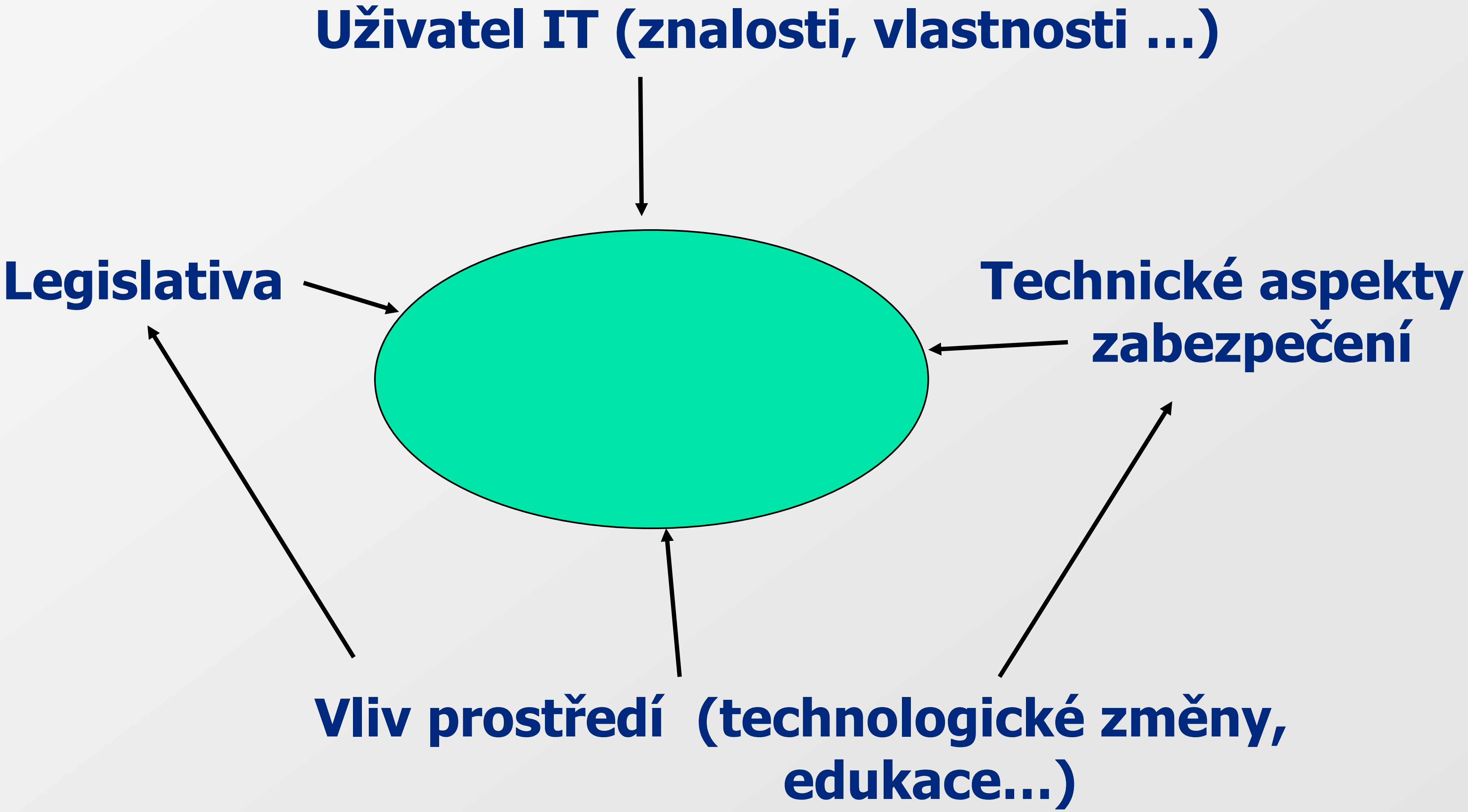
MASARYKOVA UNIVERZITA

# Experimentální výzkum online bezpečnosti

prof. David Smahel, Ph.D.

