International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:6, 2015

Creation of a Care Robot Impact Assessment

E. Fosch-Villaronga

***Abstract*—**This paper pioneers Care Robot Impact Assessment (CRIA), a methodology used to identify, analyze, mitigate and eliminate the risks posed by the insertion of non-medical personal care robots (PCR) in medical care facilities. Its precedent instruments [Privacy and Surveillance Impact Assessment (PIA and SIA)] fall behind in coping with robots. Indeed, personal care robots change dramatically how care is delivered. The paper presents a specific risk-sector methodology, identifies which robots are under its scope and presents some of the challenges introduced by these robots.

***Keywords*—**Ethics, Impact Assessment, Law, Personal Care Robots.

I. Introduction

THE increasing demand of medical care is promoting the fast development of new robot technology. In fact, Healthcare Service Robots seem to represent an upcoming efficient response to the rising cost of Healthcare Institutions. Nonetheless, the functionalities of these autonomous robots in this field will lead us to different and unforeseeable scenarios that are worth further analysis, especially in the legal and ethical domain [1].

Up to now, only the International Standard Organization (ISO) has addressed this phenomenon when introducing ISO 13482:2014 about 'Robots and Robotics Devices – Safety Requirements for Personal Care Robots'. Yet, this standard only concerns harm-related and technological-based requirements, whereas other important legal or ethical questions are not taken into account, - such the unauthorized surveillance, the misuse of the collected data, the free will of patients, the impact of the employment of robot technology (e.g. the loss of jobs if any), etc.

Whether technology should be formally regulated is still an ongoing debate [2]-[5]. In fact, there are many ways to think about "regulation" [6]. The pathetic-dot theory of Lessig, for instance, reveals that there are four constraints that normally regulate a person in any domain (in the theory, a pathetic dot): the law, the social norms, the market and the architecture. Consequently, this is also true for technology: the existing social norms (if not legal norms), the market and the architecture of technology, already regulate it. Law is a horror vacui discipline anyway, and an inherent part of the 'complete-view' of the Lessig's concept of 'regulation'; of course technology is regulated by the Law; it is just that sometimes technology occurs before the law-making process [7]. And this is the case for Non-Medical Personal Care Robots: they are not regulated in any legal system yet, but they are already governed by their architecture (ISO), the market and social norms (in fact, they are already used in medical care institutions) [8].

This does not mean there is no need to legally regulate robots. In reality, 'a lack of legal clarity leaves device-makers, doctors, patients and insurers in the dark' [9]. Indeed, even if the complexity of the system (due to the intricate nature of each side of the pathetic-dot theory and the labyrinthian interaction among them), makes science/technology no longer just a motivation for the regulation, but a regulatory actor and a regulatory tool (due to legal compliance in risk assessments), there is still the need for a legal framework that can go along with the technology development [6], [10]. Actually, many of the arisen questions, due to their nature, can only be answered from the legal and ethical perspective (see infra).

There are certainly different ways to fill this gap within the legal and regulatory area [11]. Sometimes the existing legal framework is already able to give solutions to the upcoming challenges; sometimes the Law needs to be changed either, directly or indirectly; sometimes hybrid codes can be the best solution, or sometimes pieces of legislation inside technologies (like all the –by Design principles) are enough, [6], [10], [12]. Among all the possibilities, for assessing the impact of personal care robots on society we will on the recently used Impact Assessment (IA) methodology [13], [14].

Using a bottom-up risk-based approach, where the bottom stands for 'risk' and the up stands for 'framework', we will be able to deal with all the unanswered multidisciplinary questions that the Privacy and Surveillance Impact Assessment (PIA and SIA) cannot fully answer. Indeed, robots not only process sensitive data and have the ability to surveil part of the society, but have other features worth analyzing (see infra).

