Panel presentation by Aleksandr Konovalov
Judge of the Constitutional Court of the Russian Federation
at the Session "Combating Cybercrime: Strengthening Cross-Border Judicial Cooperation" (South Africa, Johannesburg, 4 September 2025)

Honourable Madame Chief Justice of South Africa Mrs Mandisa Maya! Honourable Presidents and Justices of Highest Courts of the G20 states!
Dear Colleagues!

1. Let me start by expressing gratitude for the possibility to speak before this esteemed forum. I am also glad to wish you a fruitful and open discussion and all the best on behalf of the Chairman of the Constitutional Court of the Russian Federation Mr. Valery Zorkin.

The topic of cybercrime, just as other topics discussed at today's summit, is undoubtedly relevant. All the issues discussed today are affecting every state to a certain extent, and they are generally cross-border, thus calling for cooperation between different countries, including judicial cooperation. It is all the more valuable that today we are engaged in these professional discussions free of political or ideological shackles.

2. For the Russian Federation, the many statements of the growing danger of crimes committed with the use of information technologies or in the sphere of computer information have a rather specific statistical dimension. In 2024, the damage from cybercrime in Russia has amounted to some 200 billion roubles (roughly 2.5 billion US dollars). According to the Ministry of the Interior of Russia, from January to June 2025 there were more than 370 thousand IT crimes registered, and only around 105 thousand of them were solved. The majority of these crimes are theft and fraud (43.1 and 185.4 thousands respectively, in total - 228.6 thousands). These are followed by the crimes in unlawful drug-dealing (63.5 thousands). There were 38.5 thousand crimes registered related to computer information, such as illegal access to such information or creation of harmful computer programs.

Thus, most crimes in the IT-sector are "old" crimes committed in the new digital medium.

And yet, this new medium creates a whole range of practical difficulties for the fight against these crimes – in their detection, qualification, proving criminals' guilt, ensuring their bringing to court and restoring the rights of the victims of such crimes.

Probably the most significant difficulties presented by the new cyber-reality to crime-fighting are the widest spread of criminal activity locations around the world, the dispersion of places where crimes are committed, interim transactions are performed, harmful results are effected, criminals, witnesses and victims are located; the many sophisticated and ever-changing facilities to cover crimes and true identities of criminals. Crime readily and actively seizes the lack of any authorities' control over major segments of the global Internet network, as well as difference in approaches of various jurisdictions to regulating the digital medium, and lack of coordination of the law-enforcement authorities placed on different sides of state borders.

3. At one of the traditional lectures during the annual St Petersburg International Legal Forum (SPILF) which many of you had the opportunity to visit the Chairman of the Constitutional Court of the Russian Federation Valery Zorkin has defined the primary risk of modern civilisation of law before the upcoming digital future as "confusion of man and society due to the changing ways of communication".

Indeed, the swift technical progress creates obstacles for timely passing of laws. The possibilities of judicial interpretation for expanding existing normative framework are often limited, and not always can be effective. Therefore, the fight against the newest manifestations of cybercrime may sometimes appear fragmented: adoption of many different normative acts, development of judicial and law-enforcement practice, inevitably slow update of international regulations. Often the authorities' reaction can be delayed and insufficient, or redundant, certain problems may be viewed out of context and cause imbalance in legal regulation. Therefore it seems that one should start with ensuring full, comprehensive and relevant monitoring and analysis of the modern cybercrime, and with forming on this basis a systemic approach to crime detection, destruction and prevention in all the necessary and required aspects of this work, combining all the types of juridical instruments, economic and humanitarian impact factors.

Combatting cybercrime requires multifaceted approach: from educating citizens in basic cybersecurity to modernisation of specialised training of law-enforcement bodies, introducing additional requirements to banks, training forensic IT-experts and specialised judicial bodies. Each component of this work has its final goal as ensuring protection of rights of citizens and society from the threat of abuse of new technologies.

