Emília RYTKÓ

Safeguards in the Hungarian election process

Acts regulate the fairness, transparency and credibility of election processes in the democratic countries.

As with all activities, risks are inherent to the entire process preparing and administering elections, a mistake or an error may question the entire process.

This is an effort in which no mistakes may be made, no deadlines may be missed, no implementation may go wrong because that **would jeopardise the faith of the people in the system of democratic institutions**.

Therefore, it is of particular importance to aim at absolute security in each element thereof.

Absolute security – in its objective meaning – may be defined as a state free from dangers and disturbances, which I believe only exists in a virtual world.

If one considers it, the focus is always on the subjective meaning of security in reality, which means something different for all. This might be the reassuring presence of a secure financial background, the guarantee of health and physical soundness but in a wider sense, the guarantee of rest in the country, the solidness of constitutionality. These are all parts of security that we wish for in our guts; however, the secure implementation of the task entrusted to us must also be guaranteed in our own activities as election specialists.

Our responsibility primarily lies in our contribution to the secure feeling of voters by ensuring maximum statutory safeguards.

When do voters feel secure in the process of voting?

On the one hand, when they take part in the voting out of their own free will and are guaranteed to cast their votes on whoever they wish.

When their votes are guaranteed to entail no retaliation whatsoever, no accountability and may not be disputed.

This means that the confidentiality of voting and votes must be ensured by all means, they may not be accessed by any unauthorised entity.

On the other hand, they must be guaranteed that their votes are unaltered throughout the election process. Their votes prevail in the conclusion of the outcome as they were cast and are not lost as much as possible.

Such requirements may be complied with if

- the spirit and letter of laws are observed precisely;
- their implementation is rendered public, the generation of their outcome is rendered accessible; and
- the controllability and reproducibility of the entire process are guaranteed.

In the following, I wish to discuss the security of three central elements of the election process in more detail, these are:

1. A reliable register of voters;
2. The security of forms and documents used in the election process;
3. A multilevel IT security of election processes.

1. A reliable register of voters

In Hungary, the register of voters is produced *ex officio*; thus, voters do not need to initiate their registration. This is subject to the availability of authentic public records on the population of the country that is suitable prior to each election at the moment of setting that particular attention for producing a register from such records.

When an election is set, the standalone registers are linked to create the register featuring citizens of age eligible for voting already broken down according to constituency.

A number of laws ensure guarantees

- preventing unauthorised access to such records,
- inaccessibility of personal details by unauthorised entities, and
- enforcing the right of disposal over the own personal details of citizens.

The register itself – right from the moment of generation – is the **central element of the election process**; therefore, its security had necessitated the setting up of numerous safeguards such as:

- IT security of the system of records;
- elimination of unauthorised access, thus, third-party interaction;
- provision of judicial legal remedy;
- protection of forwarding certain registers (foreign offices) by electronic signatures.

In the majority of instances, registers are generally produced and kept electronically. Hardcopy registers first appear in the constituencies, which are, however, not public, only the voter and the election panel may access contents thereof. Signatories, that is voters may only be disclosed during judicial legal remedy. This is an important safeguard preventing retaliation towards voters, as mentioned in my introduction for their participation in the voting process.
In case of this document, safeguards primarily concern their handling, while in case of other files, special rules apply not only to handling but to production as well, which leads me to the second component of my presentation, the security of election forms.

2. The security of forms used in the election process

The forms, voting-papers and minutes, used in the Hungarian election process are printed in a closed system, which guarantees a high level of their protection. Print-shop data is exchanged via an electronic network, with which controlling and production complies. Applicable forms are qualified as security documents with the following elements of protection:

- UV imprint not visible to the human eye, only under special lighting,
- Texts containing micro-wording to prevent photocopying,
- Handling and recording as files with strict accountability.

The above process and built-in safeguards have prevented the falsification of voting-papers and forms so far.

Special rules are applicable to the delivery and on-site keeping of forms. Not only repeated checks during their delivery and acceptance but the keeping of delivered documents in a closed and guarded place are done under strict controls.

3. A multilevel IT security of election processes

A speciality of Hungarian election laws, beyond their complexity, is that they are difficult to implement without IT support. Not only because of the short deadlines and regular checking and data-forwarding tasks calling for electronic interaction, but also because this process is subject to Internet exposure in each stage of the process.

It follows from all this that the system must be of a high capacity, maximum security and free from intrusion.