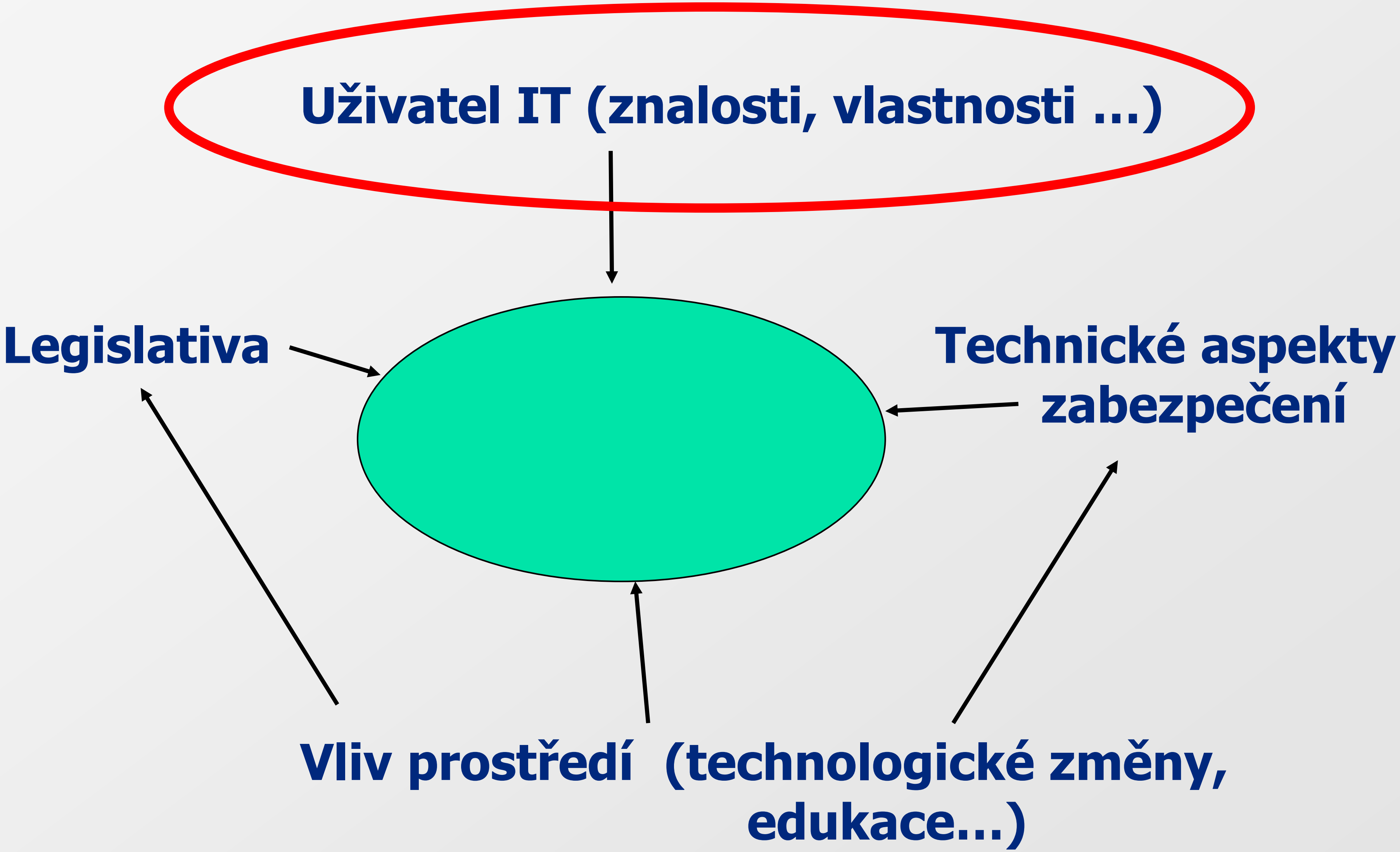


**Uživatel IT (znalosti, vlastnosti ...)**

**Legislativa**

**Technické aspekty zabezpečení**

**Vliv prostředí (technologické změny, edukace...)**

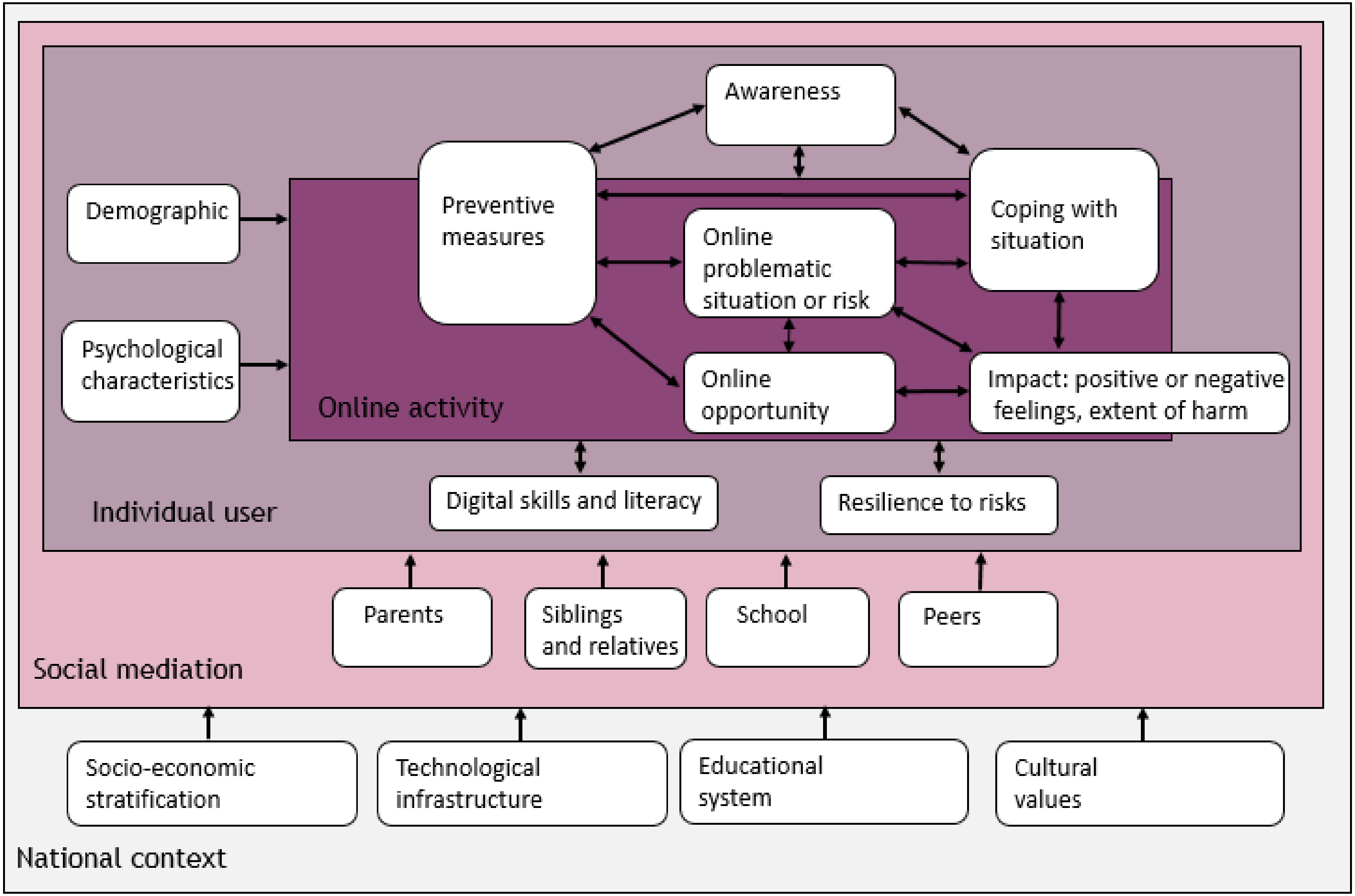


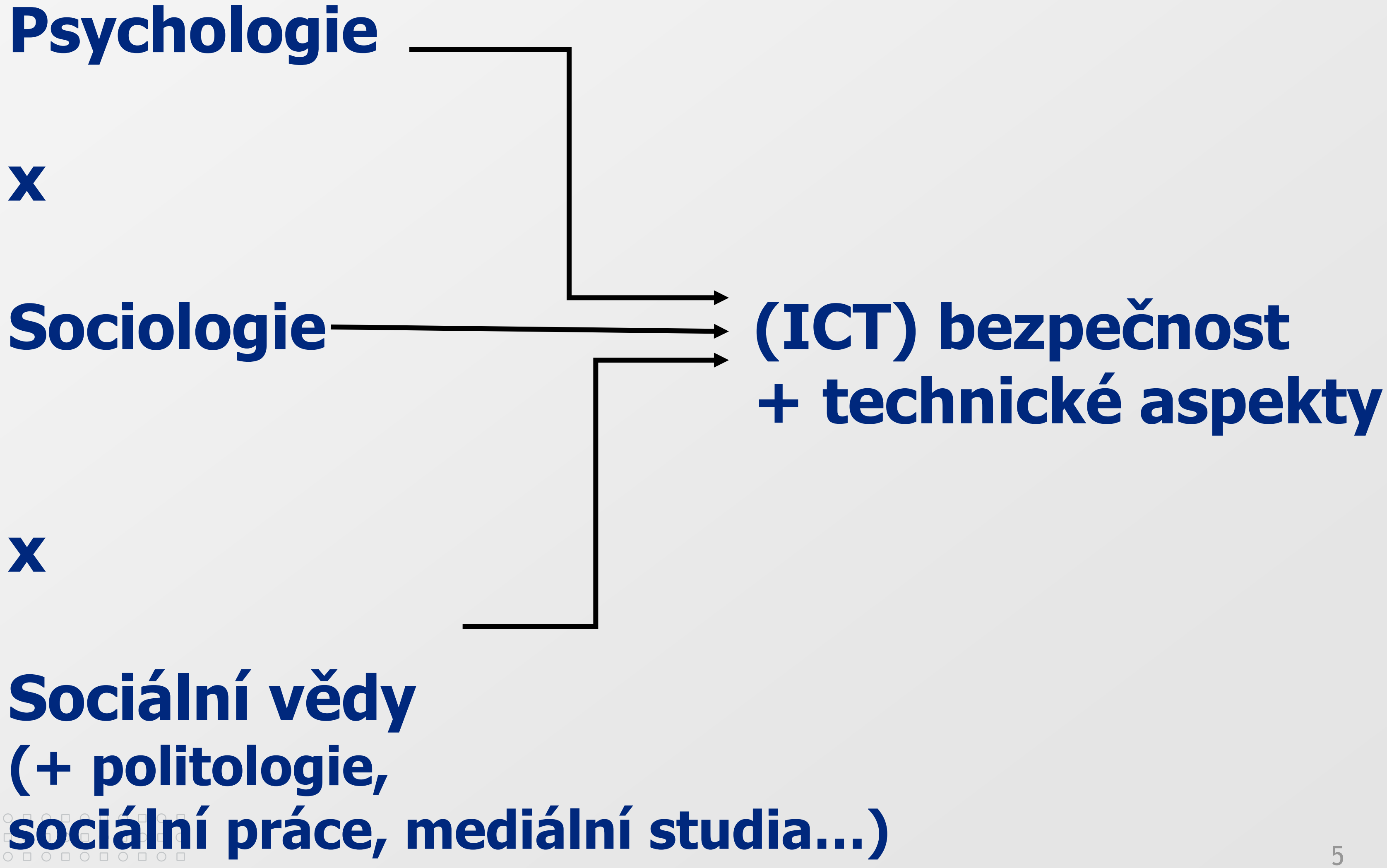
Uživatel IT (znalosti, vlastnosti …)

Legislativa

Technické aspekty zabezpečení

Vliv prostředí (technologické změny, edukace…)


Awareness
Preventive measures
Coping with situation
Demographic
Online problematic situation or risk
Psychological characteristics
Online opportunity
Impact: positive or negative feelings, extent of harm
Online activity
Digital skills and literacy
Resilience to risks
Individual user
Parents
Siblings and relatives
School
Peers
Social mediation
Socio-economic stratification
Technological infrastructure
Educational system
Cultural values
National context



**Psychologie**

**x**

**Sociologie**

**x**

**Sociální vědy**
**(+ politologie,**
**sociální práce, mediální studia…)**

**(ICT) bezpečnost**
**+ technické aspekty**

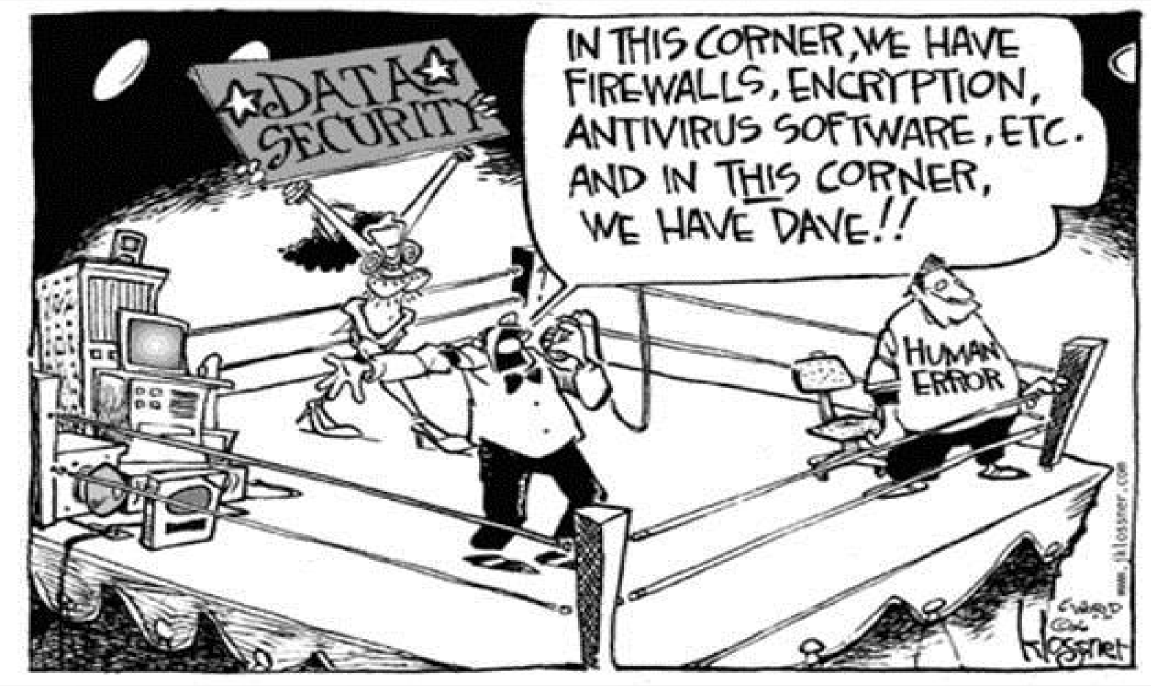
# Usable security: Experimental research of ICT user behavior in the domain of security

David Smahel
Vaclav Matyas
Vlasta Stavova
Lenka Dedkova
Hana Machackova
Kamil Malinka
Radim Polcak

Interdisciplinary Research Team on Internet and Society

CROCS
Centre for Research on Cryptography and Security

“Humans are the weakest link in cyber security.”


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

We take care of the human factor from the security perspective.

# What is usable security?

- Users and security trainings.
- Security policy design
- Warning and user dialog design.
- Authentication methods with respect to users.
- Passwords and users password habits.
- Users and privacy.
- Secure system design.

# Involved parties

- Netsuite Inc.- company producing business management software
- ICS (ÚVT) – service provider for Masaryk University
- ESET s.r.o. - security software developer
- SODATSW s.r.o. – manufacturer of robust security encryption solutions
- Masaryk University: Faculty of Informatics, Faculty of Social Studies, Faculty of Law

## Aims of the research:

- Netsuite Inc. - measurement of user adherance to the security policy depending on a type of the security policy tutorial.
- ICS (ÚVT) – measurement of user knowledge and understanding of the security policy.
- ESET, spol. s.r.o. – 2 user dialogs redesigned for their antivirus system.
- SODATSW s.r.o. - password soft recovery for their security system.

# ESET PROJECT 1 Aims

- Antivirus premium license contains many security benefits over the basic one.
- Increase user's security by increasing a number of people who upgrade the basic version to the premium license.
- Android platform.
- Only small changes in already existing user dialog.

# ESET Challenge 1 – Activities

1. Experiment 1 (14 000 participants) tested:
   - Control variant (no change).
   - Variant with a text change.
   - Variant with added „Ask later“ button.
2. Experiment 2 (60 000 participants) tested:
   - More complex combinations of persuasive principle (decoy option) and text change from first experiment.
   - A user survey for English, Czech, Slovak and German speaking participants was included to reveal user security habits.

