Semantic Workflows in Law Enforcement Investigations and Legal Requirements

Wolfgang Mayer[15], Pompeu Casanovas[245], Markus Stumptner[15], Louis de Koker[25], Danuta Mendelson[35]

[1] University of South Australia, Adelaide, Australia
[2] La Trobe Law School, La Trobe University, Melbourne, Australia
[3] Deakin Law School, Deakin University, Melbourne, Australia
[4] IDT-UAB, Autonomous University of Barcelona, Spain
[5] Data to Decisions Cooperative Research Centre, Australia

Abstract. Investigations conducted by law enforcement agencies depend on information that is obtained from a variety of sources, internal and external to the organization. Considering that investigations frequently span multiple jurisdictions and government agencies with varying objectives and powers, assessing and ensuring compliance with their policies and the legal framework is challenging. We present technical features and a semantic information modelling approach that can support compliant workflow execution in the context of law enforcement investigations and discuss how such an information system might be embedded in a complex legislative and social environment. Legal principles, and the concepts of Legal Compliance by Design (LCbD), and Legal Compliance through Design (LCtD) are also introduced.

Keywords: Workflow automation, Semantic Meta-data, Legal Compliance by Design, Legal Compliance through Design

1 Introduction

Investigations conducted by law enforcement agencies (LEAs) are dependent on information that is obtained from a variety of sources, internal and external to the organization [1]. Sole investigators with paper notebooks have been superseded by sophisticated information systems that aim to ingest, process, and enrich the collected information to help law enforcement officers conduct their investigations.

Investigations generally follow an iterative process of information collection, assessment, investigation planning, execution, and brief of evidence preparation where each step either produces new information or relies on information collected earlier in the process. Although steps in this process could be supported by automated systems, information systems in the law enforcement domain are often legacy “silos” that offer little support for collaborative investigations. Timely information sharing is crucial for the success of many investigations; however, investigations are often stalled by impediments related to sharing information [2]. Moreover, information management, investigation planning and execution are largely left to the individual case officer, which might result in poor information use. Individual investigators often have key responsibilities for ensuring compliance with complex laws and policies, slowing down collaborative investigations.

Considering that investigations frequently span multiple jurisdictions and government agencies with varying objectives and powers, determining the applicable rules and ensuring compliance with the relevant laws and policies is difficult. The implications of non-compliance are furthermore serious: evidence collected during the investigation in contravention of the legal rules might be inadmissible in court.

Therefore, an information system that can effectively support law enforcement investigations should include mechanisms for enforcing compliant processes in addition to efficient information management and analytic capabilities. Such a system responds to the *legal issues* that are relevant to information use and sharing. For example, information obtained under a warrant for a specific investigation may not generally be used in the context of other investigations, and restrictions might apply to agencies as to what information they can share [2]. In addition, many of the aspects of the relevant laws and rules require careful interpretation. An overly-conservative interpretation of laws and policies might unnecessarily restrict what can be shared while a liberal approach may not result in outcomes that are compliant. In addition to legal issues, other matters that may require consideration include workflows and policies as well as information security:

Workflows and policies may impact upon investigations. Many investigators and key offices in LEAs still adhere to antiquated processes and rely on paper forms and manual approvals for expenditure and information access. The resulting delays have potential to disrupt investigations. Moreover, the appropriate processes to follow may depend on the nature of the investigation and the involved agencies. Here, automation and electronic means of selecting, executing, and monitoring the relevant processes would streamline the investigation and provide assurance that tasks are undertaken in compliance with relevant policies and legal frameworks.

Information security and access control across system and organization boundaries can be difficult to achieve. In absence of a sophisticated access control mechanism, it is challenging to guarantee secure access to a large number of users accessing a multitude of information systems, especially where some of the information is highly sensitive and should not be accessed by anyone outside of the immediate investigative team. Often, information is obtained by means of personal communications outside the realms of the investigation management system. This is especially the case in relation to sensitive information. While such methods may provide the investigators with a sense of comfort regarding the security of the data, this approach complicates the tracking and integration of the information at later stages of the investigation and in the prosecutorial stage when proof of the integrity of the information may be crucial.

