Risk of an epidemic impact when adopting the Internet of Things: the role of sector-based resistance

Introduction

The Internet of Things (IoT) is rapidly becoming a dynamic and global internet-based architecture. It is based on standard communication protocols and has a self-configuring capability, with physical and virtual things having identities and being integrated within the information network (Sundmaeker *et al.*, 2010). The IoT is a vision of the future of internet that combines Communication Internet, Energy Internet and Logistics Internet (Rifkin, 2014); it is seen as a third revolution, and is derived from the information technology (Porter, 2014) that was instrumental in enabling the safe and reliable exchange of goods, services and data.

The term "Internet of Things" was coined in 1999 by researchers at the MIT Auto-ID Lab in Boston. Initially, the concept was used to describe a network of objects connected to the internet through radio-frequency identification (RFID) technology. Today, according to some scholars (Kellmereit and Obodovski, 2013), there is a disconnection between high-tech community and industry in the Machine-to-Machine area. The approach to IoT architecture is, however, much more organic than that of traditional networking.

Several countries have recognised the importance of the IoT for their future economic growth and sustainability (Sundmaeker *et al.*, 2010). The European Commission was the first supranational body to introduce public consultations and discussions concerning business opportunities, new services, the management of incidents, and on how to monitor human activities and address energy efficiency issues. From EU-funded studies, it has been shown that governments, industry and business have little or no awareness of the IoT or what it offers (Hochleitner *et al.*, 2012). In reality, this research starts by recognising the discrepancy between the vision of the IoT and the reality in terms of current technology and available policy instruments. In general terms, the technical issues are now being discussed in detail, while the economic and legal obstacles are still not fully understood by many authors.

Many scholars (Chandrakanth *et al.,* 2014; Gubbi *et al.,* 2013; Pye, 2014; Weber, 2009) have investigated the technical aspects and general legal obstacles to the IoT, but there are no studies that concentrate on sectorial resistance, and how it can affect the success of IoT-based innovation.

The aim of this paper is to identify the main sectorial obstacles that the IoT is facing in terms of timing and penetration in its pursuit of a new information society and knowledge economy.

By using a case study centred on the professional football industry, the objective of this study is to demonstrate that society as a whole decides to adopt a new technology according to the relative institutional structure (Mokyr, 2002). In this view, innovations must address the institutional obstacles that stem from economic and cultural resistance. In particular, when technological changes are discontinuous and affect different business areas, the uncertainty surrounding costs and benefits and the associated path dependence are all key factors in determining how new knowledge is developed (Salvato *et al*., 2010; Schimmenti *et al*., 2014).

Many business sectors are resistant to new technologies and, in particular, to the IoT. Professional football is a prime example of how institutions prevent the use of this technology. Federation bodies have actually forbidden the use of any new technology during competitive matches (Law 4, Laws on the Game, FIFA, 2014). The purpose of our case study is to identify the main types of resistance to the introduction of the IoT in professional sport, where opposition can be individual, company-specific and/or sector-specific. In this context, we have tried to show that institutional structures and laws can act as tools to overcome the obstacles to the introduction of this new technology and architecture, if awareness and education programmes are also provided to explain the potential and benefits of the IoT.

The research utilises a deductive-inductive approach, with a qualitative method and a case study analysis (Hair *et al.*, 2013; Yin, 2013). This is an exploratory research on the difficulties arising when introducing an innovation (IoT) to a specific sector (football industry).

Secondary data was used in the study. In light of the arguments presented in this section, the research questions are:

RQ_1 - Which are the causes that limit the implementation of IoT and the exploitation of big data by football institutions?

RQ_2 - Can sector-based resistance have an impact on the general success of innovation?

The article has the following structure. After the introduction, the second section contains a literature review on the IoT from the legal perspective. The methodology is described in the third section. Section four includes an analysis of the case study, examining the adoption of the IoT by professional football. In section five, the research findings are extended to a more general level. The sixth section provides our primary conclusions.

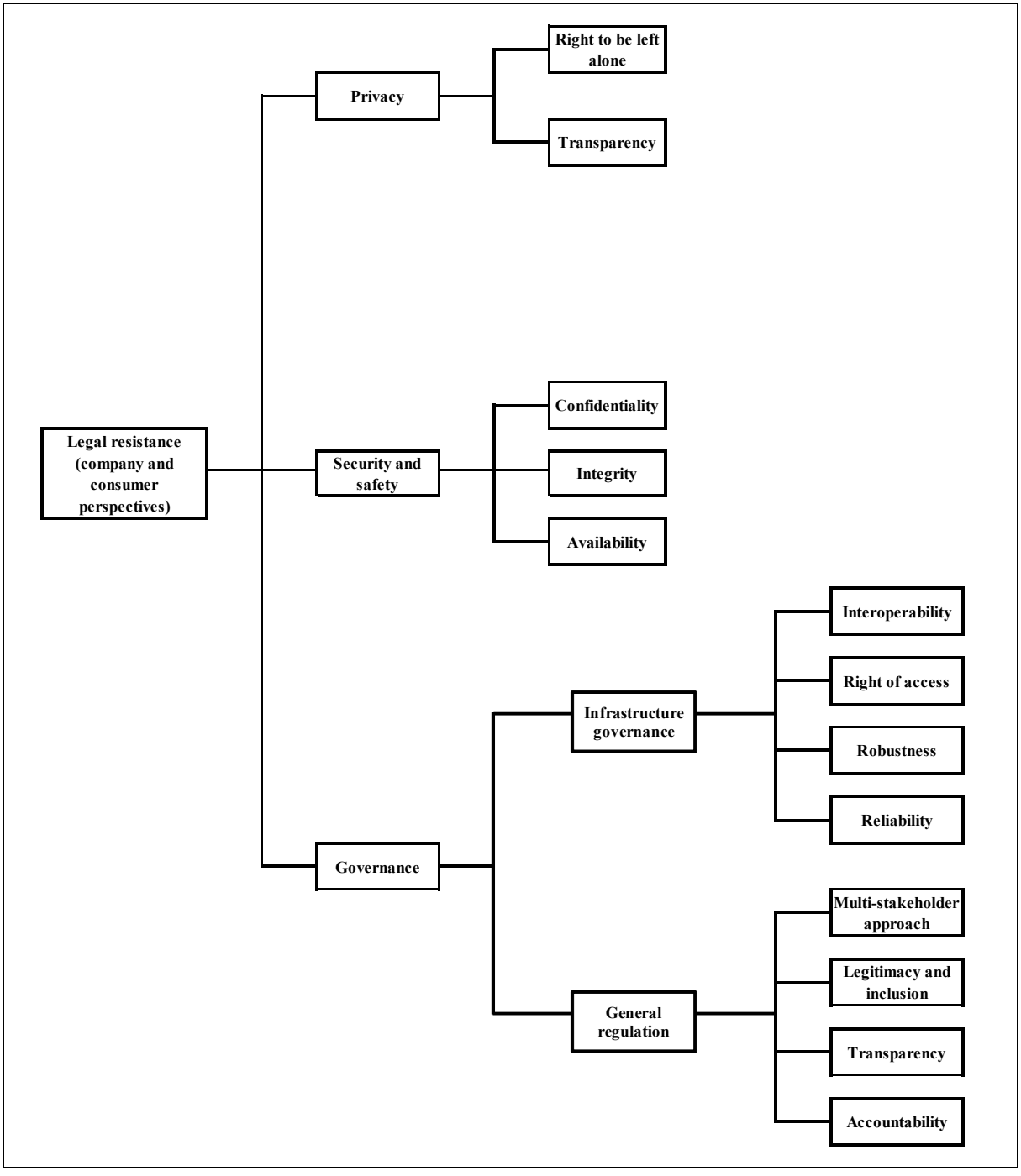
Internet of Things from the legal perspective