# ESET Challenge 1 – Experiment 1 – Results

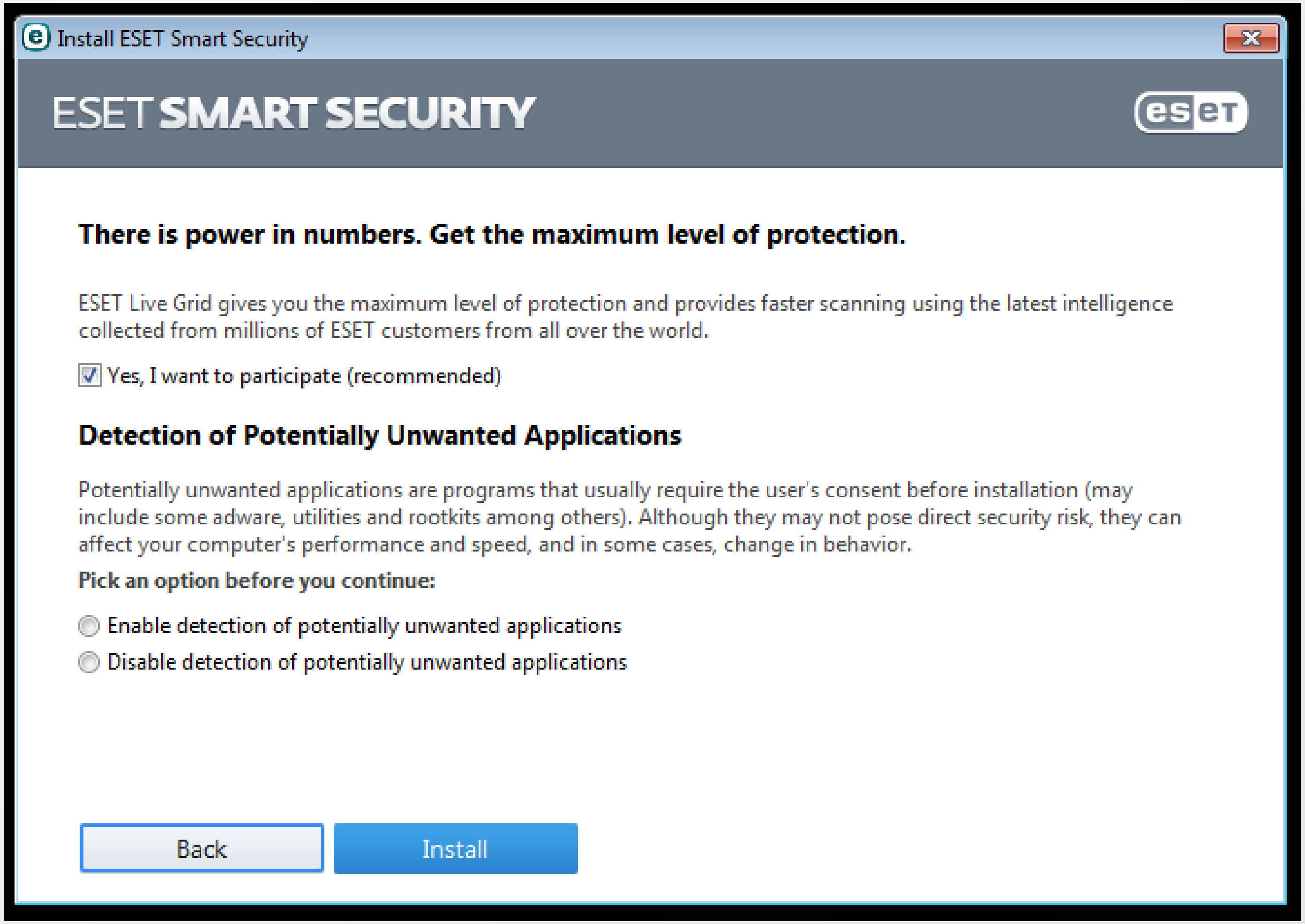
- Both new variants caused increase in number of purchases.
  - about 51% in variant with text change
  - about 21% in variant with „Ask later“ button.

# ESET Challenge 1 – Experiment 2 – Results

- No variant was significantly better in nudging user to obtain a premium license.
- Interesting results found out of questionnaire, e.g.:
  - Tablet users consider their device as less secure and purchase a license more often than smartphone users.
  - Participants who bought the premium license have more private data in their devices.
  - No statistically significant correlation with license purchase is, surprisingly, use of the device for storing passwords.
  - The older user is, the more he buys a license.

# ESET PROJECT 2 Aims

- How to encourage users to enable PUA (potentially unwanted application) detection?
- Increase user's security by increasing number of users who pick a PUA (spyware, adware, etc.) detection during antivirus installation process.
- Both options must be equal due to legal reasons.
- PC platform.
- Small changes in already existing user dialog.



Install ESET Smart Security

ESET SMART SECURITY

**There is power in numbers. Get the maximum level of protection.**

ESET Live Grid gives you the maximum level of protection and provides faster scanning using the latest intelligence collected from millions of ESET customers from all over the world.

☑ Yes, I want to participate (recommended)

**Detection of Potentially Unwanted Applications**

Potentially unwanted applications are programs that usually require the user's consent before installation (may include some adware, utilities and rootkits among others). Although they may not pose direct security risk, they can affect your computer's performance and speed, and in some cases, change in behavior.

**Pick an option before you continue:**

○ Enable detection of potentially unwanted applications

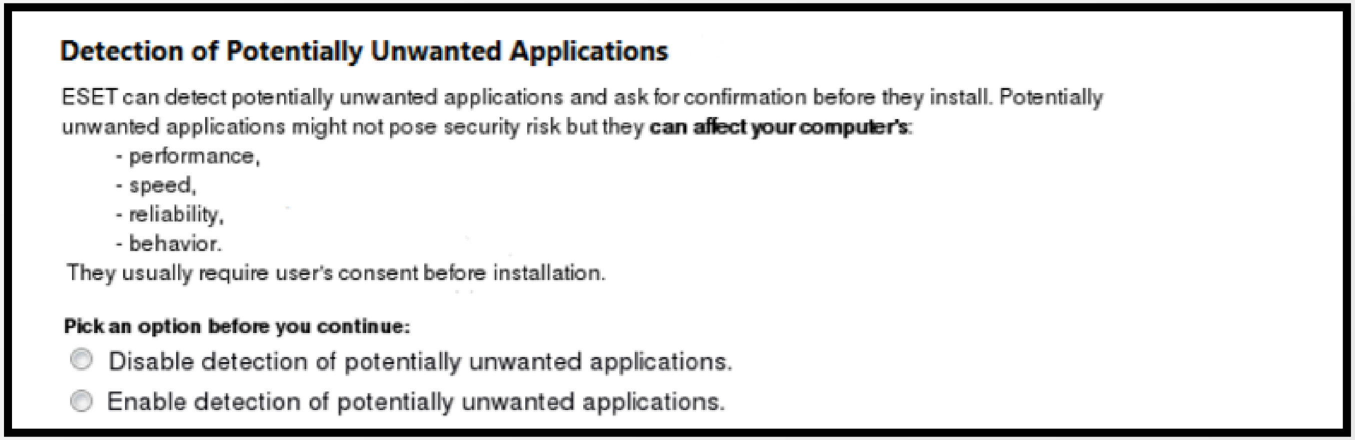
○ Disable detection of potentially unwanted applications

# ESET PROJECT 2 Activities

1. Experiment 1: Designed 15 new variants (including control variant) introduced to test on PC antivirus beta users.
   - 100 000 participants
   - We experimented with text content, colors, pictorials, bold type, bullet lists….
2. Experiment 2: Repeated with same settings, but real users.
   - 350 000 participants
   - Difference in behavior of beta x real users

# Proposed variants

- We designed 14 variants + control one



**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they **can affect your computer's**:

- performance,
- speed,
- reliability,
- behavior.

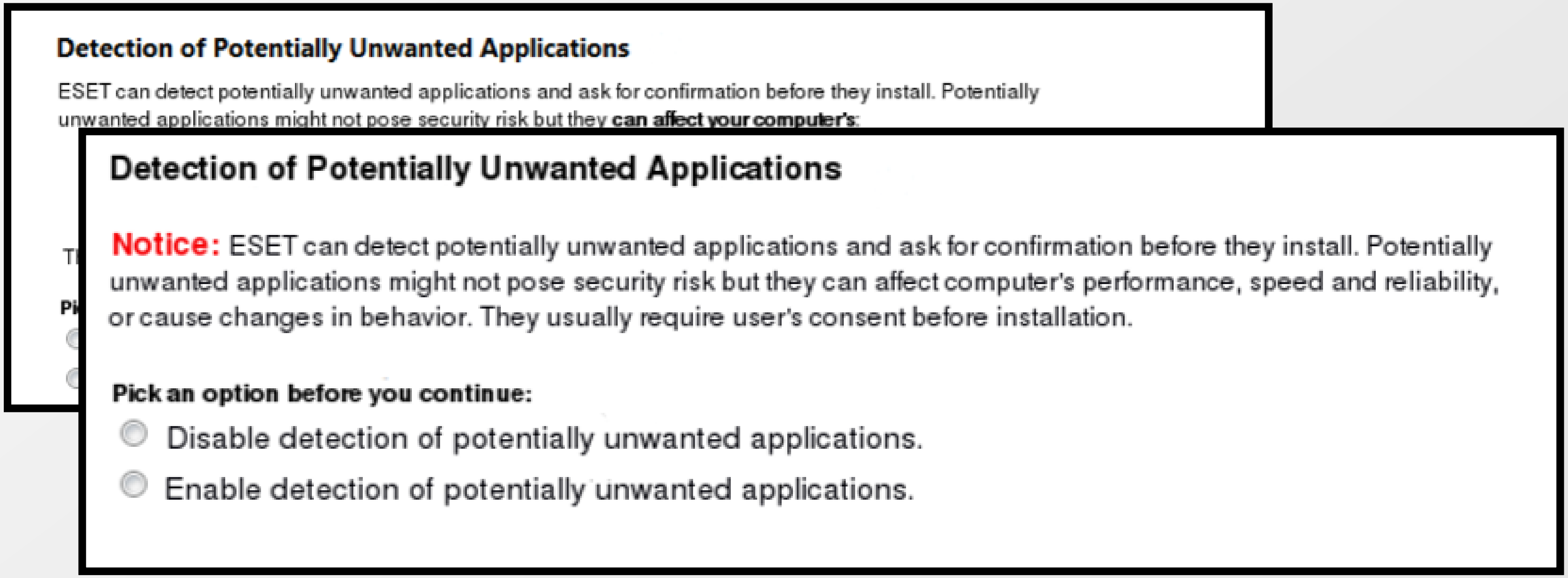
They usually require user's consent before installation.

