Human rights implications of autonomous weapon systems in domestic law enforcement: sci-fi reflections on a lo-fi reality

Andrea Spagnolo *

1. *Autonomous Weapon Systems (AWS) and human rights: An introduction to the debate*

Novelists and filmmakers have been speculating on the interaction between human beings and robots for years. Isaac Asimov, in particular, devoted an important part of his bibliography to the issue. He created a world where robots are integrated in our society and regulated by the famous three laws of robotics: '1) A robot may not injure a human being or, through inaction, allow a human being to come to harm; 2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law; 3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.'[1]

Witnessing that the scenario depicted by Asimov is becoming a reality is a strange feeling. It is even more strange to notice that the three laws he elaborated in his novels sound tremendously topical[2] in the present-day debate on the legal and ethical issues raised by the use of autonomous weapon systems (AWS). A debate[3] that is for its largest part focused on

* Research Fellow in International Law, Department of Law, University of Turin; Adjunct Professor of International Law, University of Piemonte Orientale.

[1] I Asimov, *I, Robot* (Gnome Press 1950) 40.

[2] Far from being a whimsy reference, Asimov was quoted by Angela Kane, United Nations High Representative for Disarmament Affairs: 'we should all keep in mind "The Three Laws of Robotics" put forward by Isaac Asimov back in 1942'. A Kane, 'Killer Robots and the Rule of Law', A view from the United Nations, available at <www.huffingtonpost.com/A-View-from-the-United-Nations-/killer-robots-and-the-rul_b_3599657.html>.

[3] See *ex multis* P Alston, 'Lethal Robotic Technologies: The Implications for Human Rights and International Humanitarian Law' (2012) 21 J Law, Information and Science

the use of AWS during the course of an armed conflict as this is the field in which the technological evolution is the most sensitive and already being applied.[4]

The (potential) use of AWS in the context of armed conflict has attracted not only the attention of scholars and practitioners but also that of institutions and civil society networks and organizations, in particular non-governmental organizations (NGOs).

A discussion on AWS was held at the Fifth Review Conference of the Member States of the United Nations (UN) Convention on Conventional Weapons (CCW). As an outcome of that Conference, an open-ended Group of Governmental Experts was established with the aim of discussing legal issues related to the use of AWS which an informal meeting of experts had already identified in 2016.[5] Such legal issues range from the compatibility of the use of AWS with international humanitarian law (IHL) and international human rights law (IHRL) and all related compliance issues, to more ethical and moral ones.[6] Although the meeting itself was cancelled due to insufficient State funding,[7] the topic will remain on the agenda, if only because NGOs continue to push toward this end.

35; M Wagner, 'Taking Humans Out of the Loop: Implications for International Humanitarian Law' (2012) 9 J Law, Information and Science 155; Id., 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 Vanderbilt J Transnational L 1371; MN Schmitt, JS Thurner, '"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict' (2013) 1 Harvard National Security J 231; WH Boothby, 'Autonomous Attack – Opportunity or Spectre?' (2013) YB Intl Humanitarian L 71; Id., *Weapons and the Law of Armed Conflict* (2nd ed, OUP 2016) 247 ff and 252 ff.

[4] R McLaughlin, H Nasu, 'Introduction: Conundrum of New Technologies in the Law of Armed Conflict', in R McLaughlin, H Nasu (eds), *New Technologies and the Law of Armed Conflict* (TMC Asser Press 2014) 1, 2.

[5] Final document of the Fifth Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (12-16 December 2016) CCW/CONF.V/10, Decision 1.

[6] ibid 9.

[7] Letter of the Chairperson of the 2017 Meeting of the High Contracting Parties to the Convention, Ambassador Matthew Rowland of the United Kingdom of Great Britain and Northern Ireland (dated 6 June 2017), on behalf of all the CCW officeholders concerning the announcement of the cancellation of meetings, available at <www.unog.ch/80256EDD006B8954/(httpAssets)/3D20EDEBBF0E6B68C125813A00566285/$file/Letter_CCW+MSP+Chairperson_6Jun2017.pdf>; see also R Crootof, F Renz, 'An Opportunity to Change the Conversation on Autonomous Weapon Systems' Lawfare (15 June 2017) <www.lawfareblog.com/opportunity-change-conversation-autonomous-weapon-systems>.

Indeed, in 2013 a campaign named 'Stop Killer Robots'[8] was launched by a group of NGOs headed by Human Rights Watch (HRW), which had the merit of introducing the debate by publishing a report jointly with the Harvard Law School's International Human Rights Clinic.[9] The campaign is focused on achieving a complete ban on the use of AWS or, at least, the introduction of a requirement for meaningful human control over such weapons. Recently, in August 2017,[10] Elon Musk, the founder of Tesla, and the famous Stephen Hawking joined a group of experts working in artificial intelligence (AI) in advocating a complete ban through an open letter addressed to the United Nations.[11] They warned that AWS 'will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways.'[12]

Scholars and experts, however, are not unanimous in calling for a ban on AWS.

It is true that some of them opine that a preemptive ban is the only way of addressing the legal and ethical problems that the use of AWS might raise. As seen before, this is the position maintained by proponents of the campaign 'Stop Killer Robots'; it is also supported by a variety of scholars.[13] The key points of this position are grounded on both ethical and legal reasons. It suffices here to say that AWS are deemed to be unfit to cope with the extreme variety of situations that might arise in the course of an armed conflict and, in particular, they would not be able to

[8] For more information see the website <www.stopkillerrobots.org>.

[9] Human Rights Watch (HRW), Harvard Law School's International Human Rights Clinic (IHRC), 'Losing Humanity. The Case Against Killer Robots' (19 November 2012) <www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf>.

[10] See S Gibbs, 'Elon Musk leads 116 experts calling for outright ban of killer robots', The Guardian (20 August 2017) available at <www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>.

[11] Future of Life Institute, 'An Open Letter to the United Nations Convention on Certain Conventional Weapons' (21 August 2017) The text of the open letter is available here: <https://futureoflife.org/autonomous-weapons-open-letter-2017>.

[12] ibid.

