LL.M. in Human Rights Capstone Thesis

# "Facing the future: emerging militarisation of facial recognition and public international law considerations"

by Arina Nachinova

**Supervisor:**
Tommaso Soave
Assistant Professor, Department of Legal Studies

## Abstract

Development of facial recognition technology in recent years attracted the attention of military developers and, subsequently, of states' officials. It has the potential to improve the accuracy of the existing weapons and devices used for military purposes. However, provisions of the international humanitarian law require an assessment to be carried out to check whether the new weapons, means or methods of warfare are not prohibited under the rules of international law. When this new weapons and devices with facial recognition might actually pass the test under international humanitarian law, there are some doubts about their conformity with international human rights law. The paper aims to carry this preliminary assessment and to identify potential norms and principles applicable to the weapons and devices equipped with facial recognition. In doing so it can provide military developers and their opponents with considerations and arguments on mainly pre-deployment stage as to whether such weapons and devices can be recognized as prohibited or permitted under two branches of the international law. The assessment is carried out on the basis of the selected customary rules of international humanitarian law and correlating provisions of international human rights law regulating the use of force with due regard for specificities of facial recognition technology. The research is based on the existing legal provisions, the jurisprudence of the regional human rights institutions, as well as scholarly articles on facial recognition technology and autonomous lethal weapons.

## Table of Content

## Introduction

Mankind has been testing the limits of its humanity for a while now. Back in the 17th century, W. Shakespeare reflecting on the border dividing a human and evil, mad spirit wrote "Macbeth"[1]. His main character, struggling to decide if he should commit murder, pronounces:

"*I dare do all that may become a man; Who dares do more is none*".

The weapon of his transformation into an obsessed, power-hungry creature justifying murders by initially imaginary fears, is a dagger. The dagger, that, as might be argued, has deprived him of his humanity.

The modern way to maintain humanity during times of war, when killings are inevitable, is to create more "*humane"* weapons. It is no longer a question of spiritual purity but a question of objectivity. And what can be more objective and impartial than machines? This consideration gave birth to autonomous lethal weapons ("LAWs") and now can be the driving factor behind their modernization. They acquire new features by instalment of various software to enhance their accuracy. With the world still weighing if law enforcement agents should be allowed to use facial recognition technology in everyday life, the U.S., China, Turkey and Iran are fully exploring its military potential. Evidence of facial recognition arms race, which previously were quite indirect and mostly appeared in the media[2], scientific researches by military universities[3] and in discussions around specific incidents[4], now started to take a shape of official documents and statements.

In the atmosphere of the impending revolution in the use of biometric technology for military purposes, the human rights community remains to a large extent silent. There is a significant number of literature, reports, opinions on possible consequences of the use of LAWs and devices in the form of human rights violations. However, only a few have addressed the military use of facial recognition technology and specific legal challenges it raises. This paper seeks to bridge this gap by asking the question: what does international law have to say concerning the military deployment of LAWs and devices with facial recognition?

In answering this question, the paper does not aim to settle the question if facial recognition technology performs more "*ethically*" than humans during military operations, nor does it seek

[1] Shakespeare, W. (1623) *Macbeth*. Ware, England: Wordsworth Editions. Modern ed. of 1992. Scene VII, act 1.
[2] Hambling, D. (2020). *US military face recognition system could work from 1 kilometre away.* [online] New Scientist. Available at: https://www.newscientist.com/article/2233639-us-military-face-recognition-system-could-work-from-1-kilometre-away/ [Accessed 21 Jan. 2021].
[3] Hu, M. et. al (2019). *Read + Verify: Machine Reading Comprehension with Unanswerable Questions. Proceedings of the AAAI Conference on Artificial Intelligence*, pp. 6529–6537.
[4] *Fakhrizadeh, M.* (2020). *Iran scientist "killed by remote-controlled weapon."* [online] BBC News. Available at: https://www.bbc.com/news/world-middle-east-55128970 [Accessed 21 Jan. 2021]; Arthur Holland Michel, UNIDIR technology researcher, gave evaluation on the possible use of remotely operated weapon in this incident: Michel A.H. (2021). [Twitter] 7 Dec. "*My breakdown of the technical credibility of #Fakhrizadeh attack claims [...]*" [online] Available at: https://twitter.com/WriteArthur/status/1335943421803048964 [Accessed 21 Jan. 2021].

to assess the level of autonomy of LAWs. On the contrary, it presupposes that the human element is present throughout the deployment process – from the moment of creation of a weapon to release of force[5] and after "*the deed*" is done. The main objective is, rather, to look at the legal scaffoldings in a rivalry over shackling of development and deployment of facial recognition technology by the military. More specifically, I analyse how international humanitarian law ("IHL") and international human rights law ("IHRL") can contribute to the evaluation of an emerging militarization of facial recognition technology.

The paper consists of two chapters. The first chapter defines the legal basis for an obligatory compliance assessment of the new weapons and devices under public international law norms. Then the relevant IHL provisions are identified and applied to the functionalities of weapons and devices with facial recognition, taking into account the possible consequences of their field application.

In the second chapter the assessment focuses instead on the provisions of IHRL to the extent they are applicable during hostilities. The chapter gives a brief overview of the main deficiencies and issues that the use of facial recognition can raise. In particular it: (i) identifies criteria for the compliance assessment under the right to life, the prohibition of ill-treatment, and anti-discrimination provisions with particular focus on the use of force; and (ii) evaluates whether those criteria can provide a reliable test for the compliance assessment and application of the test to modelled situations involving the use of LAWs and devices with facial recognition.

The conclusion aims to put both parts of the analysis together and to elaborate to what extent the legal provisions are developed to provide sufficient ground for compliance assessment and what are the arguments that can be put for and against the development and deployment of the LAWs and devices with facial recognition.



[5] Heyns, C. (2016). *Human Rights and the use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement*. Human Rights Quarterly, 38(2), pp.350–378; p. 356

## 1. LAWs and military devices with facial recognition under international humanitarian law

The development of means of application of facial recognition software for military purposes for now is limited to two types: 1) integration of the software into LAWs and 2) its use in either portable devices specifically designed for this purpose or in drones ("military devices"). While LAWs with facial recognition are mostly being discussed rather than developed[6], the military devices seem to be ready for field deployment[7].

The legal framework for their use is based on the already obsolete[8] (although might rather be considered fundamental) provisions of the international humanitarian law. The four Geneva Conventions do not expressly limit the types of weapons that can be used in warfare. Protocol II to the Convention on Certain Conventional Weapons[9] in art. 2 (3) provides the closest definition that can describe LAWs and military devices with facial recognition:

"*[o]ther devices means manually-emplaced ... devices designed to kill, injure or damage and which are actuated by remote control or automatically after a lapse of time*".

