COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Sensitive Personal Data, Biometrics and the Registration and Authentication of Voters: The Application of Council of Europe Convention 108

by

Professor Colin J. Bennett
Department of Political Science
University of Victoria, Canada

Paper prepared for presentation to the 44th Plenary meeting, June 15th 2023.
The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe

Table of Contents

Introduction[1]

All democratic countries require reliable methods to authenticate the identity of eligible voters. They need ways to ensure that only those eligible to vote are included in official electoral registers and that those who vote on election day are eligible to vote, and indeed, are 'who they say they are.' Over time, different democratic countries have relied on a range of methods to support both goals. For more established democratic countries, these systems of voter registration and authentication are rooted in distinct institutional and administrative practices that have strong roots in their political cultures. These practices have important legacies that are resistant to change.

In recent years, however, as a result of various forces, we have witnessed pressures in a number of countries to support or reinforce existing methods of voter authentication with new forms of identification, often based on biometric data. These trends are particularly notable in countries in the global south, where biometric methods are aggressively promoted by the burgeoning biometrics industry. Yet, biometric data is just one category of sensitive data given special protection by cross-national instruments such as Convention 108.[2] The analysis of the introduction of biometric techniques for electoral registration and authentication purposes needs to be viewed in the context of wider concerns about the processing of sensitive personal data and the potential for the profiling of the electorate.

This paper introduces the main issues relating to modern techniques for voter registration and authentication and discusses the main questions of compliance under Council of Europe Convention 108. Even where these techniques have not been introduced, the paper offers cautionary warnings about the various risks to privacy and other human rights, including rights to digital identity.

The paper begins with an overview of the main practices of voter registration and authentication. Practices vary enormously among members of the Council of Europe. Most countries do not use advanced biometrics to authenticate voters, and seemingly have no plans to do so.

The next section defines and discusses the biometric technologies promoted by the biometrics industry and their deployment in certain countries of the global south. Biometrics are often promoted to advance a wider democratic agenda to ensure that individuals have rights to a digital identity. That agenda promotes a narrative that biometrics supports the broader rights to vote and participate in democratic affairs. The next section outlines the various risks of biometric identification in the electoral context. Those risks relate to privacy, as well as to wider issues of voter discrimination and suppression.

The concluding section addresses the key principles in Convention 108 that will regulate the ways that biometric, and other forms of sensitive personal data are collected, used and disclosed within the electoral context.

[1] My thanks to Smith Oduro Marfo for assistance with the research on use of biometrics in the global south.

[2] Council of Europe (2018). Convention for the protection of individuals with regard to the processing of personal data (2018) at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (hereafter Convention 108+)

This analysis should also be read in the context of the broader questions about the processing of personal data by political organizations during, and between, elections that was the subject of earlier analysis and guidance by the Council of Europe.[3] While this earlier guidance on political campaigning was directed to political campaigning organizations, this analysis focuses more on data captured and managed by official electoral management bodies (EMBs) for the purpose of voter registration and authentication. The data controllers are therefore different, as are the relevant data protection questions under Convention 108.

Voter Registration and Authentication: A Global Overview

Democratic systems require two interlinked processes for the conduct of fair, free, and verifiable elections. The goal is to ensure that only eligible citizens can vote, and that each person has equal access to the democratic process.

First, is a process of voter **registration** – the compilation of a comprehensive list of eligible voters. In almost all countries, voters must be registered in order to be eligible to participate in an election. Voter registration is intended to ensure that everyone entitled to vote can do so, to prevent ineligible persons from voting and to guard against multiple voting by the same individual. The accuracy of the voter register is a key element in ensuring that all qualified individuals can enjoy the right to vote.

According to United Nations standards, people should not be denied registration as voters on the basis of such factors as race, sex, language or religion.[4] It is widely accepted that citizens should not have to pay a poll tax or meet literacy, income or education requirements in order to vote. Voting can legitimately be restricted, however, on the basis of citizenship, mental capacity or a criminal record.[5]

Voter registers are the consolidated official lists of all persons eligible to vote. The term '**voter list**', in contrast, is often used to refer to a list of persons registered to vote in a particular constituency or district for a particular election. Voter registers and voter lists may be assembled and maintained in a variety of ways by a range of state and local authorities. Some countries maintain national voter registers; in others, voter registers or lists are created and maintained only at the local or municipal level. Also, in some countries (such as the UK and Canada), these voter lists are shared with eligible political parties in advance of elections.

Beyond that, there are a wide variety of procedures for compiling voter registers. Some methods are *self-initiated*, such as:

[3] Council of Europe, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Guidelines on the Protection of Individuals with regard to the processing of personal data by and for electoral campaigns*. Strasbourg: Council of Europe (adopted November 19, 2021).

[4] See page 46 in United Nations (2005). Women in Elections - Guide to promoting participation of women in elections. https://www.un.org/womenwatch/osagi/wps/publication/WomenAndElections.pdf

[5] Ibid.