**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

○ Enable detection of potentially unwanted applications.

# Proposed variants



Detection of Potentially Unwanted Applications

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they **can affect your computer's**:

T

Pi

○

○

Detection of Potentially Unwanted Applications

Notice: ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

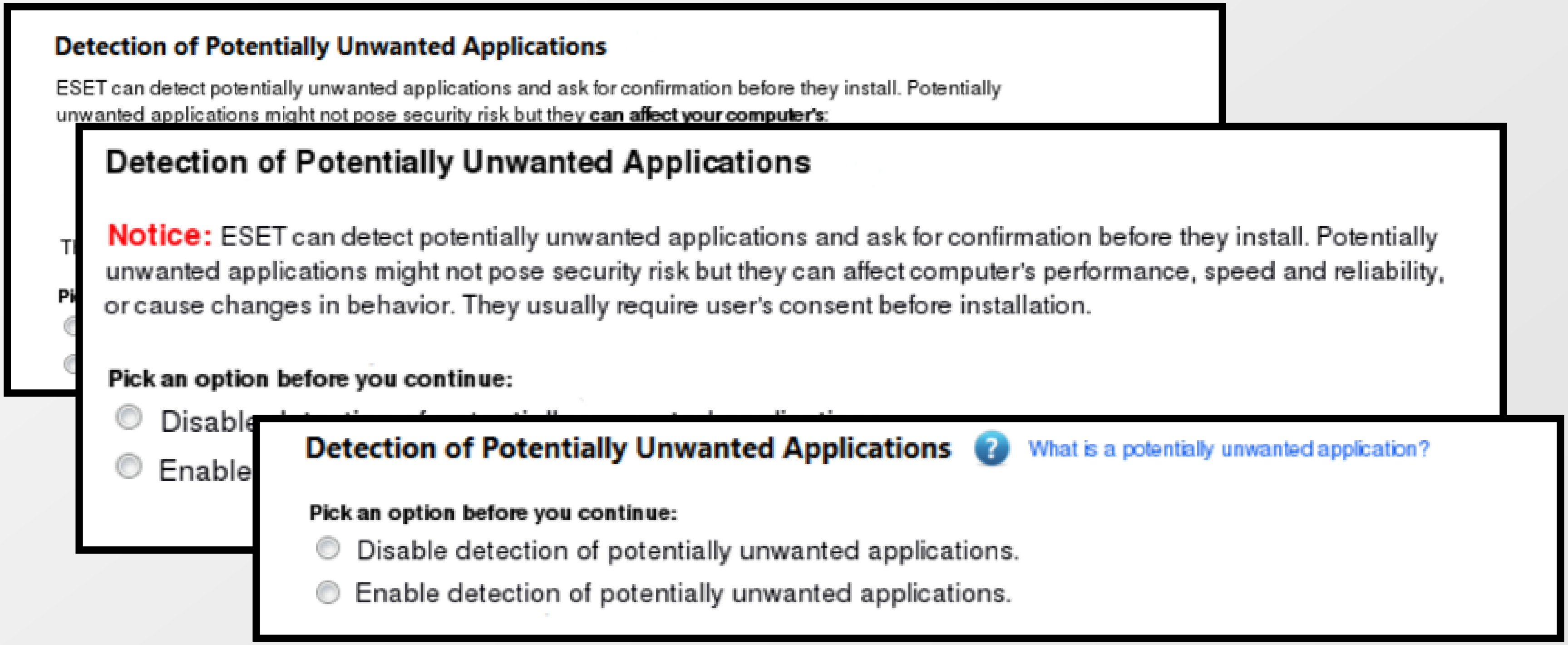
**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

○ Enable detection of potentially unwanted applications.

# Proposed variants

- We designed 14 variants + control one



**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they **can affect your computer's**:

Th

Pi

**Detection of Potentially Unwanted Applications**

**Notice:** ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

○ Disable

○ Enable

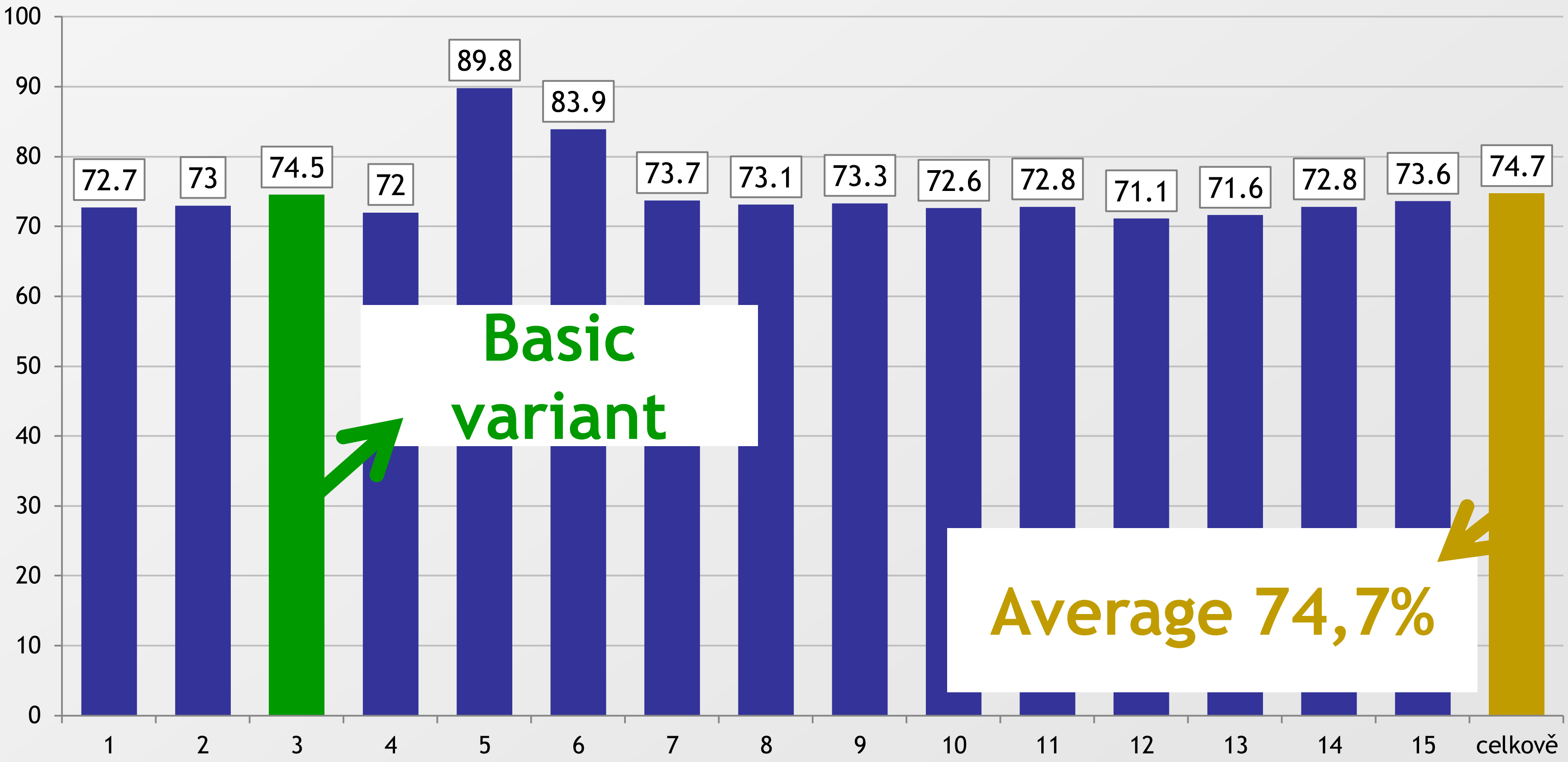
**Detection of Potentially Unwanted Applications** ? What is a potentially unwanted application?

**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

○ Enable detection of potentially unwanted applications.

# How many people allows detections across variants



Basic variant

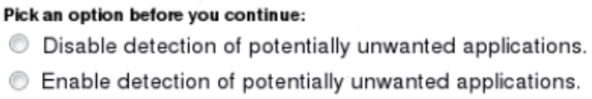
Average 74,7%

# Výsledky: co se liší

Základní verze

Změna pořadí možností: **dejte pozitivní možnost na první místo**

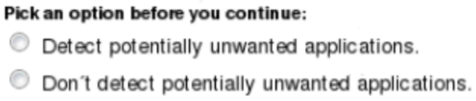
„Nová“ verze



**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

○ Enable detection of potentially unwanted applications.



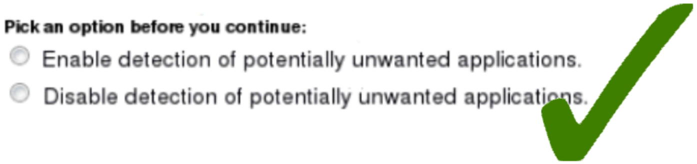
**Pick an option before you continue:**

○ Detect potentially unwanted applications.

○ Don´t detect potentially unwanted applications.

sloveso **ENABLE** funguje lépe než DETECT

**89% na této obrazovce detekuje**

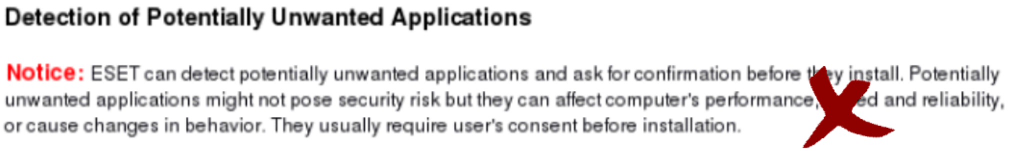


**Pick an option before you continue:**

○ Enable detection of potentially unwanted applications.

○ Disable detection of potentially unwanted applications.

