Orwellian nightmares and drone policing in Chilean municipalities: Legality, surveillance and the politics of low cost

Pablo Contreras
Universidad Autónoma de Chile (Chile)

Received: October 10, 2020 | Accepted: May 5, 2021 | Revised: June 1, 2021

How to cite: Contreras, Pablo. "Orwellian nightmares and drone policing in Chilean Municipalities: legality, surveillance and the politics of low cost". *Latin American Law Review*, no. 07 (2021): 61-80, doi: https://doi.org/10.29263/lar07.2021.04.

Abstract

This paper addresses video surveillance of Chilean municipalities using drones as a low-cost policing response to urban insecurity and its impact on the right to privacy and personal data protection. The text explains the municipal police powers that have been invoked to uphold the legality of video surveillance at the local level. In examining four municipal cases, it looks at how surveillance is being carried out with drones and how this has been supervised by the competent authorities, concluding that there are real risks to privacy in the operation of surveillance systems. To this end, the issue is contrasted with the applicable regulatory standards and comparative solutions. Chile lacks specific regulations for video surveillance and a robust legal framework to protect personal data. The paper also evaluates the action of courts that have legitimized surveillance, even without a legal basis, concluding that the combination of low-cost and highly intrusive technologies and the lack of an adequate legal framework creates a significant threat to the exercise of privacy and personal data protection at municipal level.

Keywords

Video surveillance; drones; privacy; data protection; Chile.

---

* LL.M. and S.J.D., Northwestern University. Associate professor of Law at Universidad Autónoma de Chile. Santiago de Chile, Chile. ORCID ID https://orcid.org/0000-0002-1131-182X. ✉ pablo.contreras@uautonoma.cl.

Research financed by ANID, Fondecyt de Iniciación No. 11180218. Every Spanish to English translations in this article, like citations to books or papers, are the author's, unless otherwise indicated. I am grateful to Carlos Díaz for his research assistance, Pablo Viollier for facilitating information obtained in surveillance matters, Viviana Ponce de León for her critical remarks, and Luis Eslava who carefully reviewed the paper and made enlightening suggestions. All errors are mine.

Pesadillas orwellianas y patrullaje de drones en municipios chilenos: Legalidad, video vigilancia y la política de bajo costo

Resumen

El texto aborda el problema de la video vigilancia a través de drones por municipios chilenos, como una respuesta de bajo costo frente a la inseguridad urbana, y su impacto en el derecho a la privacidad y a la protección de datos personales. El texto explica las facultades de policía municipal que se han invocado para sostener la legalidad de la video vigilancia a nivel local. Al examinar cuatro casos municipales, se comprueba cómo se está llevando a cabo la videovigilancia con drones y cómo ha sido supervisada por las autoridades competentes, llegando a la conclusión de que existen riesgos reales para la privacidad en el funcionamiento de los sistemas de vigilancia. Para ello, se contrasta con los estándares normativos aplicables y las soluciones comparadas. Chile carece de una regulación específica de la videovigilancia y de un marco legal robusto de protección de datos personales. El texto también evalúa la acción de los tribunales que han legitimado la videovigilancia, incluso sin una base jurídica, concluyendo que la combinación de tecnologías de bajo costo y altamente intrusivas y la falta de un marco legal adecuado crean una gran amenaza para el ejercicio de la privacidad y la protección de datos personales en el ámbito municipal.

Palabras claves

Videovigilancia; drones; privacidad; protección de datos; Chile.

I take a pride in probing all your secret moves
My tearless retina takes pictures that can prove
Judas Priest, "Electric Eye"

INTRODUCTION

High-tech surveillance and sophisticated means of social control are increasingly within reach for governments of the Global South. With cost no longer being an issue and little regulation in this area, Chilean mayors have begun to implement video surveillance systems. As studied in other regions, the result is a decentralized and invasive proliferation of video surveillance (hereinafter "surveillance"), with high-definition cameras recording in public and private places and storing images and data without any practical oversight.[1]

Shortly after these practices went from operating at the municipal level to functioning at the national level, the Ministry of the Interior and Public Security announced a national plan for drone video surveillance.[2] In May 2019, the Undersecretary for Crime Prevention reported a security program that integrates surveillance cameras and drones. The "Safe Street Plan" is designed to implement 1,000 CCTV cameras, 130 of them connected to police monitoring centers and with the "capacity to perform future facial recognition."[3]

---

1 David Gray. *The fourth amendment in an age of surveillance* (Cambridge, Cambridge University Press, 2017), p. 31.

2 *See* Home. *Calle Segura*, accessed on October 1, 2020, https://www.gob.cl/callesegura/

3 Subsecretaría de Prevención del Delito, E-mail answering to request *AB091T0000593*, January 24, 2020. Available at: https://www.dropbox.com/s/b859fsf2bxm129h/Respuesta%20SAI%20Drones%20Subsecretar%C3%ADa%20Delito.pdf?dl=0

Biometric data collected through these technologies is sensitive personal information which is being gathered and processed with no legal basis, proper legal authorization –a special statute on the matter–, nor individual consent.[4] Despite these normative concerns, the Chilean government, private corporations, and local municipalities are experimenting with these surveillance techniques. The results have been disastrous to say the least. In one case, a joint venture between a private shopping mall and a local government implemented a surveillance system equipped with facial recognition algorithms. The police revealed a report which showed that "90% of the facial recognitions made by the system were false positives (mistaken identity), while the other 10% were people preloaded in the database as they were employees of that same shopping center […]."[5]

A vast literature on drones and surveillance already exists, especially on video surveillance[6] and on "dataveillance."[7] Drones are "here, there, and everywhere."[8] Like other control devices, drones equipped with surveillance cameras "produce personal information for processing,"[9] particularly through "Persistent Surveillance Systems," which can "observe, record, and digitize

---

4 Romina Garrido & Sebastián Becker. "La biometría en Chile y sus riesgos," *Revista Chilena de Derecho y Tecnología* V. 6 Nº 1(2017), 67-91; Vladimir Garay. "Sobre la ilegalidad de la implementación de un sistema de reconocimiento facial en Mall Plaza," *Derechos Digitales,* November 16, 2018, Available at: https://www.derechosdigitales.org/12623/sobre-la-ilegalidad-de-la-implementacion-de-un-sistema-de-reconocimiento-facial-en-mall-plaza/; Vladimir Garay. *Mal de ojo. Reconocimiento facial en América Latina*. (Derechos Digitales, 2019), 6, https://www.derechosdigitales.org/wp-content/uploads/glimpse-cap-rec-facial.pdf

5 Policía de Investigaciones. Oficio N° 978 al CPLT, December 24, 2018, §3.2. Available at: https://www.dropbox.com/sh/90xy207cuqxo01o/AACe_1bSZ-m1fbryPgaoNMkQa?dl=0.