Of note, as of March 2015, the expression "Care Robot Impact Assessment" did not show up on the Internet; and only a 'Health Technology Assessment' could be found on Google, but that was just a report for robot-assisted surgery [15]. Thus, because of the lack of a legal/ethical framework, the different scope of PIA/SIA and for the novelty of the issue, it is necessary to develop a Care Robot Impact Assessment (CRIA) that takes into account all the questions and repercussions that robots pose to society.

E. Fosch-Villaronga is with the Joint International Doctoral (Ph.D.) Degree in Law, Science and Technology coordinated by Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica (CIRSFID), on leave from the Università di Bologna, 40121 Italy. His supervisor thesis is Antoni Roig Batalla from IDT-UAB, Universitat Autònoma de Barcelona, Spain (e-mail: eduard.fosch@unibo.it).

II. Impact Assessment Methodology: Similarities/Differences between PIA/SIA and CRIA

CRIA is based on the general risk management ISO 31000:2009 'Risk Management – Principles and Guidelines'. Accordingly, 'all activities of an organization involve risk' and 'Organizations manage risk by identifying it, analyzing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria' [16]. However, ISO 31000 is just a general risk framework that only gives some principles, establishes the main framework and provides a general overview of the risk management process [17]. That is why other concrete specific aspects have been dealt with separately, in other bodies like PIA, SIA, and the Environmental Impact Assessment (EIA). According to Cavoukian 'like other operational risks, those related to the protection of personal information benefit from the scrutiny of a formal risk management discipline' and affirms that 'Personal Information is an asset, the value of which is protected and enhanced by a suite of security practices and business processes' [16]. Likewise, inserting a robot in healthcare facilities poses multifaceted risks that could be mitigated by several actors (legislator, creator of the robot, the medical care institution, etc.) using a specific CRIA.

To date, PIA and SIA are the only existing instruments that can deal with robotics: robots process a huge amount of data and they are capable of directly or indirectly surveil patients, disabled people, third parties or medical care facilities. There is great variety of methodologies in this regard though. Here, we will refer to the PIA process in art. 33 of the future General Data Protection Regulation, used already for the Smart Grid Task Force [18]. We will make the comparisons following the studies of Wright et al. and the opinions of the Article 29 Working Party (A29WP) as well as the Commission Nationale de l'Informatique et des Libertés (CNIL).

A. Similarities

The structure of CRIA basically follows the risk management process established by ISO. The process is monitored and consulted all the time; the Impact Assessment will be based on:

1) Establishing the context
2) Risk Identification
3) Risk Analysis
4) Risk Evaluation
5) Risk Treatment

Wright and Raab add some steps in this procedure, and so does the Smart Grid Task Force [19]. But determining whether the impact assessment is necessary, identifying the team that will deal with it, preparing a plan, determining the budget for it and identifying the stakeholders, seem to be part of the general establishment of the context or of the same undertaking/institution's organization when deciding whether to carry out or not the impact assessment.

B. Differences

Specific-sector impact assessments differ in their scope, not in their structure. PIA for instance basically deals with the privacy impacts that a given technology will pose to the subjects [18], [31]. According to the CNIL, 'in the area of privacy, the only risks to consider are those that processing of personal data pose to privacy' [20]. On the other hand, SIA as a wider instrument is principally concerned with other impacts (not only privacy, but also economic, financial or psychological impacts), and focuses on groups and not individuals as PIA does [19].

To this regard, CRIA deals with all the impacts of any nature that a given care robot (more precisely, a non-Medical Personal Care Robot) can pose to the general community. We are not referring only to the huge amount of sensitive data that are being processed by the robot in cloud platforms (which could be addressed by PIA) or to the monitoring functions they might have (SIA); but also to the unanswered legal aspects concerning liability, free will of patients, or autonomy issues (see infra), ethical aspects like the fear of ICT, the use of robots by dement patients, the human emotions' projection to the machines or the morality of robotic servants [21].