Přidání červené NOTICE detekci PUA snižuje



**Detection of Potentially Unwanted Applications**

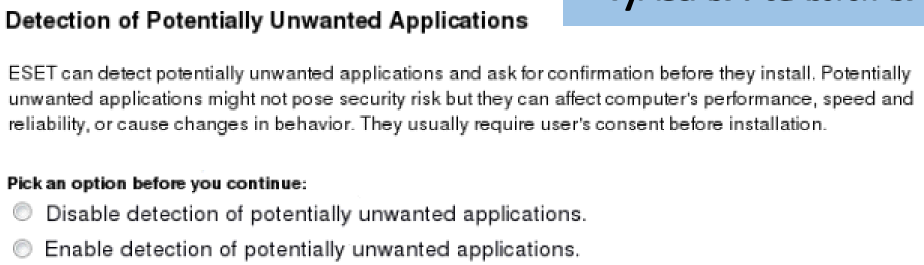
**Notice:** ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

# Výsledky co se nedošl I.

Základní verze

„Nová“ verze

## vynechání textu a nahrazení odkazem



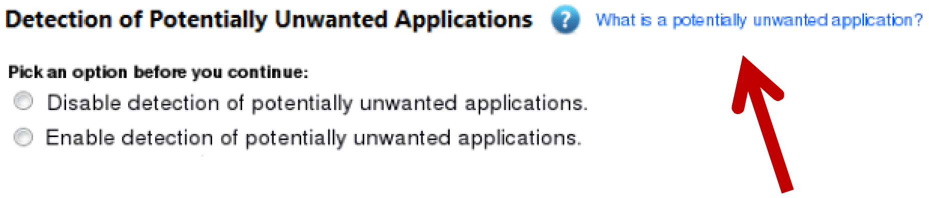
**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

○ Enable detection of potentially unwanted applications.



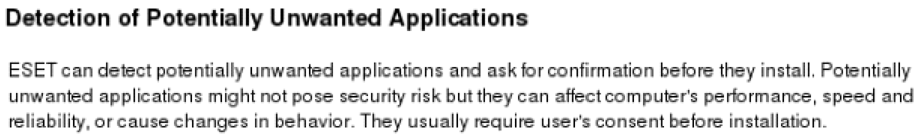
**Detection of Potentially Unwanted Applications** ? What is a potentially unwanted application?

**Pick an option before you continue:**

○ Disable detection of potentially unwanted applications.

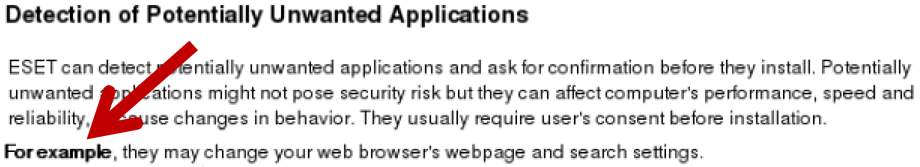
○ Enable detection of potentially unwanted applications.

## přidání příkladu PUA



**Detection of Potentially Unwanted Applications**

ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

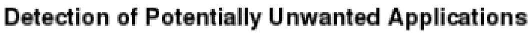


**Detection of Potentially Unwanted Applications**

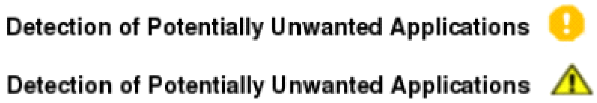
ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.

**For example**, they may change your web browser's webpage and search settings.

## výstražné symboly



**Detection of Potentially Unwanted Applications**



**Detection of Potentially Unwanted Applications** !

**Detection of Potentially Unwanted Applications** ⚠

# ESET (preliminary) conclusions:

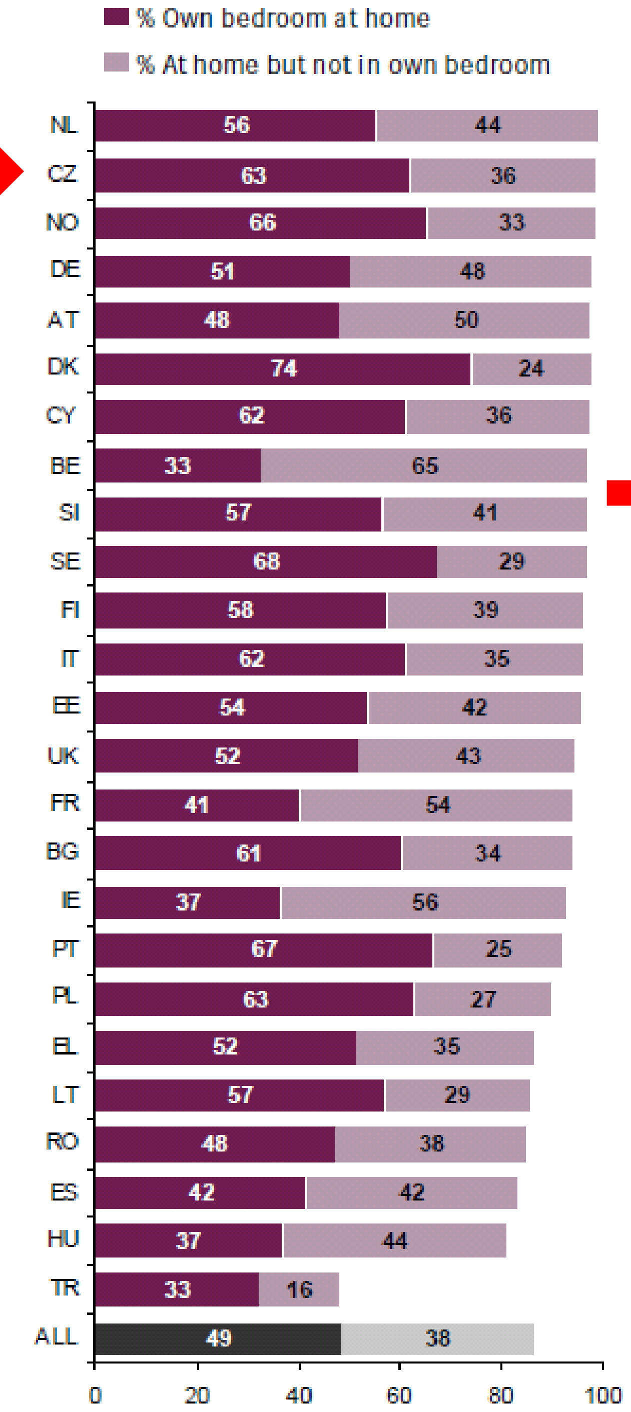
- What works:
    - positive answer as first option
    - “enable”is better than “detect”

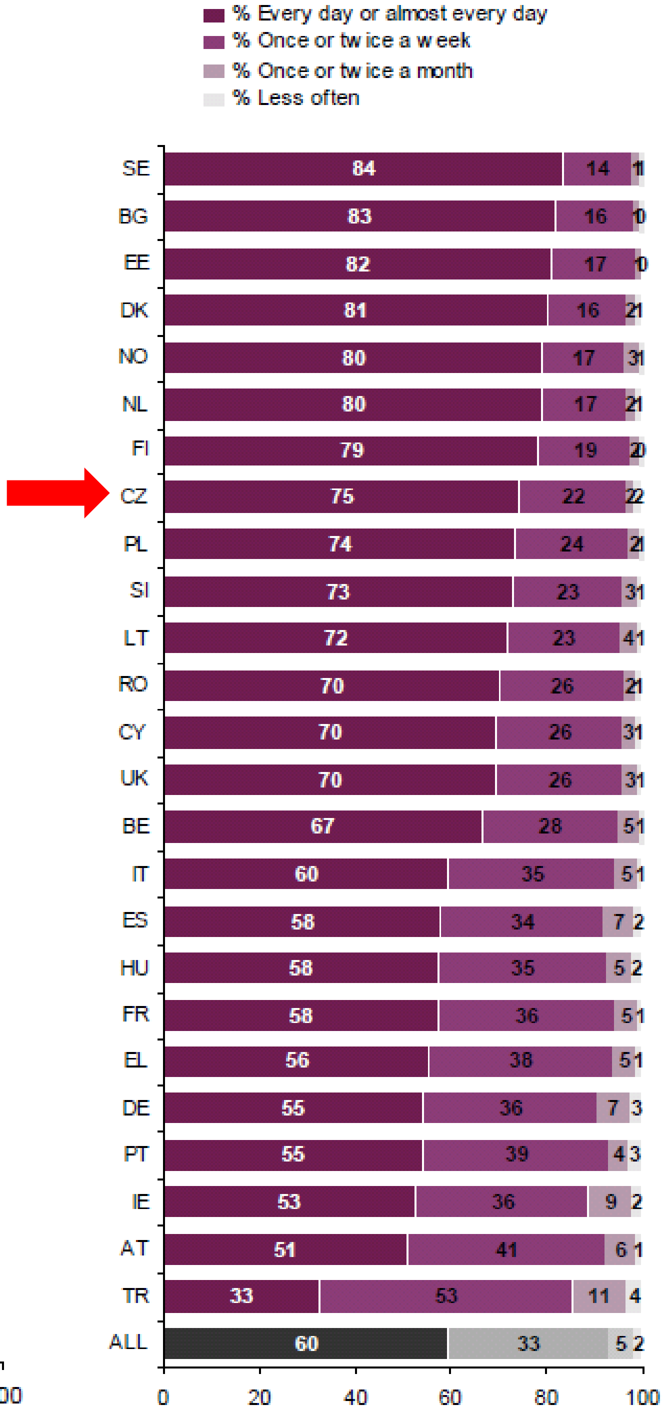
- Additional texts -> no effect
- Warning symbols -> no effect

Final remark: users are not reading longer texts in the installation process…

# PROJECT SODATSW

- 2 recovery scenarios were tested.
  - Password recovery by QR code.
  - Password recovery by help of second trustworthy person.
- Participants were university students.
- Final results were based on user surveys and system records.
- QR code recovery was considered more comfortable and usable whereas the other approach more secure.



