Technical Considerations and Data Protection in the Catalan independence referendum of 2017

Tamara Álvarez Robles
Ricardo J. Rodríguez

March 30, 2019

RootedCON 2019

About us

Tamara Álvarez Robles

- **PhD. of Constitutional Law** (University of Léon, 2018)
  PhD title: *"The right of access to the Internet in Spanish constitutionalism"*
- Lecturer at the University of Vigo, Constitutional Law
- Collaborates with the University of León teaching at MSc. level:
  - Research in cybersecurity
  - Cybersecurity Law and Digital Environment
- Also collaborates with the University of Burgos teaching in the MSc. in Business intelligence and big data in secure environments

Ricardo J. Rodríguez

- **PhD. of Computer Sciences** (University of Zaragoza, 2013)
- Professor at Centro Universitario de la Defensa, General Military Academy
- *Research interests*:
  - Performance/dependability/survivability analysis
  - Program binary analysis
  - Contactless cards security

Ethical considerations - disclaimer

- **Right to participate and to vote freely in a legal referendum**
- **None is above the laws**
- **A referendum must have a minimum set of rules to be accepted internationally as a legal referendum** ("Draft guidelines on referendum," European Commission for democracy through law [Venice Commission], techreport 371/2006, Sep. 2006)

The only immutable laws are the physical laws of nature

- Politicians shall do their job: **make politics** to change the laws without committing any illegality
  - Here, **we consider the legal point of view with regard to the Spanish Constitution**
  - Remark that, unlike the German Constitution, the Spanish Constitution does not have any intangibility clauses and hence any of its parts is susceptible of modification

Agenda

1. Introduction to Spanish Constitution & the political conflict
2. Electoral census and data protection principles
3. Censorship and censorship-resistance: Techniques used for the 1-O
4. Legal implications
5. Conclusions

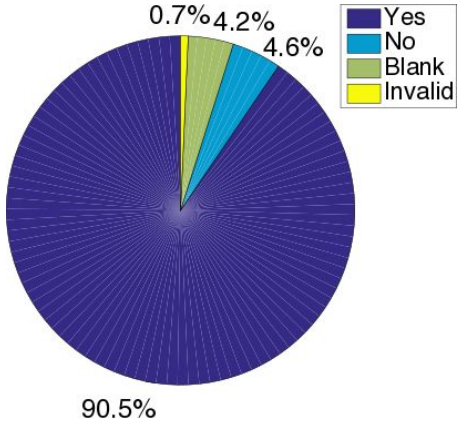
Agenda

1. **Introduction to Spanish Constitution & the political conflict**
2. Electoral census and data protection principles
3. Censorship and censorship-resistance: Techniques used for the 1-O
4. Legal implications
5. Conclusions

1. Introduction -- Spanish constitutionalism 101

The Spanish Constitution of 1978:

- Entered into force on **December 29, 1978**
  - **Ratification in referendum** by the Spanish people on December 6, 1978
  - **Total participation: 67.1% (26.632.180 electors)**
    - **Participation in Cataluña: 67.9% (4.398.173 electors)**
      - www.bcn.cat/estadistica/angles/dades/telec/ref/ref78/r22.htm



- **Influenced by other Constitutions:**
  - German, French, Portugues, Italian, Mexican
  - Spanish historicals: 1812, 1931, etc.

1. Introduction -- Spanish constitutionalism 101

TERRITORIAL ORGANIZATION

- **Mainly influenced by the Italian Constitution and the Spanish's 1931**
- Title VIII: 17 Autonomous Communities + 2 Autonomous Cities
- Two ways to create an Autonomy:
  - **Fast way**: with a higher level of competences at the beginning (first 5 years), plus a referendum. Secc. 151, DT 2nd SC.
    - First communities were Basque Country, Catalonia, and Galicia
  - **Slow way**: less competence level at the beginning and no referendum needed. Secc. 143 + 148.2 SC.

