



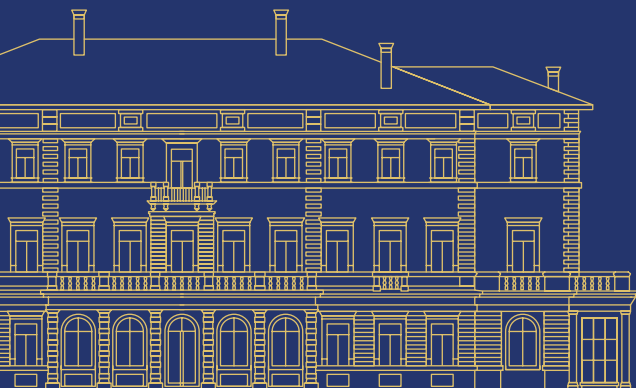
**CEELI
INSTITUTE
REPORT**

**PRACTICAL GUIDELINES ON USE
OF SOCIAL MEDIA BY JUDGES:
CENTRAL AND EASTERN
EUROPEAN CONTEXT**



ADVANCING THE RULE OF LAW

The CEELI Institute is a Czech public benefit organization (not-for-profit) based in Prague, dedicated to the development and training of an international network of legal and judicial professionals committed to advancing the rule of law. Through innovative training programs and other activities, the Institute works with judges, lawyers and civil society actors to build laws-based societies. The CEELI Institute prides itself on the diversity and quality of the programs it has developed, the peer to peer exchanges it fosters, the innovative nature of its programming, and its legacy of contributing to the advancement of the rule of law in vulnerable countries. Our efforts are focused on creating independent, transparent, and effective judiciaries, strengthening democratic institutions, fostering efforts to combat corruption, bridging difficult conflicts, promoting human rights, and supporting lawyers and civil society actors in repressive environments. The CEELI Institute is based at the Villa Grebovka, in Prague, a historic nineteenth century building now renovated into a state-of-the-art residence and conference center.





CEELI INSTITUTE REPORT

**PRACTICAL GUIDELINES ON USE
OF SOCIAL MEDIA BY JUDGES:
CENTRAL AND EASTERN
EUROPEAN CONTEXT**

November 2019

TABLE OF CONTENTS

Table of Contents	5
Aknowledgments	7
Foreword	9
Overview of Recommendations	11
The Recommendations for Social Media Use by Judges	13
1. Represent the Judiciary Well in ALL Social Media Content	13
2. Never Comment on Pending Cases	15
3. Do Not Use Social Media to Investigate Parties	15
4. Mind Whom You “Friend” and What or Whom You “Like”	16
5. Avoid Political and Commercial Comments	16
6. Adjust and Monitor Your Online Visibility	17
7. Protect Your Personal Data	18
8. Educate Your Family and Friends	19
9. Using Social Media to Educate the Public	20
10. Continue to Educate Yourself about Social Media	20
Quick Tips for Managing Your Activities on the Internet	21
Appendix I	23
1. History of Social Media	23
2. Definitions	23
2.1 Defining Social Media	23
2.2 Defining the Most Used Social Media	24
2.3 Dangerous Social Media Tools	26
3. Impact of Social Media on Society	28
4. Social Media in Politics and Public Life	28
5. Owners of Data on the Internet	29
6. Privacy Questions Relating to Social Media	30
7. Risking Abuse	31
8. Examples of Security Settings for Social Network Accounts	32
Appendix II	35
List of National and International Opinions, Regulations and Standards Related to Social Media	41

ACKNOWLEDGMENTS

The CEELI Institute wishes to thank members of the core Working Group of the Central and Eastern European Judicial Exchange Network, who conceived and drafted these Guidelines on the use of social media by judges:

Judge Katica Artuković, Bosnia and Herzegovina

Judge Marela Jevtović, Bosnia and Herzegovina

Judge Davor Dubravica, Croatia

Judge Domagoj Frntić, Croatia

Judge Ladislav Derka, Czech Republic

Judge Levente Simon, Hungary

Judge Mindaugas Šimonis, Lithuania

Judge Cristi Danilet, Romania

Thanks also to Ksenija Renko and Marko Rakar, regional public relations and communication experts, to David Sellers, Public Affairs Officer, Administrative office of the US Courts, Barbora Field and Freda Grealy, CEELI Institute Program Managers, and Katherine Sorrell, CEELI Institute Legal Intern (William and Mary Law School) for their valuable contributions in developing these Guidelines.

The Institute also wishes to thank the Hon. Judith Macaluso, Janet Katz, and Jane Mahoney for their invaluable assistance in editing this document.

They worked on this document pro bono - without compensation, as a public service to support the work of judges.

This project was made possible by a grant and ongoing support from the U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL).

FOREWORD

The CEELI Institute has trained and supported judges in Central and Eastern Europe since 2000. Not surprisingly, the issue of social media use by judges has become an increasingly important discussion at judicial events organized by the Institute and by other organizations in the region. As social media use has developed into a daily phenomenon that is part of most people's lives, the examination of ethical constraints on social media use has become a pressing concern for judges.

Since 2012, the CEELI Institute has fostered a Network of Young Judges from Central and Eastern Europe, with the support of a grant from the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL). A core working group of the Network's judges sought to examine in detail the challenges of social media use, in order to provide their colleagues with explanations and guidance on how to use social media in a way that avoided pitfalls and ethical problems. With the help of judicial, ethics, and public relations experts, the CEELI Institute has now developed this set of Guidelines for judges on appropriate behavior when using social media. They include examples of social media misconduct that can compromise the independence, integrity and impartiality of a judge, undermine public confidence in the judiciary, and/or lead to disciplinary action against a judge.

The goals of this document are to summarize these considerations, provide judges with a clear overview on the pros and cons of social media use, and offer recommendations for how to use it safely. These Guidelines will focus on the most popular social media platforms such as Facebook, Instagram and Twitter, now used by a large percentage of those with access to the internet. However, the recommendations apply to other social media platforms such as YouTube, LinkedIn, Reddit, and blogs, as well as to platforms not yet created.

There are good reasons why judges should use or at least be aware of how social media functions. On the one hand, activity on social media can lead to ethical concerns and challenges. These include the propriety of content posted by judges, unintended demonstration of bias or interest by a judge via his or her posts, and consequences arising from judicial interaction with third parties. The behavior of judges on social media is visible to the public, and therefore their online activities can harm public trust in the judiciary. Social media positions can also raise questions about the impartiality and the fairness of a judge's trial.

On the other hand, social media is an effective tool for public education, in part because it reaches a segment of the public that may not otherwise interact with the judiciary. The use of social media may also improve the public's perception and understanding of courts and

judicial officers. At the end of the day, social media is a major part of modern life. A blanket instruction to judges to simply “stay off social media” is not a realistic suggestion in the current age. Therefore, we offer a basic set of recommendations that judges can follow in order to navigate using social media appropriately.

This document is relevant to individual judges who are active on social media, and also to those responsible for setting national standards for judicial conduct, including: members of judicial councils, court presidents, officials from judicial associations, and any other members of the judiciary regulating judges’ use of social media.

It is important to stress that these Guidelines focus on the use of social media by individual judges and do not deal specifically with the use of social media by courts, ministries or national judiciaries. Although these Guidelines provide information relevant to those who establish policies on access to information about court systems, an institutional approach to social media use by courts and ministries would necessarily differ, reflecting the needs and goals of educating and informing the public about how to effectively access and use the court systems, ensuring transparency and public trust in their institutions and providing news about significant events.

While drafting this document, the CEELI Institute and the Network judges referenced a wide range of materials and sources of information, including social media policies and recommendations by international organizations. The list of references can be found at the end of this document. Finally, we note that these Guidelines are intended only as guiding principles and are not “best practices.” Social media platforms are constantly changing, so “best practices” will continue to evolve rapidly alongside future platform developments.

Before we start with a practical set of recommendations, it is important to stress that a judge’s behavior on social media should always be in line with the Bangalore Principles of Judicial Conduct¹ and other existing international standards, as well as unique national codes of judicial ethics. Also it is the responsibility of the national judiciaries to provide clear rules to follow, in case a judge does not meet the ethical standards required.