[13] For a review of the pro-ban scholarly arguments see the paper by D Amoroso, published in this Zoom-in. See also D Amoroso, G Tamburrini, 'The ethical and legal case against autonomy in weapon systems' (2017) Global Jurist 1 ff.

comply with the principle of humanity, a cornerstone of IHL. Moreover, in complex scenarios, conduct performed by AWS could hardly be compatible with the principle of proportionality, which requires a careful assessment that could not be foreseen by an algorithm.[14] Moreover, and from the perspective of *jus ad bellum*, it is also said that the use of AWS would inevitably lead States to increase their resort to military action, as this would be at no cost in terms of human casualties.[15]

According to a second opinion, calling on a ban on AWS is somehow unrealistic. Some scholars and practitioners, in fact, maintain that, as AWS are here to stay, the best way to limit the potential negative impact of these weapons is to push for international regulation.[16] Such an idea rests on the assumption that it is not reasonable to argue that technological evolution would never put at the disposal of States' Armies AWS which are equipped to respect the principle of distinction.[17] Some scholars are even more radical as they contend that it is wrong to argue that humans are better than machines in conducting hostilities.[18] Others maintain that a ban is dangerous as it would impede the evolution of a new normative framework, given that the existing one is unfit to cope with legal problems arising from the use of AWS.[19]

The debate I have tried to summarize so far is mainly shaped on the compatibility of AWS and/or the use of AWS with IHL and is deeply

[14] See accordingly M Sassoli, 'Can Autonomous Weapon Systems Respect the Principles of Distinction, Proportionality and Precaution?', in ICRC, 'Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting, Geneva, Switzerland, 26-28 March 2014' available at <www.icrc.org/en/download/file/1707/4221-002-autonomous-weapons-systems-full-report.pdf> 41 ff, 42-43.

[15] See again the arguments put forward by Daniele Amoroso.

[16] See for example K Anderson, MC Waxman, 'Debating Autonomous Weapon Systems, Their Ethics, and Their Regulation Under International Law', in R Brownsword, E Scotford, K Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 1097 ff.

[17] See for example M Sassoli (n 14) 41, who maintains that the real problem lies with the respect of the principles of proportionality and precaution, but the possibility cannot be excluded that AWS will respect the principle of distinction. Accordingly see R Crotoff, 'The Killer Robots Are Here: Legal and Policy Implications' (2015) 36 Cardozo L Rev 1837.

[18] See accordingly MN Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) 1 Harvard National Security J 1 ff. See also and again K Anderson, MC Waxman (n 16) 1114.

[19] See R Crotoff, 'Autonomous Weapon Systems and the Limits of Analogy', in C Finkelstein, D MacIntosh, JD Ohlin (eds), *The Ethics of Autonomous Weapon Systems*, 2017 (forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820727>.

explored by Daniele Amoroso in his piece to this Zoom-in. The compatibility with IHRL, on the contrary, is nowadays largely unexplored. One can easily count an article[20] written by Christopher Heyns, former United Nations Special Rapporteur on extrajudicial, summary or arbitrary executions, who deserves the credit of bringing the topic to the attention of the Human Rights Council in his 2013 Annual Report.[21] The present Special Rapporteur, Agnes Callamard, dealt with the use of AWS in her 2016 Report to the General Assembly, although she did not directly touch on the compatibility of these weapons with IHRL.[22] HRW, on the contrary, published a report on this peculiar issue in 2014[23] and the European Parliament commissioned a study that was authored and published by Nils Melzer, a section of which is dedicated to the compatibility of AWS with IHRL.[24]

The reason for the scarcity of scholarly works and research papers on the compatibility of AWS with IHRL is probably to be found in an apparent lack of practice in the use of AWS outside the context of an armed conflict. Moreover, it must be said that, contrary to IHL, IHRL does not contain specific limitations on the use of weapons.[25]

States are nonetheless limited in choosing means and methods for law enforcement activities by the standards flowing from the rules enshrined in human rights treaties and elaborated upon by the jurisprudence of international and regional human rights bodies.[26]

[20] See C Heyns, 'Human Rights and the Use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement' (2016) 38 Human Rights Quarterly 350 ff.

[21] UNCHR, 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns' (2013) UN Doc A/HRC/23/47, 16, paras 82-85.

[22] UNCHR, 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions' (2016) UN Doc A/71/372, 13.

[23] HRW, 'Shaking the Foundations. The Human Rights Implications of Killer Robots' (12 May 2014) available at <www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots>.

[24] N Melzer, 'Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare' EXPO/B/DROI/2012/12 (May 2013) available at <www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPO-DROI_ET(2013)410220_EN.pdf>.

[25] See accordingly C Heyns (n 20) 353-354.

[26] This has constantly been affirmed by the European Court of Human Rights (ECtHR) in its case-law. See eg *Ergi v Turkey* App no 66/1997/850/1057 (ECtHR (GC), 28 July 1998) para 79; *Isayeva, Yusupova and Bazayeva v Russia* App nos 57947/00, 57948/00 and 57949/00 (ECtHR (GC) 24 February 2005) paras 195–200.

In this article, I would like to analyze the way in which the future introduction of AWS will impact on the content, the nature and the extent of States' human rights obligations.

In section 2 I will first discuss that the use of AWS in domestic law enforcement operations is far from being the starting scene of a sci-fi movie, as States are more and more inclined to take the benefit of this option in other-than-war scenarios. In section 3 I will introduce a broad perspective showing that the use of AWS could trigger a negative 'cascade effect' on the whole catalogue of human rights.

After having presented the scenario, I will develop an analysis of the implications that the use of AWS might have on the nature and scope of States' obligations in relation to the right to life and the right to privacy. In particular, in sections 4 and 5, I will scrutinize the impact of AWS on the right to life, both in its negative and its positive dimension. In sections 6 I will advocate that a massive use of AWS outside the context of armed conflicts will induce States to limit the right to privacy of individuals and that, therefore, such a use must also be subject to the standards flowing from the rules protecting that right. In conclusion, I will try to show that States are called, under IHRL, to provide more transparency in the evolution of automated systems, but that this could not be enough to comply with human rights obligations.

2. *The use of AWS in domestic law enforcement: state of the art and possible future developments*

A preliminary section is needed to understand the potential for the use of AWS outside armed conflict in domestic law enforcement operations. As aforementioned, this scenario is still a primitive one, but is going to become reality in the near future, therefore it is worth exploring the state of the art and the possible future developments in relation to the use of AWS in domestic law enforcement.[27]

[27] For a comprehensive historical overview of the evolution of automation in weapons see M Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 Vanderbilt J Transnational L 1, 8-10. For more technical and technological information on autonomous weapons see R Arkin, *Governing Lethal Behaviour in Autonomous Robots* (Chapman & Hall/CRC 2009) 7-27.