1. Introduction -- Spanish constitutionalism 101

TERRITORIAL ORGANIZATION

Their basic norm is the <u>Statute of Autonomy</u>

- A Statute of Autonomy is a **special National Organic Law**
  - This means that **it needs to be first approved in the Autonomous Courts and then in the General Courts**
  - *Recall that the General Courts exercise the legislative power of the State in Spain, and is based on a **bicameral Parliamentary system**: the Congress of Deputies (the lower house) and the Senate (the upper house)*
- Autonomous Communities: Executive + Legislative Powers

1. Introduction -- Spanish constitutionalism 101

Understanding Spanish Constitutional system related with Autonomous Communities

- We have a **system of shared powers** (sec. 148 and 149)
  - *“Matters not expressly assigned to the State by this Constitution may fall under the jurisdiction of the Autonomous Communities by virtue of their Statues of Autonomy”*
  - **Close to a federal proposal** (sec. 149.3) **BUT** the competence over the matters that have not been assumed by the Statutes of Autonomy will correspond to the State
- The **prevalence clause**: *“State, whose laws shall prevail”* (sec. 149.3)

1. Introduction -- Spanish constitutionalism 101

Understanding Spanish Constitutional system related with Autonomous Communities

- Recall that **autonomy ≠ soberany** (art. 2 SC)
- The control of Autonomous Communities is based on **legal principles of jurisdiction** (sec. 153)
- Autonomous Communities participate in State decisions through:
  - The Senate (sec. 69)
  - Legislative process (sec. 87.2 and 109)
  - In planning general economic activity (sec. 131.2)

NOTE that *"under no circumstances shall a federation of Autonomous Communities be allowed"* (sec. 145.1)

1. Introduction -- Spanish constitutionalism 101

Catalonia

- **Fast way**: 2nd transitional provision + secc.151.2 SC
- **Referendum Oct 25, 1979**
  - **59.7% of participation** (4.421.965 electors), 88.2% favorable (52.66% total census)
  - Check the details in http://www.bcn.cat/estadistica/angles/dades/telec/ref/ref79/r21.htm
- **Referendum to reform the Statute of Autonomy in August 2006**:
  - **48.9% of participation** (5.310.103 electors), 73.2% favorable (35.8% total census)
  - More details in http://www.bcn.cat/estadistica/angles/dades/telec/ref/ref06/r21.htm
  - The right-wing party in Spain (opposition political party at that time) + 5 autonomous communities (Region of Murcia, Valencian Community, La Rioja, Balearic Islands, and Aragon) presented several actions of unconstitutionality against some parts of the new Statute

1. Introduction -- Spanish constitutionalism 101

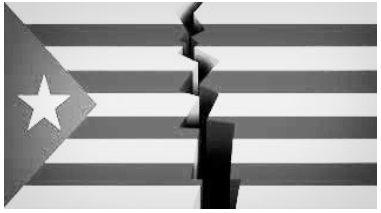
Catalonia

- **June 28, 2010:** Constitutional Court of Spain stated that 14 articles were unconstitutional while other 27 are subject to Court's interpretation
  - The Statute of Autonomy of Catalonia in 2006 was composed of 223 articles (plus provisionals)
- **July 10, 2010**: public protest organized by Òmnium Cultural
  - Supported also by 4 out of 6 political parties of the Parliament of Catalonia
  - Slogan "*Som una nació. Nosaltres decidim*" ("We are a nation. We decide")

1. Introduction

The independence process of Catalonia faced with the Spanish's Constitutional System - 1st October, 2017

A political problem that became juridical



1. Introduction - The road to Oct 1, 2017

Initial situation: 2013-2015

- **Two resolutions** adopted by the Plenum of the Catalan Parliament
  - **Resolution 5 / X of January 23, 2013**. *Declaration of sovereignty and the right to decide of the people of Catalonia*
  - **Resolution 1 / XI of November 9, 2015**: Resolution on the start of the political process in Catalonia, as a result of the electoral results of Sept 27, 2015

- **Law 10/2014, of September 26**: Non-referendum popular consultations and other forms of citizen participation
  - **Note that:** Regulatory framework is Secc. 92 SC + Organic Law 2/1980, of January 18, on regulation of the different modalities of referendum

1. Introduction - The road to Oct 1, 2017

- Radical contraventions of the basis principles of the constitutional order:
  - **Sovereignty of the Spanish people**
  - **Unity**

- Manifestations of the **democratic principle and the right to participate in public affairs**

Ø The rejection of sovereign proclamations and the constitutionality of the "right to decide" as a political aspiration

- Spanish Constitutional Court:
  - **Judgment 42/2014**
  - **Judgment 259/2015**

ØPopular queries and referendum

- Spanish Constitutional Court:
  - **Judgment 31/2015**
  - **Judgment 32/2015**
  - **Judgment 138/2015**

1. Introduction - The road to Oct 1, 2017

Wait… what was the 1-O? A referendum?

