprints mechanisms and biometrical data of minors will be introduced. Indeed, the collection and exchange of EURODAC data could facilitate cross-border tracing of missing children and verification of family links of minors, whose protection was outlined by the EC among the priority actions under the European Agenda of Migration.

Abstract 3
The use of databases in criminal cooperation within the European Union

Stefano Montaldo
Researcher in European Union Law
University of Turin

During the last fifteen years, the establishment and use of databases for the purposes of preventing and tackling serious offences in the EU has represented a major workflow for the European Union and the Member States. An intense legislative season has led to a proliferation of information tools, enabling national law enforcement authorities to exchange and receive various data and documents. The plurality of sources covers a remarkable variety of information, ranging from DNA profile to data concerning road-safety related traffic offences.
The use of EU databases and information exchange systems constitutes a test bed for the effectiveness of judicial cooperation mechanisms. The smooth functioning of such databases is grounded on complex multi-level institutional arrangements. These are intended to govern the horizontal cooperation between national authorities and the vertical division of competences between the latter and the relevant EU bodies such as Europol, Eurojust and OLAF. Moreover, they aim to overcome the barriers deriving from the fragmentation of national legal orders and to strike a proper balance between security concerns and the general principles concerning data processing and retention.
In this perspective, the analysis firstly intends to address the institutional arrangements underpinning the establishment and the functioning of these databases, in order to discuss their rationale and to identify common patterns. Secondly, the roles played by EU bodies and national authorities are discussed, with the purpose of considering advances and shortcomings of this aspect of criminal cooperation, also in light of the general principles of the EU legal order. Lastly, the analysis addresses the challenges ahead, with specific regard to information cooperation and intelligence.

Abstract 4
E-health and medical apps: a comparative analysis of domestic regulatory frameworks

Monica Cappelletti
Post-doctoral Researcher in Comparative Public Law
Dublin City University

Information and Communication Technology (ICT), Internet and Big Data[1] have a strong influence on our daily life. It is against this background that even one of the most traditional sectors, such as health care, has to be dealt with. Substantial progress has been made in recent years regarding new ways of providing health care, reshaping the very concept of health care somehow.
We are witnessing to challenging innovative paths in this sector (*i.e.* predictive medicine, personalised medicine, digital health, telemedicine[2]) which, at the same time, entail implications in terms of data protection rights (health care data are indeed sensitive personal data according to EU law). In particular, attention should be devoted to the legal consequences of at least three different "levels of use" of health care data: what (and how) is going to be shared; for which purpose(s); and how and who is going to store/retain such data.
In the attempt to investigate this challenging relationship between health care data protection and ICT, the presentation will be divided into three parts. Firstly, the main definitions used in this sector (such as e-health, medical apps, m-health) will be clarified in order to find common notions. Secondly, the EU, US and Australian legislations concerning medical apps will be examined and compared with a view of highlighting shared solutions or weaknesses. Finally, endorsing a de iure condendo perspective, innovative legal solutions potentially capable of better balancing the protection of health care data and the evolution of (bio)technologies will be considered.

[1] Among different definitions, see the following "*big data is high-volume, high-velocity, high-value and high-variety information (4Vs) assets that demand innovative forms of information processing*", in F. IAFRATE, *Big Data to Smart Data*, 2015.

[2] Recently see F. WEISGHIZZI, *Salute, perché ci cureremo con i BigData (e mappare il Dna costa già 3 mila euro)*, in *StartupItalia*, April 21, 2017, https://startupitalia.eu/71784-20170421-health-bigdata-dna.

[2] Recently see F. WEISGHIZZI, *Salute, perché ci cureremo con i BigData (e mappare il Dna costa già 3 mila euro)*,

Abstract 5
Life after death: the transmission of digital assets. An Italian perspective

Francesco Mastroberardino
Ph.D. Candidate in Civil Law
University of Modena and Reggio Emilia