Christopher Lehmann
Executive Director, The CEELI Institute

¹ THE BANGALORE PRINCIPLES OF JUDICIAL CONDUCT,
(The Bangalore Draft Code of Judicial Conduct 2001 adopted by the Judicial Group on Strengthening Judicial Integrity, as revised at the Round Table Meeting of Chief Justices held at the Peace Palace, The Hague, November 25-26, 2002
https://www.unodc.org/pdf/crime/corruption/judicial_group/Bangalore_principles.pdf

OVERVIEW OF RECOMMENDATIONS

1. Represent the Judiciary Well in ALL Social Media Content

Always maintain a professional tone and maintain an awareness of your role as a judge even if posting in a personal context. Anyone with a career in the judiciary needs to be careful about what they write and what they publish online, whether via email, text, or social media posts, since digital content is so easily and widely accessible and could impact their work in a variety of ways.

2. Never Comment on Pending Cases

In line with the Bangalore Principles comments about court judgments or ongoing cases are particularly sensitive, because they can raise suspicions about the impartiality and objectivity of judges and the judicial system.

3. Do Not Use Social Media to Investigate Parties

Judges must consider only the evidence presented by the parties and any facts properly subject to judicial notice. Judges should not independently investigate case facts by means other than those provided by law.

4. Mind Whom You “Friend” and What or Whom You “Like”

When declaring yourself a friend with someone on social media or liking particular posts, members of the judiciary should take care not to compromise their neutrality. Interaction on social media can create the perception of bias, even if it does not exist.

5. Avoid Political and Commercial Comments

Judges should stay out of political debates and not publicly disclose their political views.

6. Adjust and Monitor Your Online Visibility

Carry out regular review of your online social presence and adjust your privacy settings if necessary.

7. Protect Your Personal Data

Think twice before revealing any personal information. Once you post personal information on Facebook or any other social network, it is highly unlikely that you will be able to keep it private. Such personal data has a permanent presence and can be recovered, circulated, or printed years after being sent or posted online.

8. Educate Your Family and Friends

Talk to your family and friends to ensure they understand the sensitivity of the judicial work you conduct and potential consequences of their actions online if they reveal personal information or photographs that could be linked to your profile.

9. Using Social Media to Educate the Public

Social media platforms can be used as a positive tool to engage and educate the public, promote transparency, advocate, explain the importance of judicial tasks, and provide information about the activities of judicial institutions. Many judges throughout Central and Eastern Europe, and beyond, have successfully used social media to this end.

10. Continue to Educate Yourself about Social Media

Social media is here to stay and judicial training and continuing education on social media use is critical. Among other things, judges must be familiar with the operation of social media as issues related to its use will increasingly be relevant to the cases before them.

THE RECOMMENDATIONS FOR SOCIAL MEDIA USE BY JUDGES

1. Represent the Judiciary Well in ALL Social Media Content

Blurring the lines between public and private life is one of the characteristics of social media interaction. Informal socializing with family and friends has become part of the public sphere, especially when photos and comments are posted on the internet. Unlike emails shared between two people, it is much harder to control communications in social network environments, because they are more public. Anyone with a career in the judiciary needs to be careful about what they write and what they publish online, whether via email, text, or social media posts, since digital content is so easily and widely accessible and could impact their work in a variety of ways.

- Judges should determine what role, either professional or personal, they will appear under or serve on social media.
 - Do you want to network professionally and provide expert insight? Some judges have managed to do this successfully; others have fumbled badly.
 - Do you want to reveal the judicial function you perform? In this case, is there instruction from your institution in how to represent your professional role?
 - Will you use social media in a strictly non-professional way, to stay in touch with family and friends in an informal, personal way?
 - Or, do you want to simply want to passively participate in the social network as an observer who does not post any content (including comments on the posts of other members of that network)?
- Decide how you will present yourself on your profile. It's not just about the impression you make, but also about any potential far-reaching consequences of your activities.
 - Will you be available under your real name or pseudonym? Be aware that some networks do not allow pseudonyms and their use is considered a breach of terms (Facebook, for example, requires users to create an account using their real name). Also if your pseudonym is discovered later on, it can harm your reputation.
 - Will you use a photo of yourself or picture of a flower, animal, or caricature? Be careful what you choose. While a personal photo leaves you more vulnerable to easy identification, there was a case of a Croatian judge who used a cartoon character as a Facebook profile picture, and a lawyer who represented one of the parties in a criminal case requested the recusal of the judge, because he found the profile picture inappropriate.

- Maintain a professional tone. Clearly indicate that your published personal opinions do not reflect the views of the institution in which you work, nor are they in any way related to the cases in which you are engaged. Nevertheless, even a disclaimer may not ensure that your statements will not be perceived as a reflection of your official position. It is safe to assume that if you put “judge” or “prosecutor” in front of your name, your posts will be considered your official opinion and the opinion of the institution in which you work.
- If your posts are devoted to raising awareness about legal issues, decide whether you will use the same communication channels for private posts, including comments or images about sports, art events, politics, social trends, and family events. Mixing the professional and the personal can be confusing for your followers, but it can also help shape your image as a “real person” rather than a remote symbol of the justice system, seemingly untouchable for other members of the society in which you live.
- Avoid making private posts during work hours, as each post includes the time it was published. Spending time during the workday on social media, rather than on judicial work, opens a judge to criticism.
- Conduct that is deemed inappropriate and would not be tolerated or recommended in real world situations and interactions is also not recommended in the virtual world, even via more private communications through Facebook Messenger or other direct messaging channels. All digital communication is easily captured and documented for sharing purposes.
- Judges should avoid any inappropriate or indecent vulgarities, satirical expressions, sarcasm, or ironic criticism, which can lead to the disintegration of the judge’s integrity. As mentioned in the Recommendation of the Czech Union of Judges (attached hereto in Appendix II), a judge’s posts on social media should be consistent with the dignity of the judge’s function and should not draw criticism about the judge’s impartiality and independence. A negative perception has the potential to harm not only an individual judge, but also the whole community of judges.
- Photographs and comments on Facebook, or other social media outlets including dating apps, should be modest and decent. A safe standard is to only publish posts, opinions, or photographs that could be on the cover of a respectable daily newspaper or broadcast at prime time on national television!

² Ksenija Renko, Communication Expert, Jupiter Strategic Communication, Remarks at the Launch of the Global Judicial Integrity Network, Vienna, April 2018

2. Never Comment on Pending Cases

The following Bangalore Principle applies to any form of communication, including social media: “A judge shall not knowingly, while a proceeding is before, or could come before, the judge, make any comment that might reasonably be expected to affect the outcome of such proceedings or impair the manifest fairness of the process. Nor shall the judge make any comment in public or otherwise that might affect the fair trial of any person or issue.”

- Comments about court judgments or ongoing cases are particularly sensitive, because they can raise suspicion about the impartiality and objectivity of judges and the judicial system.
- If you are taking a picture to post on social media, keep in mind that modern cameras capture much more detail than is visible to the naked eye on your mobile phone. Most social networks allow you to download any uploaded photos, making it easy to zoom in and see details, including papers on your desk, names from private files in your office, and other identifying markers. Even if you do not intend to reveal confidential information from a case, there is a possibility that you will do so through a posted photo.

3. Do Not Use Social Media to Investigate Parties

Judges should not independently investigate case facts by means other than those provided by law. This rule extends to information available in all mediums, including electronically.

- Judges must consider only the evidence presented by the parties and any facts properly subject to judicial notice.
- Judges should refrain from researching any additional information about litigants or lawyers involved in their cases on social media.
- Keep in mind that some social media platforms, such as LinkedIn, allow the user to see who has viewed their profile. Do not assume your use of social media is anonymous.
- If someone sends a private message via social media or to your official email, especially if you are currently assigned to their case, you should warn the sender that such communication is not allowed. Also, immediately notify the appropriate authorities that an ex-parte communication has occurred. It is advisable to enclose the appropriate documentation and to refrain from further communication with the person. This will protect your integrity and the reputation of the judicial institution.

³ THE BANGALORE PRINCIPLES OF JUDICIAL CONDUCT, see fn. 1, above.

4. Mind Whom You “Friend” and What or Whom You “Like”

Certain social media communications might create an unintended judicial-third party relationship. The debate continues about whether judges should be “friends” with other lawyers, prosecutors, or representatives of parties. By accepting and declaring someone a friend on social media, it does not mean that the judge has met the person in real life, or that there is any deeper relationship between the parties. Yet, members of the judiciary should take care not to compromise their neutrality, and interaction on social media can create the perception of bias, even if it does not exist.