6 On video surveillance, *see* von Beatrice Silva-Tarouca *Setting the watch. Privacy and the ethics of CCTV surveillance* (Oxford: Hart Pub, 2018); Aaron Doyle, Randy Lippert and David Lyon. *Eyes everywhere. The global growth of camera surveillance* (London, Routlege, 2012); Colin J. Bennett, Kevin D. Haggerty, David Lyon and Valerie Steeves (eds.). *Transparent lives* (Athabasca: Athabasca University Press, 2014); Cristina Gil Membrado. *Videovigilancia y protección de datos* (Madrid: La Ley Wolters Kluwer, 2019); Grégoire Chamayou. *A theory of the drone* (Janet Lloyd trans.: New York: The New Press, 2015)

In Latin America, *see* Luis Cordero. "Videovigilancia e intervención administrativa: las cuestiones de legitimidad," en *Chile y la protección de datos personales* (Santiago: Ediciones UDP – Expansiva, 2009); Vanessa Lio. "Ciudades, cámaras de seguridad y video-vigilancia: Estado del arte y perspectivas de investigación," *Astrolabio*, nº15 (2015). 273-302; Santiago Ramírez. "Del campo de batalla a las calles: el derecho a la intimidad en la era de los drones," *Revista Derecho del Estado*, nº 35 (2015), 181-199, https://doi.org/10.18601/01229893.n35.07; Tomás Ramírez, "Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad," *Revista Chilena de Derecho y Tecnología*, v. 5, nº 1 (2016); Nelson Arteaga. *Videovigilancia en México* (Ciudad de México: Flacso México, 2018); Samuel Malamud. "Videovigilancia y privacidad. Consideraciones en torno a los casos 'Globos' y 'Drones'," *Revista chilena de derecho y tecnología*, v. 7, n° 2 (2018), 137-162, http://dx.doi.org/10.5354/0719-2584.2018.49097; Pedro Rodríguez López de Lemus. "Drones, videovigilancia con fines de seguridad privada y protección de datos personales," *Foro Jurídico*, n° 15 (2016), 235-240, https://revistas.pucp.edu.pe/index.php/forojuridico/article/view/19849; Domingo Lovera. "Privacidad: La vigilancia en espacios públicos," en *Informe anual sobre derechos humanos en Chile 2017,* editado por Centro de Derechos Humanos (Santiago: Ediciones UDP, 2018); Domingo Lovera. "Privacidad, espacios públicos y vigilancia," en *Anuario de Derecho Público UDP 2018* (Santiago, Ediciones UDP, 2018); Kristin Bergtora and Bruno Oliveira. "Revisitando el espacio aéreo latinomericano: una exploración de los drones como sujetos de regulación," *Latin American Law Review,* nº 1 (2018), 61 – 81, https://doi.org/10.29263/lar01.2018.03; Nicolás Vargas-Ramírez and Jaime Paneque-Gálvez. "Desafíos normativos para el uso comunitario de drones en México," *Investigaciones Geográficas*, nº 102 (2020), https://doi.org/10.14350/rig.60007.

7 Colin *et al, Transparent lives*, 20.

8 Bart Custers. "Drones here, there and everywhere" in: *The future of drone use,* edited by Bart Custers (The Hague, Springer, 2018).

9 Zygmunt Bauman and David Lyon. *Liquid surveillance* (Cambridge: Polity, 2013), 18.

movement in real-time and can thus be used to investigate after the fact."[10] Drones are not mere observers of events; they are active agents in the production of events.[11] As they also serve as information-gathering and information-producing machines, they allow the State to have databases with "collateral" information of a criminal act under investigation. These systems allow forms of indiscriminate surveillance, and the data collected is available for future information crossings for different uses, not initially foreseen by the surveillance activity –e.g., welfare benefits.[12]

The local irruption of these devices in Chile for social control has been possible due to factual and normative reasons. Factual reasons are costs related: the increasingly low investment required to acquire and operate drones –including recording high-definition images that makes it possible to cross personal and biometric data through facial recognition software– allows full monitoring powers in each municipality.

Normative reasons are different. One the one hand, there is an absence of a legal framework that regulates the use of these technologies (even though fixed cameras have been with us for a long time).[13] The absence of law has been replaced by police rules and protocols adopted by each municipality, targeting crime enforcement and operative issues and (conveniently) forgetting legal safeguards of rights. On the other hand, there is no general regime for protecting personal data that can be duly enforced by an independent administrative agency,[14] such as in Europe (as required by the General Data Protection Regulation).[15] Lack of enforcement has facilitated the illegal processing of personal data collected from surveillance.

However, the absence of legal authorization for surveillance has been simultaneously validated by the Supreme Court's permissive approach to broad restrictions of rights and freedoms. In two surveillance cases –on hot air balloons and drones equipped with high-tech cameras– the Supreme Court of Chile constitutionalized the 'fear card' that governments (both national and local) have displayed to justify, as well as to promote, their law-and-order initiatives to uphold powers to control people and restrict their freedoms.

The purpose of this paper is to contribute to the regional discussion of privacy threats posed by surveillance drones by local governments. Unlike other studies that focus on the regulation of these devices[16], this case study shows how the lack of specific legal regulation on surveillance or a robust legal framework for the protection of personal data enables uncontrolled massive data collection. To do so, I analyze the case of Chile by selecting four municipalities that were audited by competent authorities. Regulatory loopholes and the low cost of the devices have facilitated their use without considering the aspects of privacy and informational self-determination.

---

10 Andrew Guthrie. *The rise of big data policing* (New York: NYU Press, 2017), 98.

11 Michael Richardson. "The testimony of drones," *Sydney Review of Books (2020)*, https://sydneyreviewofbooks.com/essay/the-testimony-of-drones/

12 Timothy Takahashi. "Drones and privacy," *Columbia Science & Technology Law Review*, v. XIV(2012), 112; Hernán Blanco. *Tecnología informática e investigación criminal* (Buenos Aires: Thomson Reuters, 2020), 323.

13 Cordero. "Videovigilancia e intervención administrativa."

14 Pablo Viollier. *El estado de la protección de datos personales en Chile*. (Chile: Derechos Digitales, 2017), 7-27, https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

15 General Data Protection Regulation 2016/679 of the European Union. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=ES. *See* Hielke Hijmans. "Article 51 Supervisory authority," in: *The EU General Data Protection Regulation,* edited by Christopher Kuner *et al.* (Oxford: OUP, 2020).

16 Bergtora & Oliveira, "Revisitando el espacio aéreo latinomericano"; Vargas-Ramírez & Paneque-Gálvez, "Desafíos normativos para el uso comunitario de drones en México."

The paper is structured as follows. The first section explains municipal policing powers that sustain the legality of surveillance at local level. I examine four cases to check how drone surveillance is taking place, concluding that there are real privacy risks in the operation of surveillance systems. Section two reviews normative standards that should be considered in surveillance matters. Municipal cases show noncompliance with human rights standards. Comparative cases show that countries have normatively addressed surveillance issues with a specific statute regulating surveillance or a robust general data protection framework. Chile lacks both alternatives. Section three explains how courts have legitimized surveillance, even without a legal basis that could sustain these restrictions to privacy and data protection rights. The paper concludes by explaining how the combination of low cost highly intrusive technologies and the lack of a proper legal and administrative framework to secure the rights of citizens create a major threat of improper intensive control of fundamental rights.

1. PROLIFERATION OF DRONE SURVEILLANCE AND LOW-COST POLICING

1.1. Municipal policing powers and drones

In 2017, Joaquín Lavín, mayor of one of the wealthiest municipalities in Chile, boasted that he had a security drone that included a camera and a loudspeaker system to communicate with pedestrians (Figure 1). It had never been so cheap to politically advertise "big" advances in public security as with the entry of surveillance drones. This is the first act of the Orwellian nightmare. However, how did a mayor come to hold such police power under his office?