Nowadays everyone's life is strictly affected by the influence given by the internet and the huge amount of data which define the "online *persona*". This complex quantity of information concerns and describes us in a growing number of fields. It is more than common to have multiple electronic accounts: bank accounts, social network accounts, online shopping accounts, email addresses. At the same time, these accounts can preserve objects which represent moral and economic value, such as letters, intellectual property, digital currency.
Overall, this view shows us the fundamental role that digital assets assume within the multiple branches of the Law. This is especially relevant when dealing with an individual's destiny after physical death. Nevertheless, the Italian legislator has not properly addressed this issue. It is symbolic that digital assets have not received an explicit definition in our legal system yet.
Can we discipline these assets' faith? Could the fundamental right known as testamentary freedom be helpful to confer a decedent's digital assets to their heirs? Do service providers – such as *Google*, *Yahoo*, *Facebook* – have the right to dictate contractual clauses prohibiting the *mortis causa* succession for these online accounts? Are these standard and commonly used clauses void due to the apparent similarities with the unfair and illegal one-sided clauses?
These are only some of the question marks regarding the topic of digital assets still waiting for an answer. Only a few legal systems have addressed this topic (mainly in the United States of America): the legal expert must find a solution, using the tools already provided by the positive Law.
Inevitably, given the breadth of the topic and considered the persisting absence of an Italian legislation, we must refer to certain constitutional principles. In particular, the ones concerning email services: the rights of freedom and secrecy of personal correspondence.
Another important issue is related to the applicable law. Although service providers are usually based in foreign states (a considerable amount of them in California), they deal with citizens from other countries. Determining the applicable law has direct consequences on the regulation of contractual discipline. Moreover, it is fundamental in order to determine which inheritance law must be followed as well.

Panel 3
The (Mis)use of New Technologies: Responsibility Issues and the Role of Private Actors

Abstract 1
Attribution of cyber conducts to a subject of international law

François Delerue
Researcher in Cyber-defence and International Law
Institute for Strategic Studies of the French Military School (Paris, France)
Associated Researcher
Castex Chair of Cyber Strategies (Paris, France)

State-sponsored cyber operations, generally identified as cyber warfare, constitute a real challenge for the law of State responsibility. One of the main issues is the impossibility, at least to date, to identify clearly the perpetrators of cyber operations, either individuals or State agents, and to determine whether their conducts are attributable to States or other subjects of international law.

Most cyber operations generally alleged to be state-sponsored – e.g. the DDoS attacks against Estonia (2007), the cyber operations against Georgia in the context of the Russo-Georgian armed conflict (2008), the malware 'Stuxnet' (2009), the Hack of Sony Entertainment (2014) as well as some cyber operations taking place in the context of the on-going Ukrainian and Syrian civil wars – have not been clearly attributed to a State yet. In most of cases, when the attribution has been possible, it is because the responsible State claimed the conduct of the cyber operation, as for instance Iran for the hack of an American drone (RQ-170) in 2011.

International law cannot bring a solution to the technical problem of attribution. However, attribution cannot be limited to its technical aspects. Generally, attribution of cyber conducts has three different dimensions: firstly, the attribution to the machine from which the cyber operation was launched or had transited; secondly, the attribution to the person who conducted the cyber operations; and thirdly, the attribution to an aggregate entity, notably a State.

Attribution of conducts to a State is an important question in international law. The attribution, also referred to as the imputation, is the legal operation aiming at determining that an act or omission is to be characterized as an act of the State under international law.

The presentation will focus on attribution from an international law perspective, that is to say attribution of a conduct to a State or another subject of international law. The State is an abstract entity and thus can only act by the medium of one or more persons, which are considered for the purpose of the attribution to a State, as the mean by which the State acts. This question cannot be studied without dealing with the questions of the imputation of cyber conducts to computers or individual perpetrators. Consequently, the presentation will detail the three components of attribution and focuses more specifically on the question of attribution from an international law perspective.

Abstract 2
Education and training of armed forces in the age of high-tech hostilities

Marco Longobardo
Adjunct Professor in International Law and European Union Law
University of Messina
Research Fellow in Public International Law
University of Westminster, London

New technologies have radically changed current warfare and, consequently, the very law of armed conflict. In recent decades the employment of unmanned aerial vehicles and cyber attacks has become very frequent, and autonomous weapon systems are being developed in some high-tech laboratories.
This presentation will focus on an underexplored topic linked to this apparently unstoppable high-tech trend in warfare: the education and training of the personnel of the armed forces in the contexts of high-tech hostilities.
Two different sub-issues will be dealt with in this presentation. First, attention will be paid to exploring the duties that States have with respect to high-tech means and methods of warfare, considering, in particular, whether the law of armed conflict requires that States employing these means and methods provide a specific technological training to their armed forces' personnel. This problem is related to the respect of the principle of precautions in attack and is particularly relevant in contemporary armed conflict where high-tech armies seem to be unable to avoid the commission of fatal mistakes regarding the targeting of civilians and protected objects (as happened very recently in Syria and Afghanistan). It will be argued that States may be held responsible for the inadequate training of their soldiers as long as this results in a violation of the principle of precaution in the attacks.
Second, the question will be tackled of whether, pursuant to Article 83 of the 1977 First Additional Protocol, States are under a duty to disseminate international humanitarian law rules with specific regard to high-tech means and methods of warfare. This part of the presentation will take into account State practice regarding the dissemination of international humanitarian law and the lack of rules specifically envisaged to regulate some high-tech means and methods of warfare (such as cyber attacks). It will be argued that States may be held responsible for a lack of adequate international humanitarian law education only if they exclude the applicability of the law of armed conflict to high-tech means and method of warfare.