- Generally, judges should be cautious and selective in choosing Facebook “friends.” In most cases, judges should not befriend lawyers, police officers, or other parties who regularly appear in front of the judge at court. There is less concern, however, with a judge having Facebook “friends,” so long as the judge does not allow such a “friend” to exert any special influence. If a social media friendship exists with someone who becomes involved in a case, it is recommended to disclose information about the relationship on record.
- Be particularly careful about “liking” or “following” a political group, religious group, media outlet, or other Facebook pages that can undermine the public’s view of your independence. The organizations, institutions, and people you like and follow are publicly visible.
- In all circumstances, avoid liking or following inappropriate pages that promote racism, hate, homophobia, bigotry, intolerance, or prejudice of any kind.

5. Avoid Political and Commercial Comments

A judge must always be cautious that comments made on social media or elsewhere, including those made in public speeches, do not jeopardize the dignity of the judge’s function. If their reputation is called into question, public trust in the justice system, and personal impartiality and independence is undermined.

- As a general rule, a judge should not publicly disclose his or her political views, except on issues related to justice, on any social media platform. The risk and possibility of objection bias can occur, especially if the judge were to rule on a matter related to the political party, movement, or political issue.

⁴ Opinion of Judicial Ethics Advisory Board in South Carolina, Kentucky and Ohio

- It is also advisable to stay out of political debates. If a judge participates in exchanges of political opinion on social media platforms, even as a neutral party, their own objectivity becomes questionable by being associated with the conversation, which then indirectly and directly discredit the objectivity of the entire justice system.

6. Adjust and Monitor Your Online Visibility

Each social network has its own policy for accessing published content, and it is necessary to be aware of these policies, as well as those of other internet services such as a blog or email, before using them.

- Every time you post something online, it is best to assume anyone can see it, because you cannot know if others have already shared it with their friends, within or outside the network. It is completely beyond your control if, when, and in what context your post could be reposted elsewhere on the internet. When you delete a post, it may no longer be visible to you or your friends within the social network, but it is best to assume that it exists elsewhere online or can still appear in online searches.
- On Facebook, all posts are limited to members of the network, with the ability to determine the level of publicity of your posts: public, only friends, only friends with some exceptions, or directed at one person. If your posts on Facebook were initially marked as “public” or, available to all members of the network, and at some point, you decide to change the status of your messages to “private,” this change will only apply to your posts from that moment. Previous posts and comments will continue to be available to everyone in the network. Please also keep in mind that Facebook’s rules on content and privacy settings can at any time. The same is true for any other platform.
- On Twitter, all messages are publicly available to those who are not members of that network, and a tweet can be copied and shared by email or other means without the knowledge of the person who wrote the tweet. You can delete a tweet, but there is no guarantee that someone did not save or take a screenshot of the tweet.
- It is strongly advised to search your name regularly using major search engines. While conducting the search, you will be able to find online posts, articles, and images related to your name; you can see whether you have posted something that is still visible, or whether someone else mentioned you in a topic of discussion.

⁵ Czech Union of Judges, Ethical limits on a judge’s activities on social networks, 2017

- On occasion, you should also search various platforms to see if you have any fake profiles. If someone is impersonating you or posting inaccurate information about you, report these profiles to the appropriate contact on the social media provider where the profile appears.
- If you use pseudonyms to avoid being identified there is no guarantee you will remain anonymous. There was a case of a Greek judge who allegedly published a racist comment on her blog under a pseudonym, but her identity was soon discovered.

7. Protect Your Personal Data

Once you post personal information on Facebook or any other social network, it is highly unlikely that you will be able to keep it private. Such personal data has a permanent presence and can be recovered, circulated, or printed years after being sent or posted online.

- Opening a profile on a social network involves filling in basic information about yourself, primarily your name and email address. Each social media tool has its own rules for required information, which may include biographical data, gender, age, and other basic identifiers. Most also allow for the entry of optional personal and professional details.
- Think twice before revealing any personal information, including your home address, family pictures, or information about the school your children attend.
- Setting up an email or social media account on any social network also means selecting a username and password. The quality of the selected password is crucial in preserving the integrity of your communication. When choosing a password, avoid common words from the dictionary, characteristic numbers such as year or date of birth, postal code, or phone number. Never use the same passwords for accessing different internet services; when you use the same password for securing accounts, if the password is detectable on one of the accounts, it helps attackers abuse both of your services more easily. Avoid writing down your passwords, especially on sticky notes you place somewhere visible. Since it is not easy to remember a large number of different passwords, you may wish to consider the following examples:
 - Use the beginning of the verse of a song, proverb, or rhyme you know by heart.
 - Add a term that you will easily remember and which has no content/associative links, completely out of context.
 - Combine upper and lower case letters.
 - Add numbers.
 - Add special characters (# & / \$ %).

- If available, consider using dual-factor authentication (also called 2FA, or “two-factor authentication”). Most services on social networks today use it to provide secure access for account users. Besides using your password, you can use an additional code (number or combination of numbers and letters). The most common method is to have a code sent via SMS to your mobile phone. If you use SMS based 2FA, always have your SIM protected with a pin code. Bear in mind that since phones and especially SIM cards are increasingly under attack, it is recommended to choose another way to generate an additional code for additional verification of identity.
- Avoid using public devices, such as a computer at the airport terminal or hotel reception. If you must use such devices, always log out after using internet services. Even if you use your own devices, including your laptop or mobile phone, it is a good idea to log out and close your browser. Ideally avoid using devices that you cannot control, particularly to access any of your email, business, and banking or social media accounts.
- Official email addresses are to be used exclusively for official correspondence and business purposes. For private communication with family and friends, and for personal business, a private email should be used.
- While increasingly large numbers of email messages are transferred between servers in an encrypted state, you should always assume the content of your email message is accessible to others. This is particularly true of email sent on official or work email accounts.

8. Educate Your Family and Friends

Judges should be aware that even when they are not present on social media, their family members or friends might share pictures or information related to them, which can be misused or manipulated in an attempt to influence a judge.

- Your family members and friends should respect boundaries and avoid undermining your judicial impartiality, integrity, or dignity through their own social media accounts and online presence.
- Talk to them to be sure they understand the sensitivity of the judicial work you conduct and potential consequences of their actions online.
- Ask them not to reveal any personal information like addresses, holiday photos, or any other information that could be misused.

9. Using Social Media to Educate the Public

So far we have only discussed recommendations about what not to do on social media. There are, however, many benefits to using these tools and establishing an online presence, especially for judges.

- Social media is a great tool for engaging the public, promoting transparency, advocating, or explaining the importance of judicial tasks, and providing information about the activities of judicial institutions. Many judges throughout Central and Eastern Europe, and beyond, have successfully used social media to this end.
- If you use social media as an educational tool, however, be aware that there is the potential for trolls (see Appendix for definition) to ridicule anything you say or do. Engaging with an internet troll rarely has any benefit, and will often result in a downward-spiraling discussion. In order to deal with trolls, you can certainly ignore them or set your own personal boundaries on the types of comments you will acknowledge or allow on social media platforms that you use.
- Social media platforms can also be used for groups, or associations, rather than individuals. For example, a Judicial Association might choose to set up a curated social media page.

10. Continue to Educate Yourself about Social Media

Social media is here to stay and will continue to play an important role in society, politics, and the economy. Judges should keep pace with modern technological advances, educate themselves about its functions, and understand the context in which certain technological disputes arise. Keep in mind that platforms, and rules governing their use will continue to change often.

- Judicial training and continuing education on social media use is critical. Among other things, judges must be familiar with the operation of social media as issues related to its use will increasingly be relevant to the cases before them. A profound and robust knowledge of a judges' environment, including the interplay between technology, social media, and the law, will increase public trust and confidence, legitimizing judicial institutions and practices in the eyes of the public.
- The rules will continue to evolve over time. Always proceed with caution and try to adhere to codes of conduct and national and international regulations, such as the Bangalore Principles.

⁶ 10 Tips to Dealing With Trolls, Jonh Rumpton, 2015, <https://www.forbes.com/sites/johnrampton/2015/04/09/10-tips-to-dealing-with-trolls/#14d484c54f42>

⁷ Tips for Dealing with Internet Trolls and Haters in Business, Carol Roth, <https://www.carolroth.com/blog/tips-for-dealing-with-internet-trolls-and-haters-in-business/>

QUICK TIPS FOR MANAGING YOUR ACTIVITIES ON THE INTERNET

If you are a judge or judicial official, the recommendations for the use of new communication technologies are significantly more important to follow than those that apply to average users. By adhering to these recommendations, we hope that it will keep you safe from making some of the more common mistake.