- Up to 2015, three judgments of the Constitutional Court on the **unconstitutionality of such consultations**. Then, it is a **non-referendum**

➔ **Substantive reasons**: **such consultations are materially referendal** in nature
  - Involve an appeal to the citizens by voting and establish a procedure and guarantees for this (Judgement 32/2015)

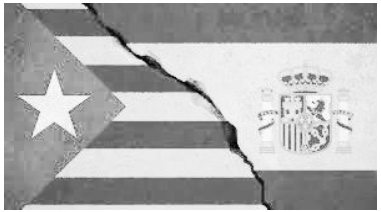
➔ **A competence aspect**: **jurisdiction over referendum corresponds to the State**
  - Article 149.1.32 SC (Judgment 32/2015)

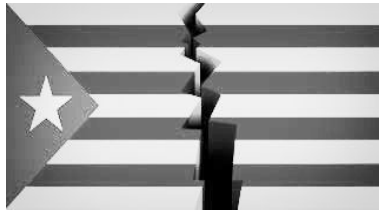
➔ **Competence order**: popular consultations, including participatory processes, **cannot alter the procedure of the constitutional review or be considered as preparatory acts of itself**
  - So, they cannot take place (Judgement 138/2015)

1. Introduction

The independence process of Catalonia faced with the Spanish's Constitutional System - 1st October, 2017

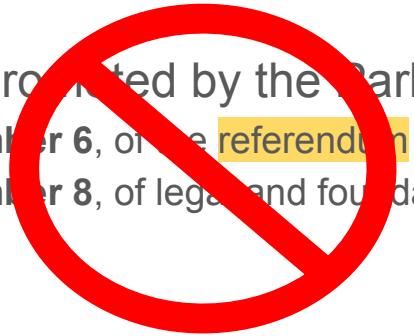
2nd round





1. Introduction - The road to Oct 1, 2017

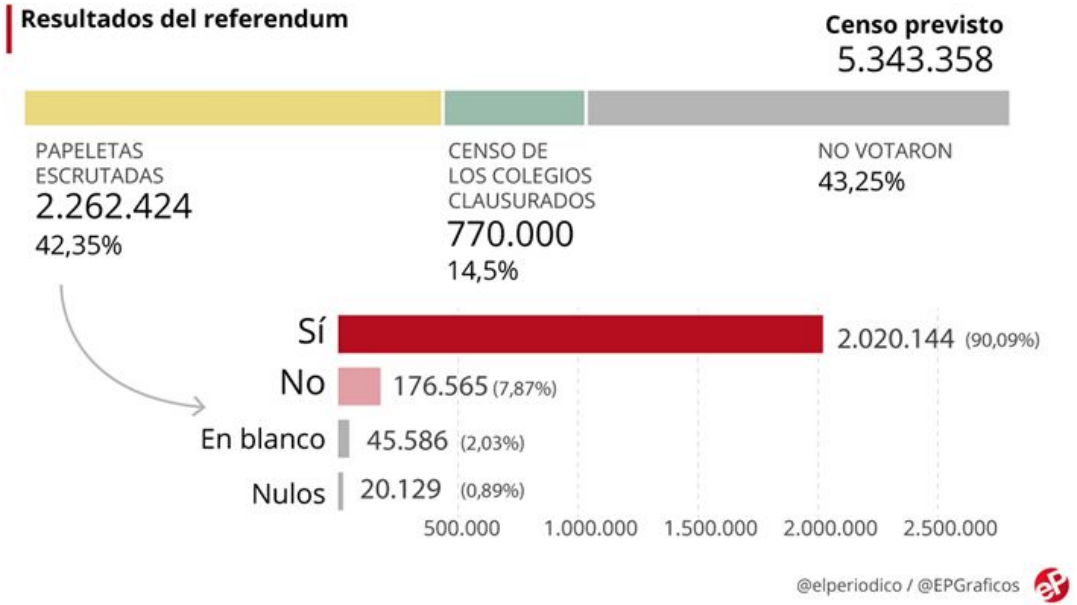
- Relevant laws of 2017 promoted by the Parliament of Catalonia:
  - **Law 19/2017, of September 6**, of the referendum of self-determination
  - **Law 20/2017, of September 8**, of legal and foundational transitoriness of the Republic