Abstract 3
Hybrid governance or... nothing? The EU Code of Conduct for Countering Illegal Speech Online

Karolina Podstawa
FRAME Senior Researcher
EIUC Venice

On 31 May 2016 the European Commission presented the Code of Conduct on Countering Illegal Speech Online. The tool, which was elaborated together with the IT companies, is considered a flagship voluntary measure representing what Gráinne de Búrca, Joanne Scott and Mark Dawson describe as the hybrid governance, i.e. the form of managing of a given policy field through the mix of legal and non-legal measures, which are, however, inextricably linked and dependent on one another.
The Code aimed at obtaining, on the one hand, the removal of illegal speech from the platforms ran by the said companies in implementation of the range of the legislative measures, and, in particular, of the Framework decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. On the other hand, the Code was to facilitate the establishment of the channels of communication between the said IT companies and the Member States authorities.
The adoption of the Code got mixed reception from the NGOs and the broader public. Some claimed this was the right way to go emphasizing the necessity to collaborate with the IT companies on the matter, others warned against the assault on freedom of speech online (i.e., Gatestone institute). The initiative has taken shape, however, and currently we are expecting the second 2017 review of Code's implementation by IT companies.
The purpose of this presentation will be to determine which are the aspects of the policy focused on combatting certain forms and expressions of racism and xenophobia that calls for employment of such measures and what could be the alternatives to such initiative. The working hypothesis points to the fact that due to the difficult relationship between law and Internet (territoriality of law v. omnipresence of Internet, extraterritoriality of application of rules, problems with obtaining personal data of the perpetrators etc…) hybrid governance may be the only available evolutionary way forward permitting also the co-ownership and self-management of the 'web' both by service providers and users. The successful implementation of such measures seems, however, to be dependent on the architecture of legal measures providing for a narrower leeway to the private actors (IT companies) involved.

Abstract 4
Bringing social networks to court for complicity in terrorism
Missing

Abstract 5
Protection of personal reputation in the social networks era: new challenges

Massimiliano Lanzi
Postdoctoral Research Fellow in Criminal Law
University of Parma

The protection of personal reputation (both in a private and public perspective) is one of the areas of traditional interest for criminal law. In particular, defamation entails special difficulties in finding a proper balance among the different and opposite interests at stake, namely, the protection of the personal reputation, on the other hand, and the public and private interest in the free circulation of information, on the other hand.
New technologies and new communication systems make the task even harder. It is well known how people, all over the world, are experiencing new and still partly unexplored models of communication based on the Internet and on the wide use of internet-based social networks.
In this respect, the protection provided by criminal law of personal reputation is challenged under different aspects. First of all, it falls within the historical problem of adapting the enforcing of criminal law to new technologies, in terms of "traditional" offences committed through "new" instruments. The Convention on Cybercrime (Budapest, 2001) represents the efforts of the States parties to adapt traditional crimes to new technologies and instruments. Following the ratification of the Convention in 2008 (Act No. 48/2008), several new provisions were introduced, in this respect, in the Italian criminal code: for instance, articles 635 *bis* and 635 *quater* contain new hypothesis of malicious mischief occurred to data or informatics instruments. Yet, no provision has been introduced so far in order to adapt defamation to new tools by which people express their opinion and, therefore, by which defamation might be committed. Secondly, another issue concerns the definition itself to be given to "communication" and how traditional principles should be applied in this renovated scenario. The given balance between the right to freedom of speech and personal reputation is traditionally found considering press and professional journalism as one of the most efficient watchdog of a democratic system, the first being therefore predominant over the second. This is the frame of the guarantees set forth in Article 10 of the European Convention on Human Rights, as well as (from a domestic perspective) in Artcle 21 of Italian Constitution. New technologies ensure that people have free access to new information sources that can be hardly considered as "press", since they are not based on any professional or institutional frame. But still, these sources are suitable to be considered as effective "opinion making" instruments, as well as one of the fastest ways for the circulation of information.
Italian case law is facing the new scenario drawing a new and wider border to the concept of "press", with the view to acknowledging some of the new internet-based sources to which constitutional guarantees should be granted (Cassation Court, decision No. 31022/2015). However, the same balance between different interests (in favour of the freedom of speech) cannot be reached when other forms of communication are involved, such as social networks and non professional blogs. The frame of application of criminal provisions involving defamation will be defined accordingly: the wider the guarantees to the freedom of speech are recognized, the less the criminal law is to be applied.