This paper describes the approach to comprehensive and compliant information access pursued by the Integrated Law Enforcement project conducted by the Data to Decisions Cooperative Research Centre (D2D CRC) in Australia. We discuss the architecture of the Investigation Management System that is currently under development and highlight its technical features that underpin workflow automation and investigation planning. We focus on the semantic linked information model underpinning the system's workflow automation functions and discuss how they can facilitate compliant investigations in a complex legislative and social environment.

2 Investigation Management System

The project Integrated Law Enforcement (ILE) aims to develop a platform where investigators can manage the information collection, analysis, and processes pertaining to a case through a consistent single user-facing portal. The portal offers functions for information ingestion, management and classification, searching, linking of entities, as well as investigation planning and evidence export that are tailored to the needs of investigators. Supporting the portal is an extensible software architecture for searching for information within the collective information base, extraction of entities and relationships from text documents, linking of entities to form a "knowledge graph" pertaining to one or more investigations, and integration of external data sources. As such, the platform aims to serve as a single point of access for investigators to manage their investigations, request, obtain, and explore information from several sources. The conceptual architecture of the platform is depicted in **Fig. 1.** Conceptual system architecture. The individual components are described in [5]. In this paper, we focus on the process aspect of the architecture.

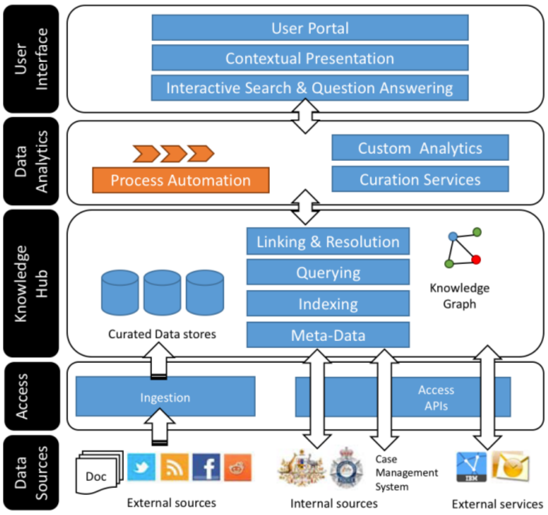

Fig. 1. Conceptual system architecture

3 Workflow Automation

Automatic data collection and integration offer tremendous opportunities to increase efficiency and effectiveness of investigations, the sensitivity of information that is collected and analyzed in this context raise serious legal compliance and governance challenges. Indeed, compliance with existing laws and principles is a pre-condition of the whole process [3]. Transparency and privacy should be preserved to foster trust between citizens and national security and law enforcement agencies. Even more so as prevalent data collection and sophisticated data analysis methods have the potential to undercut the due process (procedural fairness) safeguards built into the traditional criminal justice model of operation [4]. Therefore, we advocate the view that technical developments that enable such activities should be informed by and reflect the principles of the rule of law.

The approach taken in this work rests on a comprehensive semantic model of the domain that includes entities and relationships relevant to investigations, a meta-data framework that captures provenance and restrictions on information use, and an investigation planning and execution model. As information is acquired through the platform, it can be enriched with meta-data about its lineage, time of acquisition, and the line of inquiry task that led to this information within the overall investigation plan.

Semantic models extend to the process aspect of investigations, whereby investigators can rely on investigation planning functions to open and close lines of investigations. A taxonomy of offences linked to proof elements that must be established and templates of potential lines of enquiries can support the investigation planning activities. The integration of workflow planning and information acquisition functions helps to maintain detailed lineage of each piece of evidence collected. Moreover, it enables the system to automate parts of the process.