- In-person registration: This method involves individuals physically visiting a designated location, such as a government office or an electoral registration center to register as a voter. They typically fill out a registration form providing their personal information and may be required to present source identification documents.
- Online registration: Many countries have introduced online voter registration systems to make the process more convenient and accessible. Eligible voters can visit a dedicated website or online portal to submit their registration information electronically. This method often requires providing personal details and verifying identity through various means, such as matching the information with existing government databases.
- Mail-in registration: Some countries allow individuals to register by mail. In this method, voter registration forms are sent to eligible individuals, who fill them out and return them by mail to the relevant electoral authorities.

Other countries have adopted *state-initiated* or "automatic" registration systems. Under this method, eligible citizens are automatically registered as voters based on information available in other government databases such as:

- Residence and population records maintained by local police or administrative offices
- Census records
- Tax records

The second, and of course related process is the **authentication** of the voter when he or she casts a ballot. What form or forms of identification is/are required to verify eligibility before the ballot is filled? Is that credential permanently recorded at the time of voting? In countries, such as many in Europe, which have mandatory national identity cards, this card tends to be used as the main method of voter authentication.

In some countries which have never introduced mandatory ID systems, however, there are relatively new requirements for the presentation of a valid photo identification at the time of voting. In the United Kingdom and in some states in the US, this has led to widespread accusations of voter discrimination against poorer and more marginalized citizens, and to searching questions about the underlying partisan motivations for introducing new voter ID methods, given that incidents of voter fraud and/or impersonation are very low.[6]

In summary, systems of voter registration and authentication vary widely across democratic countries, including members of the Council of Europe. They are rooted in distinct institutional and administrative practices that have strong roots in their political cultures. These practices have important legacies that are resistant to change but they also tend to inspire trust and confidence. Incidents of voter fraud, impersonation, double-voting and so on, are not commonly found in the established democratic countries of the Council of Europe, even though misinformation on voter

[6] UK Electoral Reform Society, Voter ID: An Expensive Distraction at: https://www.electoral-reform.org.uk/campaigns/voter-id/ ; National Conference of State Legislatures, Voter ID Laws (March 9, 2023) at: https://www.ncsl.org/elections-and-campaigns/voter-id

fraud (especially with postal voting systems) regularly appears on social media, most frequently circulated by right-wing conspiracy theorists. These claims are regularly debunked.[7]

Elections and the Biometrics Industry

It is in the foregoing context that the larger debate about the use of biometric forms of identification needs to be addressed. According to the International Standardization Organization (ISO) biometrics refers to the "automated recognition of individuals based on their biological and behavioral characteristics."[8] Those characteristics are the "biological and behavioral characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition."[9] Biometric identification requires the following: a reader or scanning device to record the biometric factor being authenticated; software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data and a database to securely store biometric data for comparison.[10] Biometrics might be physiological (e.g. facial recognition, fingerprints, iris recognition, retina scanning, voice recognition) or behavioral (e.g. gait recognition, finger and hand movements). The Council of Europe has issued important guidance on the use of facial recognition that will inform any future guidance on electoral registration and authentication.[11]

A number of companies have been promoting the use of biometrics to authenticate voters, especially in countries of the global south. Such companies advance a narrative that biometrics are the only viable mechanism to secure the 'one voter, one vote' principle, especially in countries that do not have long-standing and stable traditions of competitive elections. Consider the promotional language of Thales, the large multinational technology company deeply involved in Big Data, AI and digital innovations for the defence and security, transportation, and security industries now professing to be a promoter of democracy: "A pioneer in digital security worldwide and a key player in Africa, Thales is deploying its biometric identification systems and solutions to modernize electoral rolls and open the way for people to exercise their civic rights."[12] The company then explains that "in electoral law, *the ballot is considered fair* if it meets the requirements of equality and liberty, and the secrecy of voting is respected. The usage of biometric systems in electoral processes makes it possible to meet challenges involved in implementing the principle of "one voter, one vote," which is necessary for the holding of democratic, free and transparent elections."[13]

[7] Many examples could be cited but see some of the data at EUfactcheck.eu such as: "Mostly false: Postal Voting is a big problem and electoral fraud is a sad truth in Germany" at: https://eufactcheck.eu/factcheck/mostly-false-postal-voting-is-a-big-problem-and-electoral-fraud-is-a-sad-truth-in-germany/

[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en

[9] Ibid.

[10] Alexander Gillis, Peter Loshin and Michael Cobb, "What is biometrics?" at: https://www.techtarget.com/searchsecurity/definition/biometrics

[11] Council of Europe, Guidelines on Facial Recognition (2021) at: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

[12] Thales Inc. Biometric Voter Registration: Trends and Best Practices. (March 23, 2021) at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/enrolment/biometric-voter-registration

[13] Ibid.