Figure 1. Las Condes Mayor Joaquín Lavín, tweeting about his administration's new surveillance drones equipped with loudspeakers

Source: Lavín's Twitter account.[17]

17 Joaquín Lavín. Twitter Post. April 15th, 2017, 1:51pm, https://twitter.com/LavinJoaquin/status/853289617361178624

In Chile, public order is a constitutional mission reserved for the police.[18] Chile is a unitary State, and there is no vertical separation of powers in matters of public security. However, municipalities have increasingly become involved in public safety tasks, investing a considerable amount of resources.[19] Municipal powers now include the "[…] adoption of measures in the field of public security at community level, notwithstanding the functions of the Ministry of the Interior and Public Security and the Forces of Order and Security […]."[20] This has been called "non-exclusive" or "shared" functions of local governments.[21] Several regulatory changes have broadened municipalities' powers in public safety matters,[22] supported by polls and security studies,[23] and under a decentralization of security discourse promising more efficient results.[24]

Whether local policing is achieving efficiency and better security rates is not clear. Recent evidence suggests otherwise.[25] In any case, it is undoubtedly politically profitable. Municipal guards, cars, and call centers have proliferated all over the country. Neighbors seem to like the idea of having a municipal guard that that can call, who acts almost as a private guard. What is new, however, is the fast proliferation of aerial mechanisms accessible for under US$1,500. The Chilean case shows new trends in surveillance at local levels of government, with little or no regulation or control.

According to public and private information, drones and, more generally, surveillance is now easily accessible, even for the budgets of small towns.[26] Municipalities are acquiring surveillance balloons and drones to advertise new ways to fight crime.[27]

1.2. Four municipal cases

The Council for Transparency ("CPLT") has audited four municipalities that operate surveillance drones for public safety purposes: Las Condes, La Florida, Quintero, and Cartagena.[28] The following table summarizes the items audited by the CPLT.[29]

---

18 Art. 101 of the Chilean Constitution.

19 Iván Silva. *Costo económico de los delitos, niveles de vigilancia y políticas de seguridad ciudadana en las comunas del Gran Santiago*. CEPAL, 2000, https://repositorio.cepal.org/bitstream/handle/11362/7258/1/S00010053_es.pdf

20 Article 4, letter j), Ley Orgánica Constitucional de Municipalidades.

21 Jorge Bermúdez. *Derecho administrativo general* (Santiago: Thomson Reuters, 2014), 729.

22 Romina Garrido ad Jessica Matus. "Las cámaras que no atrapan delincuentes: Situación de la videovigilancia en Chile," 2017, 13. https://lavits.org/wp-content/uploads/2017/09/P2_garridomatus.pdf

23 Lucía Trujillo and Juan Pablo Arévalo. "Gestión municipal de la prevención en seguridad en barrios vulnerables," *Conceptos*, nº 23 (2011), 3. https://pazciudadana.cl/biblioteca/documentos/conceptos-no-23-gestion-municipal-de-la-prevencion-en-seguridad-en-barrios-vulnerables-su-articulacion-con-el-nivel-central-de-gobierno-un-factor-clave/

24 Sergio Galilea, Leonardo Letelier and Katherine Ross. *Descentralización de servicios esenciales* (Santiago de Chile: Cepal, 2011), 108 – 109, https://repositorio.cepal.org/bitstream/handle/11362/3835/1/S2010976.pdf

25 Lio. "Ciudades, cámaras de seguridad y video-vigilancia," 295 y ss.; Arteaga. *Videovigilancia en México,* 27 y 41-43.

26 Datos Protegidos. *Drones en Chile*. (Datos Protegidos: Chile, 2017), 13-14, 37-41. https://datosprotegidos.org/wp-content/uploads/2017/04/Informe-Drones-español.pdf

27 Instituto Nacional de Derechos Humanos. *Informe Anual 2018: situación de los derechos humanos*. (Chile: INDH, 2018), 236. Available at: https://bibliotecadigital.indh.cl/handle/123456789/1173

28 The information was obtained through the Freedom of Information Law No. 20.285. Access request No. CT001T0011331. Available at: https://www.dropbox.com/sh/90xy207cuqxo01o/AACe_1bSZ-m1fbryPgaoNMkQa?dl=0

29 CPLT, Oficio No. 2309 (06.03.2017).

Table 1. Summary of items of CPLT audits

Auditable item	Content	Evidence – Observations
1. General measures.	1.1. CPLT recommendations were adopted. 1.2. Notification to the CPLT. 1.3. Municipality has internal rules on access rights to the images collected. 1.4. Municipality has the DGAC's permission to fly drones.	Communications to the Council. Manual, protocol, or other documentation. DGAC' administrative act.
2. Purpose of processing: exclusively for public safety reasons.	2.1. Municipality has documented procedures (access permissions and access to recordings). 2.2. Personnel with access to the recordings are trained. 2.3. System keeps a record of access and activity performed by the user.	Backups of data, traceability of user logins. Documentation on personnel's training. Mayor's decree validating documentation.
3. Municipality as controller.	3.1. Personnel contracts. 3.2. Protocols of administrative liability.	Certificates.
4. Security measures.	4.1. Proceedings are documented on personnel's logins and access to information requests. Traceability. 4.2. Personnel training. 4.3. Operations room is technically secure. 4.5. Data encryption.	Traceability documented. Personnel's training certificates. The operating room where the storage disks are located has restricted access; only authorized personnel can access it.
5. Destruction of the images collected.	5.1 Protocols certifying data erasure and data storage. 5.2 System's configuration and privacy by default. 5.3. Security measures for data storage. 5.4. Internal review of data erasure.	Manuals, protocols, or other documentation. Software settings. Protocol to deliver data to the office of the Public Prosecutor.
6. Municipal certification that images have been lawfully recorded.	6.1. Manual, protocol, or other documentation. 6.2. Data erasure act.	Documentation. Act.
7. Rights of the data subject.	7.1 System allows blurring of images and erasing video segments. 7.2 Record of the action, date, and time, who requests it, who executes it.	A protocol is in place. People can request to see the recordings. A deletion procedure is not implemented at the request of the user. The recording is only given to the prosecutor's office.
8. Registration of the images database under the Civil Registry.	8.1. Means of verification.	Database list at the Civil Registry.

Source: CPLT's audit reports on drone surveillance.[30]

30 Ibid.

The municipalities' responses demonstrate how far they are from full compliance with the Law and show a significant disparity in the levels of effectiveness of legal regulations.

Firstly, there is no documentation or internal protocols in the municipalities that adequately regulate image processing, either in surveillance drones or CCTV systems that may have been in place before the CPLT recommendations.[31] In Las Condes and Quintero, internal documentation is not officially sanctioned.[32]

Secondly, there are no basic data security measures in place. The operations room in Las Condes has no physical access control and the door is kept permanently open.[33] The Council has recommended encrypting the images, which is an essential measure that most municipalities have not implemented.[34]

Thirdly, the audits show no evidence regarding the training and education of the personnel in charge of surveillance systems.[35] Training is required for the technical operation of the devices themselves, as well as to comply with the standards judicially defined by the Supreme Court.[36] Without it, there is a higher risk of recording in prohibited locations, unauthorized logins to the system, non-anonymization or imperfect anonymization when handling FOI requests, or problems deriving from information security failures.

