

LESSON 12: YOUNG PEOPLE & THE ONLINE WORLD

Law & Citizenship Course • *Ghid practic de educație
juridică - „Elevul și legea”* • Judecător Cristi Danileț



CONNECTED SAFE & RESPONSIBLE



The Internet opens doors to
learning, expression, and
friendship — but also to risks.
The law protects your privacy,
identity, and reputation online.

LESSON CONTENTS

PART 1

DIGITAL LIFE & RESPONSIBILITY

What the law says about online behavior, privacy, and respect for others

PART 2

CYBERBULLYING & ONLINE SAFETY

How to recognize, prevent, and report online harassment or threats.

PART 3

DIGITAL RIGHTS & DATA PROTECTION

Understanding your right to privacy, consent, and control of personal information.

PART 4

WHEN THINGS GO WRONG

What to do if your image, data, or messages are misused — where to ask for help.

PART 5

REVIEW & PRACTICE

Quiz, key concepts, and reflection tasks — review what you've learned and apply it

LAW & CITIZENSHIP COURSE

WHAT YOU'LL LEARN IN THIS CHAPTER

In this chapter, you'll discover how **freedom and safety** must work together in the **digital world**. The Internet connects us, but it also **records our actions**. Every click, post, or message leaves a **trace** that can **help** or **harm**. The law protects your **privacy, identity,** and **digital reputation**, yet it also expects responsibility and respect for others online. You'll learn why **sharing photos** or **personal data** requires **consent**, how to spot **online manipulation**, and what **cyberbullying** or **fake profiles** can mean in **legal terms**. We'll also explore how **freedom of expression** applies online and where it ends when it violates someone else's rights.

By the end, you should be able to explain what **digital responsibility** means, **identify risks** and **safe practices**, and know which authorities can help if your rights are violated online.

CONNECTED, BUT RESPONSIBLE

WHY DIGITAL FREEDOM NEEDS RULES TO STAY SAFE

The Internet gives us **freedom to learn, share, and express ourselves** — but that freedom ends where another person's rights begin. What we **post, record, or forward** can build trust or cause harm, and once online, **it rarely disappears**. The law protects **privacy, identity, and digital security**, yet it also **holds us accountable** for what we say and do. Clear **online rules don't restrict expression** — they keep it fair, so everyone can be safe and respected.



Warm-Up Activity



Think of one online rule that helps protect people — for example, asking permission before posting a photo. Why do you think this rule matters?

Digital respect builds real-world safety.

WHY DO WE NEED DIGITAL RULES?

Just like in real life, **digital spaces** need rules to keep everyone safe and respected. Without them, **hate speech**, **fake accounts**, and **cyberbullying** could **silence others** or **destroy reputations**. **Online freedom** doesn't mean doing whatever we want — it means using technology responsibly so no one is hurt. Rules protect your **privacy**, your **image**, and your **data**. They define what's acceptable, **set limits**, and **stop online harm** before it spreads. Whether at home, school, or on the internet, **respect** and **awareness** are the keys to safety.



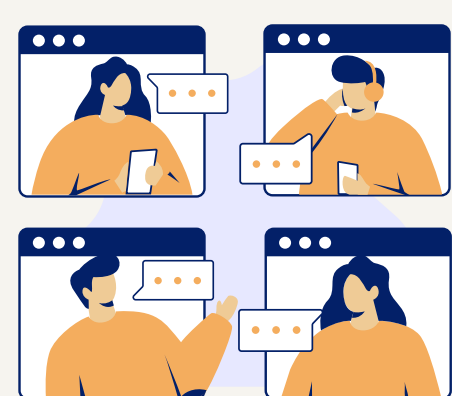
Fairness, Not Fear

The Internet should be a space where everyone can express themselves without being attacked.



At School & Online

Think before you post; protect your passwords; don't share or forward hurtful content.



In Group Chats & Games

Be respectful in messages and comments; don't exclude, insult, or expose private things.



Why it Helps

Digital rules protect your reputation and others' dignity — kindness is never outdated.



Boundaries Online

Share only what you'd say face-to-face; private stays private, even in groups.



On Social Media

Report fake accounts, offensive pages, or threats; check what you share and with whom.

Imagine and Reflect

Think of one post, comment, or photo you shared that got reactions — good or bad. How did it make others feel? Would you post it again today? Why or why not? Write 2–3 sentences below.

WHO DOES WHAT ONLINE

Rule Makers



Rule Makers

- **Parliament & EU rules** — set the legal frame for privacy, consent, profiling, platform duties, and minors' protection (e.g., data protection laws).
- Define what counts as personal data and when it can be used.