Another active company in the promotion of biometrics in elections is Innovatrics. In its Trust Report, Innovatrics claims that countries across the world can utilize biometrics to cultivate democracy: the number of democracies is declining, as is the number of citizens who can exercise democratic rights. Biometrics can "come to the rescue" by instilling higher levels of trust, the bedrock of democratic processes.[14] The company offers an integrated "biometric voter registration system" combining "customizable registration software, accurate biometric deduplication and automated detection of children or minors based on AI-powered age estimation." These systems produce "clean voter lists" in countries with "unreliable ID systems."[15]

There is little reliable or objective evidence on whether or not biometric systems do indeed enhance democratic institutions and procedures in the global south. They can be effective in supporting voter registration drives where national population registers are non-existent or fragile. Biometrics can be used effectively to prevent multiple registrations and to prevent the registration of disqualified voters. Multiple registrations are not necessarily motivated by nefarious reasons, such as desire to vote multiple times to influence election outcomes. More likely, multiple registrations occur because of inefficient procedures for registering a change in address. Many electors may re-register without having their existing record deleted. Biometric registration can mitigate this problem.[16] It is also claimed that the more efficient voter registration that biometrics arguably removes one potential argument for the challenge of results by the losing candidate or party.

At the same time, biometrics have no direct impact on voter intimidation or vote buying or on the manipulation of rules on ballot access, on campaign finance support, or on the restrictions on access to campaigning tools and platforms. Even with a clean and comprehensive voter list, votes can be intentionally miscounted, vote tallies altered or large numbers of votes ignored.[17] It has also been claimed that biometric election strategies can be counterproductive, creating a symbolic impression of fairness and efficiency, in order to legitimize elections fraudulently manipulated by elites by other means. For some political elites, "biometrics can help sustain an undemocratic political order."[18]

Biometric systems are also costly, of course, in terms of readers and infrastructure, maintenance and upgrades, and the training of staff and volunteers, many of whom have to operate in remote and often rural locations, with weak or unstable communication networks. The technological investment costs can produce a dependency on Western companies, and may represent the latest example of "liberal interventionism." Developing, and particularly African, countries have

[14] Innovatrics, "Biometrics to the Rescue: Helping democracies to build elections that can be trusted." Trust Report, Issue #3 (December 2022) at: https://innovatrics.com/trustreport/

[15] Ibid.

[16] Rawlson King, "Biometric voter enrollment engenders rewards and risks," Biometric update, April 11, 2014 at. https://www.biometricupdate.com/201404/biometric-voter-enrollment-engenders-rewards-and-risks

[17] Alan Gelb and Anna Diofasi, Biometric Elections in Poor Countries: Wasteful or a Worthwhile investment? -- Working Paper 435. Center for Global Development, August 15, 2016 at: https://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment

[18] Marielle Debos, "The productive failures of biometric voting in Africa," June 14 2021 at: https://democracyinafrica.org/the-productive-failures-of-biometric-voting-in-africa/

become laboratories for the trialling of these new technologies while leaving other reasons for democratic deficits unaddressed.[19]

Appendix 1 presents a table of biometric voter registration and authentication systems in nine countries of the global south, together with: metrics of democracy, the biometrics collected at registration and at the time of voting, and their current data protection status.

Data from the Institute for Democracy and Electoral Assistance demonstrates that the use of any biometric data for registration and/or voter authentication in Europe is still rare.[20] The vast majority of European states (86%) construct their national electoral registers from existing population and civil registries. Some countries, however, do use online access to the central voting register, or the local polling register, to authenticate voters. The overall picture from these data is that the vast majority of European states, and signatories to Convention 108, continue to use relatively traditional and legacy methods to register voters and to authenticate the voter on election day.

That said, pressures from international business interests, and from the familiar technological imperative of ‘function creep’ will presumably attract attention in more long-standing democratic countries as well as others. Mail-in voting processes became increasingly adopted, and popular during the COVID-19 pandemic. Online voting procedures, requiring new forms of authentication, are also actively considered in some countries. It cannot be assumed that these pressures for the use of biometrics will not be experienced in the more established democracies within the Council of Europe. Experience of the spread of biometrics, such as facial recognition, suggests that, even without evidence of widespread problems, technological solutions will continue to be advocated.

Digital Identity Rights

Biometrics, as claimed by companies such as Thales and Innovatrics, also facilitate wider agendas by international organizations for rights to digital identity. So, concerns about privacy, data protection and human rights associated with the introduction of biometrics into elections, are confronted by considerable pressures for rights to digital identities, supporting the provision of government services, including the right to vote. The United Nations Sustainable Development Goal 16 seeks to “Promote peaceful and inclusive societies for sustainable development, provide Access to justice for all and build effective, accountable and inclusive institutions at all levels.”[21] One of the targets is “to provide legal identity for all, including birth registration” “by 2030”.[22]

The World Bank’s Identification for Development Initiative (ID4D) articulates the aim of enabling “all people to exercise their rights and access better services and economic opportunities in line with the Sustainable Development Goals” as “especially important as countries transition to digital

[19] Katja Lindskov Jacobsen, “Biometric voter registration: A new modality of democracy assistance,” *Cooperation and Conflict* (2020), Vol. 55(1): 127-148.