Lastly, Quintero shows a systemic failure to comply with the current CPLT recommendations, which demonstrates how surveillance devices operate without proper oversight. The municipality does not have a manual or protocol for surveillance. The surveillance system is used for security purposes and other goals –such as traffic-related issues– in direct violation of the Supreme Court's judicial standards. Private contractors operate the system, and there is no effective administrative supervision, not even a public employee in charge of implementing judicial standards. There are no records of user logins or FOI requests, making it impossible to

---

31 CPLT *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de Cartagena*, February 29, 2019, 13-14, https://www.dropbox.com/home/2.%20Publicaciones/Bases%20de%20datos%20de%20investigaciones%20publicadas/Solicitud%20CT001T0011331%20CPLT; CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de La Florida*, February 19, 2019, 13, https://www.dropbox.com/home/2.%20Publicaciones/Bases%20de%20datos%20de%20investigaciones%20publicadas/Solicitud%20CT001T0011331%20CPLT; CPLT. *Informe de inspección IPDP No. 1-2019. Municipalidad de Quintero*, December 20, 2019, 3-4, https://www.dropbox.com/home/2.%20Publicaciones/Bases%20de%20datos%20de%20investigaciones%20publicadas/Solicitud%20CT001T0011331%20CPLT

32 CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de Las Condes*, December 13th, 2018, 4. https://www.dropbox.com/home/2.%20Publicaciones/Bases%20de%20datos%20de%20investigaciones%20publicadas/Solicitud%20CT001T0011331%20CPLT

33 Ibid.

34 CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de Cartagena*, 14; CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de La Florida*,13; CPLT. *Informe de inspección IPDP No. 1-2019*, 4.

35 CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de Las Condes*, 11; CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de Cartagena*, 14; CPLT. *Informe de auditoría en transparencia. Seguimiento de recomendaciones dispositivos de videovigilancia. Municipalidad de La Florida*,13; CPLT. *Informe de inspección IPDP No. 1-2019*, 4.

36 *Infra* 3.2.

trace and demonstrate compliance with the CPLT recommendations. Even primary legal obligations –such as filing the database in the Civil Registry– are not fulfilled.[37]

Another point worth highlighting involves the empirical background obtained on the operation of these surveillance technologies. Discourses on the legitimacy of the implementation of drone surveillance state that these devices are tools that help crime prevention and support criminal prosecution. How do these technologies achieve such ends? Regarding criminal prosecution support, there is an objective measure that should serve to back its usefulness: the number of criminal complaints supported by images obtained through these devices. However, the reality is different. Through an FOI request, Las Condes and Lo Barnechea disclosed the number of complaints made based on images obtained through surveillance balloons during the year 2016: "there are no complaints to date"[38] or "[n]o complaints have been made to the Eastern District Attorney's Office or the police between the dates requested."[39] In other words, zero.

Drone surveillance is represented as highly sophisticated and accurate. But, is it effective? Let us take the case of facial recognition and biometric identification of individuals. Facial recognition algorithms have shown their worst performance in Chile. As I mentioned in the introduction, the municipality of Las Condes, in collaboration with a chain of shopping malls, decided to implement a surveillance system with facial recognition. A Council audit made it possible to obtain an Investigations Police report on the facial recognition system's operation and the margin of error. According to the report, misidentification of individual faces reached 90% of the cases, showing a gross level of failure.[40]

2. SURVEILLANCE WITHOUT REGULATION

2.1. Surveillance and human rights standards

As technology continues to improve, the scope of surveillance is escalating. In Chile, there is no legal basis to legitimize new surveillance techniques. Video surveillance interferes with the legitimate exercise of several rights: the right to privacy,[41] freedom of expression,[42] and the

37 CPLT. *Informe de inspección IPDP No. 1-2019,* 3-5.

38 Municipalidad de Las Condes, Respuesta No. MU135T0001765 a Sebastián Becker, March 1st, 2017 https://www.dropbox.com/s/0zigxal1vt8751t/Repuesta%20de%20Las%20Condes%20por%20operatividad%20de%20Globos.pdf?dl=0

39 Municipalidad de Lo Barnechea, Oficio Adm. Municipal No. 117/2017 I.D.Nº 577469 a Sebastián Becker, March 1st, 2017, https://www.dropbox.com/s/y81wxga3mi6zc1i/OFICIO%20SR.%20SEBASTIAN%20BECKER%20CASTELLARO.pdf?dl=0

40 Policía de Investigaciones. Oficio N° 978 al CPLT, December 24, 2018, §3.2. https://www.dropbox.com/sh/90xy207cuqxo01o/AACe_1bSZ-m1fbryPgaoNMkQa?dl=0.

41 Manuel José Cepeda Espinoza. "Privacy," in: *The Oxford Handbook of Comparative Law,* edited by Michel Rosenfeld, and András Sajó (Oxford: OUP, 2018), 971-972; Daniel J. Solove. *Nothing to hide. The false tradeoff between privacy and security* (New Haven: Yale University Press, 2011), 178 y ff. In the Chilean case, see Rodolfo Figueroa. *Privacidad* (Santiago: Ediciones UDP, 2014), 111-115 and 123-127.

42 Lovera, "Privacidad, espacios públicos y vigilancia," 41-47; Datos Protegidos. *Drones en Chile*, 24-26; Arteaga. *Videovigilancia en México*, 65-81.

right to informational self-determination.[43] Under the Constitution and human rights treaties, a fundamental right can only be legitimately restricted if there is a legal basis, a legitimate purpose, and a need for the functioning of a democratic society. The first requirement is absent as far as surveillance is concerned: there is no general legal framework that authorizes such surveillance as a means to ensure public security.[44] All there is –in the best of cases– are some internal municipal protocols or manuals –as was described in the previous section.

Human rights standards concerning CCTV have been developed by the European Court of Human Rights. Video surveillance restricts the right to private and family life under article 8 of the European Convention on Human Rights.[45] Such restriction covers a broad range of data processing.[46] The Court has reviewed surveillance cases under its system of rights restrictions, mainly focusing on the legality of the measure and its proportionality. In terms of the former, the Court has stated that "the law must provide protection against arbitrary interference" and "must be sufficiently clear to give citizens an adequate indication of the circumstances and conditions under which public authorities may employ these techniques."[47] With respect to the latter, the proportionality principle commands that "the law cannot grant blank and indiscriminate powers" in surveillance matters.[48]

Inter-American human rights standards are fully applicable in Chile. The Inter-American Court has adopted requirements to justify restrictions upon a right established in the American Convention. In its early case law, the Court adopted three conditions: a. Restrictions must be previously established in the Law, b. they must fulfill a legitimate aim under the Convention, and c. they must be necessary for a democratic society.[49] The legality of a restriction is critical in this case. The Court interpreted the word "laws" as requiring both "formal" and "material" elements. "Law," in its formal meaning, relates to the procedure under which rules restricting rights are created. According to the Court, the word *law* "can have no other meaning than that of formal law, that is, a legal norm passed by the legislature and promulgated by the Executive Branch, under the procedure set out in the domestic law of each State."[50] As the Court has interpreted it, the law approved by the legislature connects a democratic procedure with the protection of rights.[51] That is not the case in Chile on the issue of surveillance.

---

43 Gil Membrado. *Videovigilancia y protección de datos*; Rachel Finn and Anna Donovan. "Big data, drone data: Privacy and ethical impacts of the intersection between big data and civil drone deployments," in: *The future of drone use*, edited by Bart Custers (The Hague: Springer, 2016); David Wright and Rachel Finn. "Making drones more acceptable with privacy impact assessments," in: *The future of drone use,* edited by Bart Custers (The Hague: Springer, 2016).