This generic definition does not cover the specificities of the weapons we look into. Or rather it is too vague to allow us to clearly squeeze LAWs and military devices within it. Nonetheless, if the main functions of the machine will resemble the described characteristics, it can be considered as a weapon and should be compliant with art. 36 Additional Protocol I[10]. It stipulates, that:

"*[i]n the... development... or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would... be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party".*

The drafters, however, set no criteria or guidelines on how should a state determine that - lacuna noted by the International Committee of the Red Cross ("ICRC")[11]. The legal enigma is getting more complex when one thinks about the varying number of international instruments each

[6] Cox, M. (2019). *Army's Next Infantry Weapon Could Have Facial-Recognition Technology*. [online] Military.com. Available at: https://www.military.com/daily-news/2019/06/01/armys-next-infantry-weapon-could-have-facial-recognition-technology.html [Accessed 1 Dec. 2020].

[7] Gershgorn, D. (2020). *The Military Is Building Long-Range Facial Recognition That Works in the Dark.* [online] Medium. Available at: https://onezero.medium.com/the-military-is-building-long-range-facial-recognition-that-works-in-the-dark-4f752fa713e6 [Accessed 1 Dec. 2020].

[8] Gnaedinger, A. (2006). *Is IHL still relevant in a post-9/11 world?* [online] icrc.org. Available at: https://www.icrc.org/en/doc/resources/documents/article/other/ihl-article-300906.htm [Accessed 28 Jun. 2021].

[9] UN, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II) (as amended on 3 May 1996), 10 October 1980

[10] UN, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3

[11] Treaties, States parties, and Commentaries - Additional Protocol (I) to the Geneva Conventions, 1977 - 36 - New weapons (1987). [online] icrc.org. Available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F095453E41336B76C12563CD00432AA1 [Accessed 20 Dec. 2020], paras 1472 - 1475

state is a party to, and disbalance of the military clout created by the prohibition of some weapons in one part of the world and endorsement in another[12]. Nonetheless, the article obliges as a minimum running an assessment against customary rules, applicable to every state. Within the IHL those will be: 1) prohibition of violence to life and person, 2) principle of distinction between civilians and combatants, 3) precautions in the attack, 4) prohibition to resort to attacks and weapons that are indiscriminate.

### 1.1. Prohibition of violence to life and person

Prohibition of "*violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture*" in a common article 3 Geneva Conventions should be a starting point of our analysis. According to Additional Protocols I[13] and II[14] this is one of the fundamental guarantees in IHL, whose scope is, however, not absolute. The principle of proportionality[15] requires the state to weigh the anticipated military advantage of the attack or placement of military devices against the possible incidental loss of civilian life and/or injury to civilians. Civilian casualties thus are not only the possible but, in some cases, the lawful outcome of a military operation. However, Article 75(8) Additional Protocol I specifies that the guarantees provided by the Protocol cannot limit or infringe "*any other more favourable provision granting greater protection, under any applicable rules of international law*". The scope of protection according to this clause can be wider and therefore LAWs and military devices with facial recognition, when it comes to prohibition of murder, mutilation and cruel treatment, might have to meet higher standards.

This is important because applying a proportionality test to facial recognition reveals some potential challenges. Imagine that a new fully autonomous machine gun with facial recognition (or, in fact, any biometric identification software) was developed, passed all stages of legal tests, was placed on the bulwark and launched. Now, suppose that a small bug in the system was overlooked in the process of installation. One night a medical worker carrying out his/her duties was misidentified by our machine gun on the approach of bulwark and shot to death. Can a lawyer, building a defence case, with 100% confidence claim that this death was an incidental loss? We can play with factual circumstances more or less accurately adjusting this story to the regulatory framework but the puzzle itself remains. Will mistakes in the algorithm influence qualification of the deaths during the hostilities, knowing that the main idea behind the LAWs with facial recognition is to identify a particular person and to kill only this particular person? One military objective was supposed to be killed, one innocent civilian actually died. One might say, since the military advantage was not gained hence the death of a civilian is not incidental, it is a war crime. But what if it was one civilian among 100 correctly identified

[12] ICRC concluded that even "[*i]f a weapon is found to be illegal by a State, this does not by itself create a mandatory rule of international law vis-à-vis third parties, even for the State first mentioned...*" (see footnote 12)

[13] Article 75(2)(a)

[14] Article 4(2)(a)

[15] Article 85(3)(b) Additional Protocol I, Article 3(3)(c) Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II) (as amended on 3 May 1996), 10 October 1980

enemies? Does proportion play a role in a qualification if machine gun will continue killing people until the bug is found and fixed?

### 1.2. Principle of distinction

Let us turn to the principle of distinction between civilian population and combatants under art. 48 Additional Protocol I and customary rules of IHL. For the purpose of distinguishment combatants, civil defence, medical staff must all bear special signs (the rule established e.g. in art. 12 Additional Protocol II) or, where applicable to some of them, carry arms openly (art. 44(3) Additional Protocol II). However, the battlefield never allows having 100% clarity on who stands in front of you: civilian, who accidentally picked up a gun, or combatant, wearing a sign of Red Crescent to trick belligerent party. When a soldier makes evaluations many factors play their role: his/her experience, body language, signs, surroundings, aural characteristics, etc. While several seconds might be enough for a soldier to make a correct decision simply going "*with a gut*", facial recognition software or device delivers a decision based only on a match between an image and facial or physical features. The task becomes even more complicated when we speculate about multiple persons verification or identical twins. What about some non-physical factors, like a person's (absence of) intent to attack or signs of mental illnesses[16]? Those possibilities, of course, can be overlooked by a soldier too, but if taken into account, can also change an approach to a military operation and its outcome.

To pass the distinction test, a weapon or a device with facial recognition should be advanced to the point it would be able to take into account not only biometric characteristics but also additional "*markers*" proving that the person identified was not confused with a civilian looking alike or is not *hors de combat*. Another pitfall to keep in mind is the distance of verification. Not every intelligence with a military device with facial recognition allows reaching a distance close enough for a high accuracy match.

### 1.3. Principle of precaution in the attack

The principle of distinction goes hand in hand with the obligation to take necessary precautions in the attack to either exclude or minimize civilian casualties. Under art. 57(2)(a) Additional Protocol I those precautions consist of:

i) feasible actions in order to verify a target;
ii) feasible precautions in the choice of means and methods of attack;
iii) refrainment from an attack when such an attack is expected to cause incidental loss of civilian life or injury to civilians.

The first element is particularly important to fulfil when military devices with facial recognition are being deployed to identify a target, second - before attacks, which are planned to be carried out with the help of the LAWs with facial recognition and the third must be fulfilled when

[16] Ibid., 8, pp.350–378; p. 364

deploying both. However, these 3 elements, which supposed to provide guidance for senior military leadership, do not simplify the assessment.