A number of research studies, sponsored by supranational bodies, have investigated the various application settings, the main legal risks and the architecture of the Internet of Things. The European Commission, in a 2009 communication (2009/387/EC), outlined an action plan for Europe on the IoT, stating that RFID technology and IoT factors promote growth and employment, quality of life and efficiency of businesses. The reports drafted by governmental entities and regulatory bodies tend to focus on the actual implementation and the expected economic benefits of the IoT (Weber, 2009). They also seek to address all the consequences issuing from the emergence of the IoT. From existing studies and reports, it can be seen that there are a number of legal issues concerning the IoT, where a more coherent legal system must be created to address the specific challenges set by the IoT (Weber and Weber, 2010). In general, the main challenges concern data protection and accountability, and these two aspects are essential in order to establish a legal framework for trust in the IoT (Hochleitner *et al*., 2012).

The IoT, as a global internet-based information architecture, helps the process of exchanging goods and services, while highlighting the need for new internet governance.

The framework of the literature review concerning legal issues is shown in the following Figure 1.

Figure 1 – Literature review framework



According to this view, generic legal resistance to the IoT can be addressed differently for two groups, companies and consumers. The main disparity between these two groups concerns their different understanding of hard and soft law approaches. In terms of these approaches, Jacobsson (2004), and Trubek and Trubek (2005) make reference to three main issues (privacy and data

protection; security and safety; governance), which are also set out in the European Commission's public consultation for the period from April to July 2012 (European Commission Report, 2013).

Privacy and data protection

With reference to privacy and data protection in cyberspace (Reidenberg, 2000), the current data protection framework is considered to be adequate by industry, while, according to consumers, there should be a greater focus on privacy and data protection matters within the context of the IoT. First generation laws on the protection of individual privacy were based on Article 8 of the European Convention for the Protection of Human Rights. This first generation legislation, defended by Warren and Brandeis (1890), basically grants consumers the "right to be left alone". In recent years, technological progress has led to second generation laws on the protection of individual privacy (Convention no. 108 of the Council of Europe8, Directive 95/469 or Article 8 of the European Charter of Human Rights), with its resulting need for transparency, which is necessary to restore the balance and guarantee the informed right of self-determination for all. However, IoT technology creates a new type of data or possibly a new generation of data. Many authors (Atzori *et al*., 2010), indeed, argue that the law must be adapted to new technological developments because, at present, data protection law seems powerless to regulate the IoT.

Security and safety

A second form of resistance concerns the security and safety of the IoT (Mayer, 2009). According to both groups, industry and consumers, it is necessary to create guidelines and standards to ensure data confidentiality, integrity and availability. Industry believes that it is important not to over-regulate the technical environment, which can create unnecessary boundaries that can limit free trade or the emergence of better IoT architecture (Weber, 2013). Consumers, instead, demand protection against data being used by external subjects for other purposes than those intended, considering this as a more important issue than economic freedom (Buttarelli, 2010). Several authors (Dutton, 2014) are in agreement that collecting data and making it available can cause problems of trust and privacy, because individuals become wary of data surveillance and the secondary use of information.

Governance

The third legal form of resistance to the introduction of RFID technology in different business sectors is the issue of IoT governance (Weber, 2013).

This matter can be analysed from two perspectives, infrastructure governance and general regulation.

The IoT is a system involving a great number of interconnected technological devices, and it must satisfy four main conditions in order for trust in its infrastructure to be established (Weber and Weber, 2010):

- interoperability, in terms of connectivity between computers and networks, between people and things and among things;
- right of access, in order to guarantee a fair and non-discriminatory use by all interested stakeholders and businesses and to avoid any increase to the digital divide (Norris, 2001) in the IoT environment;
- robustness of the infrastructure, meant as the capability of dealing with change or loss of functionality, and especially important for businesses;
- reliability of the system, referred to the users' acquired confidence in the infrastructure and its performance.

With reference to general legislation, the European Commission consultation (2013) shows that industrial organisations maintain that there is no need for specific IoT governance, since the existing rules and schemes set in place for the internet can be used. Industrial organisations are, however, also concerned that general regulations may damage their interests. Consumers have a different view of the need for general regulations to manage the IoT. Civil society and consumer organisations support the creation of a new body to establish a basic general framework for IoT applications and services.

It is, nevertheless, widely asserted by both groups (Weber, 2013) that there is the need for a multi-stakeholder approach to regulating important issues, such as privacy, interoperability and ethical standards. The concept of multi-stakeholder governance has emerged as a new approach to debating matters concerning the structure, root system and institutional issues of the IoT. The purpose of these debates is to promote an open mechanism of cooperation between market stakeholders and consumers, through which the principles of IoT governance can be defined (Malcolm, 2008). Weber (2013) identifies two possible approaches to multi-stakeholder regulation. In a top-down/centralised approach, single body coordinates all the actors; in a bottom-up approach, the exchanges between different stakeholders take place horizontally.