44 Cordero. "Videovigilancia e intervención administrativa," 94.

45 Peck v. Reino Unido, App. No. 44647/98, January 28, 2003, ¶63.

46 Xavier Arzoz. "Derecho al Respeto de la Vida Privada y Familiar," in *Convenio Europeo de Derechos Humanos,* edited by Iñaki Lasagabaster (Madrid: Civitas-Thomson Reuters, 2015), 391.

47 Ibid, 392.

48 Ibid, 392.

49 IAHRC. Claude-Reyes et al. v. Chile, Merits, Reparations and Costs, Judgment, (ser. C) No. 151, ¶¶89-91 (Sept. 19, 2006).

50 The Word "Laws" in Article 30 of the American Convention on Human Rights, Advisory Opinion OC-6/86, Inter-Am. Ct. H.R. (ser. A) No. 6 (May 9, 1986), at ¶27.

51 Scott Davidson. *The Inter-American Human Rights System* (Aldershot: Dartmouth Publishing, 1997), 52.

However, before we examine Chile in this regard, we must review the alternatives other countries have implemented to regulate surveillance.

2.2. Regulating surveillance: specific statutes and general data protection laws

In European countries, surveillance has been regulated in two different ways: special regulations on video surveillance, and general data protection laws.[52] Two examples of each strategy are examined in this section. Spain and England are cases of special surveillance statutes, and Germany and Italy are examples of a general data protection regulation on the issue.

Spain's law authorizes surveillance devices and creates legal checks and balances for police and private security.[53] The collection of an individual's image is also considered processing of personal data and is, therefore, also regulated by the national data protection regulation (LOPDGDD),[54] as has been interpreted by the data protection authority: *Agencia Española de Protección de Datos Personales* (AEPD).[55] Article 22 of the LOPDGDD sets the rules for surveillance, establishing a specific end –"preserving the safety of people and property, as well as their facilities" –and requiring a necessity or proportionality test– "images in the public space may only be captured to the extent that is essential for the purpose mentioned in the previous section." The LOPDGDD also establishes a term limit for image storage, which cannot last more than one month from its collection. If the image must be kept as proof in criminal cases or damages against persons, goods, or facilities, the data must be delivered to the competent authority within a maximum period of 72 hours from the time the recording is known.[56]

England too has enacted a special statute: *Protection of Freedoms Act* (POFA) which created the Surveillance Camera Commissioner, an authority to supervise the proper use of surveillance (POFA, §34).[57] However, if the images can identify a specific individual, then the *Data Protection Act* of 2018 also applies. Commentators have stated that such rules must also apply even if unknown persons are being recorded, who may be identified by further processing of information with another dataset.[58] The Information Commissioner's Office (ICO) enforces data protection rights in surveillance cases, requiring data protection impact assessment

52 Marcos Correa, J. Carlos Lara and María Paz Canales. *La construcción de estándares legales para la vigilancia en América Latina. Parte II*. (Chile: Derechos Digitales, 2018) https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-II.pdf

53 Spain regulates these matters under Ley Orgánica 4/2015, de protección de la seguridad ciudadana, and Ley Orgánica 4/1997, sobre utilización de videocámaras por parte de las Fuerzas y Cuerpos de seguridad. Before these statutes, there were constitutional doubts on whether police and security forces had the legal authority to conduct video surveillance. *See* Díez-Picazo, Luis María (2003): *Sistema de Derechos Fundamentales* (Madrid, Thomson Civitas), p. 257.

54 Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales.

55 AEPD, Instrucción 1/2006.

56 Paloma Llaneza "Tratamiento de datos con fines de videovigilancia y denuncias internas," en *Tratado de protección de datos,* edited by Artemí Rallo Lombarte (Valencia: Tirant lo Blanch, 2019), 807-808.

57 *Protection of Freedoms Act*, UK Public General Acts, 2012.

58 Peter Carey. *Data Protection* (Oxford, OUP, 2015), 288.

for processors before using CCTV.[59] The assessment must show whether there are other less intrusive means to achieve the goals for which surveillance is necessary.[60] Controllers must also inform the ICO of the purpose for which the images are being recorded (e.g., prevention and prosecution of crimes). Failure to notify constitutes unlawful data processing.[61] There are no fixed term limits for data storage, although ICO has limited this to the purpose declared, ensuring both the quality and the security of the data.[62]

Other countries regulated the issue under general data protection laws. Although they may not cover surveillance in its entirety,[63] such laws have proven to be among the most efficacious means to address some of its critical features.[64] In Italy, CCTV may have different purposes, but data processing must be strictly circumscribed to the purpose declared, either by legal authorization or personal consent.[65] A previous impact assessment must be conducted for in biometric recognition systems or "intelligent systems" that may detect deviant behavior.[66] Data storage is carefully regulated: "images should not be retained for longer than a few hours, and up to a maximum of 24 hours […]."[67] Exceptions to this term are limited: in the case of festivities or images used in a judicial investigation. There is also a specific rule for municipalities, which limits retainment to a maximum of seven days.[68]

In Germany, surveillance which can lead to the identification of an individual is legally classified as the processing of personal data, covered under the Federal Data Protection Act (*Bundesdatenschutzgesetz*).[69] Section 4 of the BDSG regulates video surveillance of publicly accessible spaces. As such, surveillance is only legally permitted "as far as it is necessary 1. for public bodies to perform their tasks, 2. to exercise the right to determine who shall be allowed or denied access, and 3. to safeguard legitimate interests for specifically defined purposes and if there is nothing to indicate legitimate overriding interests of the data subjects." (BDSG, §4(1)). In terms of storage, the BDSG states that "[t]he data shall be deleted without delay, if they are no longer needed for the intended purpose or if the data subject's legitimate interests stand in the way of any further storage." (BDSG, §4(5)).

Italy and Germany provide examples of the regulation of surveillance from a general data protection framework. By supervising compliance with these laws, administrative agencies are indirectly protecting other rights such as freedom of expression or due process rights by

---

59 ICO. *In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information*, (ICO, 2017) https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

60 Ibid., 9.

61 Carey. *Data Protection,* 288.

62 ICO, *In the Picture,* 12.

63 Bennett, Haggerty, Lyon and Steeves. *Transparent lives,* 84.

64 In Italy, *see Garante per la Protezione dei Dati Personali*, Video Surveillance Decision, April 8, 2010 [1734653], Available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1734653. For Germany, *see* von dem Bussche, Axel & Voigt, Paul (2017): *Data Protection in Germany* (Kumhausen, C. H. Beck).

65 GPDP (2010), §2.a.

66 GPDP (2010), §3.2.1.

67 GPDP (2010), §3.4.

68 GPDP (2010), §3.4.

69 von dem Bussche & Voigt (2017), p. 47.

enabling the right to access personal data and commanding data processors to erase the images after a short time.

2.3. Lack of surveillance regulation in Chile

Chile does not have a specific legal framework regulating the use of surveillance and only has an outdated data protection law with severe regulatory deficits. There is no special law that regulates video surveillance. Cordero has examined some of the internal regulations that the police have adopted for surveillance.[70] Nevertheless, from a constitutional point of view, and according to the Inter-American human rights standards already reviewed, this internal regulation does not fulfill the first requirement for restricting fundamental rights: it is not a "law," *strictu sensu*, that is suitable for restricting privacy or data protection rights. Cordero reaffirms this: "surveillance cameras *lack an explicit regulatory coverage* […]."[71] The same conclusions apply to the internal regulations that some municipalities have adopted for the surveillance of their CCTVs and drones. The law has not defined the specific municipal powers, control mechanisms, and liability rules.