For example, if a search of premises related to a suspect is to be conducted, and the semantic model of the activity indicated that this search requires a warrant, the request for the warrant could be generated and workflows for obtaining approval of that warrant, planning of the search, and approval of related expenditure, could be initiated automatically. Once all approvals have been obtained, the investigator would be notified that the search activity can proceed. Any evidence obtained from the search would be entered into the system and it would be automatically linked to the line of inquiry, the task in the process, and its associated warrant. Given that the information is linked to the investigation process and its legal documents (e.g., warrants), the lineage of the information can then be used to determine how, when, and by whom that information may be used, provided that an appropriate semantic model of the conditions and restrictions is maintained. This approach is comparable to semantic policy annotations advocated for linked data [7].

The technology underlying this platform rests on process templates that are instantiated in the context of a specific investigation. Our current implementation rests on a Business Process and Notation (BPMN) workflow engine for execution. Configurable process templates specify the dependencies between activities, whereby process parameters determine the fillers for placeholder roles, data elements, and concrete sub-processes that implement hierarchical process steps. For example, business rules embedded in process templates select appropriate sub-processes tailored for communicating with different external organizations (to address variety in required information and technical submission procedures), determine who shall approve a request, etc. The information required for this configuration can be obtained from the knowledge graph capturing the current investigation, organization structure, and external parties' systems. Information that cannot be acquired automatically is entered by the investigator. Where processes cannot be completed successfully, for example due to the external organization requiring further information or an organization refusing to cooperate, the process reverts to manual intervention (for example, initiating another request for information with additional information attached). This simplifies the approach; as exceptional cases do not need to be modelled in detail for each process. In the context of law enforcement investigations, a semi-automated approach is sufficient, provided that all actions and responses are duly captured on a timeline in a log.

The approach described in the previous paragraphs rests on the assumption that the relevant procedures and policies are known, well understood, and that they have been expressed in the form of semantic models that the machine can interpret in the context of an investigation. Although semantic models may be devised using natural language processing techniques [6] challenges remain in the disparity between rigid formal representations (e.g., formal modal logics) and the often context-dependent interpretation of legal texts. In the context of law enforcement investigations considered in the project, the relatively small number of defined (internal) workflows can be modelled and validated manually. A library of workflows, tasks, and information objects complemented with rules that govern process execution and information use can be created and used to support the execution of the system.

Further work is required to address issues related to the reconciliation of partly incompatible norms that can arise when information is exchanged between agencies embedded in different legal systems. Even if appropriately detailed and complete semantic models were available, questions would still arise in relation to the reconciliation of differences in permissions, obligations, and processes. Moreover, suitable mechanisms for enforcing norms across organizational and legislative boundaries must be developed to instill trust in the overall information sharing arrangements.

4 Legal Principles

In previous presentations [5] [8], we already have highlighted the main sets of legal problems that we are addressing in this project: (i) the coexistence of both artificial and human decision-making and information processes; (ii) the identification, representation and modelling of specific legal requirements arising from different legal and government sources; (iii) the definition of a blended Regtech perspective to be applied to law enforcement and security; and (iv) the formulation of general principles for big data regulation in the Australian environment. Risks that should be mitigated include over-collection of data; production and use of inaccurate data; biased analysis; inappropriate data collection, storage, management and handling; inconsistent or uncontrolled inferences; and breaches of privacy and data protection.

Security platforms can collect, store, manage and reuse personal data under Open Source Intelligence (OSINT) provisions. Where warranted, subject to strict conditions and appropriate controls, they have to do so [9]. This is of course controversial, as such collection and use of data affects human, civil, and personal rights. It is therefore crucial to observe the basic principles of the rule of law. This view has also found support among technologists: there is a general agreement on fundamental rights and ethical values that the sciences of design have embraced [10] [11] [12].

However, the specific instruments set to protect and ensure the relevant rights are embedded in laws that differ globally and are even absent in some countries. Different legal cultures have therefore taken different approaches. For example, the European Regulation on Privacy contemplates the possibility to apply by design and by default the rights initially protected by the Directive 95/46/EC, now replaced by Regulation (EU) 2016/679, the EU General Data Protection Regulation (GDPR). Some authors advocate for regulatory, legal and technological enforcement of privacy to prevent major breaches and abuses [13].