- The Constitutional Court issued the *Auto 123/2017, of September 19, 2017*:
  - Challenge of anatomical provisions 6330-2015
  - Estimate the incidence of execution of the Judgement 259/2015
    - Recourse to the Law 19/2017
- *Judgement 114/2017, October 17, 2017*
  - Unconstitutionality of the Law 19/2017
- *Judgement 124/2017, November 8, 2017*
  - Unconstitutionality of the Law 20/2017

1. Introduction - The road to Oct 1, 2017

42.35% total participation: 90.09% Yes = 38.15%



Agenda

1. Introduction to Spanish Constitution & the political conflict
2. **Electoral census and protection principles**
3. Censorship and censorship-resistance: Techniques used for the 1-O
4. Legal implications
5. Conclusions

2. Electoral census and data protection principles

Let's start talking about 1-O...

- So, **what is needed to develop a referendum?**
  - **An electoral census!**
- **What does the electoral census contain?**
  - **Personal data** (requires special protection by law)
- **Where is the electoral census generated?**
  - At the local / municipal level
- **Who is the owner of the electoral census?**
  - It belongs to the **State** (public ownership)

Principles: Competence and legality, consent, and purpose

2. Electoral census and data protection principles

Electoral census: 2 ways to incorporate personal data

- **From publicly-owned files**
  - Electoral census for Catalan autonomous elections or general elections (2015/2016)
  - Municipal Registers
  - Other Catalan Administrations:
    - Health, Idescat, Catalan tax agency, etc.
- **From private contributions and voluntary data**

Note: LAW 19/2017, of September 6, of the referendum of self-determination.
DECREE 140/2017, of September 6, of complementary norms for the realization of the Self-Determination Referendum of Catalonia
DECREE 139/2017, of September 6, calling for the Self-Determination Referendum of Catalonia

Agenda

1. Introduction to Spanish Constitution & the political conflict
2. Electoral census and data protection principles
3. **Censorship and censorship-resistance: Techniques used for the 1-O**
4. Legal implications
5. Conclusions

3. Censorship and censorship-resistance techniques

Censorship techniques

- **Sept 06, 2017**: Publication of http://www.referendum.cat to inform the Catalan citizens about the voting process
  - No information regarding voting stations

- One week later, a **take-down order** was issued by the Court of First Instance of Barcelona after an official request of the Civil Guard

3. Censorship and censorship-resistance techniques

Censorship techniques

- The former president of the Government of Catalonia, Carles Puigdemont i Casamajó, publicly announced in Twitter a set of **cloned websites** (e.g., ref1oct.cat, ref1oct.eu)
  - https://twitter.com/krls/status/908028550707597312
- **Information about voting stations was published on Sept 21, 2017** (website http://onvotar.garantiespelreferendum.com)
  - https://twitter.com/krls/status/910888426026749952

3. Censorship and censorship-resistance techniques

- **Input data:**
  - DNI
  - Birthdate
  - Postal code
- **Output data:**
  - Polling building
  - Polling place address (street and city)
  - Polling station

3. Censorship and censorship-resistance techniques

Censorship techniques

- **Sept 22, 2017**: High Court of Justice of Catalonia issued **other take-down order**
  - Facilitating information to conduct to the holding of the 1-O referendum, **not law-abiding conforming to the formal suspension of the referendum law**
- **Sept 23, 2017**: **replica websites were provided**
  - Source code was released shortly before (https://github.com/ref1oct/ref1oct.github.io)
  - Also contains **instructions to set up a new web server very quickly**
  - List of mirrors in https://github.com/GrenderG/referendum_cat_mirror
    - Catalan hacktivism community (very deep historical roots in Spain, see HackStory) helped to disseminate the website replicas
- Again, the High Court of Justice of Catalonia issued **several take-down orders**
  - *For those new websites and for any website or domain publicly announced by any member of the Government of Catalonia*

3. Censorship and censorship-resistance techniques

Censorship techniques

- Censor's capabilities defined as attack models in "Sok: Making sense of censorship resistance systems," PETS, vol. 2016, no. 4, pp. 37-61
- **Take-down orders are direct censorship by means of blocking destination**
- **Filtering techniques used by ISPs**
  - *DNS tampering*
    - Easy to bypass: change your DNS, use VPN
  - *HTTP blocking* (regex on HTTP GET request)
    - Hold the HTTP GET request for 11 seconds, use VPN, ...