On the second matter, Chile's data protection law does not meet basic enforcement standards, securing people's personal information. Law No. 19.628 on the Protection of Private Life has gaps and inadequacies which are recurrently denounced.[72] Multiple draft bills have been promoted in an attempt to fix this.[73] The Law has two fatal flaws: it lacks an independent agency with powers to enforce data protection rights, and effective rules to sanction its violation. In sum:

> "[…] the absence of a complete regime of violations and sanctions in the law was highly criticized, as were the current low fines. Likewise, the absence of sanctions for public or private entities that suffer a data leak and do not give notice to the affected owners was also questioned.
>
> It should be noted that the absence of an oversight authority and an expeditious complaints procedure directly influence the impunity of those who violate the law."[74]

To this day, there is a need to adjust Chilean regulation to the 1980 OECD recommendations.[75] Chile accepted these recommendations and committed itself to implementing them before the end of 2011. However, the commitment remains pending.[76]

---

70 Cordero. "Videovigilancia e intervención administrativa, 89-92, citing Carabineros (1994): "Directiva para los servicios del sistema de vigilancia policial por cámaras de televisión," Orden General (reservada) No. 996/1994.

71 Cordero. "Videovigilancia e intervención administrativa, 94 (emphasis added).

72 Renato Jijena. "La Ley Chilena de Protección de Datos Personales. Una Visión Crítica desde el Punto de Vista de los Intereses Protegidos," *Cuadernos de Extensión Jurídica*, nº. 5 (2015); Pedro Anguita. *La Protección de Datos Personales y el Derecho a la Vida Privada* (Santiago, Edit. Jurídica de Chile, 2007).

73 Ibid.

74 Comité de Evaluación de la Ley. "Evaluación de la Ley No. 19.628," 2016. Available at: http://www.evaluacionde laley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf (last visited 03.10.20), p. 84.

75 OCDE. "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales," 1980 http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

76 Comité de Evaluación de la Ley, "Evaluación de la Ley No. 19.628" 67.

In conclusion, Chile does not have a special statute or a robust general data protection regime to place checks and balances on surveillance. Therefore, there is no legal basis for surveillance and no control or enforcement measures to secure people's rights.

3. JUDICIAL ACQUIESCENCE AND THE THREAT TO OUR RIGHTS

Constitutional safeguards could have provided a means to redress the illegal use of surveillance. However, such an attempt was defeated after Supreme Court decisions on two cases that reached the courts based on the actions of local NGOs via writs of *habeas* (*recurso de protección*) in 2016 and 2017.

3.1. Surveillance balloons

In the first case, NGOs complained that an aerostatic surveillance balloon, recording public venues and inside citizens' apartments, infringed their right to private life under article 19 No. 4 of the Chilean Constitution. According to the *recurso de protección*, the use of this device was contrary to the Constitution because municipalities do not have such policing powers under the law and because they disproportionately interfered with people's right to privacy. Concerning the privacy issue, the plaintiffs argued that there were no administrative safeguards against recording neighbors' private activities since the cameras were technically fit to film inside their private homes.[77]

The Supreme Court decided in favor of the municipality,[78] though this matter is not regulated under the law.[79] The Court recognized a legal basis for municipalities to guarantee public safety in their communities by stretching a vast and unspecific power in their organic laws. The decision states that "it is indisputable that the support and promotion of public safety is, at present, a relevant municipal function."[80] Such recognition does not comply with constitutional and human rights standards that require sufficient precision and specificity regarding the restriction of fundamental rights. Some authors have regarded this line of criticism as "formalistic and legalistic."[81] Nevertheless, the decision does not have an "assessment of strict legality (i.e., identification of normative sources that expressly confer authority), and even less so, a scrutiny of the specificity and proportionality of the measures."[82] By recognizing a legal basis, the Court set four judicial standards for municipal surveillance.

---

77 Garrido and Matus, "Las cámaras que no atrapan delincuentes," 3.

78 Sentencia Corte Suprema, Rol 18.458-2016 (01.06.16).

79 Francisco Leturia. "Comentario de sentencia: Uso de globos de vigilancia," en Libertad y Desarrollo, *Sentencias destacadas 2016* (Santiago: LyD, 2017); Garrido and Matus, "Las cámaras que no atrapan delincuentes," 210.

80 Sentencia de la Corte Suprema, Rol 18.458-2016 (01.06.16), c. 7º.

81 Ibid., 211.

82 Lovera. "Privacidad," 409.

3.2. Judicial standards for municipal surveillance

First, cameras can record in publicly accessible spaces and private spaces in the pursuit of a criminal act.[83] The Supreme Court reversed its long-standing jurisprudence on privacy in the public sphere and also eroded the right to the inviolability of the home. The evolution of the *recurso de protección* case law went from a tacit waiver of privacy in public places[84] to the requirement of prior and express consent for the disclosure of the image.[85] The case law requires that the person be identifiable: it requires that "the image used must be recognizable, that is, it allows for its undoubted identification."[86] Therefore, blurred images or images of individuals who cannot be identified, are not protected. Consent does not distinguish whether the image is captured in a private or public place.[87] As Figueroa has stated, "[t]he distinction between a public place and a private place depends on property rights," so that "a public place cannot be confused with the sphere of the public or made public."[88]

Allowing to record images in private spaces constitutes an infringement of the inviolability of the home (article 19 No. 5, Chilean Constitution). Such right only allows restrictions as prescribed by law and not merely by a judicial authorization in a case that can only have an *inter partes* effect.

Second, a municipal inspector or delegate must certify, every month, "that no images have been captured from spaces of a private nature such as the interior of homes, commercial or service establishments, gardens, patios, or balconies."[89] By setting this duty to a public employee, the Court is trying to secure the possibility to pursue administrative liability of the people in charge of the surveillance system. It also excludes any possible private contractors, that is, employees that could run the system without proper administrative supervision.

Third, the Court establishes a term period for data retention: "[t]he destruction of the recordings will be made effective by the person responsible for their custody after 30 days, except if the recording has captured a criminal offense or other misconduct, in which case the municipality appealed against will take the measures for their prompt delivery to the competent bodies."[90] Why 30 days? No rationale can be found behind this; it seems an exercise of pure judicial discretion. The rule commands the destruction of images "after 30 days", establishing a minimum for data retention but not a fixed term for destruction itself. If the exception concurs –that is to say, images of criminal offense or misconduct–, the rule sets a prudential guideline (an obligation to a "prompt delivery" of the images to the authorities). Part of the term's ambiguity regarding the installation of surveillance devices by municipalities was later clarified

83 Sentencia Corte Suprema, Rol 18.458-2016 (01.06.16), parr. resolutivo 1.

84 Sentencia Corte Suprema, Rol 14.598-1989.

85 Sentencia Corte de Apelaciones (Santiago), Rol 3322-97, c. 4°.

86 Sentencia Corte de Apelaciones (Santiago), Rol 469-2000, c. 4°.

87 Sentencia Corte de Apelaciones (Santiago), Rol 3322-97, c. 5°.

88 Figueroa. *Privacidad,* 363.

89 Sentencia Corte Suprema, Rol 18.458-2016 (01.06.16), parr. resolutivo 2.

90 Sentencia Corte Suprema, Rol 18.458-2016 (01.06.16), parr. resolutivo 3.

under the CPLT recommendations.[91] Section 5 of the recommendations document prescribes that "images must be destroyed within 30 days after being recorded or captured."[92] Therefore, under the Council's standards, 30 days is a fixed term and a deadline for the destruction of images.