The internet provides an outlet and space for greater professional productivity, improved visibility, scope, and broader engagement across the world. Your online activities, however, are not only a technical channel for communicating within the professional or private sector, but also a reflection of your overall personality and opinions. It is necessary to understand the specifics of this environment, so that you can incorporate them into an effective framework within the existing rules of behavior and ethics. This integration ensures your safety on the internet and out in the real world.

When deciding on using an internet service, observe the following recommendations:

- ▶ Choose your internet service provider wisely, keeping in mind the purpose of your activities. Are they professional or private, or both?
- ▶ Remember that content you enter (from alphanumeric data, to photos and video clips) from your device is not only available on that specific device, but also to the operator itself, and potentially to other users of the same service.
- ▶ Deleting entered content or any other post, does not mean that this data is permanently unavailable to others, or that it cannot be dug up or tracked by your internet service provider, or by another user, in its original or altered form.
- ▶ Get to know the basic characteristics of the internet service provider that you will be using, and bear in mind the general recommendations from your internet provider.
- ▶ When opening a user profile (email or profile on a social network), decide:
 - The name of your profile, it does not have to be identical to your username. This is important for your (professional and private) internet identity. Remember that even if you use pseudonyms, you must comply with all ethical standards related to your profession.
 - Use unique authentic information.

-
- Choose a high-quality password that is safe (use small and large letters, numbers, special signs), and one that you will easily remember.
 - Read all security messages from the operator of your internet service provider and confirm them only after you are sure that they are authentic.
 - ▶ Notify your service provider if you see something that is not in line with your online identity, or related to your profile.
 - ▶ Communicate with colleagues in court or people from private spheres in the same manner that you would in everyday life. Wait, and consider the pros and cons before you send any public or private messages.
 - ▶ Refrain from commenting on opinions and discussions of other participants, especially if you notice those discussions are crossing a line. Make sure the public sees you as a respected individual, when it comes to communicating.
 - ▶ Before joining a discussion on a topic that is currently popular make sure it is authentic, and that you have all the relevant facts. Keep in mind that your comments will always be an important contribution to any discussion.
 - ▶ Repeat: Think before you post!
 - ▶ Pay special attention to communications with colleagues and potential or current clients conducted on the web. Web communications are still subject to the same rules and regulations as the real world. If you notice that any communication is inappropriate, end it and notify someone about the issue. For example, you can report an incident by reporting the issue to the social media network or service provider about the potential inappropriate communication.
 - ▶ Limit your use of internet services during the workday, in order to avoid a potential negative impact on the performance of your work, and on your private life
 - ▶ The goal is to control your use of new technologies, but not limit your own participation in social communications, use it in the most efficient and positive way possible.

APPENDIX I

1. History of Social Media

Early social media networks like AOL Chat Rooms, LiveJournal and MySpace emerged in the late 1990s. Current, popular social websites developed since then include: Facebook, Twitter, LinkedIn, Instagram, Snapchat, YouTube, Google+, WeChat, Pinterest, Snapchat, Tumblr, Viber, WhatsApp, Wikipedia, Reddit, VKontakte in Russia, Weibo in China, and others. The biggest boost to social media came with the introduction of smartphones, which permit billions of users to seamlessly connect on a daily basis, and since the early evolution of social media, internet users have continuously increased the amount of time spent on social media sites. The benefits of participating in social media have also extended beyond simple social sharing. Users now focus on building a reputation, expanding career and business opportunities, and earning income. By mid-2018, the global population was around 7.6 billion people, and 4.3 billion people have access to the internet. Currently, over 3 billion people use at least one social network. Today, social media consists of thousands of social platforms. While some social media platforms are more popular than others, each platform offers something different. For example: Instagram caters to people through photography, and those who use Instagram are usually under the age of thirty-five. People over thirty-five are more likely to use Facebook to share their personal experiences, and to connect with people from their social circle and beyond. Twitter is perfect for those wishing to communicate in short bursts of 280 characters or less.

Facebook alone has over 2 billion users. Other social media targets users from certain countries or areas of linguistic similarity with a much smaller number of users, but a more significant impact on the local environment(s) and population(s) it serves. For instance, the Russian network Vkontakte (VK) has 477 million users from the Russian-speaking world, while the most popular Chinese social network, Weibo, has over 500 million users. There are hundreds of other social networks that connect users interested in specific topics and areas of interest; although less popular in terms of member usage and social impact, they are still useful and important.

2. Definitions

2.1 Defining Social Media

While social media has changed individual and organizational communication, it differs from print-based communications and media (e.g., magazines and newspapers) or traditional electronic media (such as TV broadcasting) in many ways. These differences include: quality, reach, frequency, usability, immediacy, and performance. Social media outlets have many

sources and many receivers, whereas traditional media such as radio or newspaper only have one transmission source and many receivers. The greatest difference is that unlike traditional media, social media allows anyone to create and share their own content, whether a blog post, image, video, or status update. And because of the influence and reach of the internet, a social media profile, blog or a YouTube channel can be more widely accessed than those of traditional media in some countries.

Wikipedia defines social media platforms as, “Interactive, computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests, and other forms of expression via virtual communities and social networking services.” It also notes that, “Users typically access social media services via web-based technologies on desktops, laptops, tablets, or smartphones. When engaging with these services, users can create highly interactive platforms through which individuals, communities, and organizations can share, co-create, discuss, and modify user-generated or pre-made content posted online.”⁸

2.2 Defining the Most Used Social Media

The following social media sites are particularly popular in Central and Eastern Europe: Facebook: a popular, free, social networking website that allows registered users to create profiles, upload photos and videos, send messages, and keep in touch with friends, family, and colleagues. Facebook is constantly evolving, and is currently available in more than 37 different languages. It includes public features such as:

- Marketplace, allowing members to post, read, and respond to classified ads.
- Groups, allowing members with common interests to find one another and interact.
- Events, allowing members to publicize an event, invite guests, and track who plans to attend.
- Pages, allowing members to create and promote a public page built around a specific topic.

Each individual user can set the privacy conditions and visibility (or invisibility) of their Facebook page and posts. All interactions are published in a news feed, which is distributed in real-time to the member’s friends.⁹ Facebook has introduced a variety of response buttons that users can utilize to respond to posts. Based on a user’s privacy setting, others can see what you like or otherwise respond to. This issue is very important when considering possible conflicts of interest.

⁸ https://en.wikipedia.org/wiki/Social_media

⁹ Pedagogy of Social Sciences, MANGAL, S. K., MANGAL, UMA, PHI Learning Pvt Ltd., 2018

Instagram: Instagram is a social network (owned by Facebook) for publishing photos and video clips. Instagram has the ability to apply a large number of photo filters so that photos look more professional. Users can like and comment on posts by other users, and they can sync a published photo on Instagram so that it instantly uploads to a user's Twitter feed and/or Facebook profile. Based on the number of users (which was 1 billion as of June 2019), Instagram is positioned as one of the most popular social networks.¹⁰

LinkedIn: LinkedIn is a social network designed for professionals to present their personal business profiles. It allows you to set a profile that presents educational background, professional qualifications, and memberships in professional groups and associations. LinkedIn profiles are basically a professional biography that gives a user's business associates insight into the user's current professional position and contact details. LinkedIn users can build a network of professional contacts with other people from their work environment. Users can become members of different LinkedIn professional/thematic groups, which serve as a platform for exchanges of opinion about different professional matters.

Tinder: No discussion of social media would be complete without reference to dating applications (apps), as they are often used by judges too. One of the most popular apps is currently Tinder, a location-based dating mobile app that allows users to create their profile, post a picture and add a description. After their profile is created they can "like" (swipe right) or "dislike" (swipe left) other users. It also allows users to chat if both parties "like" each other in the app. The information available to the users is based on the uploaded pictures and a short bio that users write about themselves. While it is not our intention to advise or regulate a judge's use of this and other dating apps, they are additional streams of social networking. There are plenty of other dating apps, including Match.com, Badoo, Grindr, and Bumble, although Tinder seems to be the most popular. Judges obviously need to be particularly careful and prudent about information and photos that they reveal about themselves on these platforms.