According to Weber (2009), the second principle of IoT governance is the legitimacy and inclusion of stakeholders. The different stakeholders must be represented suitably if the interests of all are to be protected and fair procedures put in place.

Transparency is generally considered as a key governance issue, because it underpins the operational mechanisms and procedures of markets and organisations. The concept of transparency includes ethics, procedural elaboration of rules and decision-making processes.

Accountability within the IoT governance is the final fundamental aspect. As a result, harmonised standards must be improved to ensure that governing bodies are accountable for their operations and able to impose sanctions for non-compliance to accountability criteria. Standards can help in implementing structures and guidelines regulating governance principles.

Dutton (2014) argues that architectural principles must be developed and elaborated in an international multi-stakeholder legal framework. Since the IoT is international and not restricted geographically, many authors (Hildner, 2006) wonder how this new vision of a future internet can be regulated and which institutions have the authority and capability to lay down rules.

In order to determine the regulation model to be applied, Weber and Weber (2010) proposed four approaches that can be used to regulate the IoT. These are no-regulation, traditional government regulation, international agreements and self-regulation.

According to no-regulation, an economic environment defined by free trade is paramount. The new technology is so important that rules are not deemed to be appropriate. According to traditional government regulation, such as a State law, citizens are forced to comply with fixed rules through a geographically-limited legitimacy. Through the international agreement approach, it is possible to establish a completely new supranational organisation or create a new committee for the World Trade Organisation or the Organisation for Economic Co-operation Development. This is unlikely to be achieved in the near future. Finally, self-regulation is currently considered by many authors (Li and Ma, 2013) to be the key approach for bringing the IoT to every business sector. Self-regulation follows the principle of subsidiarity, with rules being developed that are independent of the principle of territoriality. It is a soft law, since the State legislator can set the general pillars of the legal framework with a co-regulation approach related to that of the private sector. Self-regulation can also be defined as a model of social control enforced through reputational sanctions.

Many authors (Chandrakanth *et al*., 2014; Bandyopadhyay and Sen, 2011; Gubbi *et al.,* 2013; Pye, 2014) focus their studies on the technical development of IoT architecture, despite being aware of several institutional issues that hinder the depth and speed of penetration of the IoT within the business environment.

Chandrakanth *et al.* (2014) describe the applications and challenges faced by the IoT, examining the technical aspects relating to the adoption of Internet Protocol Version 6 (IPv6), investments in data storage and the management of security. Bandyopadhyay and Sen (2011) have studied the state-of-the-art of the IoT, illustrating key technological drivers and potential applications for the IoT, while

discussing the different perspectives in academic and industry communities. In the paper by Gubbi *et al*. (2013), the authors present a cloud-centric vision for the worldwide implementation of the IoT and present the key enabling technologies and application domains that can drive IoT research in the near future. Pye (2014) debates the potential of the IoT in terms of future revenues for industries, especially those involved in communications and automation.

All these studies, however, have led to a gap in the literature, whereby there is the need to align the IoT vision, the available technical instruments and the institutions involved.

For this reason, it is possible to assert that there is a lack of research that specifically covers the institutional obstacles that prevent the IoT from being widely applied, caused by economic and cultural uncertainties. In the light of this proposition, our analysis investigates how sector-based resistance can influence the way in which an innovation is received and the extent to which it is trusted. In the paper, we have also tried to find and suggest how to overcome sector-based resistance to the IoT, by analysing the professional football industry, which provides the context of our research.

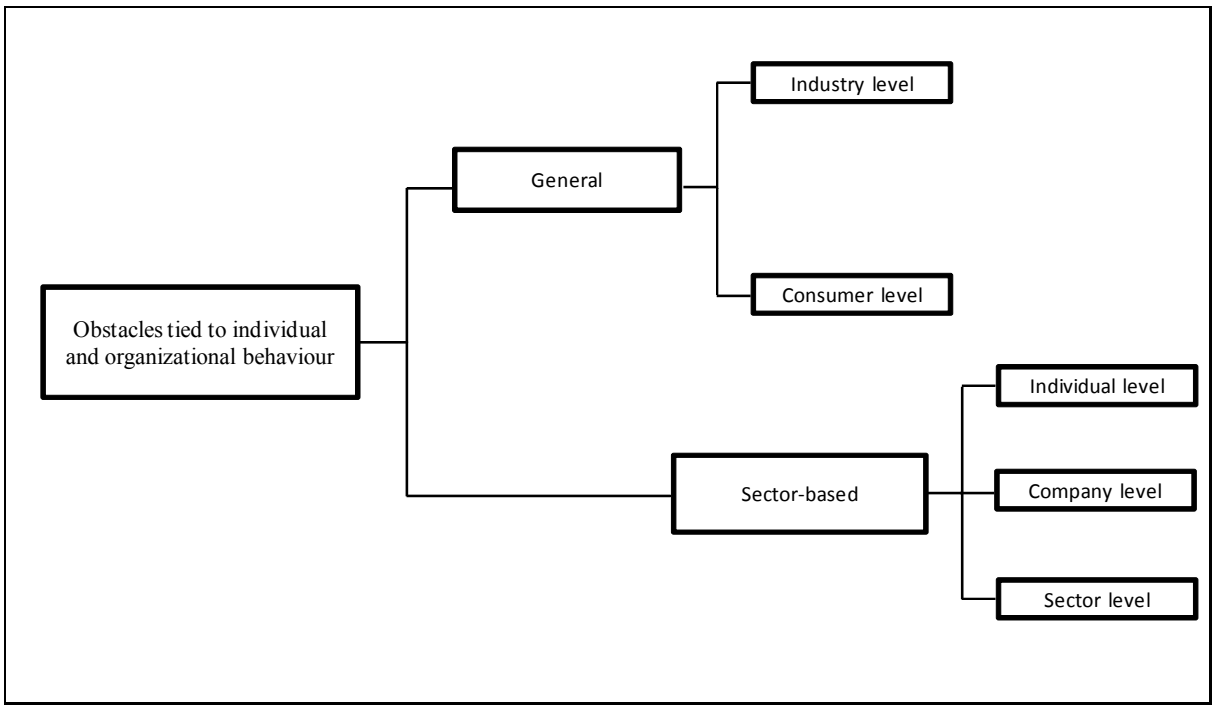
Methodology

The research is based on a qualitative method (Myers, 2013), using a deductive-inductive approach with a case study analysis (Eisenhardt, 1989; Hair *et al.*, 2013; Yin, 2013). This paper is an exploratory research to examine the difficulties of introducing innovation to the sports sector and, therefore, to investigate the effect of sector-based resistance on the general acceptance of the IoT.