Before zooming in into this, it is necessary to clarify that, for the purposes of this article, domestic law enforcement is meant to cover 'traditional public forces or police services [...] with the primary objectives of maintaining law and order in civil society, and who are empowered by State to use force and/or special powers for these purposes'.[28] It derives from that the following reflections are applicable if and when robots come to substitute for or be employed by law enforcement officials, as defined by the UN Code of Conduct.[29]

It is also necessary to clarify what is meant by AWS. Daniele Amoroso, in his piece, devotes a section to explore what he calls 'the definitional conundrum' of the concept of autonomy. He affirms, and I agree with him, that a technical and operative definition of AWS is counterproductive, as what counts is the concept of 'meaningful human control'. Against this, I will use in the present paper a categorization based on the level of human control exercised on weapons. Accordingly, the terms 'human-in-the-loop', 'humans on the loop' and 'human out of the loop' will be employed to describe the level of automation of the machine: from the less to the full automated.[30]

Indeed, armed robots (or drones) have already been employed in domestic law enforcement scenarios, as happened in Dallas, in the United States, in 2016, when the police used a Northrop Grumman Remotec Andros, which is a remotely controlled bomb disposal robot, to deliver an explosive that killed an individual who was posing a threat to public order.[31] This example does not prove much as the robot employed was

[28] This definition is coined by the Committee of Ministers of the Council of Europe: 'Recommendation Rec(2001)10 of the Committee of Ministers to member States on the European Code of Police Ethics' (2001) Rec(2001)10, Appendix.

[29] 'The term "law enforcement officials" includes all officers of the law, whether appointed or elected, who exercise police powers, especially the powers of arrest or detention'. See UNGA Res 169 'Code of Conduct for Law Enforcement Officials' (1979) GAOR 34th Session, art 1 (UN Code of Conduct).

[30] This is the approach followed by Human Rights Watch and the Harvard Law Clinic in their joint 2012 Report. See HRW, IHRC (n 9) 2. See accordingly N Sharkey, 'Staying in the Loop: Human Supervisory Control of Weapons' in N Bhuta, S Beck, R Geiss, H-Y Liu, C Kress (eds), *Autonomous Weapons Systems. Law, Ethics, Policy* (CUP 2016) 23, 26-27. A similar approach is taken by M Wagner, 'The Dehumanization of International Humanitarian Law' (n 27) 11-13.

[31] For more information, see PW Singer, 'The Police Used a Robot to Kill – The Key questions', available at <http://edition.cnn.com/2016/07/09/opinions/dallas-robot-questions-singer/index.html>.

remotely controlled; however, it is interesting to note how police forces in the US are more and more tempted to use machines in law enforcement operations. Such a trend is demonstrated by the fact that a growing number of robots are due to be transferred from the Pentagon to US law enforcement agencies. According to public available information, these exchanges take place under what is known as the 1033 Program[32], a Defense Logistics Agency Disposition Services (DLA) initiative to reutilize, transfer, donate, or sell excess military equipment to civil agencies. The 1033 Program covers the transfer of a wide variety of usable property items each year, including many robots. While most of the robots that are acquired by police are intended primarily for bomb disposal, they may also be used for a variety of other missions such as reconnaissance and entering a building ahead of a squad.[33]

The extreme variety of usages of AWS for law enforcement purposes is demonstrated by other concrete examples. One of this is represented by the AWS currently used by South Korea to guard the demilitarized zone that separate it from North Korea, the SGR-A1, developed by Samsung.[34] When the SGR-A1 notices an intruder, it can issue verbal warnings and recognize surrender motions, such as if the target drops their weapon and raises their hands.[35] It appears from many reports that the robot is capable of engaging with light machine guns any intruder who does not surrender after the warnings. Although disputed by Samsung, some commentators regard the robot as a 'human on the loop' one, meaning that it can, in principle, decides on its own to shoot.[36]

[32] Defence Logistic Agency, 'The 1033 Program' available at <www.dla.mil/DispositionServices/Offers/Reutilization/LawEnforcement/JoinTheProgram.aspx >.

[33] For a complete coverage of this data see Center for the Study of the Drone, 'Law Enforcement Robots Datasheet' (11 July 2016) <http://dronecenter.bard.edu/law-enforcement-robots-datasheet/>.

[34] See on this A Velez-Green, 'The Foreign Policy Essay: The South Korean Sentry – A Killer Robot to Prevent War' Lawfare (1 March 2015) <www.lawfareblog.com/foreign-policy-essay-south-koreansentry%E2%80%94-killer-robot-prevent-war>.

[35] ibid.

[36] For an overview of the debate see M Brehm, 'Defending the Boundary. Constraints and Requirements on the Use of Autonomous Weapon Systems Under International Humanitarian and Human Rights Law' (2017) Geneva Academy of International Humanitarian Law and Human Rights, Briefing no. 9, 44.

Robots are currently employed to patrol borders in other geographic areas, such as the line dividing Israel and Palestine along the Gaza Strip[37] and between the US and Mexico.[38]

In May 2017, in Dubai, the first police robot was 'recruited' and unveiled to the world.[39] At present, the machine developed by PAL Robotics is capable of performing a limited number of functions, but, it would appear from the news that it can help in identifying wanted criminals and collecting evidence and it will patrol busy areas in the city; to do so, the robot is equipped with cameras and facial recognition systems.[40] Apparently, the first model of the 'Dubai Robocop' will not be alone for long as the Government's intention is to increase both the number of machines and their tasks and duties.

According to the latest news, India is also planning to deploy its first police robot in October. It will perform more or less the same functions as Dubai's one, but the interesting thing about this model is that it will be probably also be available for private security.[41] As it would appear from a report published by the Carnegie Endowment for International Peace, the Indian Government is favourable to the employment of robots in domestic law enforcement and will increase their production in the upcoming years.[42]

[37] See N Schactman, 'Robo-Snipers, "Auto Kill Zones" to Protect Israeli Borders' Wired (6 April 2007) <www.wired.com/2007/06/for_years_and_y/>. Recently, the Israeli Government has begun to use autonomous vehicles to patrol the border with Gaza, apparently they are not armed; see J Rogers, 'Robot patrol: Israeli Army to deploy autonomous vehicles on Gaza border' (1 September 2016) Fox News available at <www.foxnews.com/tech/2016/09/01/robot-patrol-israeli-army-to-deploy-autonomous-vehicles-on-gaza-border.html>.

[38] The Guardian, 'Half of US-Mexico border now patrolled only by drone' (13 November 2014) <www.theguardian.com/world/2014/nov/13/half-us-mexico-border-patrolled-drone>.

[39] See BBC News, 'Robot police officer goes on duty in Dubai' (24 May 2017) <www.bbc.com/news/technology-40026940>; and Reuters, 'Robocop joins Dubai police to fight real life crime' (1 June 2017) <www.reuters.com/article/us-emirates-robocop-idUSKBN18S4K8>.