During the discussion of the draft article, the words "*everything feasible*" were understood by some delegates as "*everything that was practicable or practically possible, taking into account all the circumstances at the time of attack, including those relevant to the success of military operations*" [17]. The interpretation of the article heavily relies on common sense and good faith of the parties[18]. It is presumed that a party will use all the means at its disposal to make an identification before attacking, of course within its own, subjective, understanding of such means. This also correlates with the provision of art. 3(2) of the Protocol II to the Convention on Certain Conventional Weapons prohibiting "*in all circumstances to direct weapons to which this Article applies, either in offence, defence or by way of reprisals, against the civilian population as such or against individual civilians*".

Moreover, paragraph 2(a)(ii) of art. 57 is not without its flaws. Although suggesting to be demanding in choosing means and methods of attack, it does not prohibit any particular means or methods *per se*. Additionally, there is always a possibility of a performance error, but is simply a possibility of an error enough to invoke a third component and refrain from an attack? How much testing of LAWs and military devices with facial recognition should be done to negate expected incidental losses of civilian life or injury to civilians?

The existence of the principle is important but broad requirements leave a room for manoeuvring in or avoiding complicated conformity review procedures when deploying discussed LAWs and military devices.

### 1.4. Indiscriminate attacks and weapons

The general prohibition of indiscriminate attacks and weapons is set out in art. 51(5)(b) Additional Protocol I and in art. 3(3) Protocol II to the Convention on Certain Conventional Weapons[19]. However, both articles basically encompass two principles, already mentioned above, being proportionality and precautions in the attack[20], and therefore do not require additional assessment.

Summing up all the legal provisions and principles of the IHL applicable to LAWs and military devices with facial recognition, a very frustrating conclusion can be drawn. There is no updated definition of military devices that would cover machines we put under scrutiny in this paper. It is true that they logically do not fully fall out of the regulation. Machine guns are still weapons, even with facial recognition on them. But existing flexible regulations do not take into account

[17] *Declarations and reservations made upon ratification of the 1977 Additional Protocol I* (1999), Ireland, para 6
[18] Ibid., 11, p. 682.
[19] Ibid., 12
[20] And ICRC in its commentary to art. 51 Additional Protocol I (see footnote 11) explicitly refers to art. 57 Additional Protocol I

that these weapons can be so developed as to formally comply with IHL. That is why assessment under art. 36 of the Additional Protocol I should not be conducted solely on the basis of IHL. Assessment should go beyond, consider more favourable treatment that might be offered, as Article 75(8) Additional Protocol I suggests. And here is where human rights law can provide additional "*bricks for the defence wall*"[21].



[21] Heyns, C. (2014) *Autonomous weapons systems and human rights law*. Presentation by state parties on the Convention on Certain Conventional Weapons, Geneva, p. 4

## 2. LAWs and military devices with facial recognition under the international human rights law

LAWs and devices with facial recognition in the existing literature and soft law on IHRL mostly discussed in the context of separate use by law enforcement agents[22] and counter-terrorism forces. Even so, IHRL protection does not cease to exist if we change the focus of discussion on the development of these weapons and devices for military purposes.

A well-known shortcoming of the system of guarantees under the IHRL is the disbalance of the IHRL instruments and institutions in the world, which offer greater protection on one geographical region (e.g. Europe, where human rights legislation operates on four levels: universal, CoE, the EU and constitutional) and almost none in another (e.g. Asia, where development of the human rights is limited to universal, weak ASEAN level and constitutional). During the application of IHL we do encounter the same problem but more on a state-by-state level rather than within the entire region.

Yet together, those systems can offer a mutually reinforcing framework for the assessment of the LAWs and devices with facial recognition on the stage of their design and development.

### 2.1. Human rights concerns about facial recognition technology

Human rights activists name a number of problems with the use of facial recognition primarily outside the military context. They claim that it is biasedly and discriminatively designed[23], erroneous[24], that gathered data are poorly protected from hacking[25], and that it infringes the right to private life[26]. Not every problem listed will be equally relevant for our assessment but the following must be taken into account.

#### 2.1.1. Technology bias, equality and discrimination issues

Equal protection against any discrimination is a human rights standard[27] everyone should have a possibility to rely on in any situation, during war and peace. The failure of facial recognition technology developers and law enforcement to uphold this standard in each and every case has drawn the attention of scholars and human rights defenders. Throughout the years, they have

[22] A/HRC/44/24, paras 24, 30 - 39, 53 - 54

[23] Buolamwini, J., et. al. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research*, [online] 81, pp.1–15. Available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [Accessed 22 Dec. 2020]. p. 1

[24] *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* FRA Focus. (n.d.). [online] EU FRA. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf [Accessed 22 Dec. 2020]. p. 4

[25] *Clearview AI: Face-collecting company database hacked*. (2020). [online] BBC News. Available at: https://www.bbc.com/news/technology-51658111 [Accessed 22 Dec. 2020].

[26] *Police use of facial recognition technology infringes European Convention on Human Rights* (2020). [online] Human Rights Law Centre. Available at: https://www.hrlc.org.au/human-rights-case-summaries/2020/8/28/police-use-of-facial-recognition-technology-infringes-european-convention-on-human-rights [Accessed 22 Dec. 2020].

[27] art. 26 ICCPR, art. 7 UDHR, art. 24 ACHR, art. 14 ECHR, art. 2 ACHPR

managed to comprehensively single out the various types of possible biases and their potential risks.

The first type of bias is a database bias or biased enrolment[28], which takes forms of underrepresentation or overrepresentation[29]. Both will not be relevant for our assessment.

The second type of bias is the identification bias, i.e. a demonstrably higher level of inaccuracy when matching female faces, people with dark skin[30] and young people[31]. The root cause of inaccuracy may hide in a "*training process*", when the developer of the technology uses a disproportionate number of photos of one racial/gender/age group, therefore causing algorithmic cross-race effect. Military staff using this technology may never find out that the problem was there since the beginning.

The third type of bias is human bias. The human element is inevitably a part of a decision-making process after the match is done by the algorithm (if we do not take into account potential human-out-of-the-loop LAWs, which will both identify a target and engage with it leaving for an operator only post-control functions). For example, criminal investigation process in the US is done with the help of Clearview AI requires investigating officer to make a personal check of the result and only then to act on it, if there are sufficient grounds to believe that the person identified is "*the guy*". The decision heavily relies on the decency of the person conducting the check. The possible negative outcome of bias human assessment needs no explanation. This type of bias calls into question the whole idea of the efficiency of the meaningful human control concept[32].



[28] Ruhrmann, H. (2019). *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement* [online] ResearchGate. Available at: https://www.researchgate.net/publication/340934371_Facing_the_Future_Protecting_Human_Rights_in_Policy_Strategies_for_Facial_Recognition_Technology_in_Law_Enforcement [Accessed 5 Jan. 2021], p. 28

[29] Ibid., 30

[30] Ibid., 25, p. 10

[31] Klare, B.F., et al. (2012). *Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security*, [online] 7(6), pp.1789–1801. Available at: http://openbiometrics.org/publications/klare2012demographics.pdf [Accessed 22 Dec. 2020]. p. 3

[32] *Killer Robots and the Concept of Meaningful Human Control*. (2016) [online] Human Rights Watch. Available at: https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control [Accessed 9 Jun. 2021].