The study is based on the economic theory proposed by Mokyr (2002). This states that, in economic history, innovation in the knowledge economy is subject to resistance to transformation. According to the theory of self-regulated systems (Mokyr, 1990), organisations are inherently stable, and therefore, technological progress is a deviation from the norm.

In order to answer the research questions and fill the literature gap, the research framework (Figure 2) starts by reviewing the literature on IoT studies concerned with the legal issues relating to its introduction, and by identifying general obstacles. The focus of the analysis then moves to sector-based obstacles by investigating how the IoT is implemented within the football industry. The aim of the study is to understand how institutional-type boundaries are caused by resistance at player, club and football industry level.

Figure 2 – Research framework



Data were collected through secondary sources, and include interviews in TV programmes, documents, reports, news items, scientific papers, books and databases (Creswell, 2012; Yin, 2013). With reference to this particular case study, the following sources were analysed:

- official new releases by the International Federation of Association Football (FIFA) and the Union of European Football Association (UEFA);
- FIFA Laws on the Game 2013/2014;
- official web pages of companies providing IoT technology for football clubs;
- Sky Sport Italia TV programme on big data in football on April 25, 2015, with reference to interviews with players and managers.

The interviews were selected from a database containing a Sky Sport Italia programme on the use of big data in the football industry. The football experts interviewed are shown in the following table 1.

Table 1 – List of football experts on big data in the football industry

Experts interviewed on Big data	
Gianluca Vialli	Former footballer - Juventus F.C., U.C Sampdoria and Chelsea F.C. / Former coach - Chelsea F.C.
Gianfranco Zola	Former footballer - S.S.C. Napoli,Parma F.C. and Chelsea F.C. / Former coach - Cagliari and Watford F.C.
Luigi Di Biagio	Former footballer - Roma and International Milan F.C. / Coach - Italian Under 21
Simon Kuper	Journalist - Financial Times
Alessandro Costacurta	Former footballer A.C. Milan
Mario Gomez	Footballer - A.C.F. Fiorentina
Mateo Kovacic	Footballer - International Milan F.C.
Mario Sconcerti	Journalist - Corriere della Sera
Mauro Icardi	Footballer - International Milan F.C.
Zvonimir Boban	Former footballer A.C. Milan
Lilian Thuram	Former footballer - Juventus F.C. and Parma F.C.
Alberto Piccinini	Journalist - Il Manifesto
Stefano Pioli	Coach - S.S. Lazio
Matteo Marani	Journalist - Guerin Sportivo
Ciro Ferrara	Former footballer Juventus F.C.
John Coulson	Manager - OPTA (Pr-essional football services)
Fabio Luna	Manager - OPTA (Editorial services - South Europe)
Stefano Okaka	Footballer - U.C. Sampdoria
Simone Zaza	Footballer - Juventus F.C.
Antonio Gagliardi	Match analyst - Italian national team
Antonio Conte	Coach - Italian National team
John Foot	Professor at the University of Bristol
Giuseppe De Bellis	Director - Rivista Undici
Josep Guardiola	Coach - F.C. Bayern Monaco
Manuel Neuer	Footballer - F.C. Bayern Monaco
Christopher Kramer	Footballer - Bayer 04 Leverkusen
Maurizio Sarri	Coach - S.S.C. Napoli

This research, therefore, contributes to existing literature, offering to both the scientific community and industry a holistic concept of how the IoT tackles sector-based obstacles with a widespread impact that can affect the success of innovation.

Professional football sector-based resistance to the introduction of the IoT

According to a recent study on sports teams, leagues and federations, the global sports industry is valued at between 350 billion and 450 billion Euros (Kearney, 2011). This study contends that the

global sports industry is growing much faster than GDP rates around the world. Football remains the main sector in sport for global revenues, with annual income of 20 billion Euros. In Europe, football is a business worth 16 billion Euros involving five big leagues: the English Premier League, German Bundesliga, Italian Serie A, Spanish Liga and French Ligue 1.

Nowadays, a large number of sports are pervaded by the rapid changes in technology and media, the forces of internationalisation and globalisation, the widespread liberal thinking concerning economic and business matters and the regulatory influence of bodies such as the European Union (Sšderman and Dolles, 2013). Some authors (Beech and Chadwick, 2004) argue that football, from a simple sports competition, has become a sports contest connected to a complex set of economic, social and political structures with a huge cultural and financial impact.

Professional football clubs are run under different ownership models, although, since the mid-1990s, many follow the stock market model, in order to appeal to global investors. Global industrial groups operating in important sectors all over the world (i.e. airlines, automotive and oil) invest massively in these clubs, attracted by high media exposure and the stream of revenue generated by the new broadcasting systems (Gerrard, 2000). In reality, in terms of the economic impact of football, its greatest general effect is that hundreds of millions of fans around the globe follow the sports on a daily basis, on radio, television, social media, or through printed publications, online or in person, as spectators or participants.

On top of this, digital technologies designed for the sports industry and sports events are now expanding their reach into emerging markets. Developers are exploring and exploiting the vast potential of Information and Communication Technologies for creating value in the field of sports events. Innovative companies are working on business areas to exploit the IoT and big data in the football industry. Examples of this include the German and Italian Football Associations, which have signed agreements with two companies, SAP AG (go.sap.com) and Beast Technologies (www.polihub.it/wp-content/uploads/2014/03/2014_02_26_DATAMANAGER_BEAST.pdf) respectively, to provide RFID technologies that can be used to improve the players' performance and help coaches make well-informed decisions on the basis of contextualised information and optimise training and tactics. The purpose of innovative companies in developing IoT tools for the football industry is to gain popularity and reach mass consumers, as well as increasing their market share within different business sectors.