[40] ibid.

[41] The Times of India, 'H-Bots Robotics in process of making a police-robot' (5 July 2017) <http://timesofindia.indiatimes.com/business/india-business/h-bots-robotics-in-process-of-making-a-police-robot/articleshow/59460050.cms>.

[42] See R Shashank Reddy, 'India and the Challenge of Autonomous Weapons' (Carnegie Endowment for International Peace June 2016) 10-13 <http://carnegieendowment.org/files/CEIP_CP275_Reddy_final.pdf>

What precedes proves that automation will play a significant role in performing typical law enforcement activities, enhancing the capacity of a Government to search and detect suspects, to patrol borders, and more generally to ensure law and order.

3. *A broad impact*

In the introduction to this article, I noted that it is my intention to broaden the analysis on the human rights implications of the use of AWS. The protection of the right to life is the priority and that this will be the core issue to debate when an artificial intelligence capable of shooting to kill in a domestic scenario is employed for the first time.

The writings that tackled the issue of the human rights implications of the use of AWS set as a priority the respect of the right to life and to bodily integrity, which is embodied in all human rights treaties, both at a universal and at a regional level[43], and it is considered part of customary international law. The right to life is also of an absolute character, meaning that derogations are not permitted even in time of emergency.[44]

This is perfectly understandable: the right to life is deemed to be the cornerstone of the whole set of rules governing the use of force in law enforcement activities.[45] As seen above, should machines be tasked with law enforcement duties, the life of civilians would be endangered by a decision-making process that will be affected by an unpredictable degree of autonomy.

However, the use of lethal force – and the respect for the right to life – do not represent the only reason for concern.

[43] See Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) art 3; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 6; Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1955) 213 UNTS 222 (ECHR) art 2; American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) 1144 UNTS 123 (ACHR) art 6; African [Banjul] Charter on Human and Peoples' Rights, (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217, art 4.

[44] UNCHR, 'General Comment 6' in 'Note by the Secretariat, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies' (1994) UN Doc HRI/GEN/1/Rev.1, 176, para 1.

[45] See N Melzer, *Targeted Killings in International Law* (OUP 2009) 91 ff.

In fact, the logic of human rights is based on the relationship between an individual and the authority that exercises jurisdiction upon them. As Tomuschat pointed out, human rights 'are designed to reconcile the effectiveness of state power with the protection against the same state power'.[46] What is at stake here, therefore, is the relationship between States' authority and individuals as a whole. The protection of the right to life is just part of a broader picture.

As seen in section 2 of this article, the impact that AWS are going to have in the near future on domestic law enforcement will probably cover most – if not all – the dimensions of the exercise of States' authority: from police operations involving the use of lethal force to patrolling activities across international borders or in crowded squares during a manifestation.

Should this be the future, machines will be able to decide on their own on the basis of automated processes. Consequently, during such a process data will be collected, stored, analyzed and used through algorithms. In fact, to take autonomous decisions, machines will probably decide on the basis of software that will help them in predicting the likelihood of a given scenario.[47]

It seems reasonable to opine that when AWS are tasked with law enforcement duties, they must be aware of all the details of an operative scenario. Paradoxically, as we will see later,[48] from the perspective of the protection of the right to life this would even be desirable, as a perfect understanding of a scenario is crucial to avoid violations of the right to life. This would inevitably imply a preliminary screening of individuals and places, which involves mass surveillance operations and an automatic processing of data.[49]

What we are going to witness is a digitalization of law enforcement activities as a whole. Such a trend is not actually beginning with the introduction of AWS. Data protection is at the core of a debate on the risks that new technologies poses on the enjoyment of the right to privacy; in

[46] C Tomuschat, *Human Rights Between Idealism and Realism* (2nd edn, OUP 2008) 8.

[47] This is admitted by anti-ban scholars and experts of artificial intelligence. See for example R Arkin (n 27) 30: robots will have the technical ability 'of independently and objectively monitoring ethical behavior in the battlefield by all parties and reporting infractions that might be observed'.

[48] See *infra*, sec 4.

[49] See on this M Brehm (n 32) 52-54.

the European Union (EU) a through reform of EU data protection rules is feeding the discussion.[50]

The employment of AWS can have a fueling impact on States' recourse to new technologies for law enforcement purposes, contributing to the so-call 'bulk collection of data': a practice consisting of the indiscriminate collection of data that was recently addressed by the Obama administration in the US.[51]

The impact of the use of AWS on the right to privacy might have a cascade effect on other rights. In fact, once AWS will be required to collect and – eventually – store data, they will probably be equipped with software that will enable them to process such data. It cannot be excluded that such software will permit AWS to make predictions. Perhaps, they could be used to help in determining when the use of lethal force is necessary or proportionate.

This scenario is even admitted by the scholars who do not call for a complete ban on AWS. Schmitt and Thurnher, in fact, refers to 'pattern of life analysis', which will enable machines to detect individuals who possess certain attributes.[52] Such a conduct would probably constitute a 'profiling' activity that according to a Council of Europe recommendation can be defined as:

> 'an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'[53]

[50] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119/1. See also European Parliament and Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JH (2016) OJ L 119/89.

[51] White House, Office of the Press Secretary, 'Presidential Policy Directive 28 – Signal Intelligence Activities' (17 January 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidentiapolicy-directive-signals-intelligence-activities>.

[52] MN Schmitt, JS Thurnher (n 3) 268.

[53] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal

Profiling of personal data would bear a risk of violating not only the right to life and the right to privacy, but also the right not to be discriminated against,[54] which is affirmed in all human rights treaties.[55]

By way of concrete example, in the US, machines are currently used in criminal proceedings to determine the 'level of risk' of a defendant.[56] Only last year, in 2016, in Wisconsin a defendant appealed a judgment on the ground that he was convicted using data, which he was not allowed to challenge.[57] Some commentators allege that an algorithmic-based decision making process might be affected by a racist bias.[58] The investigative journal *ProPublica* showed, for example, that machines used in trials are biased against black persons.[59]

Should similar software be introduced in AWS which are used for law enforcement activities, the risk of discrimination would be high.

4. *Protecting the right to life as a priority*

Against the scenario depicted in section 2 and 3 it appears that the right to life plays a central role in the debate. As Christopher Heyns put it, the impact of AWS on the protection of the right to life in domestic law enforcement must be assessed on autonomous grounds, as IHL is not

data in the context of profiling, Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies. See the Appendix at 1, *e*).