See https://cdrheidelberg.org/Matthias_Brugger_Internet_Censorship_Catalan_Referendum_CDR_Heidelberg_1_Sept_2018.pdf for more info

3. Censorship and censorship-resistance techniques

Censorship-resistance techniques

- **Censorship resistance system**
  - **Client/server architecture software** that involves component interactions to facilitate an unblockable communication between user and publisher
  - **Two phases**: *communication establishment + conversation*
    - **Communication establishment**: steps that the client-side system does to access to the server-side system, avoiding the censorship
    - **Conversation**: link is up, ready to transmit information

No censorship resistance system was provided,
but technical instructions to avoid domain name blocking

3. Censorship and censorship-resistance techniques

Censorship-resistance techniques

- **Distributed File System**
  - **Sept 22, 2017**: new tweet about a new web address to access to the website with the census information
  - **Hosted in InterPlanetary File System (IPFS)**
    - **Network protocol designed to support a content-addressable, peer-to-peer distributed file system**
    - Domain name is **not in Spanish soil** (the .io TLD operates from British soil)
    - **Man-in-the-middle attacks are also prevented** (use of SSL)

3. Censorship and censorship-resistance techniques

Censorship-resistance techniques: Distributed File System

- **IPFS also provides native mechanisms against censorship** (*good idea!*)
  - Since IPFS acts like a **peer-to-peer** distributed FS, **the content served by that domain can be replicated upon user's request**
    - Domain blocking is no longer working effectively
  - Since IPFS supports also a **content-addressable** distributed FS, **any user can verify if the content has been altered checking the current hash against the distributed hash**

3. Censorship and censorship-resistance techniques

Censorship-resistance techniques

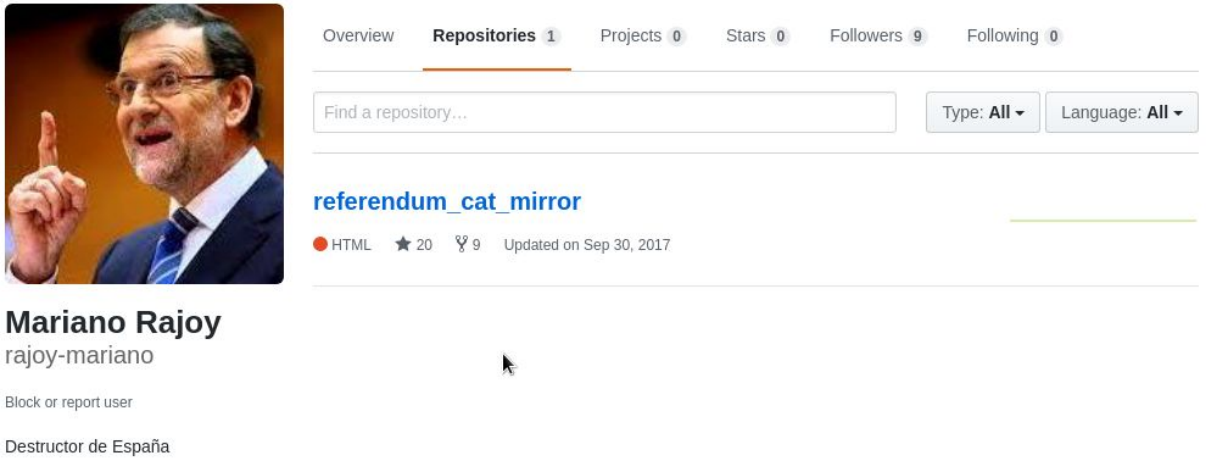
How to educate >5M of people about bypassing censorship techniques?