In countries under the Common Law rule, courts play a major role, for example to determine whether government action that infringes a fundamental right such as privacy, was reasonable and proportional. In relation to fundamental rights, for example, the High Court of Australia employs a proportionality analysis to "ascertain the rationality and reasonableness" of the restriction on the fundamental right: the greater the restriction on the fundamental right, the more important must be the public interest purpose of the legislation for the proposed restrictive measure to be proportionate.[1] Our work includes discussion of legal principles to set the general framework to provide such a balance for national security law enforcement [NSLE] purposes. At present, these principles could be summarized as follows for purposes of Australia [14]:

1. Big Data analytics involving personal information should be employed when justified, and only in so far as is reasonably necessary to achieve defined and legitimate national security and law enforcement (NSLE) objectives.
2. The design, operation and management of all elements of the information lifecycle, including the application of Big Data analytics, must be proportionate.
3. The regulatory framework should be clear, consistent, and well-articulated.
4. Integrity of data and analysis should be supported
5. Data and systems must be protected.
6. NSLE agencies and all officers using data at all stages of the information lifecycle must be accountable.
7. Principles, rules, processes and systems should be reviewed regularly and, outside the review cycle when warranted.
8. The regulatory framework should support openness and transparency while safeguarding operational secrecy, where necessary and justified.

While the principles are still under development, it is clear that principles and statements about values cannot resolve the monitoring of the workflow and the regulation

[1] As quoted in [14]: "The term 'proportionality' in Australian law describes a class of criteria which have been developed by the High Court of Australia over many years to determine whether legislative or administrative acts are within the constitutional or legislative grant of power under which they purport to be done." *McCloy v New South Wales* [2015] HCA 34 at [3] per French CJ, Kiefel, Bell and Keane JJ.

of the platform at the technical level. They convey values that can be turned into guidelines, but similarly to Fair Information Practices (FIPs) or privacy and data protection principles (PP, DPP) [15], they do not provide any mechanism to easily implement or embed them. Principles, however, can be interpreted to inform individualized case-based decisions once a problem or conflict has arisen. They may also be fleshed out through use case applications, reflected into more specific contents, and represented/translated into a formal language to minimize risks and prevent law suits and conflictive situations. However, the scope of fundamental rights and freedoms, including privacy, procedural fairness, and Australian tests of proportionality, is still to be settled. Hence, the complexity of translating them into a working tool for compliance should not be underestimated.

5 Legal Compliance by Design (LCbD)

Legal compliance by design can be defined as "the process of developing a software system that processes personal data in such a way that its ability to meet specific legal provisions is ascertained" (i.e. compliance of evolving security policies against formal rules derived from legal provisions) [16]. LCbD is however not limited to the processing of personal data. The scope of this approach is potentially much wider, extending to all compliance requirements. The point of departure of LCbD is that all legal content is semi-automatically or automatically extracted from legal documents —represented, processed, and eventually implemented. While the correctness of this assumption can be questioned (see 6 below) LCbD is currently a "hot trend" in AI & Law.

Compliance by Design (CbD) emerged in the business field, to facilitate a better understanding and modelling of the ongoing mechanisms of monitoring, evaluating, and auditing.[2] The objective to be compliant with the law was also fueled by the enactment of Sarbanes-Oxley Act (2002), the economic crisis that followed, and by the increasing regulatory and supervisory pressure on companies to professionalize and document compliance management. Transparency and accountability became important to maintain credibility and the corporate image in the market in relation to business counterparts and consumers [18]. Thus, Compliance by Detection (CbDt) —which entails a conformity check during and after the runtime stage to detect internal violations— has been increasingly completed by CbD — which entails a conformity check with regulations and laws in the runtime stage, designed in advance as a whole [6].