### 2.1.2. Algorithmic errors and cybersecurity threats

Biases aside, algorithms (and machines in general) are vulnerable to malfunction. Cases of misidentification already occur in the US[33], the UK[34], Russia[35], and China[36]. False-positive and false negative results can in peaceful times lead to either persecution of an innocent person, omissions during an investigation or troubles with the border-control.

Facial recognition software and databases with biometric data are also exposed to hacker attacks. Malicious intrusions might aim to gather (biometric) data[37], sabotage identification system[38], cause algorithmic errors mentioned above, or have no aim at all - accidentally caught a notorious virus or warm destroys programs or files just because it was design to do so.

All of these potential and already appearing problems with facial recognition technology led to the push-back reaction from human rights defenders. 2020 was an important year for them: in July the first complaint to the European Court of Human Rights ("ECtHR") (and three sisters' system in general) against facial recognition and mass surveillance was submitted[39] and in August the UK court ruled that facial recognition is in violation of Article 8 of the European Convention on Human Rights ("ECHR") and national data protection laws[40]. While the first decision by the authoritative human rights institution on the use of technology in everyday life is yet to come, the same problems threaten to cause irreparable damage during hostilities.

## 2.2. International human rights law considerations on the military application of facial recognition

Before diving headlong into the analysis, it is worth mentioning that the practice of international institutions on the use of LAWs and military devices in general and in the context of hostilities in particular is quite modest. Moreover, it is hard to disagree with N. Melzer's observation that "*while the provisions of [IHRL] on the use of lethal force against individuals, and on humane treatment, may arguably be interpreted to accommodate certain military*

[33] *Lawsuit Claims Facial Recognition AI Sent the Wrong Man to Jail* (2020) [online] Futurism. Available at: https://futurism.com/the-byte/lawsuit-claims-facial-recognition-ai-sent-wrong-man-jail [Accessed 6 Jan. 2021].

[34] Fox, C. (2018). *Face recognition police tools "staggeringly inaccurate."* [online] BBC News. Available at: https://www.bbc.com/news/technology-44089161 [Accessed 6 Jan. 2021].

[35] *Жительницу Сахалина оштрафовали на 15 тысяч рублей за нарушение карантина. Из-за 61-процентного сходства с другой женщиной* (2020) [online] Meduza. Available at: https://meduza.io/news/2020/04/15/zhitelnitsu-sahalina-oshtrafovali-na-15-tysyach-rubley-za-narushenie-karantina-iz-za-61-protsentnogo-shodstva-s-drugoy-zhenschinoy [Accessed 6 Jan. 2021].

[36] Borak, M. (2019). *Man mistaken for his co-workers illustrates the flaws of facial recognition*. [online] South China Morning Post. Available at: https://www.scmp.com/abacus/tech/article/3029424/man-mistaken-his-co-workers-illustrates-flaws-facial-recognition [Accessed 7 Jan. 2021].

[37] Ibid., 24

[38] Hao, K. (2020). *The hack that could make face recognition think someone else is you*. [online] MIT Technology Review. Available at: https://www.technologyreview.com/2020/08/05/1006008/ai-face-recognition-hack-misidentifies-person/ [Accessed 8 Jan. 2021].

[39] *Moscow's Use of Facial Recognition Technology Challenged.* (2020). [online] Human Rights Watch. Available at: https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged [Accessed 6 Jan. 2021].

[40] R (Edward Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058, para 210

*operations, the enormous scale of devastation entailed by the conduct of hostilities in major armed conflicts simply exceeds the regulatory capacities of [IHRL]*"[41]. Therefore one should keep in mind that the assessment from the IHRL point of view will be predictive and based on the rules and tests applied mostly to law enforcement and cases based on the action of states under art. 51 of the Universal Declaration of Human Rights ("UDHR").

### 2.2.1. Right to life

Any possibility of death on the battlefield, stemming from previously mentioned deficiencies in facial recognition software, will inevitably put forward a question of whether the right to life under IHRL[42] is threatened.

The right to life under IHRL is well-known to be not so much of an absolute. While IHL talks in categories of "*civilian casualties*"[43] and "*incidental losses*", IHRL follows the "*intention*" and "*arbitrariness*" approach, allowing resorting to deprivation of life in exceptional circumstances. This slight contradiction in the approaches of two branches of international law nevertheless does not, according to the UN Human Rights Committee, prevent them from being "*complementary, not mutually exclusive*"[44]. The interaction between the basic rules of IHL and IHRL when it comes to the right to life has been defined as follows:

"*[u]se of lethal force consistent with international humanitarian law and other applicable international law norms is, in general, not arbitrary*"[45].

As the language above indicates, there exists a "loop" between the provisions of art. 36 Additional Protocol I and the interpretation of art. 6 International Covenant on Civil and Political Rights ("ICCPR"). The former sends those who are interested in the search for conformity to the latter and the latter sends them back. When we finally step out of this loop, agreeing that IHL is not enough to conduct a proper assessment of LAWs and military devices with facial recognition, we might need some objective criteria (test) in order to run a compatibility check with the IHRL.

In paragraph 65 of the General Comment no. 36 the Human Rights Committee[46] has stated that when a weapon 1) lacks in human compassion and judgment and 2) raises difficult legal and ethical questions concerning the right to life, including questions relating to legal responsibility for their use, it should not be developed and put into operation. Thus, the question to consider here is whether embedding facial recognition into LAWs and military devices means making a step towards the fulfilment of the criteria or *vice versa*?

[41] Melzer, N. (2008). *Targeted killing in international law*, Oxford: Oxford University Press., pp.384-385
[42] art. 2 ECHR, art. 3 UDHR, art. 6(1) ICCPR, art. 4 ACHPR, art. 4 ACHR
[43] e.g. art. 57(4) of the 1977 Additional Protocol I
[44] UN Human Rights Committee (HRC), General comment no. 36, Article 6 (Right to Life), CCPR/C/GC/35,3, September 2019, para 64. Joint application of these two branches of law further reaffirmed by the ECtHR in Hassan v. the UK, ECtHR GC, Application no. 29750/09, Judgment of 16 September 2014, para 104
[45] Ibid., 48, para 44
[46] Ibid., 48, para 65

The arguments militating in favour of the deployment of facial recognition LAWs revolve around the idea of their enhanced accuracy. LAWs indeed may lack in compassion but bear human judgement in the form of facial recognition itself. And if the whole process includes additional human evaluation, the weapon might be considered to meet this criterion. Facial recognition, one may add, is actually a way out of a difficult legal question - it resolves the problem with the indiscriminate character of LAWs. Ethical concerns will never appear as weapons with facial recognition will strike, without prejudice, a pre-configured target after it is carefully determined by the military officers in headquarters. The human eye will make an extra comparison of two images raising accuracy to the 99% level.