[20] Institute for Democracy and Electoral Assistance, ICTS in Elections Database at: https://www.idea.int/data-tools/continent-view/Europe/61

[21] https://sdgs.un.org/goals/goal16

[22] Ibid.

economies, digital governments, and digital societies" and to this extent, "inclusive and trusted ID systems are key to ensure the benefits are realized by all as well as for safeguarding privacy."[23]

The Council of Europe published guidelines on National Digital Identity in 2022.[24] These Guidelines recognize that: "A key justification for digitizing 'legal identity' and creating national digital identity schemes and systems (NIDS), is that they ensure and guarantee legal security and certainty but could also facilitate easier access to social and economic rights and entitlements and provide broader societal protections such as personal and societal security."[25] However, "while NIDS may bring significant benefits and protections in multiple contexts, and allow individuals to obtain and assert important rights, they may also have adverse consequences for the human rights of individuals and communities and groups of individuals. These consequences can range from discrimination and exclusion to marginalization, to unwarranted profiling and surveillance, to a person's loss of control over their identity or even the misuse or theft of one's identity."[26] The Guidelines then go on to demonstrate how national identification schemes should explicitly integrate human rights considerations as anchored in international human rights law into the policy, design, implementation, and operation of national digital identity schemes and systems.[27]

Before analyzing the more specific application of Convention 108 to the use of biometrics in voter identification, it is important to outline the various possible threats to privacy and other human rights. In light of these guidelines, what are the specific 'human rights considerations' that need to be considered in the design of biometric identification systems?

Biometric Voter Registration: The Risks to Privacy and other Human Rights

In addition to the broader questions about whether biometric voter registration and authentication systems actually do promote democratic institutions and practices, there are also, of course, a number of interrelated risks to privacy and human rights, specific to biometrics and specific to voting.

First, there are risks to *the secrecy of the ballo*t. Ballot secrecy is one of the cornerstones of democracy, and is guaranteed in national constitutions and international conventions. The secret (or Australian) ballot is typically defined as having four essential elements: an official ballot being printed at public expense; on which the names of the nominated candidates of all parties and all proposals appear; being distributed only at the polling place; and being marked in secret.[28]

The secret ballot is normally justified in instrumental terms: it prevents or discourages attempts at bribery and intimidation. But there is a deeper, and more substantive, justification. As expressed

[23] ID4D Initiative (n.d). About us. https://id4d.worldbank.org/about-us

[24] Consultative committee of the convention for the protection of individuals with regard to Automatic processing of personal data- convention 108 - *Guidelines on National Digital Identity*. November 18, 2022: https://rm.coe.int/t-pd-2021-2rev9-guidelines-digital-identity-2761-5846-6310-2/1680a95e1e

[25] See page 3

[26] Ibid.

[27] See page 4

[28] See, for example, the campaign of the Electronic Privacy Information Center (EPIC) on "Voting Privacy." https://epic.org/privacy/voting/

by Anabelle Lever: “citizens’ rights to vote does not depend on the approval of others, or on the demonstration of special virtues, attributes or possessions. While democratic rights to freedom of expression and association mean that citizens are free to consult anyone they want, the secret ballot means that they can share in collectively binding decisions without having to bare their souls to anyone who asks.”[29] The secret ballot, and the privacy upon which it depends, marks our status as citizens. It is important in itself, regardless of what functions it performs.[30]

The introduction of any new election technology needs first to be tested against this fundamental principle. The non-violation of the secret ballot goes to the heart of democratic practice. The use of biometrics for registration and/or authentication purposes can only be justified if it serves this essential and long-standing principle.

There are *risks of voter discrimination and disenfranchisement*, especially for marginalised communities. Although biometric forms of identification have improved over time, they are still imperfect and susceptible. Furthermore, there is compelling evidence that errors are not randomly distributed across populations, but tend to disfavor certain groups and communities. In the electoral context, problems of data quality can therefore lead to persistent disenfranchisement.

At the moment, most countries using biometrics for electoral registration use fingerprints, often claimed as a highly reliable source of identification in the law-enforcement context. However, fingerprints suffer from a range of problems. There are a range of physiological issues (injured fingers, dry fingers, worn ridges due to occupation). Fingerprints also degrade over time. Women tend to have lower quality images than men. There are behavioral problems, when the subject is nervous or uncooperative. There are environmental variables – such as humidity and temperature - and there are operational and technical issues ranging such as unclean scanners, and the ease of use of the graphical user interface. Fingerprints are not secure; they can be easily extracted from surfaces.[31]

A smaller number of countries have deployed facial recognition technology (FRT) systems for electoral registration. There is a wide and complex literature on facial recognition systems, and an intense debate over the extent to which the underlying algorithms manifest a racial bias. According to a National Institute of Standards and Technology analysis of 189 facial recognition algorithms, most falsely identified black and Asian faces more often than white faces.[32] The technologies also falsely identified women more than they did men, making Black women particularly vulnerable to algorithmic bias.