Emerging technologies are actually allowed during training sessions. They are not during matches, where "a player may use equipment other than the basic equipment provided that its sole purpose is to protect him physically and it poses no danger to him or any other player. The use of electronic communication systems between players and/or technical staff is not permitted" (Players'

equipment, Law 4, FIFA, 2014). This statement provides a good explanation of why the football industry is not open to new technologies, such as the IoT. As asserted by Anderson and Sally (2013), "the beautiful game is steeped in tradition". International football bodies have clearly set strong restrictions to the use of the IoT during sports events. It is possible to argue that this prohibition is an expression both of cultural and economic resistance and of the scepticism that has washed over the regulations, delaying any innovation from being implemented. Such resistance towards the application of the IoT can be analysed according to the perspective of the player, club and industry.

Player level resistance

A number of interviews with professional football players and managers were analysed to understand the reasons behind the lack of trust in the use of RFID technology to collect performance and training data. The study of athletic-physical data is at the cutting edge of science applied to football. Professional football players can be monitored on a daily basis through the technological tools produced by innovative companies using IoT architecture as their operating field.

During an interview, a popular former Juventus defender, Lilian Thuram, expressed the common fear of footballers that there is "no longer the right to fail" (Sky sport interview, April 25, 2015). Clubs that use the IoT and big data are able to control every aspect of a player's condition and performance, hindering them from trying out any format or action not previously agreed with coaches during training sessions. In addition, other professional players have stated that data analysis and statistics can be used off the field, especially by journalists, but "footballers play by instinct" (Mauro Icardi, Sky Sport interview, April 25, 2015). In short, resistance in this perspective comes from uncertainty about the reliability of the data gathered (Razali and Vrontis, 2010) and the managers' ability to interpret the information, so that players do not become merely numbers.

Club-specific resistance

When considering whether to introduce an innovation to their business model, football clubs usually carry out an assessment of the costs and revenues associated to the change (Del Giudice *et al.*, 2013; Lombardi *et al.*, 2014; Maggioni and Del Giudice, 2011). In reality, clubs are not happy about investing in RFID technology because they are concerned that the data gathered will not be put to any useful purpose, be it because of the football institutions' lack of commitment or through technical inefficiency. For a club, investing in IoT technology generally involves employing analysts and specialists to collect and interpret the data, so these company resources are

counterbalanced by an increase in labour costs. Furthermore, clubs have no guarantee under law that the data collected are their own property (Sandy, 2014). It is possible to foresee a situation in which the subjects analysed want ownership of their data, forcing clubs to pay twice, first to implement the IoT technology and then to have access to the data.

Generally, football club boards look favourably at using the IoT and collecting big data. It is, instead, the managers who are less enthusiastic, because they are afraid of being replaced by technology (Sky Sport interview, April 25, 2015). In some cases, managers will agree to use data only to prove their beliefs scientifically.

Football industry resistance

Football institutions are interested in the appeal of competitive matches for sports viewers and supporters. According to the Csikszentmihalyi flow model (1990), the optimal experience is felt by those who are completely absorbed, in a state of automatic consciousness, "in the zone". Optimal experience is driven by the degree of challenge and of skill. Football bodies will try to delay any introduction of the IoT to competitive matches, as this may reduce the competitive imbalance on which optimal experiences are based. Football institutions believe that the IoT can adversely influence the relational component and the uncertainty component linked the supporters' experience. Generally, the greater the value of these two components, the greater the involvement of supporters and, as a consequence, the more it affects football federations' revenues and the relative decision-making processes. In addition, federations and clubs incur costs to introduce new technologies, and institutional bodies are generally very concerned about increasing the gap between large and small clubs and between major and minor leagues, seeing it as having a negative effect on both uncertainty and relational components.

Opponents of the technology present a range of issues that can alter the appeal of competition, arguing that these technologies take away the soul of game (Jerker and Svantesson, 2014). This is the reason why use of the IoT and big data are authorised during training sessions, but not during actual sports events.

Discussion

In this section, we discuss how IoT resistance in the professional football industry can influence different sectors. In order to demonstrate the risk of extensive opposition, the analysis was carried out on three levels.

Personal level of resistance to the IoT

High media coverage of football players, in general, results in greater relational capital value, since the players are seen to be role models, especially for young people. If the footballers are wary about the reliability of RFID technology and worried about being continuously examined without the possibility of failure, this perception can rub off on society in general. The main consequence concerns the lack of trust in terms of privacy, because individuals may become suspicious of data surveillance and the secondary use of gathered information.