However, human compassion and judgement are out of the way if LAWs and military devices with facial recognition will be fully, from deployment up until the decision to strike, automatic. The ethical question then would be: how can fully automatic machine make identification in situations where subjective element might play a role in the decision to strike or to abstain?

Regional and international IHRL institutions developed some jurisprudence on the second component of the rule of conformity with IHRL. They established comprehensive tests to be applied when ruling on a situation or a case where the use of lethal force is involved. These tests to some extent can constitute part of the assessment under art. 36 Additional Protocol I. And modelling situations of the potential application of LAWs and military devices with facial recognition on the battlefield might tell us if the machines are ready to be deployed.

Regardless of which notion IHRL institutions refer to, arbitrariness or intent, the test in various IHRL systems consists pretty much of the same four cumulative elements[47]:

1. Sufficient domestic legal framework

The ECtHR in 2005 in the case *Nachova and others v. Bulgaria,* ruling on the use of firearms by military police stated that *"... Article 2 implies a primary duty on the State to secure the right to life by putting in place an appropriate legal and administrative framework defining the limited circumstances in which law enforcement officials may use force and firearms..."*[48]. The position was reaffirmation of the principle previously established in the case *Isayeva, Yusupova and Bazayeva v. Russia* in the context of a war in Chechnya in 1999[49].

The Inter-American Court of Human Rights ("IACtHR) in the case *Tarazona Arrieta et al. v. Peru* in 2014 looked into the issue in the military context stating that "*adequate internal*

[47] IACtHR also identifies principle of exceptionality. See e.g. Zambrano Velez v. Ecuador, IACtHR, Judgement of 4 July 2007, para 83

[48] Nachova and others v. Bulgaria, ECtHR GC, Applications nos. 43577/98 and 43579/98, Judgment of 29 March 2011, para 96

[49] Isayeva, Yusupova and Bazayeva v. Russia, ECtHR, Application no. 57947/00, 57948/00 and 57949/00, Judgment of 24 February 2005, para 198

*regulations to prevent and circumvent the use of force*"[50] should be adopted including "*safeguards to prevent the lethal use of force*"[51].

This element is a guarantee of legality of the use of LAWs and military devices with facial recognition. Domestic legislation in our view should be expected to cover as a minimum:

- standards of designing, developing and testing of LAWs and military devices with facial recognition, including guidelines of ethical committee's check;
- circumstances of the military operations during which they can be used;
- conditions under which they can be used;
- military officials authorised to use LAWs and military devices with facial recognition (relevant training should be provided);
- situations when military official should refrain from using them;
- course of action in case of malfunctions, etc.

In the absence of sufficient domestic legal framework machines discussed might not pass the test because states have no *carte blanche* in actions when it comes to the right to life[52]. Deprivation of life should always be conditioned to a narrow list of situations and the list itself should be clear and transparent as any law.

2. Necessity

Three aspects of necessity (quantitative, qualitative and temporal), that N. Melzer describes basing distinction on the practice of human rights institutions[53], are undoubtedly important to take into account. However, all of them can be applied only when dealing with known circumstances of a particular situation (case). To make that kind of assessment one should know the legitimate aim of the operation during which LAWs and military devices are planned to be used (quantitative necessity), degree or the manner of their use (qualitative necessity) and if their use was absolutely necessary at the very moment when the operation was run (temporal necessity).

Yet, the necessity element still plays a role when providing training for military personnel. The operators of the LAWs and military devices with facial recognition should be properly qualified "*to assess whether or not there is an absolute necessity to use firearms, not only on the basis of the letter of the relevant regulations, but also with due regard to the pre-eminence of respect for human life as a fundamental value"*[54].

3. Proportionality

[50] Tarazona Arrieta et al. v. Peru, IACtHR, Judgment of 14 October 2014, para 165
[51] Ibid., 54, para 167
[52] Ibid., 48, para 3
[53] Ibid., 45, pp. 102, 117
[54] Esmukhambetov and Others v. Russia, ECtHR, Application no. 23445/03, Judgment of 29 March 2011, para 139

As much as necessity, fulfilment of the proportionality requirement in the context of security operations or (un)acknowledged (non-)international armed conflicts is always a subject of a very strict scrutiny by the human rights courts and institutions.

For instance, the IACtHR requires[55] state officials before resorting to the use of force to give an evaluation of the severity of situation, including "*among other circumstances, … the level of intensity and danger of the threat; the attitude of the individual; the conditions of the surrounding area, and the means available to the agent to deal with the specific situation*". In addition, it is expected of state officials "*to use the lowest level of force required to achieve the legitimate purpose sought*".

The ECtHR meanwhile operates with the notion of "*strict proportionality*"[56]. Article 2(2) ECHR provides a limited number of situations when deprivation of life does not constitute a violation of the Convention. However, those situations either do not provide a room big enough to fit the use of lethal force during military operations or do not cover them at all. Thus, the Court had to tacitly depart from a traditional understanding of these situations and accept, that military objectives can be a justification for deprivation of life via the use of lethal force. It, nevertheless, did not agree to lower the threshold of protection. Carrying its assessment the Court will be interested, for example, in the plan of the operation, if the "*assessment of the perceived threats and constraints had been made, or what other weapons or tactics had been*"[57] used. The Court will also look into "*where deliberate lethal force is used, taking into consideration not only the actions of the agents of the State who actually administer the force but also all the surrounding circumstances including such matters as the planning and control of the actions under examination*"[58].

The proportionality test in IHRL in this context is not so detailed and coherent as in IHL or in IHRL jurisprudence with regards to law enforcement activities. However, the fact that its aspects are stemming from the case-law rather than conventional provisions means that proportionality assessment can be wider and can adjust to the new types of weapons and technologies. On the other hand, assessment of the pre-developed and pre-deployed LAWs and military devices with facial recognition based on ever-evolving jurisprudence becomes a challenge for the lawyers in the military uniform. Still, some developed principles can already be used for the purposes of art. 36 Additional Protocol I.

For instance, as was provided by the IACtHR and mentioned above, when planning a military operation, one should consider the attitude of the individual. This condition almost excludes the possibility to use the human-out-of-the-loop type of LAWs with facial recognition. At least

[55] Landaeta Mejias Brothers et al v. Venezuela, IACtHR, Judgment of 27 August 2014, para 136
[56] see e.g. Khatsiyeva and others v. Russia, ECtHR, Application no. 5108/02, Judgment of 17 January 2008, para 129
[57] Ibid., 53, para 175
[58] McCann and Others v United Kingdom, ECtHR, Application No 18984/91, Judgment of 27 September 1995, paras. 149–150

as long as the technology did not evolve so far as to able to make conclusions about people's intentions basing itself on analysis of body language, behaviour, etc. Then there is a consideration about any other means available to achieve the purpose sought[59]. There is no such thing as a "safe" weapon or military device. Thus, sometimes using other, safer means would mean not resorting to the LAWs and military devices with facial recognition at all. For example, during night operations, when the accuracy rate falls drastically. The same example illustrates well also the necessity to take into consideration constraints and all the surrounding circumstances, required by the ECtHR.