- **Proxy connections**
  - The use of web proxies were recommended to **access to banned websites**
    - **Very simple and yet effective** solution to bypass blocked website mechanisms

3. Censorship and censorship-resistance techniques

Censorship-resistance techniques

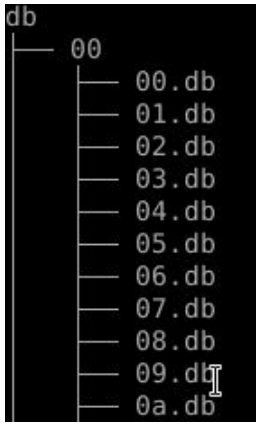
- **Electoral census**
  - Distributed also as part of the website in IPFS
  - Freely available on the Internet
    - *I chose this GitHub repository, the author is very reliable*



3. Censorship and censorship-resistance techniques

Censorship-resistance techniques

- **Electoral census**
  - Files with extension “.db”, stored in different folders
  - **Folder name**: first byte of a SHA-256 key
    - Recall that a SHA-256 key is a 32-byte length hash
    - The key was conformed after few operations with a voter personal data
  - **Filename**: next byte of the SHA-256 key
  - **Every file contains lines of 412-character length**
    - First 60 characters are the remaining bytes of the SHA-256 key
    - The other 352 characters conform the voting information, ciphered with a symmetric cryptographic schema



3. Censorship and censorship-resistance techniques

```python
def sha256_text(text):
    return hashlib.sha256(text).hexdigest()

def sha256_times(text, times):
    result = text;

    for x in range(0, times + 1):
        result = hashlib.sha256(result).hexdigest()

    return result

def lookup(dni, birthdate, zip):
    plaintext = 'not found!'
    key = dni + birthdate + zip
    passkey = sha256_times(key.encode('utf-8'), 1714)
    search = sha256_text(passkey.encode('utf-8'))

    dir = search[:2]
    file = search[2:4]
    path = './db/' + dir + '/'+ file + '.db'

    info = ''
    with open(path) as f:
        for line in f.readlines():
            if line[:60] == search[4:]:
                print decrypt(line[60:], passkey).split('#')
                info = decrypt(line[60:], passkey).split('#')[:-1]
                break

    return info

def main(argv):
    usagetext = 'usage: test.py -d <5 last DNI digits + letter> -b <birthdate,
    YYYYMMDD format> -z <5-digit zip code>'
```

Algorithm 1: Deciphering algorithm to search the voting place of a given person.

Input: Part of DNI d, birthdate b, zip code z

Output: A #-separated value text m containing the voting place information

1 Append d, b, and z to conform the string k, i.e., $k = d||b||z$.

2 Compute password key p_k as the SHA-256 hash iteratively computed over k 1715 times, i.e., $p_k = \text{SHA-256}_{1714}(h_i), h_i = \text{SHA-256}_{i-1}(h_{i-1}), h_1 = \text{SHA-256}_0(k), 1 \leq i < 1715$.

3 Compute search key s_k as the SHA-256 hash over p_k, i.e., $s_k = \text{SHA-256}(p_k)$

4 Open filename fn located at folder $s_k[0]||s_k[1]$ and named as $s_k[2]||s_k[3]$ (with extension ".db")

5 **foreach** *line* l *in* fn **do**

6 | **if** $l[0]||\ldots l[59] = s_k[4]||\ldots||s_k[63]$ **then**

7 | | Decipher $m = l[60]||\ldots||l[411]$ using AES-256 with CBC mode, PKCS#7 padding scheme, and p_k as key, i.e., $m = \text{Decrypt}_{\text{AES-256}}^{\text{CBC}-PKCS\#7}(l[60]||\ldots||l[411], p_k)$

8 | | **return** m

9 | **end**

10 **end**

3. Censorship and censorship-resistance techniques

Some notes on the algorithm

- ***Why 1714+1 iterations?***
  - A hash function is a one-way function ($f : \{0,1\}^* \rightarrow \{0,1\}^*$)
    - Easy to compute on every input, but hard to invert given the image of a random input
  - The value of 1714 refers to the Siege of Barcelona (War of Spanish Succession)
    - **Army of Catalonia was involved, defending Archduke Charles of Austria**
- **Output of the algorithm:** A “#”-separated value string
  - Voting centre name
  - The address (street and city)
  - The specific voting information (as the specific district, section, and table)
  - A 47-byte string (redundancy check?)