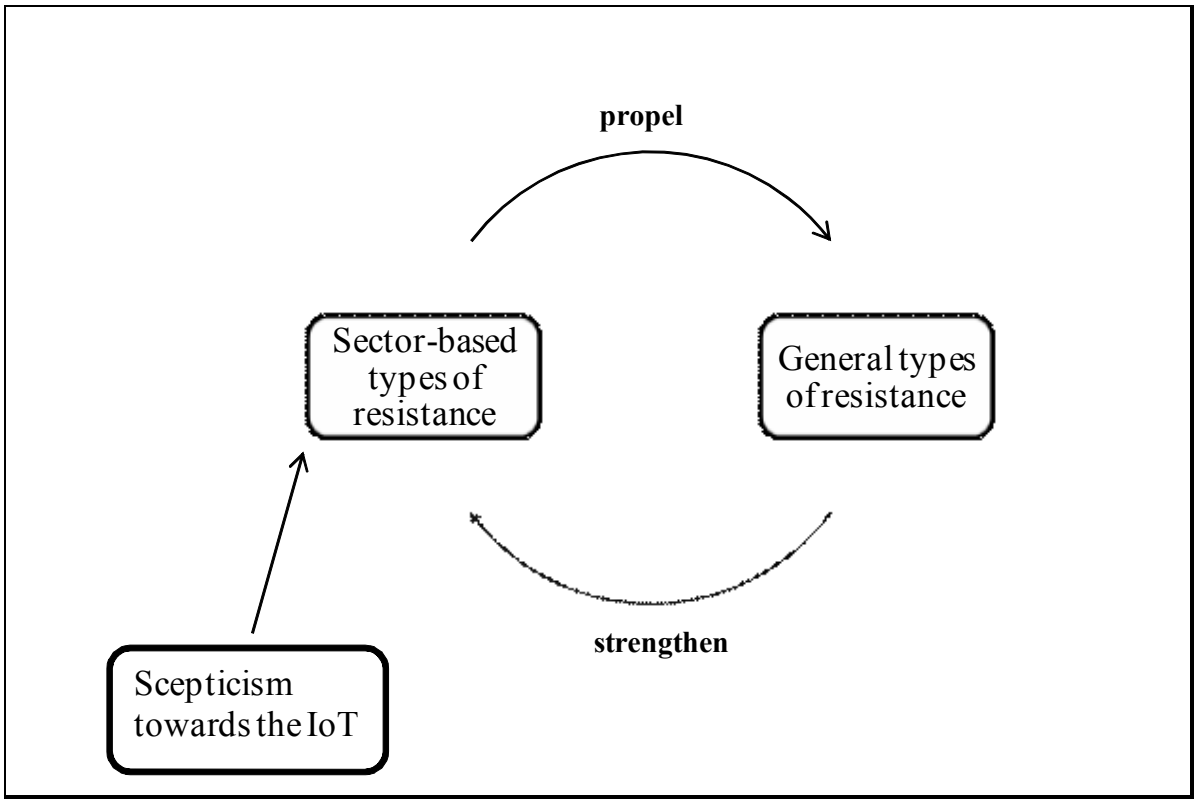
Company level of resistance to the IoT

Many industrial groups across the world invest in the football industry. Scepticism towards the IoT can, therefore, increase, since companies have no guarantee that it will make economic sense to invest in technology that can be ineffective or blocked by sector-based regulations. This uncertainty affects the process of analysing the potential costs and benefits that every company, including football clubs and indeed other companies in different industries, normally carries out before investing in new technology. The additional issue of legal ownership concerning gathered data is also relevant, and affects the company's ability to assess the costs linked to the use of RFID technology. A number of issues have to be settled in order to build these companies' trust, so that they will invest in the IoT vision, including future licensing agreements, the costs involved and to what level can the technologies be used.

Sectorial institutions' resistance to the IoT

In the football industry, the uncertainty relating to IoT governance is reflected in the reticence of introducing the IoT in certain activities. Self-regulation or sector-based rules may be relatively ineffective in regulating the IoT, but, today, they are the best tool available since it is impossible to identify international organisations that are sufficiently representative and so able to make decisions that affect all the parties involved.

Figure 3 – Risk of the epidemic impact of sector-based resistance to the Internet of Things



In light of the findings of this study (Figure 3), it is possible to assert that a combination of scepticism and lack of trust in the IoT vision, caused by cultural and economic resistance to innovation in the football industry, results in obstacles being erected by sectorial institutions. In turn, sector-based resistance can lead to an increase in generic obstacles hindering the acceptance of the IoT vision within every business sector, for companies, and in every-day life, for consumers. Through a chain-reaction, the general resistance emboldens the sectorial institutions, leading them to delay the adoption of IoT instruments, using the argument that cultural and economic issues must first be resolved.

The results of this exploratory research are a primary contribution to the field; in particular, the existence of the risk of an extensive opposition effect should be validated by other studies using statistical analyses on significant samples.

Conclusions

Many studies have been carried out by supranational institutions and researchers with the aim of identifying suitable strategies to introduce the IoT. These contributions focus on examining the technological issues and a number of legal arguments highlighted by the various opponents. This

paper involved investigating the reasons behind the general resistance to acknowledging the IoT vision. Through a case analysis of the football industry, the research has shown that, in every business sector, there are powerful economic forces at play that resist the change, because they are more interested in maintaining the *status quo*, according to a vision of path dependence.

The findings of this study indicate that institutional prohibition or delays in introducing an innovation are the result of economic and cultural resistance at a sector-based level. In particular, sector-based resistance in the football industry, with its high media exposure and revenue streams typical of this business, can engender a general scepticism towards IoT related technologies. The set of obstacles at player, club and industry level have led international football associations to define an anti-technology law. If the regulations are to be changed, economic agents must alter their stance and ditch their scepticism.

In order to exploit the enormous potential of the IoT, the vision, related technologies and policy instruments must all be aligned. With particular reference to the football industry, the diffusion of studies demonstrating that the IoT vision can improve the game and the attractiveness of competitive matches is a first step in increasing trust and reducing cultural and economic distrust. Once the potential and benefits of the IoT are understood, institutional bodies and laws can act together to overcome the obstacles hindering the introduction of the new technological architecture.

Regulation concerning football match procedures and guidelines must be put in place in order to avoid the risk of such widespread opposition, which can, in turn, affect different business sectors. In addition, this study makes several suggestions that can help the process of introducing the IoT to the football industry. To address resistance at sector level, spectators and teams must be informed that RFID devices are being used; to address resistance at club level, devices can be used only if both teams are using them and the less wealthy teams are given financial incentives to develop the technology, so that the competitive balance in matches is retained; to address the players' resistance, the data obtained through the IoT must be covered by confidentiality.

These suggestions originate from the assumption that actions are needed at sectorial level in order to avoid the risk of an extensive opposition effect. Supranational regulations regarding the introduction and governance of the IoT are most certainly important, but self-regulation of the sector should not be underestimated, because of the risk that the IoT may face widespread scepticism.

Future research can be carried out to extend the findings of the present study. This can involve analysing empirically the impact of major opposition, which is worrying for the professional football industry, and identifying which business sectors are most affected. In order to expand these initial proposals, it will be beneficial to carry out additional studies to produce further correlations

between the interconnected concepts and issues (Shams, 2013) connected to scepticism towards the IoT, sector-specific resistance, general resistance associated with the risk of widespread impact in terms of the adoption of the IoT. It would also be useful to analyse different markets and industries comparatively, in order to look at this initial framework from different socio-economic settings and considering different competitive forces. Furthermore, future research can be directed towards analysing the perceived risk level of the epidemic impact of surrounding the adoption of the IoT. If the assumptions concerning this epidemic risk are confirmed in future research, the practical implications contained in this paper will have to be taken into greater consideration.