Proportionality test under IHRL, in general, is a tricky thing to apply in the context of hostilities. Human rights courts intentionally abstain from calling situations revised by them an armed conflict and try to pave the way for IHRL, which allows for more flexible application of the proportionality test. The existence of an actual threat within IHRL's will be the key to assess if the proportionality test is passed because, unlike IHL, it does not distinguish combatants and non-combatants, equally protecting soldiers and civilians.

4. Precaution

The understanding of precautions under IHRL also cannot be fully compatible with the context of hostilities. IHRL usually requires e.g. necessity to make a prior warning[60] or offer an opportunity to surrender[61]. That is something that military commanders cannot always afford when carrying military operations. However, this is standards e.g. of the ECtHR. As N. Melzer put it, "*[a] deprivation of life, even if absolutely necessary in the immediate circumstances of a case, violates Article 2 ECHR if… operation or a general security set-up... is not planned, organized and controlled so as to minimize, to the greatest extent possible, recourse to lethal force*". To keep the balance with the "*greatest extent possible*" requirement the Court introduced the warning against imposing an unrealistic burden on the state[62].

For the assessment of pre-deployed LAWs with facial recognition this does not mean a lot. However, there are also precaution rules governing intelligence, which can be important for military devices with facial recognition. The Court in its case-law on counter-terrorism operations agreed that "*intelligence assessments might, in some respects at least, be erroneous*" but the possibility of an error is not a justification to "*automatic recourse to lethal force*"[63]. What might justify the use of lethal force is "*an honest belief which is perceived, for good reasons, to be valid at the time but which subsequently turns out to be mistaken*"[64].

What this basically means is that blind reliance on intelligence gathered by the military devices with facial recognition in situations when errors resulting in deaths occur, the ECtHR at least

[59] Ibid., 55, para 136
[60] Alejandre v. Republic of Cuba, IACmHR, Case 11.589, Report Nº 86/99 of 29 September 1999, para 42
[61] Camargo v. Colombia, Human Rights Committee, Communication No. 45/1979; U.N. Doc. CCPR/C/15/D/45/1979, Views of 31 March 1982, para 13.2
[62] see e.g. Ibid., 62, para 200
[63] Ibid., 62, para 213
[64] Ibid., 62, para 200

will find a violation of the right to life. Therefore a safeguard mechanism required to use those military devices. This mechanism can be technically placed in the military device (e.g. approval of the match by the military personnel) or can be established in the legal framework (e.g. via putting an obligation on the military personnel to check the intelligence sent by the military device).

All the four elements of the test might be in one way or another applicable to LAWs or military devices with facial recognition. There are certain elements, like proportionality or precaution, which can in the likeness of rules applied to law enforcement and counter-terrorism operations serve as an additional "safety net" for the assessment under art. 36 Additional Protocol I. But for now, the case-law on the right to life has not very broadly and coherently developed rules directly applied to the use of various LAWs and military devices. While this is yet to be crystalized, principles existing in the case-law cannot be disregarded. Taking it even further, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions analysing an impact on the right to life proposed "*to declare and implement national moratoria on at least the testing, production, assembly, transfer, acquisition, deployment and use of LARs*"[65], which includes also those with facial recognition.

### 2.2.2. Prohibition of cruel, inhuman or degrading treatment

Prohibition of torture, inhuman or degrading treatment or punishment[66] will come into play if LAWs and military devices with facial recognition, will be aimed to cause life-threatening and non-life-threatening injuries[67] to a military objective or to non-combatants.

Conformity check for violation of this human rights provision will be based on the same four elements described in the previous section. The ECtHR confirmed this in the case *Abdullah Yaşa and Others v. Turkey*:

"*…Given the dangerous nature of the equipment used, the Court considers that its case-law on the use of potentially lethal force should apply in the instant case mutatis mutandis. It should be noted in this connection that in the context of Article 2 of the Convention, the Court has always held that unregulated and arbitrary action by State agents is incompatible with effective respect for human rights… The same applies to Article 3 of the Convention. This means that police operations … should not only be authorised but should also be sufficiently delimited by domestic law, under a system of adequate and effective safeguards against arbitrary action, abuse of force and avoidable accidents.*"[68]

[65] A/HRC/23/47, para 113, which also provided a definition of "LARs" as lethal autonomous robotics
[66] art. 5 UDHR, art. 7 ICCPR, art. 3 ECHR, art. 5 ACHPR, art. 5 ACHR
[67] It is worth noting that the practice of the ECtHR can consider a case with the lethal outcome to fall within art. 3 of the ECHR rather than art. 2 (right to life)
[68] Abdullah Yaşa and Others v. Turkey, ECtHR, Application no. 44827/08, Judgement of 16 July 2013, para 43

Running the conformity check of the use of LAWs and military devices with facial recognition against provisions on the prohibition of ill-treatment requires placing possible consequences under one of three forms of ill-treatment.

An interesting approach to this task was suggested by C. Heyns. He argued that "*application of force by a machine to a human being ... is inherently, or by definition*" amounts to inhuman treatment simply because the decision is made not by a human being[69]. He brought the use of trained dogs against people as a similar example showing that both means lack control and can result in physical harm.

To simply put doubts about placing the use of LAWs and military devices with facial recognition within those three to rest, some short considerations should be given to other forms of ill-treatment. We can put aside the torture as it is as a minimum an "*act inflicted on a person for such purposes as obtaining from him or a third person information or a confession…*"[70]. This element, distinguishing torture from other forms of ill-treatment, in this case is simply absent. LAWs and devices with facial recognition are not designed to perform functions of some "*torture devices*" and using them for such purposes is pointless. One can of course argue, that if the weapon will be used in a particularly intense and cruel way, its application might reach a threshold of severity to constitute torture, but on the initial stage of assessment of the weapon bearing in mind its primary purpose, such assumption would be far-fetched. Apart from the fact that degrading treatment is the least harmful form of ill-treatment, it is rarely associated with cases involving severe traumas from lethal weapons. Although injuries from LAWs and military devices with facial recognition will cause distress to a person, its severity, especially taking hostile context, will exceed simply "*feelings of fear, anguish and inferiority capable of humiliating and debasing them and possibly breaking their physical or moral resistance*"[71].

The possibility to classify the use of LAWs and military devices with facial recognition on the stage of development as inhuman treatment, let alone to declare indisputably that such LAWs and devices are actually in violation of the prohibition of ill-treatment, is highly questionable. However, when we talk about field application, there is a high probability that if they (being a type of the lethal force) will be used without the necessity principle taken into consideration, it automatically will be considered to be a violation[72].