Panel 4
New Technologies in International and Domestic Adjudication

Abstract 1
Killing to the Sound of Trumpets, Dying in the Silence of Courts: the Impact of Avoidance Doctrines on Targeted Killing

Luca Gervasoni
Ph.D. in Public International Law
University of Milan-Bicocca

In recent years much research has been dedicated to targeted killing, an issue often considered in relation to the deployment of new technologies such as unmanned aerial vehicles.
Quite surprisingly, however, not much attention, if any, has ever been devoted to the issue of access to justice for victims of targeted killing and their right to reparation for any unlawful use of deadly force.
While the underlying assumption of the presentation will be that targeted killing may be either lawful or unlawful depending on a series of factors, its scope will be neither to dig into potential violations of the substantive limb of the right to life, nor to assess compliance with due process guarantees in the selection of individuals as targets. It will rather focus on access to justice and reparation for persons who have already been so selected and/or so deprived of their lives.
This is a matter that is rapidly gaining momentum as a considerable number of cases in various jurisdictions have been brought to court by victims of targeted killings and their relatives in these last years, and many more such cases should be expected to ensue in the near future.
This presentation will show that the great majority of domestic lawsuits related to targeted killing have been dismissed on procedural grounds before ever reaching an adjudication on their merits, mainly as a result of domestic courts' reliance on non-justiciability clauses or avoidance doctrines, i.e. on theories that prevent any adjudication on the core content of a lawsuit due to procedural bars embedded in national legislations and generally geared around principles of separation of powers.
After providing an overview of the specific avoidance doctrines most often resorted to in the proceedings adjudicated so far and offering a comparative analysis of relevant judgments, the presentation will turn to international law. In so doing, it will take into consideration applicable legal regimes, in particular international human rights law and international humanitarian law, trying to highlight which rights victims of unlawful targeted killing enjoy at the intersections of these *corpora juris*, and which corresponding duties States bear in this regard.
In this connection, the presentation will thus confront avoidance doctrines with international law standards emerging from the right to an effective remedy read in connection with the procedural limb of the right to life as well as from the right to a due process. In particular, analyzing the former in light of the latter, the presentation will argue that the duty to investigate and prosecute, as well as the duty to grant victims of gross human rights violations full reparation are hardly reconcilable with avoidance doctrines, which may in and by themselves entail a potential violation of victims' fundamental rights.

Abstract 2
The development of driverless cars and the future of cross-border traffic accident litigation

Nicolò Nisi
Research Fellow in Private International Law
University of Halle-Wittenberg

The use of driverless cars (also known as self-driving vehicles) in the future will offer major benefits in terms of road safety, social inclusion, reduction of emissions, and avoidance of congestion, with a significant reduction of human error, which is currently a crash factor in the vast majority of car accidents. Such development will inevitably raise questions of liability and will probably result in a shift in liability from the vehicle-holder (strict liability) to the vehicle-manufacturer or technology producer (product liability), due to fact that accidents occurring with driverless cars will be mainly caused by a system malfunction rather than by the misconduct of the human driver. Against this backdrop, it is interesting to evaluate which is the impact of the introduction of new technologies on the European private international rules determining jurisdiction and applicable law in the case of a cross-border traffic accident. As is known, different legislative instruments come into play: the Brussels I-*bis* Regulation for jurisdiction; the 1971 Hague Traffic Accident Convention or the 1973 Hague Products Liability Convention or the Rome II Regulation for applicable law, depending on the State where the claim is brought. Concerning the first aspect, the victim has often the choice between the courts of different countries to claim for compensation (e.g. the defendant's domicile or the place where the accident occurred). In contrast, the situation is more complex for applicable law, because the instruments mentioned above provide for different connecting factors, that in some case may lead to the application of different laws. Such variety entails that the choice of forum by the claimant may have a significant impact on the outcome of a case. The lack of foreseeability that marks traffic accident litigation is likely to become more problematic with the new risks raised by defects of technologies connected to the functioning of driverless cars. Accordingly, the overall regime currently applicable need to be updated both at the substantive law and the private international law level, for instance with the use of new concepts (e.g. car users instead of drivers) or the provision of new connecting factors (e.g. forum at the victim's domicile for claims against the manufacturers of new technologies), in order to ensure a better protection of the victims of cross-border accidents.

Abstract 3
Enforcing rights through electronic means
Missing