[54] See for example: UNCHR, 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance' (2015) UN Doc A/HRC/29/46.

[55] ICCPR (n 43) art 17; ECHR (n 43) art 8; ACHR (n 43) art 11.

[56] J Tashea, 'Courts Are Using AI to Sentence Criminals. That Must Stop Now' Wired (17 April 2017) <www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/>.

[57] M Smith, 'In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures' The New York Times (22 June 2016) <www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html>.

[58] J Dooris, 'Killer Robots And Racist Software: Are There Decisions Only Humans Should Make?' Huffington Post (10 July 2017) <www.huffingtonpost.com.au/jason-dooris/killer-robots-and-racist-software-are-there-decisions-that-only_a_23022933/>..

[59] See J Angwin, J Larson, S Mattu, L Kirchner, 'Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks' ProPublica (23 May 2016) <www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

applicable outside the context of armed conflicts.[60] In domestic law enforcement, in fact, the use of lethal force by a Government is subjected to stricter rules than those applicable in the context of an armed conflict.[61]

The rules governing the use of lethal force outside the context of an armed conflict are more demanding than those provided for by IHL. The standing point of IHL, in fact, is that killing is permissible and should only be regulated and not forbidden. Law enforcement officials, on the contrary, are deemed to 'have a vital role in the protection of the right to life, liberty and security of the person.'[62] Exceptions to this legal construction must abide by the principles of legality, strict necessity, proportionality and precaution.[63]

Deprivation of life is only permitted if it happens within a legal framework. The ICCPR and the ACHR employ the term 'arbitrarily' to identify those situations in which the deprivation of life is not tolerated. The ECHR is more detailed: 'No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law'. The common denominator of the three major human rights treaties is that deprivation of life could be tolerated only if it has a 'sufficient legal basis', which is the first requirement governing the use of force in IHRL.[64] A 'sufficient legal basis' represents a demanding test; in fact, the jurisprudence of the ECtHR set the bar high and any law enforcement operation must not only be authorized by law, but also 'sufficiently regulated by it'.[65]

In the context of the protection of the right to life, therefore, national law should be publicly available, and must make the recourse to firearms dependent on a careful assessment of the circumstances including the nature of the offence committed, and the threat posed by the suspect or fugitive. Moreover, the national law regulating policing operations must

[60] C Heyns (n 20) 353.
[61] ibid.
[62] UN, 'Basic Principles on the Use of Force and Firearms by Law Enforcement Officials Adopted at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August to 7 September 1990' (1990) UN Doc A/CONF.144/28/Rev.1, 112, Preamble.
[63] ibid principle 5.
[64] See N Melzer, *Targeted Killings* (n 45) 100 and 116.
[65] ECtHR, *Makaratzis v Greece* App no 50385/99 (ECtHR (GC) 20 December 2004) para 11; see also *Nachova and Others v Bulgaria* App no 43577/98 (ECtHR (GC) 6 July 2005) para 97.

secure a system of adequate and effective safeguards against arbitrariness and abuse of force and even against avoidable accident.[66]

In general, to be compatible with IHRL, domestic law must enable individuals to predict and to be protected against the use of lethal force by State agents.[67]

Along with the principle of legality, the principle of strict necessity is of a central importance in the protection of the right to life. A deprivation can have a sufficient legal basis, but nonetheless it can be judged contrary to IHRL if it is not necessary. Necessity means that force should be used only as a means of last resort, when all other non-violent means fail.[68] Such a principle is enshrined in Article 2(2) of the ECHR[69] and confirmed by the jurisprudence of the ECtHR. Although the ICCPR and ACHR do not explicit mention this principle, the practice of the Human Rights Committee[70] and that of Inter-American Commission on Human Rights[71] join that of the European Court in affirming that deprivation of life must be necessary. This principle is also stated in the UN Code of Conduct: 'Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty.'[72]

Accordingly, lethal force can be used only against a person who is posing an imminent threat to the population or to the States' agents involved in an emergency situation. IHRL requires a careful factual assessment of a scenario before deciding to employ lethal force.

Finally, the use of deadly force must comply with the principle of proportionality, which requires States' agents to choose means and methods to avoid excessive harm. More precisely, the principle of proportionality calls for a value judgment of the relation between harm and benefit:

[66] *Makaratzis* (n 65) para 58.
[67] See N Melzer, *Targeted Killings* (n 45) 224.
[68] See C Heyns (n 20) 364; N Melzer, 'Human Rights Implications' (n 24) 31.
[69] ECHR (n 43) art 2(2): 'Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary'.
[70] UNCHR, 'Pedro Pablo Camargo v. Colombia' (1982) UN Doc CCPR/C/OP/1, para 13.2.
[71] Inter-American Commission on Human Rights, 'Report on terrorism and human rights' OEA/Ser.L/V/II.116, Doc 5 rev 1 corr (22 October 2002) paras 87-89.
[72] UN Code of Conduct (n 29) art 3.

lethal force might be necessary, but it should be employed only if the threat is sufficiently grave to justify the deprivation of life.[73]

All the commentators that dealt with the compatibility of the use of AWS with the right to life highlighted that it would be very difficult for a machine to undergo a complex decision-making process, such as the one demanded by IHRL.[74] This is particularly evident for completely autonomous machines, where humans are 'out of the loop'. However, this is also true for AWS that involve humans, in or on the loop.[75]

At present, in fact, it is reasonable to doubt that robots will have the technical ability to assess properly if it is necessary to employ lethal force or if their action would be proportionate to the aim pursued. This is a major issue, which differentiates radically and significantly the discourse on the compatibility of AWS with IHRL from that under IHL. In the latter there is room for debate on the possibility that AWS will be able to respect the principle of distinction in the targeting decision making process of machines.[76] In the former discourse, the decision-making process is subject to more demanding requirements, in particular those represented by the principles of necessity and proportionality.

5. *The extent to which the positive obligation to protect life apply to the use of AWS*

Another layer of discussion is represented by the nature of human rights obligations that States must fulfil in the field of human rights. It is known, in fact, that IHRL does not merely place limitations on the exercise of States' authority, but it also imposes positive duties on Govern-

[73] The case-law of the European Court of Human Rights is particularly instructive on the operation of this principle. See the judgment and decisions in the cases: *McCann and Others v the United Kingdom* App no 18984/91 (ECtHR (GC) 27 September 1995) para 192; *Nachova and others* (n 65) para 95. See more recently *Giuliani and Gaggio v Italy* App no 23458/02 (ECtHR (GC) 24 March 2011) para 209.