[69] Ibid., 8, pp.350–378; p. 363 (footnotes)

[70] UN General Assembly, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 10 December 1984, United Nations, Treaty Series, vol. 1465, p. 85

[71] Ireland v. the UK, ECtHR, Application no. 5310/71, Judgement of 18 January 1978, para 167

[72] Bouyid v. Belgium, ECtHR GC, Application no. 23380/09, Judgment of 28 September 2015, paras 88, 100; Barrios Family v. Venezuela, IACtHR, Judgment of 24 November 2011, para 52

### 2.2.3. Principle of non-discrimination

Although considered to be an autonomous right[73], in the process of evaluation of potential situations, non-discrimination principle[74] will traditionally be tied to the rights mentioned above. It offers broader protection under IHRL but when it comes to hostilities concerns are mainly centred around identification bias and human bias.

Human bias claims under provisions on the prohibition of discrimination are quite simple. When making a decision together with the machine or verifying a face matched, a person controlling a partially autonomous weapon or a military device ("the operator") must do it without any prejudice on the grounds listed in international or regional IHRL instruments. The operator will essentially have control over one's life. And the probability that military personnel might be guided by hatred towards e.g. a particular nationals or race is very high. Dehumanization of the enemy and development of a sense of antipathy had been proven to be a part of any war. It is almost impossible to stay objective when the only thing you see is a fighter of an army responsible for the death of your friend. The variations of the motives behind human bias are many. The establishment of these motives will be a tricky thing to do. ECtHR, for instance, requires a convincing *prima facie* case to be made in order to invoke Article 14 of the ECHR[75]. In jurisprudence discrimination can be proven by oral statements or comments made with respect to a victim[76]. However, providing some evidence of bias in the situation where a victim and an alleged perpetrator are not in direct contact with each other will be almost impossible. The operator might as well blame death of a civilian on deficiencies of the algorithm. When human bias cannot be fully avoided it can be at least reduced by choosing the operators carefully and providing them sufficient training as well as psychological support.

Identification bias is a deficiency of a programming or a training process. It may not be dependent on the operator but the state using technology will still be responsible for deploying discriminative LAWs or military devices. The conformity check here will heavily rely on the debate between those who will say that even the smallest possibility of identification bias must be enough to discourage the military from using LAWs and military devices with facial recognition and those who will allow for some percentage of possible biased inaccuracy. The level of the development of technology will play a crucial role here.

Unlike the right to life and prohibition of ill-treatment, there are no criteria to apply when running a conformity check of the LAWs and military devices with the prohibition of discrimination. Two elements, legitimate aim and proportionality, will make no sense in this context. It is hard to imagine a situation where discrimination on the battlefield by using LAWs and military devices will pursue an aim legitimate under IHRL. Proportionality is a requirement arising from the existence of a legitimate aim. Thus, the whole assessment under provisions on

[73] UN Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination, E/C.12/GC/186, 10 November 1989, para 12
[74] art. 7 UDHR, art. 14 ECHR, art. 2 ACHPR, art. 1 ACHR
[75] Adzhigitova and Others v. Russia, ECtHR, Applications nos. 40165/07 and 2593/08, Judgment of 22 June 2021, para 271
[76] Ibid., 78, para 273

the prohibition of discrimination will be a matter of weighting if quite real concerns about human and identification biases are enough to stop the development of LAWs and military devices with facial recognition.

IHRL in its current state of interpretation is not comprehensive enough to provide clear criteria for the assessment under Article 36 Additional Protocol I. However, several principles and guiding elements crystalized enough already to be extracted from the jurisprudence of the human rights institutions and their commentaries. The key to such assessment is, as a minimum, the existence of a sufficient legal framework and training programs envisaging modes of dealing with potential deficiencies of facial recognition technology and biases. The position that there is already enough evidence that the technology being put on LAWs and military devices harmful and unpredictable to see the light also has a right to exist, of course. What is certain is that IHRL cannot be ignored in the whole process of assessment.

## Conclusion

As we saw from the analysis, LAWs and military devices with facial recognition are controversial technologies. Technologies, that are also instruments of life and death decisions and therefore an object of particularly high scrutiny on the development stage. The legal basis for this scrutiny is established by the IHL but cannot be limited to it.

Scarce provisions of IHL require conformity with at least four customary law principles, being the prohibition of violence to life and person, the distinction between civilians and combatants, precautions in the attack and prohibition to resort to attacks and weapons that are indiscriminate. LAWs and military devices with facial recognition are very close to being consistent with those principles. Mainly because the characteristics of facial recognition as a technology enhancing accuracy fall under desirable characteristics of weapons described in IHL provisions. However, these provisions are (arguably) outdated and therefore were not able to foresee drastic technological changes and new challenges stemming from them. For this reason, and because human rights defenders have separately from military application context established problems with facial recognition technology per se, it is important to study the LAWs and military devices from the IHRL point of view.

Under IHRL several concerns closely tight up to the potential infringement of the right to life, prohibition of ill-treatment and non-discrimination can be raised. Although IHRL is more up to date in its application, it cannot provide comprehensive assessment tests on LAWs and military devices with facial recognition just yet. What we can rely on is jurisprudence on the use of force.

What can be derived from the mutual application of provisions of IHL and IHRL on the stage of development of discussed LAWs and military devices, is the necessity, as a minimum to provide an adequate legal framework for the future use of these technologies and sufficient training for the operators. Later on, in the case and if these LAWs and military devices will be developed and deployed, other principles, like proportionality and precautions will come into play.

## Bibliography


**International instruments:**

- Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5;
- League of Arab States, Arab Charter on Human Rights, 15 September 1994;
- Organization of African Unity, African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982);
- Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969;
- United Nations, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977;
- United Nations, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II) (as amended on 3 May 1996), 10 October 1980;
- UN General Assembly, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 10 December 1984;
- United Nations General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III);
- United Nations General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171;

**Official comments**

- Declarations and reservations made upon ratification of the 1977 Additional Protocol I (1999), Ireland;
- International Committee of the Red Cross, Treaties, States parties, and Commentaries - Additional Protocol (I) to the Geneva Conventions, 1977 - 36 - New weapons - Commentary of 1987;
- United Nations Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination, 10 November 1989, E/C.12/GC/186;
- United Nations Human Rights Committee (HRC), General comment no. 36, Article 6 (Right to Life), 3 September 2019, CCPR/C/GC/35;

**Reports by authoritative institutions:**

- A/HRC/44/24: "Impact of new technologies on the promotion and protection of human rights in the context of assemblies – Report of the United Nations High Commissioner for Human Rights";
- A/HRC/23/47: "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns";
- Facial recognition technology: fundamental rights considerations in the context of law enforcement. FRA Focus. (n.d.). [online] EU FRA. Available at:

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf;