III. Types of Care Robots

When we talk about "Care Robots" we basically refer to Personal Care Robots. Personal Care Robots can be classified depending on their functionalities, their Human Robot Interaction (HRI) or their use. [22]. Here, we refer personal care robots as service robots 'that perform(s) actions contributing directly towards improvement in the quality of life of humans, excluding medical applications' [23], [24].

A. Robots Out of the Scope: non-Personal Care Robots

After specifying that ISO 13482:2014 only applies to earthbound robots, it states that it is not applicable to:

- Robots travelling faster than 20 km/h;
- Robot toys;
- Water-borne robots and flying robots;
- Industrial robots, which are covered in ISO 10218;
- Robots as medical devices; nor
- Military or public force application robots.

B. Robots within the Scope: Personal Care Robots

ISO 13482:2014 identifies then three kinds of personal care robots that, given their functionalities, can improve the quality of life of humans: (1) mobile servant robot (2) physical assistant robot and (3) person carrier robot. Their respective definition is:

- 'Personal care robot that is capable of travelling to perform serving tasks in interaction with humans, such as handling objects or exchanging information'
- 'Personal care robot that physically assists a user to perform required tasks by providing supplementation or augmentation of personal capabilities'. ISO identifies two sub-types of Physical Assistant Robot, a restraint type (that is fastened to a human during use) and a restraint-free type (that is not fastened to a human during use).
- 'Personal care robot with the purpose of transporting humans to an intended destination'. ISO adds other

objects like pets and property to be transported by personal care robot.

C. Other 'Personal Care Robots': Confusion

Sometimes, this in-scope/out-scope classification may picture a restricted vision of the reality. Actually, reality always goes beyond strict boundaries and classifications (see Table I). Therefore, it is important to draw special attention to what kind of robot is being inserted in the medical care institution independently of the classification we want to use. That way the exact features, HRI and the usage that this will have within the institution will be the base for the impact assessment.

TABLE I
ISO 13482:2014 CONFUSING CATEGORIES

Robot	Environment	Confusion
Exoskeleton	Military	Military robots
Exoskeleton	Rehabilitation	Medical devices
Toy Car	Person Carrier Robot	Robot-toy
Seal Robot Toy (NUKA)	Rehabilitation	Personal Care Robot
Resyone (Bed/Wheelchair)	Mobile Servant Robot	Restraint-free Physical Assistant Robot
Automated Guided Vehicles (AGV)	Mobile Servant Robot	Person Carrier Robot
Drone	Surveillance/Security in Hospitals or Dwellings	Personal Care robot
Docent Robot	Education in Healthcare (children, patients)	Personal Care Robot
Mobile Service Robot	Home and non-care facilities	Personal Care Robot

The usage of a robot cannot determine the regulation under which it falls. On the contrary, clearer regulatory definitions embracing real cases are needed to better define and give response to some categories.

IV. DEVISING A CARE ROBOT IMPACT ASSESSMENT

The basis for the construction of a CRIA is identifying the robot that will be inserted in the Healthcare institution. Depending on the type and its sub-class, impacts on subjects will vary substantially. The kind of institution is also highly important since a nursing home, a hospital or the patient's private dwelling is not the same. To this regard, the extension of the robot usage to private homes will also be significant.

A29WP established in an opinion regarding the Data Protection Impact Assessment (DPIA) Template prepared by the Smart Grid Task Force that 'DPIA should clearly identify actors and their responsibilities, focus on data protection and privacy risks to the individuals concerned, better guide the actors to match each risk with adequate controls, and offer more specific and practical guidance on how to address data protection and privacy risks in the smart grid context'. Similarly, this specific-sector impact assessment should include a specific structure that could plainly:

- Identify all the stakeholders: roles and the linked responsibilities;
- Distinguish the category and sub-category of robot and its specific features;
- Define all the risks: real impact on subjects featuring legal, ethical and technological aspects;
- Discern what is the likelihood of occurrence
- Identify all the controls and countermeasures: one risk, one control.
- Implement them: monitoring and consultation

If we combine all these factors, and we integrate them as an essential part of the company/institution's management process, a CRIA will help us to have a clearer picture of what the insertion of a non-medical personal care robot in medical care institutions will be like and it will also address real risks with updated and multifaceted solutions through legal-ethical-social instruments [25].