[29] Lever, A. (2015). Privacy and democracy: What the secret ballot reveals. Law, Culture and the Humanities, 11(2), 164-183.

[30] Ibid.

[31] Rama Krishnan, *Fingerprint capture: Challenges and Opportunities*. US Department of Homeland Security (2021) at: https://www.nist.gov/system/files/documents/2021/08/19/krishnanl_bquality_workshop1_version_for_proceedings.pdf

[32] Patrick Grother, Mi Ngan, Kayee Hanaoka, Face Recognition Vendor Test (FRVT): Demographic Effects, Department of Commerce, National Institute of Standards and Technology (NIST) (December 2019) at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=4

Studies on FRT are typically directed towards discrimination in law enforcement. The main recent experience of the use of FRT in elections is in Nigeria where, despite the use of both fingerprint and facial recognition, nearly 45% of completed registrations were invalid, necessitating a massive clean-up of the database in advance of the 2023 elections.[33]

There are huge *risks of security and data breaches*. The collection, use and storage of biometric data in the electoral context opens up a range of critical questions about data security and safeguards. Election registration data has been vulnerable to accidental breaches, as well as malicious hacking, in many countries. The addition of a biometric dimension to these systems probably exacerbates the various security risks. As Appendix 1 demonstrates, many of the countries in which biometric identification has been introduced, do not have robust or established data protection rules and oversight. Standard data protection questions about appropriate security of the data at rest and in transmission, about access controls, about retention rules and about levels of encryption, all need to be addressed. The distribution of registration data to remote polling places also exacerbates security issues.

There are risks of *spill-over of election registration data to political campaigning organizations*, political parties and candidates, who might use it for: political marketing; voter intimidation or suppression; the integration of formal registers with other forms of personal data on political views and behavior. In some countries (e.g. the UK, Canada, Australia and the United States), official voter lists may be shared with official political parties and candidates in advance of an election, for the sole purpose of communicating with electors and distributing political messages. The distribution and retention of these lists is regulated by national election legislation, which often contains strict penalties for illegitimate use and disclosures. However, the official registration data has also allowed political parties in these countries to build large voter relationship management systems, supplemented by a range of data from many other sources, and permitting the profiling of the entire electorate on various indices of political affiliation and persuasion.[34]

In conclusion, there are always risks associated with the *integration of election registers with other state databases.* The collection, use and disclosure of voter registration data have typically been tightly regulated in European societies under both data protection and election law. Any sharing of these data for legitimate purposes is also governed by information sharing/matching agreements and overseen by data protection and election supervisory authorities.

In other countries, however, the development and expansion of election registration databases, based on biometric identifiers, has produced enormous pressures for the wider integration of these systems with national identification systems. In India, for instance, the famous Aadhaar database is now one of the world's largest biometric identity programs designed to facilitate Indians accessing various state subsidies. Aardhaar is based on fingerprints and iris scans. In 2021, the Election Commission of India announced that it wanted to link their voter registration database with Aadhaar, to combat fraud and registration errors. In December 2021, the legislature passed the Election Laws Amendment Bill, creating a legal framework for integrating the two

[33] Nigeria adds facial verification for voter verification. *Digwatch,* April 13, 2022 at: https://dig.watch/updates/nigeria-adds-facial-recognition-for-voter-verification

[34] Colin J. Bennett, "Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?" *International Data Privacy Law* (2016): Vol. 6. No. 4.

systems. Critics have argued that the linkage of the two systems could lead to disenfranchisement and increased voter microtargeting. Further, India's plans for integration of the biometric identification system with its voter registration database provides a model and precedent that other governments in the global south would be tempted to emulate.[35]

Convention 108+ and the Use of Sensitive Data for Election Registration and Voter Authentication

There are clearly a different set of data protection issues relating to the management of data about electors for purposes of registration and authentication, from those associated with political campaigning. Most notably, election registration data is identifiable, and has to be in order to satisfy the right to vote.   In that sense, it is quite different from the range of personal data – identifiable, aggregate, anonymized – that might be processed for the purpose of targeting electors in political campaigns.   Further, the legitimate purpose of the capture of these data is to promote the official right to vote, fairly, equitably and in secret.   That public interest is different from that supporting the right of political organizations to communicate with the electorate, and any guidelines need to reflect those differences.

The following outlines the main issues relating to the application of Convention 108 to the sensitive data captured on electors, by and for EMBs in order to satisfy the right to vote and free and fair elections.   This outline suggests a possible framework for future guidelines on the subject, directed to EMBs and third party processors (including those in the biometrics industry) who may process personal data on electors at any stage in the electoral cycle.