**Case-law:**

**ECtHR**

- Abdullah Yaşa and Others v. Turkey, Application no. 44827/08, Judgement of 16 July 2013;
- Adzhigitova and Others v. Russia, Applications nos. 40165/07 and 2593/08, Judgment of 22 June 2021
- Bouyid v. Belgium, Application no. 23380/09, Judgment of 28 September 2015;
- Esmukhambetov and Others v. Russia, Application no. 23445/03, Judgement of 29 March 2011;
- Hassan v. the UK, Application no. 29750/09, Judgment of 16 September 2014;
- Ireland v. the UK, Application no. 5310/71, Judgement of 18 January 1978;
- Isayeva, Yusupova and Bazayeva v. Russia, Application no. 57947/00, 57948/00 and 57949/00, Judgement of 24 February 2005;
- Khatsiyeva and others v. Russia, Application no. 5108/02, Judgment of 17 January 2008;
- McCann and Others v United Kingdom, Application No 18984/91, Judgment of 27 September 1995;
- Nachova and others v. Bulgaria, Applications nos. 43577/98 and 43579/98, Judgement of 29 March 2011;

**IACtHR and IACmHR:**

- Alejandre v. Republic of Cuba, Case 11.589, Report Nº 86/99 of 29 September 1999;
- Barrios Family v. Venezuela, Judgment of 24 November 2011;
- Landaeta Mejias Brothers et al v. Venezuela, Judgment of 27 August 2014;
- Tarazona Arrieta et al. v. Peru, Judgement of 14 October 2014;
- Zambrano Velez v. Ecuador, Judgement of 4 July 2007;

**Human Rights Committee**

- Camargo v. Colombia, Communication No. 45/1979; U.N. Doc. CCPR/C/15/D/45/1979, Views of 31 March 1982;

**National courts**

- R (Edward Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058

**Scholarly literature**:

- Heyns, C. (2016). Human Rights and the use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement. Human Rights Quarterly, 38(2), pp.350–378;
- Hu, M. et. al (2019). Read + Verify: Machine Reading Comprehension with Unanswerable Questions. Proceedings of the AAAI Conference on Artificial Intelligence;
- Buolamwini, J., et al. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research;
- Ruhrmann, H. (2019). Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement;
- Klare, B.F., et al. (2012). Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security;
- Melzer, N. (2008) Targeted killing in international law, Oxford: Oxford University Press;

**Literary works:**

- Shakespeare, W. (1623) Macbeth. Ware, England: Wordsworth Editions. Modern ed. of 1992. Scene VII, act 1.

**Online publications and media reports:**

- Borak, M. (2019). Man mistaken for his co-workers illustrates the flaws of facial recognition. [online] South China Morning Post. Available at: https://www.scmp.com/abacus/tech/article/3029424/man-mistaken-his-co-workers-illustrates-flaws-facial-recognition;
- Buolamwini, J., et. al. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification *. Proceedings of Machine Learning Research, [online] 81, pp.1–15. Available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf;
- Clearview AI: Face-collecting company database hacked. (2020). [online] BBC News. Available at: https://www.bbc.com/news/technology-51658111;
- Cox, M. (2019). Army's Next Infantry Weapon Could Have Facial-Recognition Technology. [online] Military.com. Available at: https://www.military.com/daily-news/2019/06/01/armys-next-infantry-weapon-could-have-facial-recognition-technology.html;
- Fox, C. (2018). Face recognition police tools "staggeringly inaccurate." [online] BBC News. Available at: https://www.bbc.com/news/technology-44089161;
- Gershgorn, D. (2020). The Military Is Building Long-Range Facial Recognition That Works in the Dark. [online] Medium. Available at: https://onezero.medium.com/the-military-is-building-long-range-facial-recognition-that-works-in-the-dark-4f752fa713e6;
- Gnaedinger, A. (2006). Is IHL still relevant in a post-9/11 world? - ICRC. [online] icrc.org. Available at: https://www.icrc.org/en/doc/resources/documents/article/other/ihl-article-300906.htm;

- Hao, K. (2020). The hack that could make face recognition think someone else is you. [online] MIT Technology Review. Available at: https://www.technologyreview.com/2020/08/05/1006008/ai-face-recognition-hack-misidentifies-person/;
- Hambling, D. (2020). US military face recognition system could work from 1 kilometre away. [online] New Scientist. Available at: https://www.newscientist.com/article/2233639-us-military-face-recognition-system-could-work-from-1-kilometre-away/;
- Heyns, C. (2014) Autonomous weapons systems and human rights law. Presentation by state parties on the Convention on Certain Conventional Weapons, Geneva [online] icrc.org. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj096PrjL_xAhUpg_0HHS-VAJUQFjABegQIBBAD&url=https%3A%2F%2Fwww.icrc.org%2Fen%2Fdownload%2Ffile%2F1707%2F4221-002-autonomous-weapons-systems-full-report.pdf&usg=AOvVaw1JixkHVpPvSagMFYBfmWVS;
- Iran scientist "killed by remote-controlled weapon." (2020). [online] BBC News. Available at: https://www.bbc.com/news/world-middle-east-55128970;
- Killer Robots and the Concept of Meaningful Human Control. (2016) [online] Human Rights Watch. Available at: https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control;
- Klare, B.F., et al. (2012). Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security, [online] 7(6), pp.1789–1801. Available at: http://openbiometrics.org/publications/klare2012demographics.pdf;
- Lawsuit Claims Facial Recognition AI Sent the Wrong Man to Jail (2020). [online] Futurism. Available at: https://futurism.com/the-byte/lawsuit-claims-facial-recognition-ai-sent-wrong-man-jail;
- Michel A.H. (2021). [Twitter] 7 Dec. "My breakdown of the technical credibility of #Fakhrizadeh attack claims [...]" [online] Available at: https://twitter.com/WriteArthur/status/1335943421803048964;
- Moscow's Use of Facial Recognition Technology Challenged. (2020). [online] Human Rights Watch. Available at: https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged;
- Police use of facial recognition technology infringes European Convention on Human Rights (2020). [online] Human Rights Law Centre. Available at: https://www.hrlc.org.au/human-rights-case-summaries/2020/8/28/police-use-of-facial-recognition-technology-infringes-european-convention-on-human-rights;
- Ruhrmann, H. (2019). Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement [online] ResearchGate. Available at: https://www.researchgate.net/publication/340934371_Facing_the_Future_Protecting_Human_Rights_in_Policy_Strategies_for_Facial_Recognition_Technology_in_Law_Enforcement;

- Жительницу Сахалина оштрафовали на 15 тысяч рублей за нарушение карантина. Из-за 61-процентного сходства с другой женщиной (2020) [online] Meduza. Available at: https://meduza.io/news/2020/04/15/zhitelnitsu-sahalina-oshtrafovali-na-15-tysyach-rubley-za-narushenie-karantina-iz-za-61-protsentnogo-shodstva-s-drugoy-zhenschinoy.