Lastly, the Court recognized a right to access recordings of oneself. The mayor must appoint a municipal employee to be in charge of granting access, and the requester must indicate the day when he or she was recorded.[93] The CPLT later recommended that the municipality have a procedure to anonymize third-party images.[94]

3.3. The second case: drone surveillance

The surveillance balloon decision opened the door to the proliferation of these devices. After being ratified by the Supreme Court, municipalities were now legally authorized to buy and use aerial surveillance devices, even without proper legal authorization.

The second case concerned not an aerostatic surveillance balloon but the use of drones. Again, the case was filed before the courts by NGOs. According to the plaintiffs, surveillance drones did not have a legal basis to operate at municipal level and such surveillance restricted their rights to respect private life, the inviolability of the home, property rights, freedom of expression, freedom of reunion, and the right to personal integrity.

The Court of Appeals dismissed the case,[95] following basically the same arguments as the Supreme Court in the previous surveillance balloons case. The Appeals Court case, based on the previous decision, reaffirmed, and entrenched the legal authority under which the devices are operating. On the legality argument, the Court considered the CPLT recommendations –which, in turn, were developed under the Supreme Court's judicial rules.[96] The Court recognized that "the capture and recording of images of people constitute data processing" under the law. Still, such processing is legal by the reading of two rules: first, under the Constitutional Organic Law of Municipalities, which provides municipal powers of policing and public safety at local level and, second, under a general rule which provides legal authorization to process personal information for any state body under their legal powers as described by Law (art. 4(j) Constitutional Organic Law of Municipalities and art. 20 of the Law No. 19.628).[97]

The Court seems to follow the decision on the surveillance balloons, partly on the privacy issue. According to the Appeals Court,

> "the implementation of remote surveillance is not detrimental to the privacy of actors if they can circulate in public spaces where the drones fly in response to the way the

91 CPLT, Oficio No. 2309 (06.03.2017).

92 CPLT, Oficio No. 2309 (06.03.2017), §5.

93 Sentencia Corte Suprema, Rol 18.458-2016 (01.06.16), parr. resolutivo 4.

94 CPLT, Oficio No. 2309 (06.03.2017), §7.

95 Sentencia Corte de Apelaciones (Santiago), Rol 34.360-2017 (21.08.17).

96 Sentencia Corte de Apelaciones (Santiago), Rol 34.360-2017 (21.08.17), c. 14.

97 Sentencia Corte de Apelaciones (Santiago), Rol 34.360-2017 (21.08.17), c. 14.

> measure has been implemented by the municipality, because there has been a regulation of the activity […]."[98]

The criterion added by the Court is that there is a prior warning by the municipality about drone surveillance, which has been regulated internally with certain elements that are accessible to citizens. However, this criterion has no conceptual or normative connection with the scope of the right to privacy in public spaces. In other words, while the municipality may have a surveillance device that is publicly advertised, it does not follow that the right to privacy is not applicable or that a reasonable restriction upon it can be inferred. Moreover, it is an oblique way of presuming a specific consent: since it is a security policy adopted by the municipality and has a particular regulation, then it should be understood that citizens know (accept?) the surveillance executed.

The Supreme Court later ratified the Appeals Court's decision. Nevertheless, the decision does not even provide a single argument to confirm the first instance decision.[99] In just one phrase, the Supreme Court authoritatively dismissed the appeal. This is the final part of the Orwellian nightmare: judicial acquiescence of the use of drones by municipalities. Surveillance as low-cost policing is here to stay, without legal basis or proper oversight.

CONCLUSION

Aerial surveillance technologies have long ceased to be science fiction or a privilege of developed countries. Today, a municipality in Chile can acquire the latest technology and use it as a means to prevent crime and support public safety.

The paper attempts to dialogue with Chilean and regional literature on the problems and threats posed by drones as local surveillance devices. In the case of the national literature, I sought to go beyond the general discussion of drones or the discussion of their case law to show the systemic dimension of the problem concerning its regulatory framework and comparing it with European experiences. In addition, the results of the audits carried out on municipal drone surveillance systems show that the standards set by the Supreme Court and the CPLT are not being met. From a regional point of view, this case study exhibits in detail the gaps in existing in terms of privacy and personal data protection when implementing surveillance drones.

The implementation of these new surveillance technologies does not respect minimum legal requirements for restricting rights such as privacy and data protection. The informality of the use of these systems also seems to correlate with their effectiveness: the images they capture are not helpful for a criminal prosecution, and facial recognition algorithms simply do not work.

The use of these systems lacks legal regulation in Chile. No specific statute addresses the dimensions of policing powers, checks, balances, and surveillance operators' responsibility. In addition, Chile's data protection legislation does not meet the minimum standards for necessary enforcement.

---

98 Sentencia Corte de Apelaciones (Santiago), Rol 34.360-2017 (21.08.17), c. 27.

99 Sentencia Corte Suprema, No. 38.527-2017 (11.12.17).

The Orwellian nightmare is sealed with judicial acquiescence. Courts have endorsed the use of these technologies and reversed the constitutional protection of privacy in public spaces. Thus, they have generated a series of judicial rules to make up for the absence of a legal basis in order to validate the use of these surveillance mechanisms. The result is the worst scenario for citizen freedom: increased local surveillance, no empirical evidence of its utility, no legal basis, and with the courts' seals of approval.

REFERENCES

1. Anguita, Pedro. *La Protección de Datos Personales y el Derecho a la Vida Privada*. Santiago: Editorial Jurídica de Chile, 2007.
2. Arteaga, Nelson. *Videovigilancia en México*. Ciudad de México: Flacso México, 2018.
3. Bauman, Zygmunt & Lyon, David. *Liquid surveillance*. Cambridge: Polity, 2013.
4. Bennett, Colin J. et al. (eds.). *Transparent lives*. Athabasca: Athabasca University Press, 2014.
5. Bermúdez Jorge. *Derecho administrativo general*. Santiago: Thomson Reuters, 2014.
6. Bergtora, Kristin & Oliveira, Bruno. "Revisitando el espacio aéreo latinomericano: una exploración de los drones como sujetos de regulación", en *Latin American Law Review,* nº 1 (2018), 61-81.
7. Blanco, Hernán. *Tecnología informática e investigación criminal*. Buenos Aires: Thomson Reuters, 2020.
8. Carey, Peter. *Data Protection*. Oxford: OUP, 2015.
9. Cepeda Espinoza, Manuel José. "Privacy", in: *The Oxford Handbook of Comparative Law*, Michel Rosenfeld & Sajó, András (eds.). Oxford: OUP, 2012.
10. Cordero, Luis. *"Videovigilancia e intervención administrativa: las cuestiones de legitimidad", en Chile y la protección de datos personales*. Santiago: Ediciones UDP – Expansiva, 2009.
11. Correa Marcos, *et al*. *La construcción de estándares legales para la vigilancia en América Latina*. *Parte II*. Santiago: Derechos Digitales, 2018.
12. Custers, Bart. "Drones here, there and everywhere", in: *The future of drone use*. edited, Bart Custers (ed). Netherland: Springer, 2016.
13. Chamayou, Grégoire. *A theory of the drone*. New York: The New Press, 2015.
14. Davidson, Scott. *The Inter-American Human Rights System*. Aldershot: Dartmouth Publishing, 1997.
15. Díez-Picazo, Luis María. *Sistema de Derechos Fundamentales*. Madrid, Thomson Civitas, 2003.
16. Doyle, Aaron et al. *Eyes everywhere. The global growth of camera surveillance*. London: Routledge, 2012.
17. Figueroa, Rodolfo. *Privacidad*. Santiago: Ediciones UDP, 2014.
18. Finn, Rachel & Donovan, Anna. "Big data, drone data: Privacy and ethical impacts of the intersection between big data and civil drone deployments," in: *The future of drone use*, Bart Custers (ed.). The Hague: Springer, 2016.