[74] C Heyns (n 20) 366; N Melzer, 'Human Rights Implications' (n 24) 36. Similar conclusions can also be drawn from the debate on the compatibility of AWS with IHL. See for instance WH Boothby (n 3) 79-80, P Alston (n 3) 54, NE Sharkey, 'The evitability of autonomous robot warfare' 94 Intl Rev of the Red Cross 787, 789.

[75] See again N Melzer, 'Human Rights Implications' (n 24) ibid.

[76] See in this regard M Sassoli (n 14).

ments to protect individuals from human rights violations, and in particular from violations of the right to life.[77] This obligation applies both when the harmful conduct is performed by a State's agent or by a private person or entity[78] and extends to 'any activity, whether public or not, in which the right to life may be at stake.'[79]

Such a duty has broadly been interpreted by the ECtHR, which has constantly affirmed that:

> 'The positive obligation to take all appropriate steps to safeguard life for the purposes of Article 2 entails above all a primary duty on the State to put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life'.[80]

If applied to the use of AWS, the extent of the positive obligation of States to protect the right to life is dependent on the degree of automation of the machine.

In cases of AWS that foresee a human control (whether *in* or *on* the loop), the *Osman* test developed by the ECtHR appears to be the applicable one: States are responsible if they 'knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual'.[81] Accordingly, if the State's agent that remotely controls a drone or a robot notices an imminent threat to the life of a person, he or she should intervene to halt the machine. This duty imposes on Governments, as a corollary, the duty to plan, organize and control a law enforcement operation to minimize the use of lethal force. To the

[77] See in general on this issue R Pisillo Mazzeschi, 'Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme' (2006) 333 Recueil des Cours de l'Académie de Droit International 390 ff.

[78] See Human Rights Committee, 'General Comment No 31. The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' UN Doc CCPR/C/21/Rev.1/Add. 13 (26 May 2004) para 8. Human Rights Committee, 'CCPR General Comment No 6: Article 6 (Right to Life)' (30 April 1982) para. 3: 'The Committee considers that States parties should take measures not only to prevent and punish deprivation of life by criminal acts, but also to prevent arbitrary killing by their own security forces'.

[79] *Öneryildiz v Turkey* App no 48939/99 (ECtHR (GC) 30 November 2004) para 71.

[80] ibid para 89.

[81] *Osman v the United Kingdom* App no 23452/94 (ECtHR (GC) 28 October 1998) para 116; *Demiray v Turkey* App no 27308/95 (ECtHR (GC) 21 November 2000) para 45.

same end, this also implies that law enforcement officials must be trained to cope with emergency scenarios.[82]

Should the AWS be completely autonomous ('humans *out* of the loop' model), the positive obligation to protect life could in principle entail a duty to avoid malfunctioning in the machines' performance. During the Fifth Conference of the States Parties to the CCW, it was highlighted that

> 'one of the dangers is that these weapons could lead to strategies diluting or concealing true responsibilities in case of collateral damages. If armed machines provoke such damages it is easy and tempting, on the part of those who use them, to invoke technical malfunctions rather than face their responsibility.'[83]

The positive obligation to prevent loss of life should therefore bind States to constantly monitor the correct functioning of AWS. This appears to be a manifestation of the principle of due diligence to prevent human rights violations.[84]

In the case of AWS, one might wonder whether the principle of due diligence can force States to scrutinize the performance of the machines from the moment of their inception and, therefore, to liaise manufacturers in order to avoid the development of machines that could potentially act contrary to human rights. This appears to be a far-reaching conclusion, as it would impose a disproportionate burden on States in relation to the transfer of arms as a whole.[85] However, it is clear that the positive obligation to protect life should bind States to a pro-active review of the AWS at their disposal.

Last, but not least, the positive obligations of States to protect life entail a duty to investigate into an alleged deprivation of life. Although it is clear in the case law of international courts that this is an obligation of

[82] *Nachova and Others* (n 65) para 97; see also the Court's criticism of the 'shoot to kill' instructions given to soldiers in *McCann and Others* (n 74) paras 211-214.

[83] Comments Supporting the Prohibition of Lethal Autonomous Weapons Systems Working Paper submitted by the Holy See, 7 April 2016, 2.

[84] See again R Pisillo Mazzeschi (n 77) 394, specifically. See also from the same Author: 'The Due Diligence Rule and the Nature of the International Responsibility of States' (1992) 35 German YB Intl L 9. See also RP Barnidge Jr, 'The Due Diligence Principle Under International Law' (2006) 8 Intl Community L Rev 81.

[85] See accordingly M Brehm, 'The Arms Trade and States' Duty to Ensure Respect for Humanitarian and Human Rights Law' (2008) 12 J Conflict & Security L 359, 382-383.

means and not an obligation of result,[86] investigations must be immediate, exhaustive and impartial, as well as independent in hierarchical, institutional and practical terms.[87] The draft General Comment on the right to life goes even further by requesting that 'investigations into allegations of violation of article 6 must always be independent, impartial, prompt, thorough, effective, credible and transparent.'[88] This means that investigations can either be publicly available or result in securing accountability.[89]

Applying the duty to investigate in cases of lethal, or quasi-lethal, incidents might prove to be a difficult task for States if completely automated machines are to be employed. Indeed, accountability would hardly be secured as it is not feasible to envisage a 'court for robots' as machines cannot be punished.[90] Proposals to hold accountable commanders and programmers have already been criticized as incompatible with the *mens rea* requirement.[91]

The least a Government can do is to properly assess the decision-making process that leads to civilian casualties. However, would an explanation based on complex probabilistic and algorithmic analytics be acceptable for the relatives of a victim?[92]

[86] R Pisillo Mazzeschi (n 77) 414-417. The ECtHR put it clearly in *Kelly and Others v United Kingdom* App no 30054/96 (ECtHR (GC) 4 May 2001) para 96. The same approach is adopted by the Inter-American Court of Human Rights in *Velasquez Rodriguez Case*, Judgment, Inter-American Court of Human Rights Series C No 4 (29 July 1988) paras 176-177.

[87] This is confirmed in international jurisprudence: See, for example, *Isayeva, Yusupova and Bazayeva v Russia* (n 26) para 210; Inter-American Commission on Human Rights, *Report No. 55/97, Case No 11.137: Argentina*, OEA/ Ser/L/V/II.98, Doc 38 (6 December 1997) para 412.

[88] 'General comment No 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life, Advance Unedited Version' <www.ohchr.org/Documents/HRBodies/CCPR/GCArticle6/GCArticle6_EN.pf>.

[89] *Özkan and Others v Turkey* (ECtHR 6 April 2004) para 314.