1) The legitimacy of processing and the quality of data in light of the questions of legitimate purposes of voter authentication (Article 5)

Convention 108 stipulates that "data processing shall be proportionate in relation to the legitimate purpose and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake." [36] Data processing shall either be carried out on the basis of "free, specific, informed and unambiguous consent of the data subject" or of some other legitimate basis laid down by law. Further, the data controller "is not permitted to process data for undefined, imprecise or vague purposes."[37]

The Convention also specifies "freedom of expression" as a legitimate interest that needs to be balanced against the rights of the data subject. The Explanatory Report mentions "journalistic, academic, artistic or literary expression" in this context. There is no mention of political expression, and voting rights   but it can be presumed that the purpose of registering and

[35] Patrick Jones, "Lessons from India's attempt to marry biometric and voter ID databases,"   Brookings, Tech Stream.   April 27, 2022 at: https://www.brookings.edu/techstream/lessons-from-indias-attempt-to-marry-biometric-and-voter-id-databases/

[36] Convention 108+ Article 5.

[37] Council of Europe (2018). Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, p. 8. CETS 223 at: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

authenticating voters is a strong and universal one, and a "legitimate basis for the processing laid down by law." The legitimate purpose should be clearly understood as that of advancing the right to vote, and promoting the fairness and integrity of the electoral system.

In some countries, complete voters' lists are shared legally with parties and candidates at the beginning of each electoral cycle to assist their communication efforts. Practices differ on how those lists are transferred, whether they are done digitally and for how long they may be retained. The conditions of those transfers should also be clearly stipulated by law.[38]

2) Special categories of data: Biometric data that uniquely identifies an individual and relates to political opinions and behavior (Article 6)

Under Convention 108+, "personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention." It goes on: "Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."[39] The dangers of discrimination from the inappropriate processing of sensitive biometric data are highlighted above.

In the context of election registration and voter authentication, it can be presumed that the personal data in electoral registers is defined as a special category of data. EMBs may not only capture basic identification information, but necessarily data on who has, and has not, voted in any given election. Those records will not reveal how an individual voted, but most certainly whether they voted. And while national practices will vary concerning the retention of such data, it can be presumed to be a special category. If biometrics are also employed, "for the purpose of uniquely identifying a natural person" then the need for the appropriate safeguards stipulated by the Convention is reinforced.

3) Data security and confidentiality (Article 7)

The conduct of free and fair elections inevitably involves access to data on voters by large numbers of election workers and volunteers in distributed locations. EMBs should take appropriate security measures to prevent accidental or unauthorized destruction, loss, use, modification, disclosure or access to personal data. These measures include: training in privacy and security; access controls; confidentiality agreements; and physical controls. EMBs are involved in processing voters' data on a large-scale over several election cycles. Applying appropriate security measures to this data, and its processing environments both at rest and in transit, is vital to ensure voters' data are protected to the highest standards. Security measures should consider the current state of the art data-security methods and techniques in the field of data processing. Their cost should be commensurate with the seriousness and probability of the potential risks.[40]

[38] Guidelines on Political campaigning, Section 4.8.

[39] Convention 108+, Article 6

[40] Explanatory report, para 63.

EMBs should report to supervisory authorities as prescribed by Convention 108+ and to the data subjects themselves in the event of data breaches which may seriously interfere with the rights and fundamental freedoms of voters in accordance with Article 7(2) of the Convention. Notification should include adequate and meaningful information about possible measures to mitigate the adverse effects of the breach.[41]

The use of biometric identifiers in election registration and authentication also involves responsibilities by a range of by third party service providers. EMBs should demonstrate that all processors comply with their obligations in accordance with Articles 7(1) and 10 of the Convention. Privacy impact assessments prior to processing should assess whether data is protected against unauthorised access, modification and removal/destruction. Risk assessment should seek to embed high standards of security throughout the processing. Assessments should be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data on electors.

4) The transparency of processing (Article 8)

EMBs are required to be transparent about the legal basis for processing, the categories of data processed, the recipients of that data, and the means of exercising data protection rights.[42] Certain essential information about the processing should be provided in a proactive manner, and may occur at any stage of the electoral cycle. This information should include the identity of the controller, the legal basis for processing, the categories of data processed and the means of exercising rights. Information may also include the preservation period, the reasoning underlying the data processing, and information on data transfers.[43]

Convention 108+ also states that every individual has the right "not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration." [44] According to the Explanatory Report, the "data subject should have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that might have an impact on the result of the automated decision."[45] In the context of election management, this requirement means constant attention to the rights of data subjects to add their names to election registers, in order to correct name and address errors.

It is almost impossible to separate issues of automated processing from those of automated profiling, defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, heath, personal preferences, interests, reliability, behavior, location or movements."[46] In

[41] Explanatory report, para 66.

[42] Convention 108+ Article 8.

[43] Explanatory Report, p. 12.

[44] Convention 108+, Article 9.1

[45] Explanatory Report, p. 13.