[2] "Over the last years, business compliance, i.e., the conformance of business procedures with laws, regulations, standards, best practices, or similar requirements, has evolved from a prerogative of lawyers and consulting companies to a major concern also in IT research and software development. Given the increasing IT support in everyday business as well as the repetitive and work-intensive nature of compliance controls and audits, this evolution can be seen as a natural extension of current enterprise software, especially in light of the novel, technical opportunities offered by the Service-Oriented Architecture (SOA). Yet, until only few years ago, compliance management was not perceived as major concern in IT research." [17]

Several business vocabularies, languages, and methodologies have been developed so far [19]. Approaches and methodologies to identify, extract from legal documents, model, and eventually implement and enforce the resulting rules have also been proposed. These include Legal Goal-oriented Requirement language (LGR) based on URN [20], REGOROUS [21], EUNOMOS [22], and NOMOS [23]. This is a common endeavor, with several intersections, as the modelling of legal requirements; the combination of linguistic techniques (NLP, NSP) with deontic non-standard logic; ambiguity and vagueness of the legal language (interpretation); and the representation of legal arguments, constitute shared problems that can be faced in common. The emergence of semantic languages —LegalXML, LegalRuleML …— plays a major role in this endeavor. Protections are especially (not exclusively) targeted in the financial, public health, security, and consumer areas.

These perspectives require some conditions: norms should be expressed at the representation level in some (natural) language on specific written documents, valued as "legal" (such as legal Acts or court decisions), or "regulatory" (such as standards or best practices). What is legal (or "counts as legal") must therefore be determined in advance. Another condition concerns legal knowledge: it requires extensive work carried out by experts to select, manipulate, interpret, transform legal terms and concepts, and eventually decide the interpretation of "what counts as legal".

The essential role of inferential "intermediary concepts" in legal knowledge representation —property, heritage, crime, privacy …—, has long been recognized in deontic logics and in legal theory, because these concepts encapsulate the kind of semantic properties that constitute pre-conditions to trigger normative effects, i.e. produce the doctrine constructed by legal experts (legal doctrine). This raises several questions, including: under which conditions do normative effects turn into "legal" binding effects; whether legal knowledge can be completely modeled (particularly in relation to common law, which is casuistic and inherently dynamic); and to what extent artificial models reflect the law or rather legal knowledge (the law interpreted by experts through legal doctrines).

6 Legal Compliance through Design (LCtD)

While we recognize the importance of these questions, they are not addressed in this brief paper. Very likely what is called "legal knowledge" in democratic societies is the collective result of an intertwined social process involving official and non-official organisms (such as the Parliament and the media), political decision-making, legal expertise, and the reception, approval, and eventual resilience of citizens. Our contention —especially in policing and law enforcement agencies (LEA), settings, and contexts— is that compliance with the law entails a set of dynamic conditions that cannot be completely foreseen in advance, and thus, cannot be wholly modelled as a process, but only as a result. In this situation, institutional design can supply the framework in which the protections of the rule of law can be effectively implemented.

Privacy provides a good example of this assertion [24]. The relevant legal requirements, the passage from pre-conceptual to conceptual models, can be considered from at least three perspectives: (i) direct PbD (where principles are embedded using goal-oriented languages or a formalism to detect privacy violations to prevent breaches, e.g., tracking logs, sensemaking technologies and data tethering [15]], (ii) a combination between tactics and strategy (where principles are nuanced to capture more constraints to facilitate the lawyers' work and produce "near-compliance") [25] [26], and (iii) an indirect strategy, a combination between PbD and institutional rules into a regulatory comprehensive model, especially tailored for monitoring the information workflow on the platform [27] [28] Previous regulatory projects on security platforms have shown that auditing and monitoring OSINT processing and workflows require not only PbD or CbD but the structured construction of hetero and self-regulatory institutions, i.e. systems with internal and external controls able to contain functional roles within a hybrid human-machine interface (Fig.2).