As a result, studies on the perceived extent of the 'risk impact' will ensure that this initial insight will be extended to identify further emerging issues and to underpin the IoT governance.

References

Anderson, C. and Sally, D. (2013), *The numbers game: why everything you know about football is wrong*, Penguin, UK.

Atzori, L., Iera, A. and Morabito, G. (2010), "The Internet of Things: A survey", *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805.

Bandyopadhyay, D. and Sen, J. (2011), "Internet of things: Applications and challenges in technology and standardization", *Wireless Personal Communications*, Vol. 58, No. 1, pp 49-69.

Beech, J. and Chadwick, S. (Eds.) (2004), *The business of sport management*, Pearson Education, Harlow.

Buttarelli, G. (2010), "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners' Conference, Prague, Czech Republic, 29 April 2010.

Chandrakanth, S., Venkatesh, K., Mahesh, J. U. and Naganjaneyulu, K. V. (2014), "Internet of Things", *International journal of Innovation & Advancement in Computer Science*, Vol. 3, No. 8, pp. 16-20.

Charter of Fundamental Rights of the European Union (December, 2007), OJEC C 303, www.eur-lex.europa.eu.

Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "Internet of Things – an action plan for Europe", COM(2009) 278, p. 12.

Creswell, J.W. (2012), *Qualitative inquiry and research design: Choosing among five approaches*, Sage, Thousand Oak, CA.

Csikszentmihalyi, M. (1990), *Flow: the psychology of optimal experience,* Harper-Collins, New York.

Del Giudice, M. and Straub, D. (2011), "IT and entrepreneurism: an on-again, off-again love affair or a marriage?", *MIS Quarterly*, Vol. 35, No. 4, pp. 3-11.

Del Giudice, M., Della Peruta, M.R. and Maggioni, V. (2013), "Collective Knowledge and Organizational Routines within Academic Communities of Practice: an Empirical Research on Science-Entrepreneurs", *Journal of the Knowledge Economy,* Vol. 4, No. 3, pp. 260-278.

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L 281, 23 November 1995, pp. 31–50, www.eur-lex.europa.eu.

Dobson, T. and Todd, E. (2006), "Radio frequency identification technology", *Computer Law and Security Report*, Vol. 22, No. 4, pp. 313–315.

Dutton, W.H. (2014), "Putting things to work: social and policy challenges for the Internet of Things", *Info*, Vol. 16, No. 3, pp. 1-21.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of management review*, Vol. 14, No. 4, pp. 532-550.

European Commission (January 16, 2013), Report on the Consultation on IoT Governance.

European Parliament, Committee on Industry, Research and Energy, "Draft report on the Internet of Things", 24 February 2010, 2009/2224(INI), p. 9.

FIFA (2012), "IFAB approve two companies for next phase of GLT tests", FIFA Media Release, available at: www.fifa.com/aboutfifa/organisation/ifab/media/news/newsid¼1593294/index.html

FIFA (2014), "Laws of the Game 2013/2014", available at: http://www.fifa.com/mm/document/footballdevelopment/refereeing/81/42/36/log2013en_neutral.pdf.

Gerrard, B. (2000), "Media ownership of pro sports teams: Who are the winners and losers?", *International Journal of Sport Marketing and Sponsorship,* Vol. 2, No. 3, pp. 199-208.

Gibbons, L.J. (1996), "No regulation, government regulation, or self-regulation: social enforcement or social contracting for governance in cyberspace", *Cornell Journal Law and Public* Policy, No. 6, pp. 475-499.

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013), "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer* Systems, Vol. 29, No. 7, pp. 1645-1660.

Hair, Jr J.F., Celsi, M.W., Money, A.H., Samouel, P. and Page, M.J. (2003), *Essentials of Business Research Methods*, Wiley, New York.

Hamil, S. and Chadwick, S (Eds) (2010), *Managing Football: An International Perspective*, Butterworth-Heinemann, Oxford.

Hildner, L. (2006), "Defusing the threat of RFID: protecting consumer privacy through technology-specific legislation at the state level", *Harvard Civil Rights-Civil Liberties Law Review*, Vol. 41, Winter, pp. 133-176.

Hochleitner, C., Graf, C., Wolkerstorfer, P., and Tscheligi, M. (2012), *uTRUSTit–Usable Trust in the Internet of Things*, Springer, Berlin Heidelberg, pp. 220-221.

Jacobsson, K. (2004), "Soft regulation and the subtle transformation of states: the case of EU employment policy", *Journal of European Social Policy*, Vol. 14, No. 4, pp. 355-370.

Jerker, D. and Svantesson, B. (2014), "Could technology resurrect the dignity of the FIFA World Cup refereeing?". *Computer Law & Security Review,* Vol. 30, pp. 569-573.

A.T. Kearney (2011), "Sports market", available at: www.atkearney.com

Kellmereit, D. and Obodovski, D. (2013), *The Silent Intelligence: The Internet of Things*, DnD Ventures 1st edition, California.

Li, J.J. and Ma, N. (2013), "Discussing Variables Nature in Internet of Things Growth", *Applied Mechanics and Materials*, Vol. 409, pp. 1604-1607.

Lombardi, R., Trequattrini, R. and Battista, M. (2014), "Systematic errors in decision making processes: the case of the Italian Serie A football championships", *International Journal of Applied Decision Sciences*, Vol. 7, No. 3, pp. 239-254.

Maggioni, V. and Del Giudice, M. (2011), "Relazioni sistemiche tra imprenditorialità interna e gemmazione di impresa: una ricerca empirica sulla natura cognitive delle nuove imprese", *Sinergie rivista di studi e ricerche*, No. 71, pp. 171-197.

Malcolm, J. (2008), *Multi-stakeholder governance and the Internet Governance Forum*, Terminus Press.

Mayer, C.P. (2009), "Security and Privacy Challenges in the Internet of Things", *Electronic Communications of the EASST*, Vol. 17, pp. 12.

Mokyr, J. (1990), "Punctuated Equilibria and Technological Progress", *American Economic Review*, Vol.80, No. 2, pp. 350-354.

Mokyr, J. (2002), *The gifts of Athena: Historical origins of the knowledge economy*, Princeton University Press, Princeton, N.J.