A. Presenting CRIA Model

Fig. 1 presents the CRIA model. It follows the same approach used by ISO for risk management (also followed and supported by Ann Cavoukian, Smart Grid Task Force, CNIL, the proposal for a General Data Protection Regulation and A29WP in privacy contexts). The circles remind us of the life cycle of the process. Indeed, dynamism and constancy are inherent to this procedure. Names are expressly short in order to avoid unnecessary complicated nomenclatures. Moreover the circles are precisely allocated in the model:

a) The small circles should be read clockwise; the first one refers to establishing the context, and the last one to the treatment of the risk (remedies and measures) through the identification of the precise robot in context, its risks (of any nature), and the analysis of them.
b) The big circle encompasses the other small ones because consultation and monitoring are a necessary step of the whole procedure.

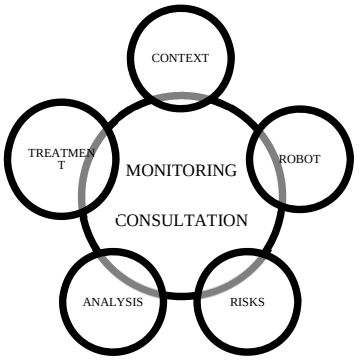

Fig. 1 CRIA Model: Care Robot Risk Management Process

B. CRIA in Detail

1. Establishing the Context

It is essential to take into consideration both the internal and the external contexts, which can affect the non-medical care robot. Regarding the internal context, the institution needs to consider: its own structure, the main objectives, roles, decision-making processes, division of responsibilities, and right timing for conducting the assessment. In the external context, the expectations of external stakeholders (patients, third-parties, companies), legal issues, and contracts with other undertakings should be considered. Moreover, it will be important also to carefully take into account the purpose of the CRIA, the team that will carry it out, and the resources to

handle it.

2. Types of Robots

Depending on the type of robot that will be inserted in the institution, risks will vary substantially. Inserting a robotic wheelchair, with all the related person-carrier-robot risks is not the same as inserting a physical assistant robot (a wearable restraint type robot). Moreover, within the person-carrier-robot category, for instance, it is not the same a wheelchair, a segway or a bed that turns into a wheelchair (for instance Panasonic's Resyone robot that has been the first to obtain ISO 13482:2014 and has been categorized as mobile servant robot) are all very different.

With CRIA, it will be easier to group risks and solutions for each kind of non-medical personal care robot. In this regard, the characteristics of the robot should be identified (hardware, software, network of transmission), the level of human-robot interaction should be defined (patients, other people, children, pregnant women, etc.), as well as what level of autonomy this robot have, who is in charge of it (the hospital, or the patient who purchased it and used it in the same facilities, etc.) and the extension of the use of the robot (if later on the robot is used in the dwelling of the patient but it stills communicates with the hospital, for instance).

3. Risk Identification

Identifying and classifying threats and risks are extremely important, and the impact assessment cannot confuse these two crucial aspects [28]. A threat refers 'to the ability to exploit vulnerabilities on the assets to be protected'. Vulnerability is a weakness that can be exploited by threats. And a risk is understood as 'the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization' [26]. This identification process can be held when carrying out a CRIA, because of the external/internal audits or because the institution has developed 'a culture of privacy' [16].

4. Risk Analysis

Threats need to be categorized based on their nature: technological, legal, ethical, sociological, etc. Subsequently, these threats need to be weighed against the likelihood of occurrence and the severity of their impact (consequences) [20]. Risks should be included in a priority-list and grouped into similar categories. If grouped and prioritized, the institution can easily solve them (because one protective measure can resolve several issues).