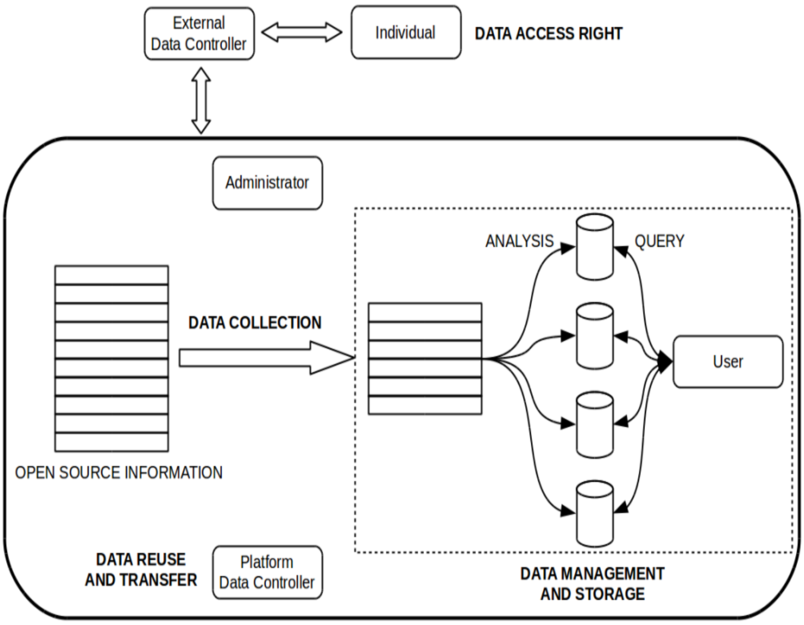

Fig. 2. Hybrid strategy: internal and external platform controls [26] [27]

A CbD approach that captures legal and regulatory constraints and expresses them as requirements we call *Compliance through Design* [CtD]. CbD entails incorporating (digitally as well as non-digitally) hard law, soft law (non-binding standards, protocols, recommendations), policies (governance guidelines) and ethics (values, best practices) into a dynamic institutional model, containing protections, rights and duties.

CbD is generally used to refer to compliance-sensitive design processes that embed compliant processes or behaviors and facilitate compliance management. In a software environment, it refers to a process of developing a software system that facilitates implementation of a business process to meet specific compliance requirements. CtD on the other hand, entails a semi-automated process embedding the interpretation of laws, regulations, principles, policies, best practices, and ethical norms both, into the workflow and into the institutional design. CtD is: (i) context-dependent, (ii) interactive, (iii) interpretive, and (iv) complex, as norms and laws must be identified and interpreted in advance to define the rules to be formulated and coded. CtD requires the description and building of a prospective legal ecosystem defining roles, functions and responsibilities for the key roleplayers.

CtD is mainly focused on institutional building, as well as on interpretation. It is worth noticing that plurality of competing legal interpretations is also respected and can be modelled using ongoing legal CbD systems [29] or, for example, a combination of reified deontic input/output logic and linguistic techniques (Natural Language Processing, Natural Language Semantics) [30]. CbD has already been successfully implemented in some public services to reduce costs of control and increase the transparency and accountability of the Administration [31]. What is proposed here does not compete with existing solutions. The idea is embedding LCbD into broader *anchoring* institutions —i.e. regulatory bodies running socio-technical systems, platforms and applications— to better frame, manage, and monitor the rights, duties and responsibilities of stakeholders producing a specific and controllable legal ecosystem.

7 Conclusion and future work

Legal requirements discussed above do not exhaust social and legal conditions. We will adopt a CtD strategy that will allow us to operationalize controls inside and outside the platform. This will be done on several non-conflictive and non-intrusive uses cases involving citizens, for example in relation to aspects of police and court history checks. A National Police History Check is available in Australia.[3] A prospective employer, a public service or volunteer organizations, for example, can request it using the National Police Checking Service Support System. The purposes of such enquiries can be quite diverse: general employment, public administration, intelligence, etc. The service provides sensitive information in many different types of cases (all kind of criminal records). For non-NSLE purposes such information can only be requested with the consent of the person concerned. This service, it is submitted, can be automatized, provided that due protections are put in place. Understanding, selecting, describing and fleshing out the legal conditions of possible scenarios for such a service is not an easy task, but

[3] https://instantchecks.com.au/TermsAndConditions.aspx

it will provide the benchmark to test the practical effectivity of our principles and the correct functioning of the platform.[4]

Acknowledgements

This research was partially funded by the Data to Decisions Cooperative Research Centre (D2D CRC), and Meta-Rule of Law (DER2016-78108-P, Spain). Views expressed herein are however not necessarily representative of the views held by the funders.