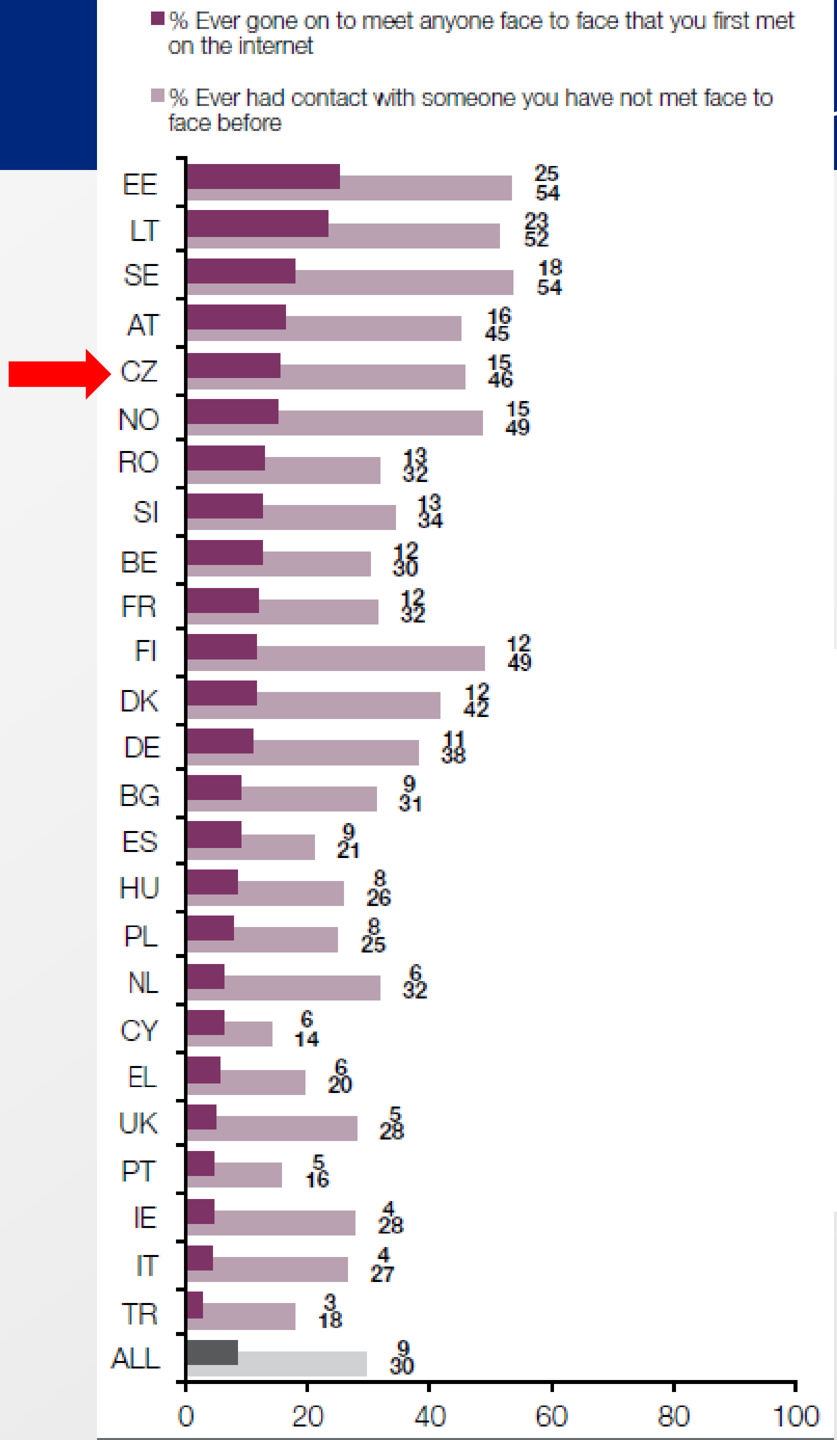


**V ČR používá internet více než 95 % dětí ve věku 12 a více (ČSÚ, 2012; Lupač, Sládek, 2008), mobilní telefony používá téměř každé dítě (ČSÚ, 2012).**

(Livingstone, Haddon, Görzig & Ólafsson, 2011):

# Online risks for children:

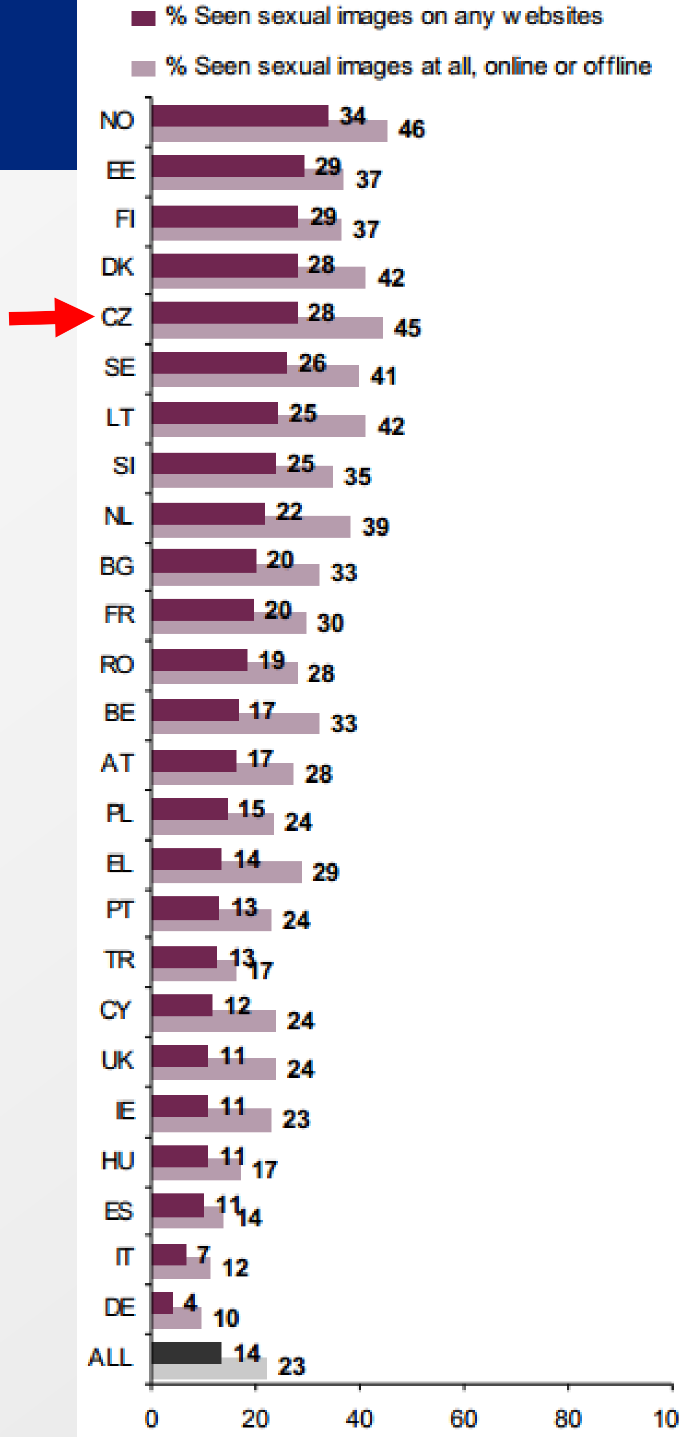
- Aggressive communication, cyberbullying, harassment
- Sexual problematic situations (pornography, sexual communication, sexting)
- Online strangers
- Privacy and misuse of personal information
- Commercials – advertisements, spam, pop-ups, fake e-mails
- Health problems (eye problems, nightmares, online addiction)



# Meeting online strangers

- 11 % from children who met someone offline, were bothered or angry about the experience from the meeting

(Livingstone, Haddon, Görzig & Ólafsson, 2011):



# Dítě vidělo sexuální obrázky online nebo offline

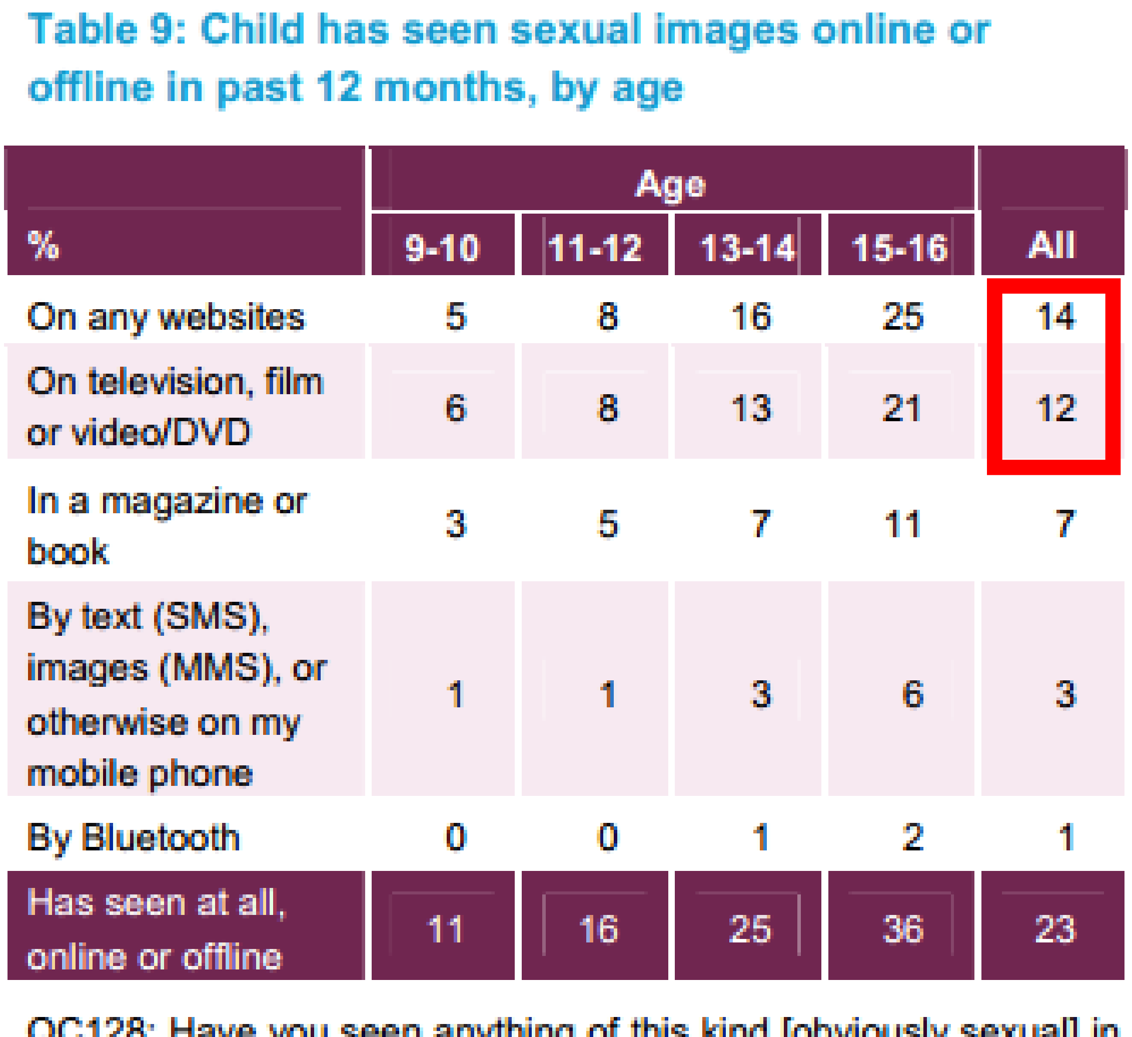
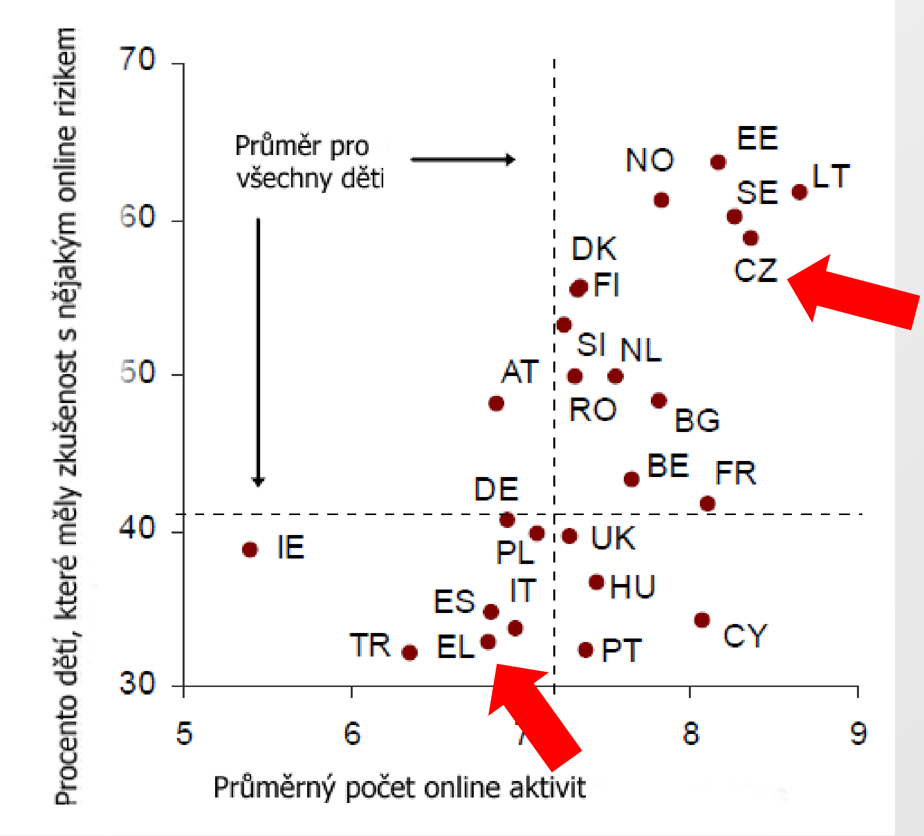