Enforcers



Enforcers

- **Government & Agencies** — the national Data Protection Authority investigates complaints, audits companies, and applies fines; cybercrime units tackle hacking, threats, and identity theft.
- Consumer watchdogs act on unfair online practices.

Courts



Judges & Remedies

- **Courts** — order takedowns and deletions, award damages for privacy breaches or defamation, and punish crimes like non-consensual intimate images or illegal access.
- Urgent injunctions can stop ongoing harm.

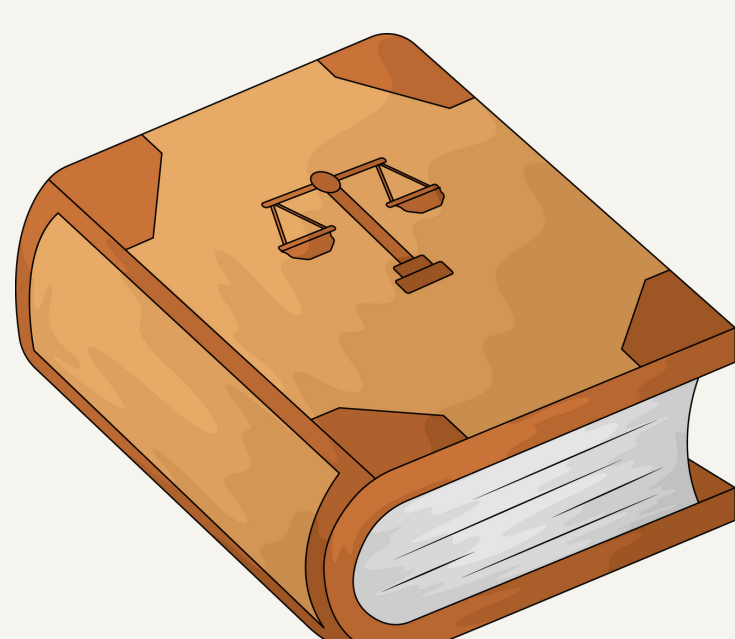
Referee



Referees & Coordinators

- **Data Protection Authority** — guides schools, firms, and platforms; mediates complaints; standardizes practice so rules are applied the same way for everyone.
- Ombudsman and child-protection bodies help vulnerable users.

Key terms



Mini-Glossary

- **Data Breach** = loss, leak, or theft of data; must be fixed fast and sometimes reported.
- **Two-Factor Authentication** = extra step that protects accounts if a password leaks.

WHEN THINGS GO WRONG ONLINE

A **digital world** connects us — but it can also harm when rules are ignored. **Online actions** can **hurt reputations**, **invade privacy**, or **expose personal data without consent**. Knowing what to do and where to turn protects both you and others. Just like laws protect rights offline, **digital laws** protect your **safety**, **dignity**, and **control online**.



PROBLEMS

From fake accounts and photo leaks to insults or threats, online behavior can become abusive. What you post or share can be copied or twisted — even after deletion.



YOUR RIGHTS

You have the right to privacy, to ask for harmful content to be deleted, and to report online abuse. Screenshots and timestamps can serve as evidence when things go wrong.



WHERE TO REPORT

Contact a parent, teacher, or school counselor first. If the problem continues, you can reach out to the Police Cybercrime Unit, the National Authority for Data Protection, or trusted NGOs working on online safety.



WHY IT MATTERS

Taking action isn't about revenge — it's about restoring safety and respect. Reporting harm protects not only you but also others who might face the same risks. Silence allows abuse to spread; responsibility stops it.

HOW TO REACT WHEN THINGS GO WRONG

Notice the Issue

If something feels wrong — leaked photos, bullying, stolen accounts — take it seriously.



Stay Alert

Collect Proof

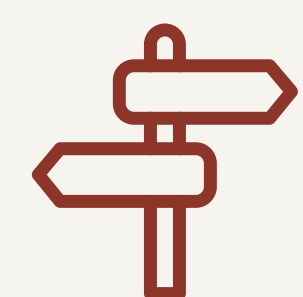
Save screenshots, messages, and links. Record dates and usernames. This helps you and authorities understand what happened.



Save Evidence

Tell a Trusted Adult

Share the situation with your teacher, parent, or counselor. They can help you stay calm and guide your next steps.



Ask for Guidance

Report the Incident

If it continues, report it on the platform and to cybercrime authorities or the Data Protection Agency if personal data was shared.



Take Action

Get Professional Support

If the event affects your mental health or school life, ask for help from psychologists, helplines, or youth NGOs.



Find Support

So what for me?

Your online safety starts with awareness. Acting early prevents bigger harm. Each report helps make the internet a safer space for everyone — ignoring abuse only fuels it.

Try it: Think of one online rule you follow — for example, asking before reposting a friend's photo. Who does it protect? What could go wrong if no one followed it?