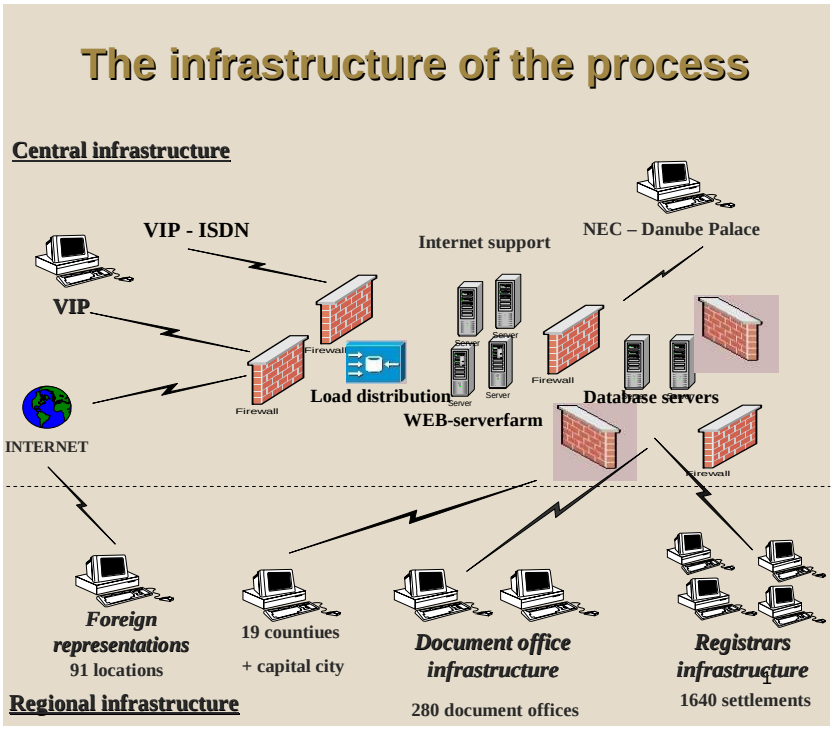
The systems supporting election decisively rely on **incumbent public administration infrastructure**, hardware and network of document offices.

In settlements without document offices, the **municipal system supplying birth and marriage certificates is engaged**.

The application of this structure allows for recording large data quantities generated in the course of the election process within short processing times in high quality and security. Systems under constant development and netware offer a stable IT background to this.

The simultaneous engagement of the infrastructure of document offices and birth and marriage certificates in the course of administering an election event **allows each local election office to take part** in the IT processing of data.

In the following, I wish to illustrate the infrastructure of administration:



Due to the particular political and societal significance of election events, the **entire process of administration** must be implemented in compliance with the most rigorous security measures.

The multilevel security system complies with the following requirements:

1. **Operational security at all times,** including
   - wideband data-transmission network (capable of transmitting many times more data than calculated in advance in the piloting stage)
   - availability of redundant network components, high-capacity device with backup repair service and forthwith incorporation capacity.

   Administration testing and piloting explicitly examines the application of bypass routes and traffic diversion in case of a potential network breakdown.
2. **Application-level protection,** which
   - refers to ensuring the identification of administrators. Only designated administrators may access pre-dedicated devices with highly rigorous access authorisations.

They perform quality controls during data capture, e.g. sit in pairs before the computer, print out dictated and captured data and compare them with the original document.

– The logging of transactions is a priority with a view to tracking and checking each data stage.

3. **As it follows from the diagram, one of the most important security elements is the incorporation of network security solutions.**

Therefore, data channel through a set of reinforced firewalls (incoming data are posted on the Internet every 3 minutes; thus, they are public almost from the moment of generation and their state at any time may be retrieved due to logging).

The hacker-watch service is a priority element of network security.

The tool employed to this end alert any activity aimed at intrusion or access to the network. The system is 24-7 and not only monitors network traffic but also analyses traffic patterns and signs appearing in the network. It allows for important conclusions by analysing traffic changes, sensing disconnections and responding to certain events.

It is not solely attributable to fortune that our system was not breached in recent years because this is probably influenced by each system functioning for a brief period of time only, e.g. the conclusion of preliminary results ends 2 to 2.5 hours after the closing of constituencies on the evening of the voting.

This not only puts intruders to a great test but their action entails penal law implications as well. Pursuant to the Penal Code, successful intrusion is “rewarded” by imprisonment for up to five years.

As apparent from the enumeration, in the course of administering elections, effective and tangible security measures beyond the applied secure forms are primarily present in IT security.

What guarantees the appearance of a vote cast by a voter in concluding the results?

Beyond the above enumeration:

- non-falsifiable voting-papers;
- securely cast votes and
- precise data capture – **authentic minutes** completed by the election panels, which are **compared with electronically posted results.**

If we had not been wrong in capturing the results, then election administration will disclose the same informative data as the result of the votes of all citizens in the end as that concluded by the election panels.

Therefore, the incorporation of results established by the panel into minutes, the signing thereof by all participants and the provision of all stakeholders with an authentic copy of the original minutes forthwith upon the establishment of the results carry extraordinary significance.

If we take these safeguards incorporated into the process one by one, then it becomes increasingly tangible that the key to every security is the performing of precise, professional and diligent election work.

Finally, to substantiate this, allow me to cite the words of Abraham Lincoln who expressed the following **in the last years of his work**:

„As I grow older, I see it ever more clearly
that there exists a single form of security:
to be capable of performing your duties outstandingly.”

And he was right.

Thank you for your attention!