Table 9: Child has seen sexual images online or offline in past 12 months, by age

| % | Age | | | | All |
|---|---|---|---|---|---|
| | 9-10 | 11-12 | 13-14 | 15-16 | |
| On any websites | 5 | 8 | 16 | 25 | 14 |
| On television, film or video/DVD | 6 | 8 | 13 | 21 | 12 |
| In a magazine or book | 3 | 5 | 7 | 11 | 7 |
| By text (SMS), images (MMS), or otherwise on my mobile phone | 1 | 1 | 3 | 6 | 3 |
| By Bluetooth | 0 | 0 | 1 | 2 | 1 |
| Has seen at all, online or offline | 11 | 16 | 25 | 36 | 23 |

QC128: Have you seen anything of this kind [obviously sexual] in

# Online rizika versus online aktivity – ve 25 zemích EU



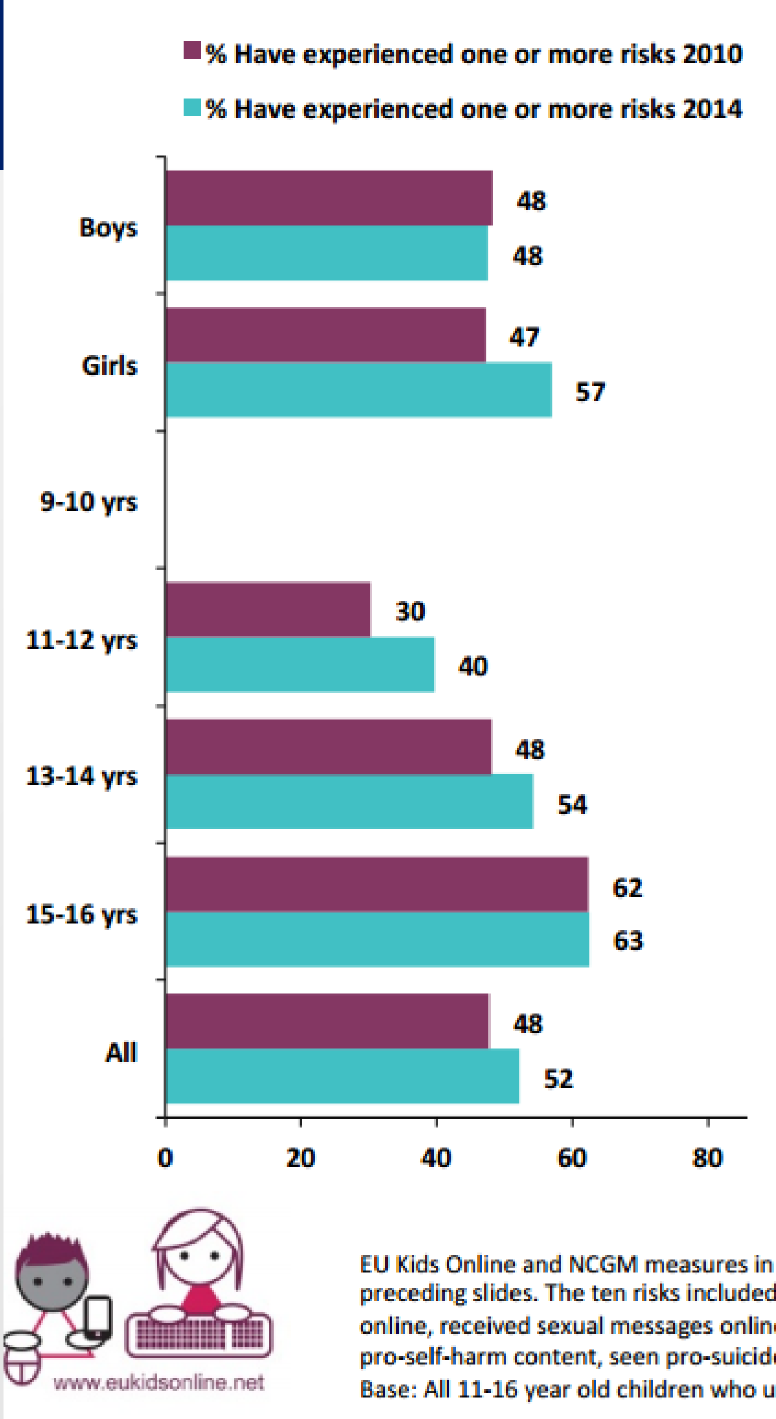
(Livingstone, Haddon, Görzig & Ólafsson, 2011):

# Online risks
# 2010 - 2014

Experienced one or more risks
-- 48 - > 52 %

- No increase among boys
- Increase mainly among young girls

Sonia Livingstone, Giovanna Mascheroni, Kjartan Ólafsson and Leslie Haddon, with the networks of EU Kids Online and Net Children Go Mobile (November 2014). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*



EU Kids Online and NCGM measures in
preceding slides. The ten risks included
online, received sexual messages onlin
pro-self-harm content, seen pro-suicid
Base: All 11-16 year old children who u