References

1. Edwards, M., Rashid, A., Rayson, P. A systematic survey of online data mining technology intended for law enforcement. ACM Computing Surveys (CSUR), 48(1), 15 (2015).
2. Scheepers, R., Whelan, C., Burcher, M., Nielsen, I. Integrated Law Enforcement Project, Qualitative End User Evaluation, Baseline Report. Technical Report, Data 2 Decisions CRC. (2017).
3. Bennet Moses, L.; Chan, J.; De Koker, L.et al. Big Data Technology and National Security - Comparative International Perspectives on Strategy, Policy and Law Australia. Data to Decisions CRC (2016).
4. Marks, Amber and Bowling, Ben and Keenan, Colman, Automatic Justice? Technology, Crime and Social Control (October 19, 2015). R. Brownsword, E. Scotford and K. Yeung (eds), The Oxford Handbook of the Law and Regulation of Technology, OUP, Queen Mary School of Law Legal Studies Research Paper No. 211/2015; TLI Think! Paper 01/2015. Available at SSRN: https://ssrn.com/abstract=2676154
5. Mayer, W., Stumptner, M., Casanovas, P. and de Koker, L., 2017. Towards a Linked Information Architecture for Integrated Law Enforcement. Linked Democracy: Artificial Intelligence for Democratic Innovation. LINKDEM@IJCAI (2017), pp.28-37, http://ceur-ws.org/Vol-1897.
6. Casanovas, P; González-Conejero, J., de Koker, L. Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey. TeReCom, Workshoon Technologies on Regulatory Compliance, 30th JURIX-2017, Luxembourg, 13 Dec. [this volume]
7. SPECIAL Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compliance. Deliverable 1.3: Policy, transparency and compliance guidelines V1. (2016) http://www.specialprivacy.eu/.
8. Stumptner, M., Mayer, W., Grossmann, G., Liu, J., Li, W., Casanovas, P., De Koker, L., Mendelson, D., Watts, D. and Bainbridge, B., 2017. An Architecture for Establishing Legal Semantic Workflows in the Context of Integrated Law Enforcement. arXiv preprint arXiv:1708.06613.

[4] We have used the term “linked democracy” to highlight that the implementation of rights and democratic values on linked data ecosystems goes beyond the idea of being compliant with rules [32]. LCbD or LCbD are only components of such a chain.

9. Casanovas, P. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In R. Taddeo and L. Glorioso, Ethics and Policies for Cyber Operations, pp. 139-167: Dordrecht: Springer International Publishing, 2017.
10. Pagallo, U. Good onlife governance: On law, spontaneous orders, and design. In L. Floridi (ed.) The Onlife Manifesto. Being Human in an Hyperconnected Era, pp. 161-177. Springer Open (2015). International Publishing.
11. Noriega, P., Verhagen, H., d'Inverno, M. and Padget, J., 2016. A manifesto for conscientious design of hybrid online social systems. In Coordination, Organizations, Institutions, and Norms in Agent Systems XII (pp. 60-78). Springer, Cham.
12. Dignum, V. Responsible Autonomy. IJCAI August 2017, Melbourne. <arXiv:1706.02513v1 [cs.AI]>.
13. Wright, D., de Hert, P. (eds.). Enforcing privacy. Regulatory, Legal and Technological Approaches. Dordrecht: Springer (2016).
14. Law and Policy Program. Draft high level policy principles on the use of Big Data analytics by national security and law enforcement agencies. Data to Decisions Cooperative Research Centre. October 2017.
15. Cavoukian, A. Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Information and Privacy Commissioner, Ontario, Canada, December 2012.
16. Ranise, S. and Siswantoro, H. Automated Legal Compliance Checking by Security Policy Analysis. In: S. Tonetta et al. (Eds.) SAFECOMP 2017 Workshops, LNCS 10489, International Conference on Computer Safety, Reliability, and Security (pp. 361-372). Springer, Cham (2017).
17. COMPAS EU Project 2009. Final Report. Compliance-driven Models, Languages, and Architectures for Services <https://cordis.europa.eu/fp7/ict/ssai/docs/finalreport-compas.pdf>
18. Claydon, J. Compliance/Legal Compliance. In: Idowu et al. (eds.), Encyclopedia of Corporate Social Responsibility, DOI 10.1007/978-3-642-28036-8, #Springer-Verlag Berlin Heidelberg 2013, pp. 429-434.
19. Ghanavati, S., Amyot, D. and Peyton, L., 2011, August. A systematic review of goal-oriented requirements management frameworks for business process compliance. In Requirements Engineering and Law (RELAW), 2011 Fourth International Workshop on (pp. 25-34). IEEE.
20. Ghanavati, S., Amyot, D. and Rifaut, A., 2014, June. Legal goal-oriented requirement language (legal GRL) for modeling regulations. In Proceedings of the 6th international workshop on modeling in software engineering (pp. 1-6). ACM.
21. Sadiq, Shazia, and Guido Governatori. A methodological framework for aligning business processes and regulatory compliance. Handbook of business process management 2 (2009): 159-176.
22. Boella, Guido, Luigi Di Caro, Llio Humphreys, Livio Robaldo, Piercarlo Rossi, and Leendert van der Torre. Eunomos, a legal document and knowledge management system for the Web to provide relevant, reliable and up-to-date information on the law. Artificial Intelligence and Law 24, no. 3 (2016): 245-283.
23. Ingolfo, S., Jureta, I., Siena, A., Perini, A. and Susi, A., 2014, October. Nomos 3: Legal compliance of roles and requirements. In International Conference on Conceptual Modeling (pp. 275-288). Springer, Cham.
24. Koops, J., Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection Law, International Review of Law, Computers & Technology, (2014) 28, 2: 159-171.