Twitter: Twitter is a social media service for posting messages of up to 280 letters and numbers. It is also possible to post photos and links to other sites, and to receive messages from followers. A popular feature of Twitter is retweeting, or reposting another user's tweet. "Hashtags" can be used to track how many people have tweeted, or posted about a certain topic, and Twitter lists the most popular topics of the day as "Trending Topics." In some countries, Twitter is considered a go-to network for quick information gathering. Twitter has also been used as an organizing tool for many recent high profile social and political events around the globe.

¹⁰ The Psychology Behind Why Instagram Is So Addictive, Drake Baer, 2014.
<https://www.businessinsider.com/psychology-of-why-instagram-is-addictive-2014-11>

¹¹ Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). IEEE Transactions on Dependable and Secure Computing, 9(6), 811-824.
<https://ieeexplore.ieee.org/abstract/document/6280553>

2.3. Dangerous Social Media Tools

Social media can be subject to a wide array of abuse and manipulation. To review a few of these vulnerabilities:

Cyborg: Cyborgs, in the social media context, are either bot-assisted humans or human-assisted bots.¹¹ A concrete example of a cyborg in the social media context is a human being who registers an account for which they set automated programs to post, such as tweets, during their absence. From time to time, the human participates, tweets and interacts with friends. Cyborgs are different from bots, as bots use automation, whereas cyborgs intertwine characteristics of both manual and automated behavior. Unfortunately, Cyborgs offer unique opportunities for the spread of fake news. While Cyborg accounts try to pose as real people; including mimicking a realistic looking number of friends or followers, many of these accounts are still manufactured and use „friend farms“ to collect a large number of friends in a short period of time.

Fake news: Fake news and propaganda are as old as humanity. However, with public access to the internet, and the speed of sharing information on social networks, it has become arguably more dangerous. There are five categories collectively referred to as “fake news”.¹² Some news categories are fake (disinformation), while others are attributed to biased information (misinformation). Regardless, they all have a very loose connection with the truth and basically sit on a continuum of intent to deceive. The following are examples of the forms fake news can take:

- Misleading news reports that are semi-true, but used in the wrong context, that are drawn from selectively chosen real facts that are reported to gain headlines, but tend to be a misinterpretation of a factual event.
- Sloppy reporting that contains some grains of truth, but is not fully verified, which are then used to support a certain position or view.
- Misleading news stories that are not based on facts, but which support an ongoing narrative. This includes news where there is no factual support, often where ideologies or opinions clash, and where unconscious biases come into play. Conspiracy theories tend to fall here.
- Intentionally deceptive news that has been fabricated deliberately to make money through the number of clicks, to cause confusion or discontent, or as sensationalist propaganda. These stories tend to be distributed through imposter news sites designed to look like “real” news brands, or through fake news sites. They often employ videos and graphic images that have been manipulated in some way.

¹² Source: 5 Types of ‚Fake News‘ and Why They Matter, Nicola Watts, <https://web.smu.edu.sg/spring/5-types-of-fake-news-and-why-they-matter/>

¹³ <https://www.techopedia.com/definition/24063/internet-bot>

Fake news is often used to discredit political or business rivals. One fake news story was published by a site created to resemble ABC News just before the presidential elections in 2016. Titled, “Obama Signs Executive Order Banning the Pledge of Allegiance in Schools Nationwide,” it generated over 2.1 million shares, comments, and reactions in just two months.

Bot: “A bot is an automated application used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform. Bots can be used for productive tasks, but they are also frequently used for malicious purposes.”¹³ A socialbot is a particular type of bot that is employed in social media networks to generate messages automatically (e.g., tweets) or advocate certain ideas, support certain campaigns, and influence public reaction by acting as a „follower“, or even as a fake account that gathers followers itself. It is estimated that 9-15% of active Twitter accounts may be socialbots¹⁴, and that 15% of the total Twitter population active in the 2016 U.S. presidential election discussion were bots.¹⁵ And during the 2016 Brexit vote, according to an economic study¹⁶, bots added 1.76 percentage points to the pro-“leave” vote as Britain weighed whether or not to remain in the European Union.

Troll: An internet troll (cyberbullying, online harassment) is a person who starts arguments or upsets people on the internet to distract and spread discord. A 2016 study for the NATO Strategic Communications Centre of Excellence on hybrid warfare notes that the Ukrainian crisis, for example, „demonstrated how fake identities and accounts were used to disseminate narratives through social media, blogs, and web commentaries in order to manipulate, harass, or deceive opponents.”¹⁷

Viral: Social media posts or sites that become popular and are shared by a great number of users and re-shared by their contacts “go viral.” It is an analogy to a viral infectious disease which is spread quickly from one person to another. Most social networks enable users to re-share the posts or site by a simple click on a “share” button.

¹⁴ „Online Human-Bot Interactions: Detection, Estimation, and Characterization“, Varol, Onur; Emilio Ferrara; Clayton A. Davis; Filippo Menczer; Alessandro Flammini (2017). Proc. International AAAI Conf. on Web and Social Media (ICWSM).

¹⁵ „Social bots distort the 2016 U.S. Presidential election online discussion“, Alessandro Bessi and Emilio Ferrara (2016-11-07), First Monday.

¹⁶ Authors of the study are Yuriy Gorodnichenko from the University of California at Berkeley and Tho Pham and Oleksandr Talavera from Swansea University in the U.K.

¹⁷ „Internet Trolling as a hybrid warfare tool: the case of Latvia“. stratcomcoe.org. Riga, LV: NATO Strategic Communications Centre of Excellence (published 28 January 2016). Archived from the original on 28 January 2016. Retrieved 28 January 2016

¹⁸ Selective Exposure, Jonathan L. Freedman, David O. Sears, <https://www.sciencedirect.com/science/article/pii/S0065260108601033#fn1>

¹⁹ Díaz-Fernández, Antonio M.; del-Real-Castrillo, Cristina (2018-07-01). „Spies and security: Assessing the impact of animated videos on intelligence services in school children“. Comunicar (in Spanish). 26 (56): 81–89. doi:10.3916/c56-2018-08. ISSN 1134-3478.

3. Impact of Social Media on Society

Despite connecting vast numbers of people, social media has been observed to reinforce existing social groupings and divides. Social media enables people to create an “echo chamber” that excludes information challenging their views. Selective exposure generally refers to people’s tendencies to favor information that reinforces their ideas and reject information that opposes their ideas.¹⁸ As technology has become increasingly more personalized, the prevalence of selective exposure has increased, which then leads to ideological polarization.

Recent research at Blanquerna University¹⁹ in Spain has demonstrated that social media, and media in general, have the power to increase stereotyping not only in children but in people of all ages. The internet activist Eli Pariser invented the name *filter bubble*²⁰, for the intellectual isolation that can result when a website algorithm selectively guesses what information a user would like to see based on information about the user, such as location, past click-behavior, and search history. As a result, users have less access to information challenging their viewpoints, effectively isolating them in their own cultural or ideological bubbles.²¹

4. Social Media in Politics and Public Life

The rapid spread of information on social media can impact political and public figures quickly, whether the information is true or not. Social media is an open forum that provides anyone with a voice to speak out against government regimes as well as individual public figures including judges. “Social media is becoming the main conduit for social mobilization and government critiques because, the government can’t control what we say on the internet.”²²

Communication platforms are persuasive and often work to influence political views because of the abundance of ideas, thoughts, and opinions circulating through the social media platform. Younger generations are becoming more involved in politics and public life, including in the examination of politics, and the role of the judiciary, due to the increase in political news posted on various social media networks. While informing younger generations of political news is important, there can be many biases within the realms of social media. It can be difficult for outsiders to truly understand the conditions of dissent when they are removed from direct involvement, and social media can create a false sense of understanding among people who are not directly involved in the issues.

²⁰ https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript

²¹ https://en.wikipedia.org/wiki/Filter_bubble

²² Social media, World Heritage Encyclopedia, Article Id: WHEBN0005897742

5. Owners of Data on the Internet

When using one of the free email services (Gmail, Yahoo etc.), we assume that all messages sent and received are visible only to us and our addressees. However, our emails are also located on servers in what is known as the „cloud“ – the IT infrastructure that allows for the mass storage of data. This infrastructure is located in large computer centers throughout the world, in multiple places at the same time.