3. Censorship and censorship-resistance techniques

Some notes on the algorithm

- **Key entropy:**
  - **5 last digits and letter of Spanish DNI**: $10^5 \cdot 23$ (≈ 21.1332 bits)
    - Letter is the reminder between 23, hence it can be computed
  - **Birthdate**, in YYYYMMDD format
    - Assuming 100 years, $101 \cdot 365.25$ possibilities (≈ 15.1710 bits)
    - Can be better upper bounded, since the minimum voting age is 18
  - **Zipcode**
    - 5 digits, 2 first ones identify the province
    - $4 \cdot 10^3$ possibilities (≈ 11.9658 bits)
    - Can be also better upper bounded, not all values are valid

48.27 bits (at best). Lower than the minimum length of 80 bits recommended by both NIST and ECRYPT to protect against eavesdropping and other offline attacks

Agenda

1. Introduction to Spanish Constitution & the political conflict
2. Electoral census and data protection principles
3. Censorship and censorship-resistance: Techniques used for the 1-O
4. **Legal implications**
5. Conclusions

4. Legal implications

Constitutional

Criminal

Administrative

4. Legal implications

Constitutional: coer-cive fines 12000€/day

- Constitutional Court on Sept 12 and 13, 2017, **prevented the Catalan authorities from creating any registry or file necessary for holding a self-determination referendum**
- On Sept 20, the Con-stitutional Court confirmed (Auto 126/2017) **coer-cive fines to achieve the execution of the Court's pro-nouncements**
    - In Auto 127/2017, the responsibility was envisaged over the Secretary General of the Vice Presidency and Economy and Finance of the Government of Catalonia and over the head of the electoral processes and popular consultations area, in view of their functions as the electoral administration of the Government of Catalonia (foreseen in the Decree 140/2017)

4. Legal implications

Criminal: imprisonment

- **Not easily deter-minable**: too many assumptions and sit-uations
  - **Evidences?!**
- We can point out **some cases of special relevance with regard to the personal data protection, if the use and abuse of those files are proven**
  - Illicit access, use of data without consent, etc.
- **Liability stated on the articles 197 and 198 of the Spanish Penal Code**
  - From 1 to 5 years of imprisonment, fines, and ineligibility for public office

4. Legal implications

Administrative: fines (+ possible administrative disciplinary regime)

- **Organic Law 15/1999 (LOPD)**: article 44.4 if data was obtained in a fraudulent form; sensitive data; or there was a prior request to cease the illicit processing
  - Fine penalties range also from **300.001 to 600.000€**, plus the possibility of an administrative disciplinary regime
- Out of these cases, fines of serious infractions range from **40.001 to 300.000€**

- **General Data Protection Regulation (GDPR) in the Royal Decree-law 5/2018**
  - Illegal data processing activities can be sanctioned with **administrative fines up to 20.000.000€**

Agenda

1. Introduction to Spanish Constitution & the political conflict
2. Electoral census and data protection principles
3. Censorship and censorship-resistance: Techniques used for the 1-O
4. Legal implications
5. **Conclusions**

5. Conclusions

- **Spanish Constitutional Court repeatedly warned** about
  - **Unconstitutionality** of the 1-O “referendum”
  - **Presumible illegalities** of other acts supporting that “referendum”

- **Technical considerations**
  - **Take-down orders** against public websites regarding 1-O voting information
    - Source code was published to allow a rapid (& freely) dissemination
    - Filtering techniques used by ISPs: DNS tampering + HTTP blocking
  - **Distributed DB + proxy connections**
    - Electoral census was distributed also, but ciphered. Low entropy
      - Strong enough to do its job (keep the information confidential)
- **Legal considerations**
  - **Basic principles of data protection: legality, purpose, and competence**
    - Violated (presumably)
    - **Criminal and administrative responsibilities**

¿?


REINO DE LEÓN
REINO DE CASTILLA
REINO DE PORTUGAL
REINO DE NAVARRA
REINO D'ARAGÓN
SEÑORÍO DE ALBARRACÍN
BARCELONA
TOLOSA
PROVENCA
CORSICA
MAR MEDITERRANIO