[46] See Article 4(4) of UK GDPR.

the electoral context, there are concerns that voter profiling can have a “chilling effect” on freedom of speech and participation. It is widely recognised that the feelings of being under surveillance can impair the exercise of fundamental freedoms, including participation in elections.[47]

It is difficult to envisage circumstances under which an EMB could legitimately “profile” voters and non-voters based on data contained in electoral registers. Nevertheless, any profiling (for example on patterns of voter turnout) should be limited to those categories that the data subject can reasonably be expected to consider in view of the legitimate purposes of the processing.[48] Profiling must contribute “both to the well-being of individuals and to the development of an inclusive, democratic and sustainable society.”[49] Profiling must not result in discrimination against individuals, groups or communities. It must “neither undermine the dignity of persons, nor democracy.”[50]

5) The rights of data subjects (Article 9)

Voters should be able to obtain on request and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, and access to that data in an intelligible form. Voters are entitled to be informed how their personal information was obtained, and from what source. Voters should be able to object to the processing of data on him or her, and to request rectification or erasure, as the case may be, if the data is inaccurate, obsolete or incomplete.[51] Voters are entitled to know about the reasoning underlying the processing of their personal data by political campaigns. This may be particularly important where a voter is contacted by a political party with whom they have not had a prior relationship. Voters are entitled to remedy if their rights are not respected by political campaign organizations. Voters are entitled to benefit from the assistance of a supervisory authority in exercising their rights.

In the case of countries with automatic, or pro-active voter registration systems, an interesting question arises as to whether, or not, voters are entitled to permanently delete their personal data from election registers if they never intend to vote, either now or in the future. The practices of national EMBs vary on this question. Some EMBs have adopted a public and comprehensive mission to increase voter turnout, to encourage registration, and tend to make it very difficult for individuals to “de-register” on the grounds that they want to take no part in the democratic process.[52] Other countries, such as Belgium, go one step further and make voting mandatory thereby necessitating the maintenance of a universal electoral register, with no, or little, opportunity to opt-out. Belgian citizens are required to present themselves at a voting place, even if they do not actually exercise their right to vote.[53]

In countries where biometric forms of identification have been adopted, a further issue arises if the voter prefers to register to vote using more traditional (non-biometric) forms of identification

[47] Joint Report of Venice Commission, June 2019, p. 20.

[48] *Profiling and Convention 108*, 7 November 2019, p. 4.

[49] Ibid, page 3

[50] Ibid

[51] Explanatory report, para. 72.

[52] The policies of Elections Canada fall within this category.

[53] “How to Vote in Belgium” at: https://www.european-elections.eu/how-to-vote/belgium

– such as a primary source document such as a birth certificate. The requirements of Convention 108 would suggest that voters should be allowed to register to vote, and to vote, using other valid forms of identification. The submission of a biometric should never, therefore, be required as a *condition* for exercising one's democratic rights. But the ability to exercise this right becomes increasingly difficult as election registers are derived from, linked with, and/or matched against other state administered and biometric-based identification systems, such as that administered by India, discussed above.

6) Additional obligations of Election Management Bodies (Article 10)

The obligation rests with the EMB to ensure adequate data protection and to be able to demonstrate that data processing follows applicable laws. The accountability of data controllers and data processors must be clearly set out in any contractual arrangements, defined by the nature of the processing, in accordance with Article 10(1) of the Convention 108+. In most countries, these obligations are also set out in relevant provisions of election law.