QUIZ — Lesson 12

Check what you've learned about digital life, safety, and your rights online. Read each question carefully and choose the correct answer.



- 1** What's the safest rule for passwords?
 - a) One strong password for everything
 - b) Different strong passwords
 - c) Write them on paper under your keyboard
- 2** A classmate posts your photo without consent.
 - a) Publicly insult them back
 - b) Report the post and ask for removal, keep evidence
 - c) Ignore it — it will disappear
- 3** What does “the Internet is real” mean legally?
 - a) Online actions can have real-world legal consequences
 - b) Things online are only jokes
 - c) Screens protect you from any liability
- 4** A stranger offers a gaming skin if you share your location.
 - a) Share a nearby place, not your home
 - b) Decline, block, and report the account
 - c) Accept but delete the chat later
- 5** Which example fits digital consent?
 - a) “It’s public, so I can repost it”
 - b) Asking before sharing someone’s image or chat and respecting “no”
 - c) Tagging friends automatically
- 6** Which is phishing?
 - a) Teacher: trip schedule
 - b) Bank “security”: confirm your PIN
 - c) Class chat: review project
- 7** What’s a red flag of grooming by an online aggressor?
 - a) They suggest moving to private chats
 - b) They correct your homework
 - c) They send a funny meme to the group
- 8** What’s the Dark Web?
 - a) Any site with dark mode
 - b) Encrypted networks accessible with special software
 - c) Private Instagram accounts
- 9** Why use two-factor authentication (2FA)?
 - a) It makes logging in slower, so hackers give up
 - b) It adds a second proof it’s you, even if a password leaks
 - c) It hides your IP address
- 10** What law-respecting reaction fits a cyberbullying case?
 - a) Collect screenshots, block, report, and tell a trusted adult
 - b) Reply with a harsher meme
 - c) Delete your account forever

QUIZ — Lesson 12

ANSWER KEY



- 1** What's the safest rule for passwords?
 - a) One strong password for everything
 - b) Different strong passwords
 - c) Write them on paper under your keyboard
- 2** A classmate posts your photo without consent.
 - a) Publicly insult them back
 - b) Report the post and ask for removal, keep evidence
 - c) Ignore it — it will disappear
- 3** What does “the Internet is real” mean legally?
 - a) Online actions can have real-world legal consequences
 - b) Things online are only jokes
 - c) Screens protect you from any liability
- 4** A stranger offers a gaming skin if you share your location.
 - a) Share a nearby place, not your home
 - b) Decline, block, and report the account
 - c) Accept but delete the chat later
- 5** Which example fits digital consent?
 - a) “It’s public, so I can repost it”
 - b) Asking before sharing someone’s image or chat and respecting “no”
 - c) Tagging friends automatically
- 6** Which is phishing?
 - a) Teacher: trip schedule
 - b) Bank “security”: confirm your PIN
 - c) Class chat: review project
- 7** What’s a red flag of grooming by an online aggressor?
 - a) They suggest moving to private chats
 - b) They correct your homework
 - c) They send a funny meme to the group
- 8** What’s the Dark Web?
 - a) Any site with dark mode
 - b) Encrypted networks accessible with special software
 - c) Private Instagram accounts
- 9** Why use two-factor authentication (2FA)?
 - a) It makes logging in slower, so hackers give up
 - b) It adds a second proof it’s you, even if a password leaks
 - c) It hides your IP address
- 10** What law-respecting reaction fits a cyberbullying case?
 - a) Collect screenshots, block, report, and tell a trusted adult
 - b) Reply with a harsher meme
 - c) Delete your account forever

KEY CONCEPTS FROM LESSON 12



DIGITAL CONSENT

Asking permission before sharing someone's image, voice, or messages — and accepting a “no.”



RIGHT TO ONE'S IMAGE

You control how your identifiable photo/video is used; others need consent or a legal basis.



PERSONAL DATA

Any info that identifies you (name, username, photo, location, device ID); collect/share with care.



TWO-FACTOR AUTHENTICATION (2FA)

A second login step (code/app/key) that protects accounts if a password leaks.



STRONG PASSWORDS

Long, unique combinations; use a password manager instead of reusing.



PHISHING & SMISHING

Fraudulent emails or texts that mimic trust to steal logins or money.



SHARENTING RISKS

Adults posting kids' data/images that can follow them for years or be misused.



DATA MINIMIZATION

Share only what's necessary; fewer details = lower risk.



PLATFORM REPORTING

Built-in tools to flag abuse, impostor accounts, or non-consensual content.



DARK WEB BASICS

Hidden networks with legitimate and illegal uses; never share personal data or buy/sell there.