[90] See HRW (n 23) 19. See more in depth on this issue R Sparrow, 'Killer Robots' (2007) 24 J Applied Philosophy 62, 72.

[91] For a discussion on this see D Amoroso, G Tamburrini (n 13) 6-7. See also HRW (n 9) 20.

[92] See on this J Burrell, 'How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms' (2016) 3 Big Data & Society 1. See also *infra*, sec 7.

6. *AWS and data collection: the content of the duty to respect the right to privacy*

As seen in section 3 of this article, the human rights implications of the use of AWS do not only regard the protection of the right to life. I have tried to explain that AWS could fuel a bulk collection of data and this could have tremendous repercussions on the right to privacy and, consequently, on democracy.[93] A failure to protect such a right would cause a cascade effect on other fundamental freedoms, as discriminatory conduct might not be excluded.

The debate related to the impact of technological evolution on the right to privacy is topical, as recent States' programmes are showing a dangerous attitude towards the treatment of personal data. The evolution of technologies, in fact, allows private and public entities to collect and store individual data. It is no coincidence that the Human Rights Council appointed, in 2015, a Special Rapporteur on the Right to Privacy[94] and that the United Nations General Assembly approved, in 2013, a resolution on this delicate topic.[95]

The major issues of concern regarding the right to privacy in the digital age lie with the constant and rapid technological development, which is going to enable individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments to undertake surveillance, interception and data collection.[96]

According to IHRL, limitations on the right to privacy can take place only if States' measures respect the principle of legality, legitimacy and proportionality.

The principle of legality is the most important among the parameters for evaluating States' interference with the enjoyment of human rights.[97] In fact, human rights violations or limitations can be justified only if they

[93] *Klass and Others v Germany* App no 5029/71 (ECtHR (GC) 6 September 1978) para 49: 'the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it'.

[94] HRC, 'Resolution adopted by the Human Rights Council' (2015) UN Doc A/HRC/RES/28/16.

[95] UNGA, 'The right to privacy in the digital age' (2014) UN doc A/RES/68/167.

[96] ibid.

[97] C Tomuschat (n 46) 93-94.

are grounded on a law that can be accessible to individuals. This is a generalized principle which is common in all human rights treaties. The ACHR put it clearly and generally in Article 30:

> 'The restrictions that, pursuant to this Convention, may be placed on the enjoyment or exercise of the rights or freedoms recognized herein may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established.'[98]

The ICCPR and the ECHR do not have such a general clause but nonetheless the principle of legality is mentioned in relation to the single rights listed therein.[99]

Interferences with fundamental freedoms and, in our specific case, the right to privacy can be tolerated only if 'they take place on the basis of law'.[100] The legality test requires that 'relevant legislation must specify *in detail* the precise circumstances in which such interferences may be permitted'(emphasis added).[101] This is confirmed in the jurisprudence of international courts, and in particular in that of the ECtHR that introduced the concept of the 'quality of the law', adding that 'there must be a measure of *legal* protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 [of Article 8 of the ECHR]' (emphasis added).[102]

States are asked to pay attention to the revision of their existing laws in order to cope with the evolution of modern technologies. This has been recently affirmed by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in its 2014 Annual Report to the General Assembly.[103]

[98] ACHR (n 43) art 30.

[99] ECHR (n 43) art 8(2). The ICCPR (n 43) in art 17 prohibits 'arbitrary or *unlawful* interference with his privacy' (emphasis added).

[100] UNCHR, 'General Comment No. 16' in 'Note by the Secretariat, Compilation of General Comments and General Recommendations adopted by Human Rights Treaty Bodies' (1988) UN Doc HRI/GEN/1/Rev.1, vol I, 191, para 4.

[101] ibid para 8.

[102] See for example *Rotaru v Romania* App No 28341/95 (ECtHR (GC) 4 May 2000) para 55.

[103] UNCHR, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' (2014) UN Doc A/69/397 para 35 ff.

The Special Rapporteur did not simply reaffirm one of the requisites of the so-called 'quality of the law' principle, firmly established in the jurisprudence of the ECtHR, but went a little further affirming that:

> 'A public legislative process provides an opportunity for Governments to justify mass surveillance measures to the public. Open debate enables the public to appreciate the balance that is being struck between privacy and security. A transparent law-making process should also identify the vulnerabilities inherent in digital communications systems, enabling users to make informed choices [...] it is also a valuable means of ensuring effective public participation in a debate on a matter of national and international public interest.'[104]

A legal basis is not the only requirement for considering acceptable a limitation on the right to privacy. In fact, interferences must pursue a legitimate aim and be proportional.

The first requirement is usually interpreted by international courts in a broad sense. Law enforcement activities seeking to maintain public order are normally regarded as legitimate aims that justify a limitation of the right to privacy. However, this approach was recently challenged by the UN Special Rapporteur on the Freedom of Expression, who stated that:

> 'The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State'.[105]

This is an interesting statement for the purposes of the present inquiry. In fact, if AWS were to be deployed for a constant surveillance action, the law enforcement justification would be perennial and, as a result, individuals would be subjected to a constant monitoring activity by their Governments.[106]

[104] ibid para 39.

[105] UNCHR, 'Report of Special Rapporteur on the Freedom of Expression' (2013) UN Doc A/HRC/23/40 para 58.

[106] In this regard, the words of Christopher Heyns in his 2013 Report are rather paradigmatic: 'The danger here is that the world is seen as a single, large and perpetual battlefield and force is used without meeting the threshold requirements. LARs could aggravate these problems.' See UNCHR (n 21) para 83. See also and accordingly A Oddenino,

International courts – and in particular the ECtHR –, on the contrary, have discussed deeply the requirement of proportionality, according to which a limitation on the right to privacy is tolerable only when there are adequate and effective guarantees against abuse. The assessment that the European Court usually makes depends on all the circumstances of a given case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[107]

Recently, the ECtHR delivered some important judgments that specify the content of States' obligation to respect privacy in the context of their surveillance programs.

In the *Szabo and Vissy v Hungary* case, the Court declared that the Hungarian anti-terrorist surveillance legislation was contrary to the ECHR because it had enabled the Government to use new technologies to intercept masses of data without offering any reasonable guarantee to individuals.[108] In the *Zakharov v Russia* judgment, the Court found that Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. For example, critical factors were identified in the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; in the duration of such measures; in the procedures for authorising interception as well as for storing and destroying the intercepted data; and, finally, in the supervision mechanism of the interception.[109]

The case-law of the ECtHR seems to pose an undeniable burden on States. If they want to employ AWS in the performance of law enforcement duties, they should strictly regulate the collection of data to which

'La violazione dei sistemi informatici contenenti informazioni riservate come illecito internazionale: tra dimensione interstatuale e tutela dei diritti umani' in M Di Stefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale* (Editoriale Scientifica 2017) 13, 14-15.