Your messages are „private“ to the extent that messages sent to the desired address will not be sent to any other address. However, the content of your messages is available to server owners who use it to provide you with a tailored user experience. Advertisements you receive are more appropriate to your taste, and the locations you have visited are stored away to be used at a later date.

Our private address books are also included in the „cloud“, and their integrity depends on the strength of our password and also on how safe the operator of this data is from external attacks. Cloud storage is advantageous for its ability to share and store data across platforms, but one disadvantage is that someone else can potentially abuse this option and download your list of contacts too. The days of physical address books that can be kept out of sight from prying eyes are long gone.

The data we leave on various internet services are not limited to biographical and contact information but also includes information about a person’s overall behavior on the internet. This means each activity (each „click“) you undertake, starting with what websites you visit and which terms you search, to each „like“ and comment on social networks. All of these data are continuously being used for commercial purposes, in order to complete your user profile. Our data—address books, emails, posts on our online profiles—are saved on our devices. When we turn off the electronic device our virtual activities are on hold until the next use. Nonetheless, we do not always realize that the camera and microphone are occasionally turned on without our knowledge.

Digital „traces“ of your activities are stored arbitrarily, and your ability to influence them is minimal or nonexistent. It’s likely that you will never be in a situation where you will be asked to revoke, delete, or alter such data. But, if you are in that situation, you will see that all popular social networks are under the jurisdiction of other countries and copies, of this data are found in several countries simultaneously.

Deleting data on your device may also allow it to be deleted from the data banks where it is stored in (e.g., after 30 days, in case you change your mind), but even then, there is no way to determine that the data (statements, photos) have been completely deleted, and that they will not appear again. For instance, social media “Friends” may have saved your posts for later use.

Finally, there is the question of ownership of social media content or the content which is generated through social media interactions. The ownership of content on social media

platforms was always unclear because it is generated by the users and hosted by a company. Added to this is the danger to the security of information, which can be leaked to third parties, or “parasites” who comb the data for their own databases. *The current situation is that the actual owners of content created on social media sites are the large corporations who own those sites, and rarely the users who created them.*

Privacy rights advocates warn users of social media about the collection of their personal data. Some information may be collected without the user’s knowledge or consent through electronic tracking and third-party applications. Data may also be collected for law enforcement or governmental purposes or by social media intelligence using data mining techniques. When you share information on social media, remember that information is no longer private. It is widely acknowledged that it is very important to monitor what you share and to be aware of whom you could potentially be sharing that information with. Some social media users do not realize that anyone outside their circle of friends would read their post; in fact, on some social media sites, unless users select higher privacy settings, their content is automatically shared with a wide audience. Once something is posted, its accessibility remains constant even if we select who is potentially able to view it.

Most users want to start using an internet service as soon as possible and give their consent to the terms of use without hesitation –and often without reading the terms, thinking little about the consequences of the legal relationship they have just entered. We recommend judicial officials read the terms of agreement usage, and after reasonable consideration of the conditions, make an informed decision on how they should proceed.

6. Privacy Questions Relating to Social Media

Today, in the time of social media networks, problems appear when communication that is private in nature - due to the specificity of internet media - become public. In this situation, it is important to decide whether and how to respond, as well as to consider the technological specificities of each communication channel.

It is important to note that any internet conversation is most often in written form. Typing a text (post and comment) or publishing a photo creates **content** that will be available to any interested party. Each „like“ or „retweet“, every two-way comment, or just an emoji (e.g., smiley face) is in fact a **document** that you have sent to another person or a general „internet audience“. This content can include your signature, location, and the device you are using. A remark made during the coffee break during a conference in front of a few colleagues will probably not remain in the minds of most of listeners longer than the end of that work day. The same remark sent as an e-mail or as a tweet or as a status on Facebook becomes content that is archived for future use and can reappear in a way you did not expect years later in a completely different context.

One of the greatest dangers in online communication is the possibility of quick response, or instant commentary on someone’s post. Technology allows you to express your attitudes

almost in real time, as if you are talking face-to-face with the person. It is important to suppress the pressure to respond immediately, especially if it is a discussion which can potentially lead to an argument. The easiest way to control your internet communication is by giving yourself more time to respond. If you cannot refrain from answering, write a statement immediately, but do not send it. Wait until the next morning and when you read your response again, you will most likely edit the message.

In any situation, behave with respect and avoid any comments about third parties, social issues, political attitudes, personal traits, etc. that could, even years later, in other contexts, negatively reflect on you or your reputation. The same goes for photos/video clips. A photo album that you shared with friends and relatives at a family gathering could have a very different meaning if one day (maybe years later) it appears on the front page of a tabloid or online portal. Try to view your own posted content through the eyes of “others”.

7. Risking Abuse

Even if you have applied all tips for choosing a quality password, your profile can still be abused. An attacker can come across your password in a variety of ways, either through malicious software installed on your computer or through a hacker attack on your internet service provider. One of the most notorious cases was the attack on Yahoo that compromised more than one billion users.²³ If you suspect that your Facebook profile has been misused, follow the instructions that Facebook has prepared for such cases.²⁴ The same applies to all other available internet services from email to social networks (Twitter²⁵, LinkedIn²⁶, Instagram²⁷, etc.).

You can usually delete unwanted comments, but to do so requires you to monitor your online profile. Although you have no direct responsibility for the comments of other people (who may or may not be on your friends list), the appearance of their comments on your profile may indicate a closeness that would be unacceptable to you in some other context.²⁸

The most difficult type of abuse is the falsification of your messages and posts, especially photos and videos. You cannot prevent these cases, but if your earlier social media content has established a certain behavioral model on the Internet, malicious falsifications can be disproven more easily. It is therefore necessary to interpret national codes of ethics (which mentions „behavior out of court“) in a context that applies to virtual spaces.

²³ <https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users>

²⁴ <https://www.facebook.com/help/hacked>

²⁵ <https://help.twitter.com/en/safety-and-security/twitter-account-compromised>

²⁶ <https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en>

²⁷ <https://help.instagram.com/149494825257596>

²⁸ Some services exist only to track deleted messages, like <https://politwoops.eu/> which can detect the deleted messages between the moment you post something and your deletion

8. Examples of Security Settings for Social Network Accounts

Facebook: Privacy settings on your account allow you to control who will see your posts, who can add a “Friend” request, or who can tag you when you appear in photos of other network members. Keep in mind that not all devices support all options (depending on the version of the operating system and device). When choosing who can see your posts, you can choose whether they will be:

- “Public” - available to all network members
- „Friends“ - available only to your friends
- „Friends except“ - available to your friends with some exceptions
- „Specific friends“ - available only to listed friends
- „Just for you“ (Only me) – available and visible only to you
- „Single“ - available to friends and lists you select
(e.g., family, close friends, acquaintances, colleagues)

When you choose the settings for one post, they remain the same for all posts until you change them again. You can also change the visibility of a post on your „Wall“ later. If you posted messages on your friend’s wall, your friend can then determine the level of visibility by adjusting the privacy settings for the post on his/her/their wall. Be sure to turn on Login Alert options, so that each time someone logs in (even if you are logging in from some other device), you will receive a notification that access has been made to your account. Pay special attention to applications that allow you to connect to your Facebook account. Almost all such applications ask you to allow them to access your data, as well as to update your accounts and posts.

Twitter: Twitter has some useful special options for using your account.²⁹

Notifications³⁰ - This option allow you to have an overview of relevant events on the „Twitter Line“ in one place (in one line of information), such as:

- When you get a new follower,
- When someone „raises“ your tweet,
- When somebody mentions you in a comment („manipulates“),
- When someone posts your tweets (retweets)

Blocking Other Accounts³¹ - This option allows you to completely remove profiles that offend you (on Twitter) which means that you will not see the deleted person’s tweets, nor will they see yours. By blocking another account, you stop following it and simultaneously prevent

²⁹ <https://help.twitter.com/en/managing-your-account/understanding-the-notifications-timeline>

³⁰ <https://help.twitter.com/en/managing-your-account>

³¹ <https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts>

the account holder from following you. The purpose of this option is not only to stop receiving notifications or updates about another account, but to completely remove followers you don't want.