25. Colesky, M. and Ghanavati, S. Privacy Shielding by Design—A Strategies Case for Near-Compliance. In Requirements Engineering Conference Workshops (REW), IEEE International (pp. 271-275). IEEE (2016).
26. Colesky, M., Hoepman, J. H., Hillen, C. A Critical Analysis of Privacy Design Strategies, IEEE Symposium on Security and Privacy Workshops, 33-40. DOI 10.1109/SPW.2016.23
27. Casanovas, P.; Arraiza, J.; Melero, F.; González-Conejero, J.; Molcho, G.; M. Cuadros, M. Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project. Legal Knowledge and Information Systems. JURIX 2014. ed. R. Hoekstra, Foundations on Artificial Intelligence núm. 271, Amsterdam: IOS Press, p. 189-199.
28. González-Conejero, J., Figueroa, R.V., Muñoz-Gomez, J. and Teodoro, E., 2014. Organized crime structure modelling for European Law Enforcement Agencies interoperability through ontologies. In AI approaches to the complexity of legal systems (pp. 217-231). Springer, Berlin, Heidelberg.
29. Ghanavati, S. and Hulstijn, J. Impact of legal interpretation on business process compliance. In Proceedings of the First International Workshop on TEchnical and LEgal aspects of data pRIvacy (pp. 26-31). IEEE Press (2015).
30. Bartolini, Cesare, Andra Giurgiu, Gabriele Lenzini, and Livio Robaldo. A Framework to Reason about the Legal Compliance of Security Standards. In Proceedings of the Tenth International Workshop on Juris-informatics (JURISIN). 2016.
31. Christiaanse, R. and Hulstijn, J., 2012, June. Control automation to reduce costs of control. In International Conference on Advanced Information Systems Engineering (pp. 322-336). Springer, Berlin, Heidelberg.
32. Poblet, M., Casanovas, P., Plaza, E. Proceedings of the Workshop on Linked Democracy: Artificial Intelligence for Democratic Innovation, co-located with the 26th International Joint Conference on Artificial Intelligence (IJCAI 2017). Melbourne, Australia, August 19, 2017. http://ceur-ws.org/Vol-1897/.
33. Sadiq, S. and Governatori, G., 2015. Managing regulatory compliance in business processes. In *Handbook on Business Process Management 2* (pp. 265-288). Springer Berlin Heidelberg.