[107] *Klass et al* (n 93) para 50.

[108] *Szabo and Vissy v Hungary* App no 37138/14 (ECtHR (GC) 12 January 2016) para 82.

[109] *Roman Zakharov v Russia* App no 47143/06 (ECtHR (GC) 4 December 2015) para 231.

machines will inevitably contribute. Should AWS carry out mass surveillance, States must provide a clear and accessible legislative framework for preventing this system from abuse.

Furthermore, enforcement duties performed by AWS might see the involvement of private companies. At present, this is normal practice in the treatment of data and indeed. It happens frequently, with data often being stored by private actors and requested by States when needed.[110]

As regards EU Member States, their responsibility in the context of data protection will be regulated from 2018 by the newly adopted General Data Protection Regulation.[111] Although it is too early to assess the impact of the Regulation, for the purposes of the present analysis it is worth mentioning that, through its implementation, a number of important rights would be granted to individuals. For example, the right to object at any time to the processing of data (Article 21) and the right not to be subject to a decision based solely on automated processing of data (Article 22) seem to offer to individuals a wide-ranging protection.

7. *An appraisal*

In this article, I have tried to evaluate the impact of the use of AWS on human rights. As I said in the introductory section, I performed this evaluation assuming that a general pre-emptive ban will not be adopted. I focused my analysis on the right to life and on the right to privacy on the assumption that AWS could have particular implications here, not only because they could decide to use lethal force on the basis of algorithmic decision-making processes, but also because, in the course of such processes, individuals' data can inevitably be mistreated.

The results of the analysis allow some final reflections to be proposed.

Both the right to life and the right to privacy demand a regulation of the use of AWS in domestic law enforcement that must meet the 'quality of the law' threshold. A threshold that is met by domestic laws that are accessible, that make future Governmental actions predictable and that

[110] A Haase, E Peters, 'Ubiquitous computing and increasing engagement of private companies in governmental surveillance' (2017) 7 Intl Data Privacy L 126 ff.

[111] See *supra* sec 3.

provide adequate and effective guarantees against abuse. In other words, laws that make the recourse to AWS 'transparent'.[112]

A call for transparency has already been made by several Governments of States Parties to the Convention on Certain Conventional Weapons in 2015[113] and by NGOs such as Human Rights Watch, Article 36 and Amnesty International.[114] Christopher Heyns, in his capacity as UN Special Rapporteur, has already brought the attention of the UN to the issue of transparency in his 2013 Report, recommending that 'it will be important to ensure that transparency, accountability and the rule of law are placed on the agenda from the start' and emphasizing 'the need for full transparency regarding all aspects of the development of robotic weapon systems'.[115]

As regards the use of AWS in domestic law enforcement, as seen, although no weapons' review mechanisms are foreseen in IHRL, a duty of reviewing the use of new weapons can be considered as necessary for meeting the 'quality of the law' requirement.

Be that as it may, a call for more transparency does not offer any solution to the issue of accountability raised in section 5 and in the final part of section 6 of this piece. The demands for justice by relatives of civilians killed as a result of the conduct of AWS will likely remain unanswered. Or, and this is even worse, the answer may be totally unintelligible, making it impossible to understand the process that led to a certain event. The same

[112] See, generally, S Knuckey, 'Autonomous Weapons Systems and Transparency: Towards an International Dialogue' and N Bhuta, S-E Pantazopoulos, 'Autonomy and Uncertainty: Increasingly Autonomous Weapons Systems and the International Legal Regulation of Risk' in N Bhuta, S Beck, R Geiss, H-Y Liu, C Kress (eds) (n 30) 164 ff and 284, 299. See also M Sassoli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified' (2014) 90 Intl L Studies 308, 338.

[113] Germany, statement on Transparency to the 2015 CCW Meeting of Experts on Lethal Autonomous Weapons Systems (17 April 2015); Sweden, statement on Transparency and the Way Forward to the 2015 CCW Meeting of Experts on Lethal Autonomous Weapons Systems (17 April 2015); Ghana, statement to the 2015 CCW Meeting of Experts on Lethal Autonomous Weapons Systems (17 April 2015).

[114] Article 36, 'Structuring debate on autonomous weapons systems: memorandum for delegates to the Convention on Certain Conventional Weapons' (November 2013) 3; Amnesty International, 'Moratorium on fully autonomous robotics weapons needed to allow the UN to consider fully their far-reaching implications and protect human rights', written statement to the twenty-third session of the UN Human Rights Council (22 May 2013); HRW (n 23) 47.

[115] UNCHR (n 21) paras 111 and 115.

goes for all the individuals whose data will be collected by AWS for law enforcement duties; a right to obtain an explanation, in fact, does not seem to exist even in the EU General Data Protection Regulation. [116]

In April 2017, the Science and Technology Committee of the Parliament of the United Kingdom launched an inquiry into algorithmic decision-making.[117] The written evidence received so far from technology experts are interesting. One expert says that 'Algorithms used in decision-making can be too complex to describe in clear English' and 'Data used in algorithms can go through multiple levels of abstraction such that it is impossible to determine the original input'.[118] Another expert proposes the introduction of a 'lingua franca' that Institutions should adopt 'to explain their decisions in cases where humans are affected and involved [...] to make sure that non-experts, courts and media can understand what went on.'[119] Finally, an expert warns that 'alone, transparency mechanisms can encourage false binaries between "invisible" and "visible" algorithms, failing to enact scrutiny on important systems that are less visible'.[120]

Transparency, therefore, is not enough if it leads to unintelligible sources. It may satisfy the principle of legality, but it does not help, as such, to ensure accountability.

It may well be the starting point of the debate on law reforms that in an unpredictable future will require the adaption of the uses and the abuses of AWS to reach human rights standards.

[116] See accordingly S Wachter, B Mittelstadt, L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 Intl Data Privacy L 76 ff.

[117] See <www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2015/algorithms-in-decision-making-inquiry-launch-16-17/>.

[118] Written evidence submitted by Dr Janet Bastiman (ALG0029) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-indecisionmaking/written/68990.html>.

[119] Written evidence submitted by Simul Systems Ltd (ALG0007) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-indecisionmaking/written/49780.html>.

[120] Written evidence submitted by Dr Alison Powell (ALG0067) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-indecisionmaking/written/69121.html>.