Verified account - Fake profiles are one of the negative sides of social networks. Your profile photo can be downloaded from another network. Your first name can be listed next to the account name (the account name can be manipulated slightly so that it is enough to change the order of letters in a word, or write the number „1“ instead of the letter „l“). You would be unaware that someone with a very similar profile is publishing tweets that could be attributed to you - whether you have your own account or if you are not even a member of Twitter at all. To combat fake accounts, Twitter introduced a category of „verified accounts“ that are recognized by a blue badge next to the name on the account profile. These official accounts prove to Twitter staff and users that your account is of public interest, and the content and opinions represent the actual user (and not someone pretending to be the user). Most often the categories of verified accounts are those whose owners are from the fields of art, public administration, politics, media, sports or business.

Additionally, you have to pay attention to other apps that request access to your Twitter account and other functions you have enabled on your Twitter account. If you do not clearly understand what it is that you need to do, check the Twitter new user FAQs (frequently asked questions), the Twitter Help Center, or frequently asked questions on the Twitter app. Consider the consequences, and decide after becoming aware of the data collection usage, terms of service, and conditions.

Instagram: You have several visibility options for your account:

„Public“ - Anyone can start to follow you, review and share your photos, videos or posts.

„Private“ - You decide whether to allow other users to follow you or not. If you are a judicial official, it is recommended that account holders set their profiles to the “private“ option. Bear in mind that published photos need to adhere to the specific terms in accordance with the code of ethics (this information can be found in the Community Guidelines Section in the app or account). Always keep in mind that the published photos, intended only for close „Friends“ can always be published where you did not expect them to appear.

Even if a person in a judicial function does not have his/her/their own profile on any social network, it is possible for false profiles to appear. This can be problematic if the photos are taken from private sources. Judges and prosecutors must be aware that they could find themselves in a situation where they may be susceptible to false profiles on social networking sites.

LinkedIn: There are two options in setting up your profile that we draw attention to, as they can have an impact on your reputation:

„Notifying connections when you're in the news"- This option is automatically turned on when creating a profile, and if you leave it turned on every time you appear in the news (media or blogs), all of your contacts will be informed. It's up to you to choose whether this option will inflict reputational damage. Keep in mind, notifications are not separated between positive and negative news, all of your contacts will still be informed.

„Mentions by others"- Every time someone mentions you in their own posting, it increases the „visibility“ of your profile. You cannot control the context in which someone is going to mention you. Accordingly, use your own judgement and decide whether to leave this option on or off.

APPENDIX II

Czech Union of Judges Guidelines

Ethical limits on a judge's activities on social networks

At the Annual Meeting of the Judicial Union held on 5 November 2016 in Mikulov, the Ethics Court of the Judicial Union was given the task of assessing the ethical limits for the activities of judges on social networks (Facebook, Twitter, blogs, etc.), in relation to the extent to which a judge's freedom of speech is limited by his or her office.¹

The Ethics Court of the Judicial Union (also referred to as the EC only) worked from the „Judicial Behaviour Principles“ adopted at the Annual Meeting of the Judicial Union (SU) on 26 November 2005 (otherwise also the Code of Ethics)². This Code of Ethics set out in general terms the basic principles of dignity, impartiality and independence in the activities and conduct of a judge. However, these principles are of a general nature and do not specifically address the activities of judges on social networks. The EC therefore also made use of the conclusions and findings from the dissertation of Mgr. Zdeněk Křivka³ entitled „Judges and the Social Media“. In drafting its opinion, the EC also took into account the legal framework applicable to the work of judges, in particular at the most general level, Arts. 81 and 82 of the Constitution, Art. 17 of the Charter of Fundamental Rights and Freedoms and Section 80 of Act No 6/2002 on Courts and Judges (hereinafter referred to as the „ZSS“), it is hardly possible to conclude that a judge could breach his legal obligations provided for in the aforementioned legal regulations while not breaching the principles of judicial ethics. However, this consideration does not apply in reverse - the mere observance of the law on the part of a judge does not mean that he has not violated judiciary ethics. See, for example, ordinary membership in a political party, which does not of itself violate the law but is not in accordance with judicial ethics (this conclusion was pronounced at the Annual Meeting of the Judicial Union held on 24 November 2007 in Kroměříž⁴. However, it would have been violation of the law (in particular, of Art. 80(4) of the ZSS) if the judge was not only a regular member of a political party or movement, but held a political function within a particular political group, i.e. would be politically more active than an ordinary member.

For the aforementioned legal framework, judicial decisions concerning the activities of judges on social networks are also relevant: the decision of the disciplinary panel of the

¹ The exacting wording was: “assessment of the limits of ethical activity for a judge on social networks (Facebook, Twitter, blogs, etc.), in order to assess the extent to which a judge's freedom of expression is limited by his judicial role.”

² <http://soudci.cz/o-nas/eticke-zasady-chovani-soudce.html>

³ KŘIVKA, Zdeněk. Judges and social media. Brno, 2015. Dissertation. Masaryk University, Faculty of Law. Available at: https://is.muni.cz/th/378547/pravf_m/DP_final_v1.0.pdf.

⁴ He considers, however, from the ethical point of view, membership of a judge in a political party as inappropriate, and that it is unacceptable for a judge to be a member of local government.”

Supreme Administrative Court ref. 11 Kss 6/2015-53 of 6 June 2016 (and the subsequent finding of the Constitutional Court ref. IV ÚS 2609/16 of 11 April 2017), ref. 16 Kss 7/2014 - 92 of 11 June 2015 and the subsequent finding of the Constitutional Court ref. I. ÚS 2617/15 of 5 September 2016, finding of the Constitutional Court ref. II. ÚS 2490/15 of 8 November 2016 (in the case of a mass e-mail communication from a judge) and the Constitutional Court's finding, ref. III. ÚS 3844/13 of 30 October 2014 (the nature of communication on Facebook by a natural person - „a non-judge“).

In other conclusions the EC does not distinguish whether the ethically problematic activities of judges outlined below are at the same time a violation of the law, as this was not the wording of the assignment given to the Judicial Union's Court of Ethics.

A judge's freedom of speech is limited, unlike that of a „non-judge“, by the fact that a judge must always take care that (and this applies in particular to his public speeches) his/her contributions do not jeopardise the dignity of the judge's function, call into question trust in justice and his/her personal impartiality and independence. Generally speaking, a judge should not as a rule publicly disclose his or her political views, except for issues related to justice. If he/she were to express an opinion on political issues (unrelated to justice), there is the possible objection to bias if he or she were then to rule on a matter related to the political party (movement) or political matter he commented on. In addition, it is advisable to stay out of political debates, not least with regard to the declining level of rules of good behaviour in these debates. If a judge comes to participate in public exchanges of political opinions, as a rule, he calls into question his own dignity (indirectly, the dignity of justice as a whole as well) and, as mentioned above, will also call into question his own future impartiality. In this context, it must be emphasised that for the exclusion of a judge it is sufficient for a reasonably observant observer to infer that he is unable to rule impartially. Concerning speeches of a judge in relation to political competition, the EC also refers to the conclusions of the Constitutional Court adopted in its finding ref. I. ÚS 2617/15 from 5 September 2016⁵.

Where a judge publishes his contributions is also of significance. It would no doubt be negative if a judge, as guardian of the rules governing a democratic society and the rule of law, published his contributions in a media space that might be considered extremist, i.e. attacking the basis of a democratic society. This applies to both printed matter and the Internet.

If a judge publishes his views on the blog or on the web (it is not important whether as an article or as a response or commentary on another article), these are publicly expressed views to which all of the above applies.

⁵ „...An individual who has taken office as a judge is bound by the duty of loyalty and restraint when exercising his freedom of speech, under Article 17 of the Charter and Article 10 of the Convention. His freedom of expression is as a consequence subject to the special constraints arising from that obligation. In particular, a judge must not disturb public confidence in his decision-making in accordance with the fundamental principles of the democratic rule of law, and confidence in the impartiality and independence of the judiciary. A judge must be restrained in comments relating to political competition, in particular the public assessment of individual candidates or parties and groups or the formation of political coalitions.”

The situation with Facebook is more complicated. This is a communication platform that serves primarily to establish and maintain online relationships and to disseminate information. Facebook allows one to create a network of social contacts, permits communication between users, the sharing of different multimedia content, the organising of events and user presentations. After signing up, a user has the opportunity to find other users of the network they would like to contact and ask them to „be friends“ (confirming mutual interest in the contact). Inter alia, a user can individually set the scope for sharing of published information, and can use privacy tools to choose who will see content posted by him/her or related to him/her, as well as who can contact and search for them and in what manner. The user profile on a social network can therefore function openly (it is public for all other Facebook users or even all Internet users) or closed (the user either generally chooses to publish their information to a circle of users or can make this option separately for individual posts and information). Facebook communication can be performed using chat (discussion), messaging (the ability to send messages to a single user or to a certain group of users), or through the user's personal profile page, on which posts can be placed by the user, but also by other users if the user's individual settings allow. Through user-selected privacy settings, a user's profile page content can be opened up only to friends, to selected circles - friend groups, all Facebook-registered persons, or to non-registered users using the Internet.