5. Risk Treatment

After having identified and analyzed the risks, the institution needs to know how to address them by using 'Best Available Techniques (BATs) [29]. Although this may seem obvious, this should be done before the risk occurrence [30]. There are several strategies to mitigate the risks: risk avoidance (creating a separate infrastructure for the robots), risk reduction (including bumpers of security, laser protectors, etc.), risk transfer (hiring insurance companies) or even risk retention (acceptance of the risk without further action). According to different criteria (normally related to efficiency and effectiveness), the institution will choose whatever is more convenient.

The most important thing anyway is to have an appropriate control to each identified risk considering its likelihood and impact. Sometimes one control will mitigate multiple risks. It does not matter if technological controls also address and affect legal risks, as this intertwinement will ensure complete compliance. Moreover, it is necessary to accept the residual risk after implementing those controls [27]. To deal with and mitigate residual risks, some safeguards and complementary protective measures can be envisaged.

6. Monitoring and Consultation

Monitoring is critical to check the success of the used controls. Risks are continuously evolving; therefore, monitoring the institution and the robots that are used inside it is fundamental to achieve efficient, and effective desired results. Monitoring can be used as a way of transparency towards the stakeholders and to get the confidence and trust of users.

ISO 31000 defines consultation and communication as 'continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk'. Within the multidisciplinary context that the insertion of non-medical care robots offers, the institution needs to establish a good communication with the staff, and the board, and needs to give feedback in case of any consultation by the stakeholders.

V. Challenges To Be Answered

With CRIA and its embedded compliance system, we should be able to answer some important questions yet unresolved due to the lack of legal regulation (here it is a numerus apertus list):

- Where is the robot processed data going and how are users' sensitive data protected [21]?
- What are the basic liability issues involving robots and how can judges deal with them when an autonomous robot misbehaves? Are robots liable for their behavior when reacting autonomously to environmental stimuli?
- What should a person do when a robot hits her/him?
- Should the robot be protected in a privileged way due to the amount of data it possesses?
- What rules do apply when replacing human-labor force by robots?
- What environmental regulation is addressing the mass use of these robots?
- What final say have the elderly who should use these robots? What protocols are used to take into account the patients' will?
- What decisions are being delegated to the robots and what consequences may this have?
- Can robots provoke feeling of presence and can this cause harm [32]? How could this be mitigated?

VI. Conclusion

By addressing all the above aspects, we will be able to create a general framework that could embrace this reality and go along the evolution of technology. This general framework could first be useful to give concrete response to many unanswered questions worth analyzing in the near future (see below); second, and most importantly, it will help the general community to better understand the main goals of robot technology and to trust them. The following crucial questions will finally be answered:

- Is the care shifting from a personalized to a depersonalized status, or are both conditions maintained at the same time?
- Are robots delivering a good care?
- To what extent physical assistant robots can improve human's abilities?
- Is human dignity properly considered and safeguarded?
- Which are the activities that humans can (or should) delegate to machines?
- What happens when a machine enhances a patient's sanity?
- Can robots cause patient's distrust and denial to access medical care?