19. Fundación Datos Protegidos*, Drones en Chile*. Santiago: Datos Protegidos, 2017.

20. Galilea, Sergio et al. "Descentralización de servicios esenciales." *Documento de Proyecto*, CEPAL, 2011, https://repositorio.cepal.org/bitstream/handle/11362/3835/1/S2010976.pdf

21. Garay, Vladimir, "Sobre la ilegalidad de la implementación de un sistema de reconocimiento facial en Mall Plaza", *Derechos Digitales (blog)*. November 16, 2018, https://www.derechosdigitales.org/12623/sobre-la-ilegalidad-de-la-implementacion-de-un-sistema-de-reconocimiento-facial-en-mall-plaza/.

22. Garay, Vladimir, "Mal de ojo. Reconocimiento facial en América Latina", *Derechos Digitales (blog)*, November 25, 2019, https://www.derechosdigitales.org/wp-content/uploads/glimpse-cap-rec-facial.pdf.

23. Garrido, Romina & Becker, Sebastián. "La biometría en Chile y sus riesgos", in *Revista Chilena de Derecho y Tecnología*, vol. 6 n°. 1 (2017): 67-91.

24. Garrido, Romina & Matus, Jessica. "Las cámaras que no arrapan delincuentes: Situación de la videovigilancia en Chile" (2017), 10, https://lavits.org/wp-content/uploads/2017/09/P2_garridomatus.pdf

25. Gil Membrado, Cristina. *Videovigilancia y protección de datos*. Madrid: La Ley Wolters Kluwer, 2019.

26. Gray, David. *The fourth amendment in an age of surveillance*. Cambridge: Cambridge University Press, 2017

27. Guthrie, Andrew. *The rise of big data policing.* New York, NYU Press, 2017.

28. Hijmans, Hielke. "Article 51 Supervisory authority", in: *The EU General Data Protection Regulation* Christopher Kuner, *et al.* (eds.). Oxford: OUP, 2020.

29. Instituto Nacional de Derechos Humanos, *Informe Anual 2018* (2019). Available at: https://bibliotecadigital.indh.cl/handle/123456789/1173 (last visited 03.10.20): 233-257.

30. Jijena, Renato. "La Ley Chilena de Protección de Datos Personales. Una Visión Crítica desde el Punto de Vista de los Intereses Protegidos." *Cuadernos de Extensión Jurídica Universidad de Los Andes*, n° 5, 2001.

31. Lavín, Joaquín. Twitter Post. April 15th, 2017, 1:51pm, https://twitter.com/LavinJoaquin/status/853289617361178624

32. Lio, Vanesa. "Ciudades, cámaras de seguridad y video-vigilancia: Estado del arte y perspectivas de investigación." *Astrolabio*, n° 15 (2015): 273-302.

33. Leturia, Francisco. "Comentario de sentencia: Uso de globos de vigilancia." *Libertad y Desarrollo, Sentencias destacadas 2016*. Santiago: LyD, 2017.

34. Llaneza, Paloma. "Tratamiento de datos con fines de videovigilancia y denuncias internas", in Artemí Rallo Lombarte (dir.), *Tratado de protección de datos*. Valencia: Tirant lo Blanch, 2019.

35. Lovera, Domingo. "Privacidad: La vigilancia en espacios públicos", in *Informe Anual Sobre Derechos Humanos en Chile 2017,* Centro de Derechos Humanos. Santiago: Ediciones UDP, 2017.

36. Lovera, Domingo "Privacidad, espacios públicos y vigilancia", in *Anuario de Derecho Público UDP 2018,* Facultad de Derecho Universidad Diego Portales. Santiago: Ediciones UDP, 2018.

37. Malamud, Samuel. "Videovigilancia y privacidad. Consideraciones en torno a los casos 'Globos' y 'Drones'." *Revista chilena de derecho y tecnología*, vol. 7, n° 2 (2018): 137-162.

38. Ramírez, Santiago. "Del campo de batalla a las calles: el derecho a la intimidad en la era de los drones." *Revista Derecho del Estado*, n°. 35 (2015): 181-199.

39. Ramírez, Tomás. "Nuevas tecnologías al servicio de la seguridad pública y su impacto en la privacidad." *Revista Chilena de Derecho y Tecnología*, vol. 5 n°. 1 (2016).

40. Richardson, Michael. "The testimony of drones," in *Sydney Review of Books*. September 25, 2020, https://sydneyreviewofbooks.com/essay/the-testimony-of-drones/.

41. Rodríguez López de Lemus, Pedro. "Drones, videovigilancia con fines de seguridad privada y protección de datos personales." *Foro Jurídico*, n° 15 (2016): 235-240.

42. Silva, Iván. Costo económico de los delitos, niveles de vigilancia y políticas de seguridad ciudadana en las comunas del Gran Santiago, *Serie Gestión Publica*, n° 2, 2020.

43. Solove, Daniel J. *Nothing to hide. The false trade-off between privacy and security*. New Haven: Yale University Press, 2011.

44. Takahashi, Timothy, T. "Drones and privacy." *Columbia Science & Technology Law Review,* vol. XIV (2012): 112.

45. Trujillo, Lucía & Arévalo, Juan Pablo (2011): "Gestión municipal de la prevención en seguridad en barrios vulnerables." *Revista Conceptos Fundación Paz Ciudadana*, n° 23 (2011): 3, https://pazciudadana.cl/biblioteca/documentos/conceptos-no-23-gestion-municipal-de-la-prevencion-en-seguridad-en-barrios-vulnerables-su-articulacion-con-el-nivel-central-de-gobierno-un-factor-clave/

46. Vargas-Ramírez, Nicolás & Paneque-Gálvez, Jaime (2020): ""Desafíos normativos para el uso comunitario de drones en México", en *Investigaciones Geográficas* (No. 102), pp. 1-14.

47. Viollier, Pablo. *El estado de la protección de datos personales en Chile*. Santiago: Derechos Digitales, 2017.

48. Von dem Bussche, Axel & Voigt, Paul. *Data Protection in Germany*. Kumhausen: C. H. Beck, 2017.

49. Von Silva-Tarouca, Beatrice. *Setting the watch. Privacy and the ethics of CCTV surveillance*. Oxford: Hart Pub, 2011.

50. Wright, David & Finn, Rachel. "Making drones more acceptable with privacy impact assessments," in: *The future of drone use*, Bart Custers (ed.). The Hague, Springer, 2016.