The nature of the Facebook social network is clearly neither private nor public. It always depends on specific users as to how they set the privacy level on their profile, or directly for individual posts. A user may communicate with only one other user through this network, without this communication being seen or affected by other users. Such a communication is purely private, although effected through a social network used by a billion users, just as a two-person e-mail communication via e-mail such as www.gmail.com or www.seznam.cz can be considered private. However, a Facebook social network user also has the ability to make their profile completely public and therefore accessible to all Facebook social network users and all Internet users. This option is widely used, for example, by political parties, interest groups, artists, service providers, merchants and others who aim to present themselves to the widest possible number of Internet users through this social network. However, some „normal“ users also choose this setting, and if they are also judges, they are subject to the same restrictions as for any public speech.

We encounter a certain ethical risk, which could lead to doubts about a judge's impartiality, in connection with being „friends“ on Facebook. By concluding a mutual agreement on inclusion in one's list of „friends“, the user expresses a certain affection (sympathy) to that person. The problem with a „friend“ of a judge may arise in a procedural situation where he rules on a case in which his „friend“ is a party to the proceedings or a representative of such a party. A place on the list of „friends“ can give the impression of an exceptional position for a judge's „friend“, who can also influence a judge in his/her judicial decision-making.

However, on the nature of „friendship“ it can be said that this concept cannot be identified with normal friendship, that is, a deeper relationship that manifests itself in regular, personal contact, spending leisure time on joint holidays, mutual visits, etc. Therefore, it is not possible to say across the board that every „friendship“ on Facebook proves the partiality of a judge (in this respect, no generalisations can be made; it will always depend on the specific case and the facts of a particular case).

For Facebook, as well as for other social networks, it should be noted that contacts on them cannot be considered strictly bilateral. „Friends“ on these networks build their own contact network, sharing posts they have already shared. A judge can therefore never be sure where his post will appear, although he originally only shared it with a limited range of contacts. The problem with Facebook may be data-sharing when other users share their content on a judge's page in order to influence a judge's decision-making (e.g. articles related to the current case). Any positive response by a judge to such shared material would be completely inappropriate.

The „like“ feature on Facebook can be described as an expression of your sympathy, affection, or agreement with a post, commentary, photo, video, profile, application, or other Facebook components. This „liking“ is (may be) visible to others, and a judge should be restrained in this respect, since by expressing his or her support he/she might give the impression that he is siding with the party to the proceedings or its representatives. The nature of the Twitter social network is different compared to the Facebook network. Twitter is intended for public communication aimed at a non-specified number of recipients. For this reason, this network has the same limitations for judges as in any public speeches. „Liking“ is possible in this network also.

All the foregoing is true even if a judge appears on social networks anonymously, i.e. not under his own name (it would hardly be a sustainable position that, for example, a judge's impartiality could be called into question only when the identity of the judge was revealed, that is, he does not defend opinions he has already published or only defends them under anonymous cover or a false identity). It would be necessary to designate as absolutely inappropriate an approach whereby the judge in question argued over his role as a judge.

There is surely no need to emphasize that any ill-considered formulation of a judge's opinions (various linguistic excesses or vulgarities) in his public speeches reduces the dignity of judges, and such forms of speech should be avoided by every judge. Such inappropriate forms of speech must also include satirical expressions and ironic criticism of everything and anything. If a judge uses such means of expression in his public appearances, he must necessarily expect to be confronted in the same style, and thus demeaned. If such a public interaction occurs, the dignity of the judge concerned (with an indirect impact on the whole community of judges) and possibly his impartiality, is reduced.

The dignity of a judge's function affects not only the particular judge, but the whole of the judicial community. If a judge interferes with this dignity, he damages not only himself but also the entire judiciary, for justice must be above all credible. If confidence in the judiciary is compromised, it is cannot be expected that the public will adopt and accept judges' decisions. Without this confidence, however, the principles of the rule of law cannot be fulfilled. See also finding of the Constitutional Court ref. I. ÚS 2617/15 dated 5 September 2016⁶.

Conclusions on the activities of a judge on social networks

- (1) All expressions from a judge (contributions, comments, photographs, etc.) must preserve the dignity of the judge's function and may not cast any doubt on his impartiality or independence.
- (2) A judge should not create such relationships as might create the impression that they can influence a judge's decision-making.
- (3) A judge does not comment on ongoing court proceedings.
- (4) A judge does not give legal advice.
- (5) A judge avoids political assessments (including, for example, support for a particular candidate for a political function, does not "like" political parties or movements, does not comment on controversial political issues, unless they concern justice).
- (6) A judge should bear in mind that he can never be sure of where his communication will appear, even if it was originally addressed to only a limited number of addressees.

Prague, 24 May 2017

Ethical Court of the Judicial Union Chairman JUDr. Ladislav Derka

⁶ "The primary duty of every judge is to protect fundamental rights and freedoms (Art. 4 of the Constitution) and to decide in accordance with the basic principles of a democratic state governed by the rule of law (Art. 1(1) of the Constitution). If a judge were to call these fundamental values into question in his comments, he would thereby be questioning his or her basic duties and could hardly generate public trust. In relation to these fundamental values, therefore, a judge has a duty of loyalty, which restricts him/her in the exercise of his/her freedom of speech."

LIST OF NATIONAL AND INTERNATIONAL OPINIONS, REGULATIONS AND STANDARDS RELATED TO SOCIAL MEDIA

Courts' Use of Social Media: A Community of Practice Model,
Jane Johnston, *International Journal of Communication* 11(2017), 669-683

Social Media and Judicial Ethics,
compiled by Cynthia Gray, NSCS Center for Judicial Ethics, 2017

Take care of your digital footprint, Barry Clarke, 2017

Ethical limits on a judge's activities on social networks,
Union of Judges of the Czech Republic, 2016

Social Media Ethics Guidelines,
Commercial and Federal Litigation Section of the New York State Bar Association, 2015

Guide to Judiciary Policy, Vol. 2B, Ch. 2,
Committee on Codes of Conduct Advisory Opinion, page 221-226, 2015

Judges & Social Media: Managing the Risks,
Themis Competition organized by EJTN and EU, 2015

The Use of Social Media by Canadian Judicial Officers,
Canadian Centre for Court Technology, 2015

IBA International Principles on Social Media Conduct for the Legal Profession,
Adopted on 24 May 2014 by the International Bar Association, 2014

Facebook and Social Networking Security, Martin Felsky,
Canadian Judicial Council, 2014

Should Attorneys and Judges be Facebook Friends? A State by State Overview,
Jessica Ballard-Barnett, 2014

Social Media and the Courts: Innovative Tools or Dangerous Fad?
A practical Guide for Court Administrators,
Norman H. Meyer, Jr., *International Journal for Court Administration*, 2014

Use of Social and Electronic Media by Judges and Judicial Employees,
Arizona Supreme Court, Judicial Ethics Advisory Committee, Advisory Opinion 14-01, 2014

Formal Opinion 462, Judge's Use of Electronic Social Networking Media,
American Bar Association (ABA), 2013

Should judges use social media? Judith Gibson, 2013

Judge Must Consider Limitations on Use of Social Networking Sites,
Opinion 2012-07, Maryland Judicial Ethics Committee, 2012

Let's be Cautious Friends: The Ethical Implications of Social Networking for Members
of the Judiciary, Washington Journal of Law, Technology & Arts, Issue 3 Winter 2012

OBA Social Media Policy, Oklahoma Bar Association, 2011

Opinion 66 Online Social Networking,
Judicial Ethics Committee, California Judges Association, 2010

Social Media 101, the National Center for State Courts,
the National Center for State Courts, 2019

UNODC Guidelines on Social Media 2019
United Nations Office on Drugs and Crime 2019





Funding provided
by the United States
Government



CEELI Institute

Villa Grébovka

Havlíčkovy Sady 58

120 00 Prague

Czech Republic

www.ceeliinstitute.org

office@ceeli.eu