Norris, P. (2001), *Digital divide: Civic engagement, information poverty, and the Internet worldwide*, Cambridge University Press, Cambridge.

Petrović, L.T., Milovanović, D. and Desbordes, M. (2015), "Emerging technologies and sports events: Innovative information and communication solutions", *Sport, Business and Management: An International Journal*, Vol. 5, No. 2, pp. 175-190.

Porter, M. (2014), "How Smart, Connected Products Are Transforming Competition", *Harvard Business Review*, November, pp. 4-23.

Pye, A. (2014), "The Internet of Things: connecting the unconnected", *Engineering & Technology*, Vol. 9, No. 11, pp. 64-70.

Razali, M.Z. and Vrontis, D. (2010), "The reactions of employees toward the implementation of human resources information systems (HRIS) as a planned change program: A case study in Malaysia", *Journal of Transnational Management*, Vol. 15, No. 3, pp. 229-245.

Reidenberg, J.R. (2000), "Resolving conflicting international data privacy rules in cyberspace", *Stanford Law Review*, Vol. 52, pp. 1315-1371.

Rifkin, J. (2014), *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons and the Eclipse of Capitalism,* Pelgrave MacMillan, New York.

Salvato, C., Chirico F. and Sharma, P. (2010), "A farewell to the business: Championing exit and continuity in entrepreneurial family firms", *Entrepreneurship and Regional Development*, Vol. 22, No. 3-4, pp. 321-348.

Sandy, A. (2014), "With big data comes big responsibilities", *Harvard Business Review*, November.

Schimmenti E., Galati A., Borsellino V. (2014), "The quality of websites and their impact on economic performance: the case of nurseries and gardening companies in the Italian "Mezzogiorno" Regions", International Journal Electronic Marketing and Retailing, Vol. 6, No. 1, pp. 72- 87.

Shams, S.M.R. (2013), "Stakeholder causal scope centric market positioning: Implications of relationship marketing indicators", in Kaufmann, H., and Panni, M.F.A.K. (eds.), *Customer Centric Marketing Strategies: Tools for Building Organizational Performance*, Business Science Reference, Hershey, PA, pp. 245-263.

Sšderman, S. and Dolles, H. (Eds.) (2013), *Handbook of research on sport and business*, Edward Elgar Publishing, Cheltenham.

Sundmaeker, H., Guillemin, P., Friess, P. and Woelfflé, S. (2010), *Vision and challenges for realising the Internet of Things*, Cluster of European Research Projects on the Internet of Things, European Commission.

Trubek, D.M. and Trubek, L. G. (2005), "Hard and Soft Law in the Construction of Social Europe: the Role of the Open Method of Co-ordination", *European Law Journal*, Vol. 11, No. 3, pp. 343-364.

Warren, S.D. and Brandeis, L.D. (1890), "The right to privacy", *Harvard law review*, Vol. 4, pp. 193-220.

Weber, R.H. (2009), "Internet of Things – Need for a new legal environment?", *Computer Law and Security Report*, Vol. 25, pp. 522–527.

Weber, R.H. and Weber, R. (2010), *Internet of Things*, Springer, New York.

Weber, R.H. (2010), "Internet of Things – New security and privacy challenges", *Computer Law and Security Report*, Vol. 26, pp. 26 et seq.

Weber, R.H. (2013), "Internet of Things – Governance quo vadis?", *Computer Law & Security Review*, Vol. 29, No. 4, pp. 341-347.

Wisbey, B., Montgomery, P.G., Pyne, D.B. and Rattray, B. (2010), "Quantifying movement demands of AFL football using GPS tracking", *Journal of science and Medicine in Sport*, Vol. 13, No. 5, pp. 531-536.

Yin, R.K. (2013), *Case Study Research: Design and Methods*, Sage, Thousand Oaks, California.

Biographies

Raffaele Trequattrini is a Professor of Business Administration in the Department of Economics and Law at the University of Cassino and Southern Lazio in Italy, where he was appointed vice-chancellor. He had his Ph.D. in Business Administration at the University of Urbino. He was associate professor of Business Administration. His research interests cover the following topics: corporate governance, accounting, corporate disclosure, decision making, crisis of firms, business network and management of intangible assets. He has published refereed articles across a wide range of topics. Infact, he's author of articles and monographs regarding accounting, corporate governance, corporate disclosure, business network and management of intangible assets. He is Editorial Board Member in Business System Laboratory.

Riad Shams is an Associate Fellow at the EuroMed Academy of Business, Cyprus. He has completed BBA, MBA and Professional Doctorate studies. Currently, he is pursuing his sponsored PhD at the University of Newcastle, Australia. His research focuses on entrepreneurship, value co-creation, international business, relationship marketing, corporate reputation, image and brand positioning. He has an emerging publication record, with papers in top-tier journals and conferences.

Alessandra Lardo is a Ph.D. student in Business Administration in the Department of Economics and Law at the University of Cassino and Southern Lazio (Italy). Her research interests cover the following topics: business management, knowledge management, intellectual capital and intellectual property rights, intellectual asset management, corporate social responsibility, international accounting, social media, evaluation of firms and business network. She's author of

articles and chapters of books regarding intellectual capital, evaluation and disclosure of intangible assets.

Rosa Lombardi is Assistant Professor of Business Administration at Link Campus University in Rome (Italy). She is eligible as Associate Professor under Italian National Qualification. She is adjunct professor of International Accounting in the Department of Economics and Law at the University of Cassino and Southern Lazio in Italy. She had her Ph.D. in Business Administration at the University of Cassino and Southern Lazio (Department of Economics and Law) and she has been post doc research fellow in Business Administration. She serves in the Editorial Board and Guest Editor of many international peer reviewed academic journals. Her research interests cover the following topics: corporate governance, corporate disclosure, intellectual capital and management of intangible assets, decision making, international accounting, evaluation firm and business network. She has more than 60 publications (books, articles, proceedings, etc.) regarding corporate governance, corporate disclosure, intellectual capital, business network and management of intangible assets. She is Chair of the Research Committee on "Intellectual Capital" and Associate EMAB Fellow at the EuroMed Research Business Institute. She is Editorial Board Member in Business System Laboratory.