References

[1] K. Rommetveit, "Impact Assessments: Quality Issues in the Policy Making Process," unpublished.
[2] J. B. Wiener, "The Regulation of Technology, and the Technology of Regulation," *Technology in Society* vol. 26, 2004, pp. 483-500.
[3] M. A. Heldeweg and E. Kica, *Regulating Technology Innovation. A Multidisciplinary Approach*, Palgrave MacMillan, 2011.
[4] R. Brownsword and K. Yeung, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, 2008.
[5] J. P., Holdren, C. R. Sunstein, I. A. Siddiqui, "Principles for Regulation and Oversight of Emerging Technologies", White House Government Communication, 2011.
[6] L. Lessig, *Code version 2.0*. Basic Books, NY, 2006.
[7] EC Research, "Taking European Knowledge Society Seriously," Report, Expert Group on Science and Governance to the Science, Economy, and Society Directorate of the Directorate-General for Research, 2007.
[8] AGV were introduced to Hospital Universitario Central de Asturias (HUCA) in Spain. The also called *manolitos* carry food and medicines from the kitchen or pharmacy to the rooms. Vid.: http://www.rtpa.es/asturias:Una-flota-de-12-robots-repartiran-comida,-ropa-y-medicinas-en-el-HUCA_111402140212.html.
[9] Anonymous, "You, Robot?" The Economist, September 2012.
[10] E. Palmerini, "The interplay between law and technology, or the RoboLaw project in context," in *Law and Technology. The Challenge of Regulating Technological Development*, E. Palmerini and E. Stradella Ed. Pisa: Pisa University Press, 2013, pp. 7-26.
[11] J. B. Wiener, "Global Environmental Regulation: Instrument Choice in Legal Context," *Yale Law Journal*, Vol. 108, 1999, pp. 677-800.
[12] M. O. Vrielink, C. Montfort, M. Bokhorst, "Codes as Hybrid Regulation," in *Handbook on the Politics of Regulation*, D. Levi-Faur, Ed. Cheltenham, Edward Elgar Publishing, 2011, pp. 978-1005.
[13] European Commission SEC (2009) 92 Impact Assessment Guidelines, 2009.
[14] D. Wright and K. Wadhwa, "Introducing a Privacy Impact Assessment Policy in the EU Member States," *International Data Privacy Law*, Vol. 3. Num. 1, 2013, pp. 13-28.
[15] HIQA, "Health Technology Assessment for Robot-Assisted Surgery in Selected Surgery Procedures," Health Information and Quality Authority, Dublin, 2012.
[16] Information and Privacy Commissioner, "Privacy Risk Management: Building a Privacy Protection into a Risk Management Framework to Ensure that Privacy Risks Are Managed, *by Default*," Ontario, Canada, 2010.
[17] ISO 31000:2009, Risk Management – Principles and Guidelines.
[18] SGTF "Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment. Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems," Smart Grid Task Force 2012-14, Expert Group 2, 2014.
[19] D. Wright and C. D. Raab, "Constructing a Surveillance Impact Assessment," *Computer Law and Security Review* vol. 28, 2012, pp. 613-626.
[20] CNIL, "Methodology for Privacy Risk Management. How to Implement the Data Protection Act," Commission Nationale de l'Informatique et des Libertés, CNIL, 2012.
[21] NIST, "Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations," National Institute of Standards and Technology, NIST, 2012.
[22] D.Y.Y. Sim and C.K. Loo, "Extensive Assessment and Evaluation Methodologies on Assistive Social Robots for Modeling Human-Robot-Interaction – A Review," *Information Science* vol. 301, 2015, pp. 305-344.
[23] ISO 8373:2012 "Robots and Robotic Devices Vocabulary", 2.10.
[24] ISO 13482:2014 "Robots and Robotics Devices – Safety Requirements for Personal Care Robots", 3.13.
[25] COSO, "Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission", 2011.
[26] ISO/IEC 27005:2008/:2011 Information Technology – Security Techniques – Information Security Risk Management.
[27] ISO/IEC 27001:2005 Information Technology. Security Techniques. Information Security Management System Implementation Guidance.
[28] 00678/13/EN, WP205, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, Article 29 Working Party, 2013.
[29] EC Recommendation 2012/148/EU on the preparation for the roll out of smart metering systems.
[30] Expert Group on the State of the Art in Responsible Research and Innovation in Europe, "Options for Strengthening Responsible Research and Innovation," Report, Brussels, 2013, p. 13.
[31] ISO 27005:2011, "Information Technology – Security Techniques – Information Security Risk Management".
[32] O. Blanke, et al. "Neurological and Robot-Controlled Induction of an Apparition," *Current Biology*, vol. 24 Issue 22, 2014, pp. 2681-2686.