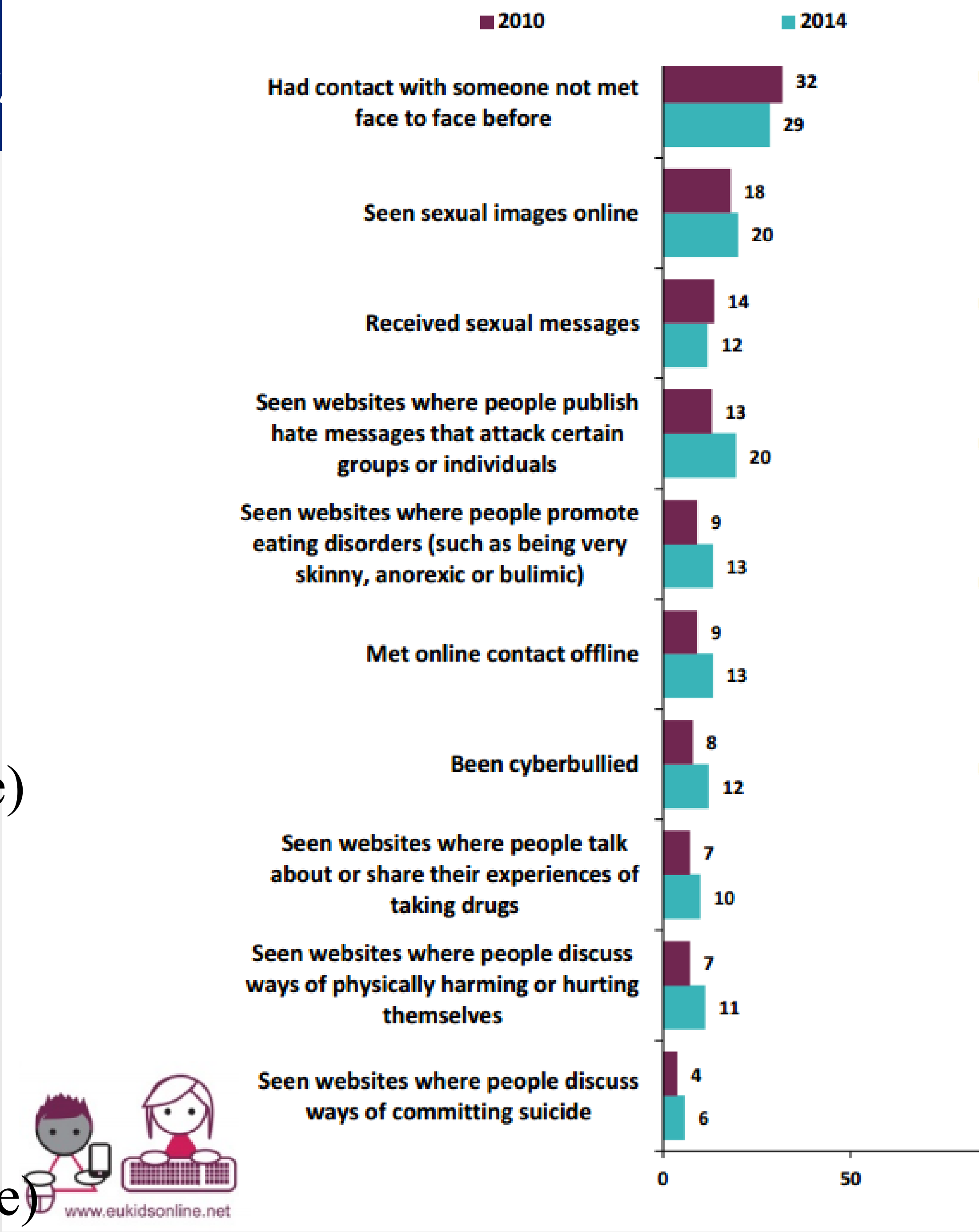
# Online risks 2010 - 2014

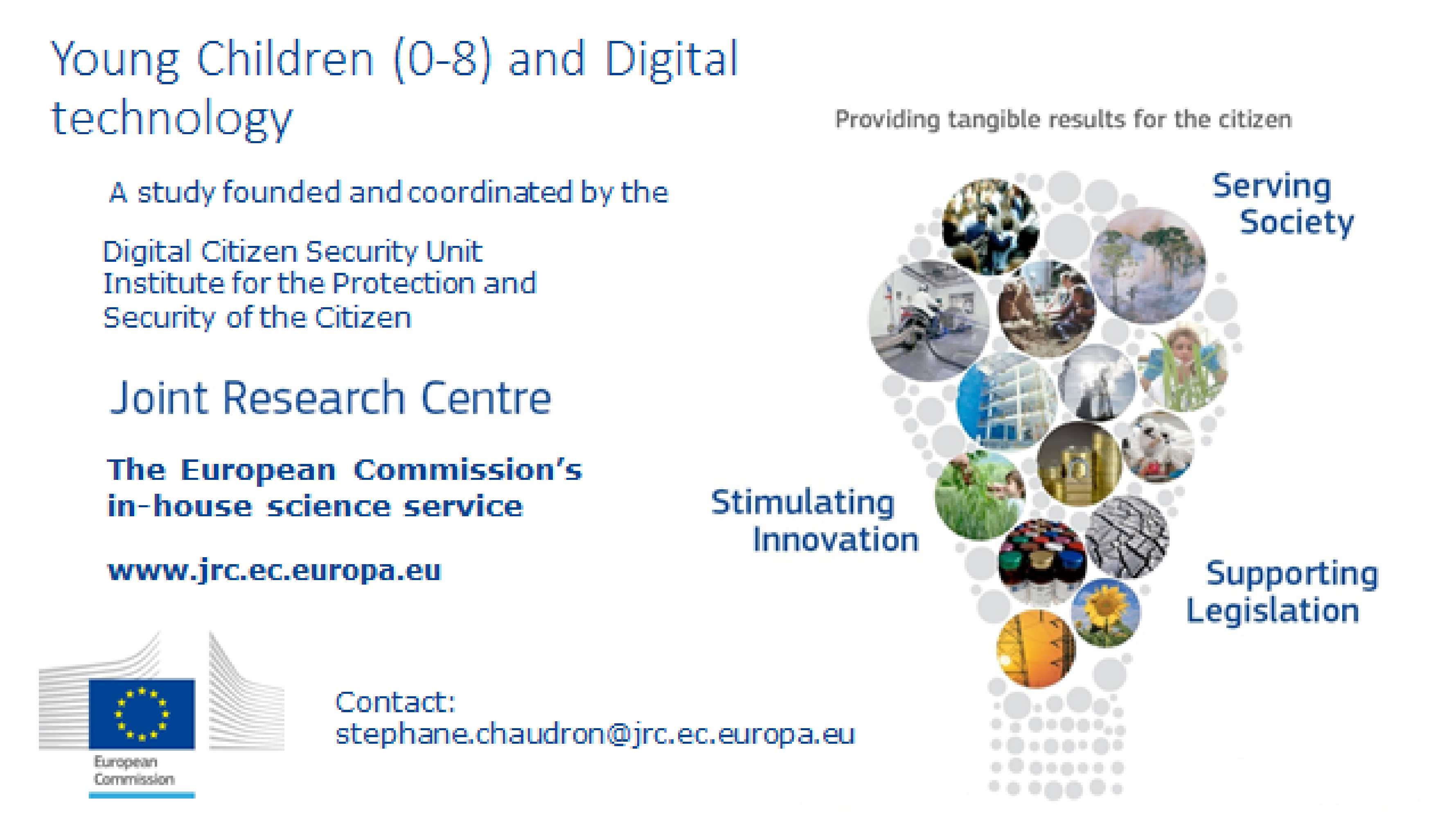
Meetings with unknow people
-- 9 -> 13%
-- ale 29 -> 26% only online

Cyberbullying
-- 8 -> 12%  (21 -> 23% offline)

Received sexual messages
-- 14 -> 12%

Saw sexual pictures online
-- 18 -> 20% (26 -> 28% offline)





# Young Children (0-8) and Digital technology

A study founded and coordinated by the

Digital Citizen Security Unit
Institute for the Protection and
Security of the Citizen

Joint Research Centre

**The European Commission's in-house science service**

**www.jrc.ec.europa.eu**

Providing tangible results for the citizen

Serving Society

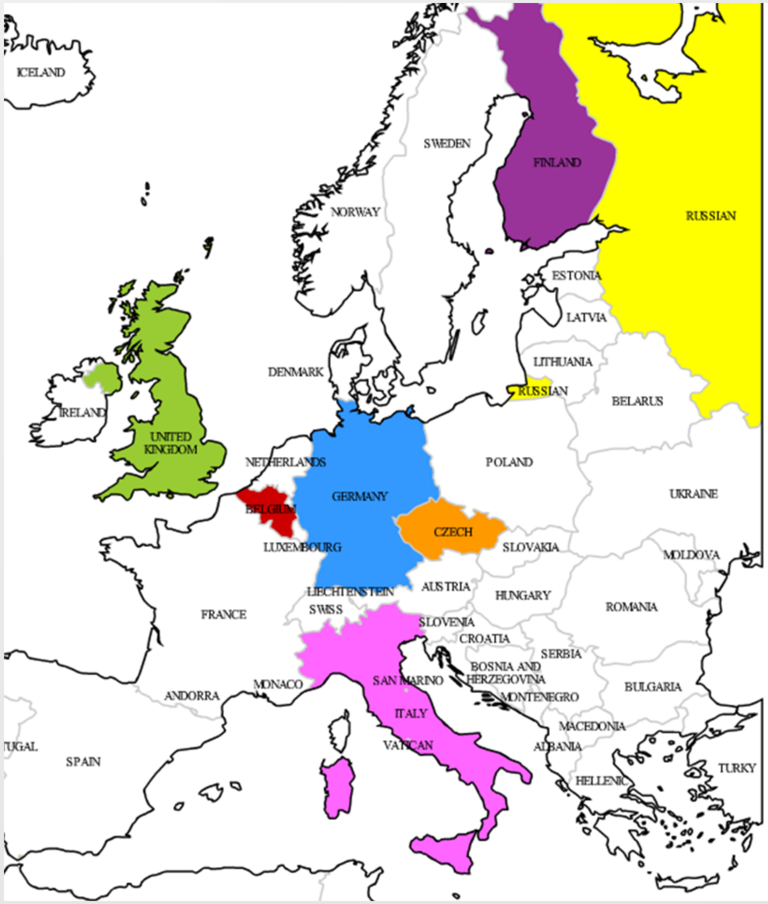
Stimulating Innovation

Supporting Legislation

Contact:
stephane.chaudron@jrc.ec.europa.eu

# Children 0-8 years and digital technology

- **10 families in all countries** (Czech Republic, Italy, Belgium, UK, Germany, Finland, Russia)
- Families with children 6-8 years
- Interview with one parent and at least one child



# Conclusions from the project Children 0-8

- Co-construction theory: online and offline worlds are intertwinned, borders are blured
- Technology is not important -> main is the ACTIVITY
- Technology usage by young children has risks although children are not using social networking
- Parents underevaluate risks for children under 8 years – they think more about future risks
- Recommendation: parents should know more what are they children doing and should be aware of possible risks

Report:

http://irtis.fss.muni.cz/joint-research-centre-report

# Project: Unlocking the Potential of mHealth Technologies to Promote Behavioral Health and Active Aging in Czech Older Adults (from 1.11.2016)

- Prof. Steriani Elavsky, Ph.D.: Pennstate University > Masaryk University
- (1) developing an interdisciplinary line of research in the area of mobile health (mHealth) technologies for improving behavioral health and active aging
- (2) pilot testing novel methods for behavioral and psychological monitoring through the application of Dynamic Real-Time Ecological Ambulatory Methodologies (DREAM)
- → search for partners!

# Project: Digital parenting Kaspersky Lab & prof. David Smahel, MU

- Survey with usage of research panel Toluna: 450 Czech parents and other people taking care about children aged 5 to 17 years participated in the survey.

Key findings:

- Mothers spend in average more time with their children than fathers, the difference is decreasing with age of the child.
- Most common activity which mothers and fathers are doing together with their children, is watching TV or video and doing homework for school. Father are playing digital games more often together with their children than mothers.

# Project: Digital parenting Kaspersky Lab & prof. David Smahel, MU

- Mothers and fathers are at most afraid that their child can get injured, how s/he is doing in school and that s/he could be harmed by other children.
- Fathers are most often teaching their children how to use digital technologies and they are also mostly responsible for security of digital devices which are children using.
- Both parents are often actively discussing with children what they do on the Internet and helping them with complicated things online. Fathers give more advices to children how to use the Internet in the safe way.

## Project: Digital parenting
## Kaspersky Lab & prof. David Smahel, MU

- Mothers are primary controllers of child’s activities on the Internet.
- About 42 % of parents is checking web sites which are children visiting. Only 15 % of families have complex software tool to control their children activities on the Internet.

- Main conclusion: mothers have primary role in solving problems of children’s safety in offline (real) life and fathers have primary role for children’s digital security