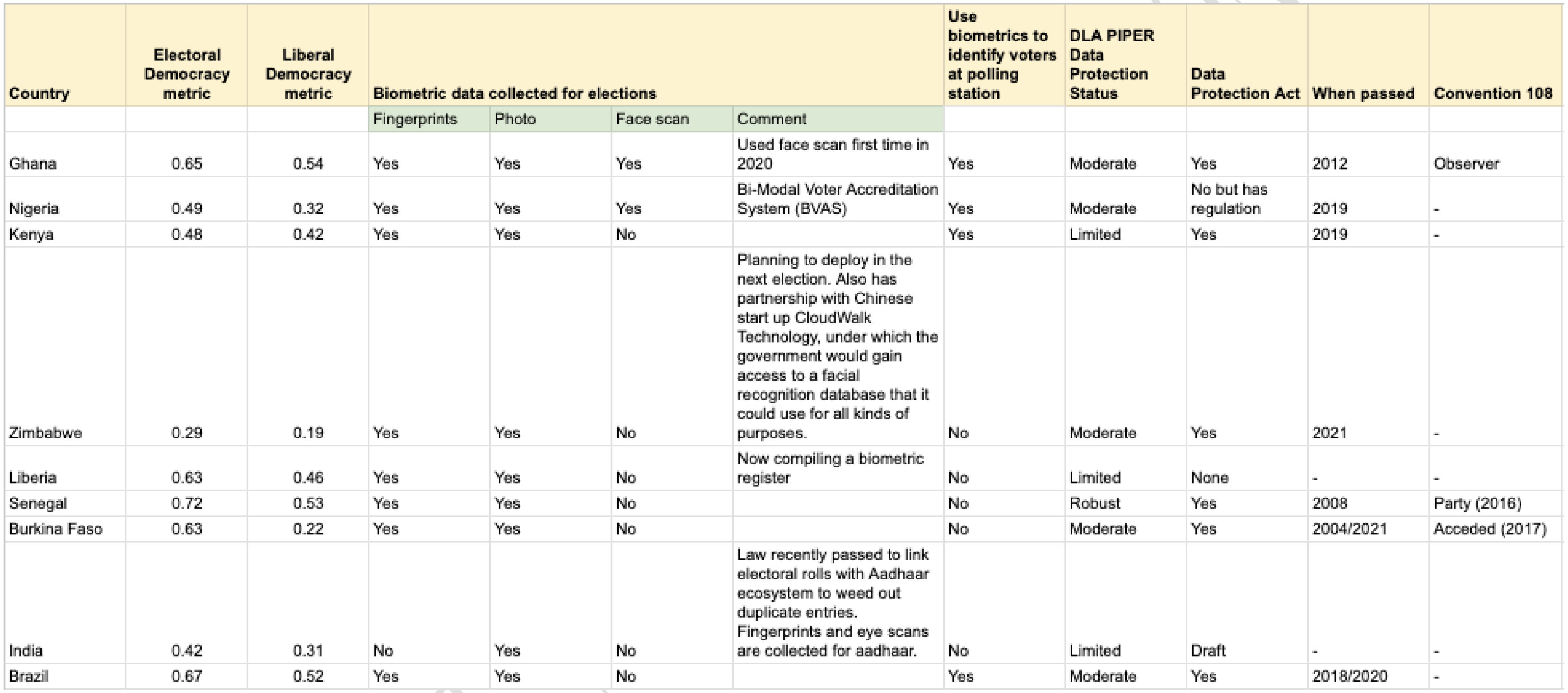
EMBs must also be able to provide a full record of how personal data has been obtained and is being processed, as well as demonstrate compliance of any third-party organization that processes personal data on their behalf. They must assess the likely impact of intended data processing on the rights and fundamental freedoms of the voter, prior to the commencement of data processing and should design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms (Article 10(2)).

Privacy risk assessments should not only assess the specific impact on an individual voter's rights, but should also consider whether the processing is in the best interests of broader democratic values and the integrity of democratic elections. EMBs should encourage and implement a comprehensive and compliant data governance culture throughout the political organization, both during and between election cycles. EMBs should appoint an officer or officers responsible for the verification and demonstration of compliance with the data protection principles enshrined within Convention 108+.[54]

In most countries, the effective enforcement of data protection principles requires close cooperation between the EMB and the data protection supervisory authority, on guidance and enforcement matters, as envisaged under Article 15.

[54] Explanatory report, para. 87.

Appendix 1: Snapshot of Biometric Data and Elections in some Global South countries[55]



Country	Electoral Democracy metric	Liberal Democracy metric	Biometric data collected for elections				Use biometrics to identify voters at polling station	DLA PIPER Data Protection Status	Data Protection Act	When passed	Convention 108
			Fingerprints	Photo	Face scan	Comment					
Ghana	0.65	0.54	Yes	Yes	Yes	Used face scan first time in 2020	Yes	Moderate	Yes	2012	Observer
Nigeria	0.49	0.32	Yes	Yes	Yes	Bi-Modal Voter Accreditation System (BVAS)	Yes	Moderate	No but has regulation	2019	-
Kenya	0.48	0.42	Yes	Yes	No		Yes	Limited	Yes	2019	-
Zimbabwe	0.29	0.19	Yes	Yes	No	Planning to deploy in the next election. Also has partnership with Chinese start up CloudWalk Technology, under which the government would gain access to a facial recognition database that it could use for all kinds of purposes.	No	Moderate	Yes	2021	-
Liberia	0.63	0.46	Yes	Yes	No	Now compiling a biometric register	No	Limited	None	-	-
Senegal	0.72	0.53	Yes	Yes	No		No	Robust	Yes	2008	Party (2016)
Burkina Faso	0.63	0.22	Yes	Yes	No		No	Moderate	Yes	2004/2021	Acceded (2017)
India	0.42	0.31	No	Yes	No	Law recently passed to link electoral rolls with Aadhaar ecosystem to weed out duplicate entries. Fingerprints and eye scans are collected for aadhaar.	No	Limited	Draft	-	-
Brazil	0.67	0.52	Yes	Yes	No		Yes	Moderate	Yes	2018/2020	-

[55] This table is constructed with data from multiple sources. Democracy scores are from Ourworldindata.org/democracy; Biometrics data are mostly from International IDEA's database on ICTs and elections: https://www.idea.int/data-tools/data/icts-elections; data protection status are based on metrics from DLA PIPER: https://www.dlapiperdataprotection.com/ ; and comments are from various news sources.