4. The tried and tested, most traditional and possibly still the most effective way of combatting dangerous harmful activities is criminal prevention. The criminal mechanism of fighting cybercrime falls within the purview of the legislator. Presently the Criminal Code of the Russian Federation, firstly, foresees as aggravating circumstance the intentional commission of any crime with its public demonstration in the media or information and telecommunication networks. Secondly, in some cases the use of Internet as means to commit a crime or facilitate its commission or as a medium for public demonstration of a crime is foreseen as a special qualifying feature of a crime. Both factors increase responsibility and severity of punishment. Thirdly, using Internet or computer networks can also be a part of objective aspect of another crime, for example in certain types of fraud (fraud with the use of electronic payment devices, or fraud in the sphere of computer information). Finally, chapter 28 of the Criminal Code of the Russian Federation lists special crimes in the sphere of computer information, such as illegal access to computer information, creation of harmful software etc.

Some provisions of criminal law were explained by the Supreme and the Constitutional courts of the Russian Federation.

The Ruling of the Plenum of the Supreme Court of the Russian Federation of 30 November 2017 “On the Court Practice in the Cases of Fraud, Misappropriation and Embezzlement” explained particularities of qualification of stealing when it is committed through using of an owner’s credentials and connecting to mobile banking systems or Internet payment services. Comprehensive explanations based on analysis of court practice are also provided in the Ruling of the Plenum of the Supreme Court of 15 December 2022 “On Certain Issues of Court Practice in Criminal Cases on Crimes in the Sphere of Computer Information and other Crimes Committed with the Use of

Electronic or Information and Communication Networks Including the Internet Network". In particular the Supreme Court has developed an approach to establishing the place of commission of a crime with the use of Internet. Since the network access can be gained via different computer devices including mobile ones, the place of commission of a crime shall be determined by the place where a person has committed actions included in the objective aspect of a crime.

According to the position of the Supreme Court of Russia, in qualification of crimes committed on the Internet one has to establish that a person has performed the relevant actions knowingly, having understood the content and social danger of the relevant actions including the nature of distributed, advertised or demonstrated information and the access of a wide range of persons thereto.

The Supreme Court has explained in detail the qualification of crimes connected to creation and dissemination of pornography, including that involving minors.

The territorial jurisdiction over cybercrimes was also subject of consideration of the Constitutional Court. In its Decision of 28 September 2021 the Constitutional Court has indicated that the rules of criminal procedure do not allow for discretion in determining territorial court jurisdiction and are subject to application in connection with criminal legislation provisions determining all the elements of crime including its objective aspect.

The Constitutional Court has also considered particularities of responsibility for continuing crimes in cyber sphere, taking into account the temporal scope of criminal law. By its Decision of 24 December 2024 the Constitutional Court has refused to accept for further consideration the complaint of a citizen who was convicted for public call to terrorist actions with the use of Internet. The Court has concluded that aggravation of criminal law that has occurred during the period of commission of a crime was fully applicable to the criminal who was able to take this aggravation into account but continued the violation of a criminal prohibition in full, as per objective aspect of the crime.

The Court has also noted that a more severe responsibility for prohibited public statements with the use of Internet is conditioned by the increased availability of the

disseminated information to users, even where this information is posted to limited segments of the web, and therefore it presents an increased public danger. The legal norms prohibiting the Internet publication of items containing public calls to terrorist activities or public justification of terrorism are therefore neither disproportionate nor discriminative.

Also, in its Decision of 29 November 2024 the Constitutional Court has proceeded from the understanding that there is a direct intention of a person who displays pornographic materials on the Internet to make those accessible to unlimited number of persons.

The court practice and legislation are called to respond as timely as possible to new forms of cybercrime and new elements of criminal schemes. As noted before, the wide opportunities to anonymising criminals create serious obstacles for criminal prosecution.

Some time ago, the phenomenon of “dropping” has spread in Russia; the criminals use bank cards of third persons to receive money they have stolen from citizens, or to create several stages of its transfer. Often the “droppers” who are accomplices of a crime are the adolescents who act for insignificant reward, a share of stolen money. The organizers of fraud themselves might remain outside Russian jurisdiction.

In this connection the legislator has introduced separate criminal liability for acquiring an electronic payment device (a bank card) for a third person, for handing such a card over to a third person, for conducting illegal operations with the use of such payment device against a payment etc.

The new norms have entered into force on 5 July 2025, and they were not yet subject to Constitutional Court assessment, but at the outset it can be noted that such solutions activate the potential of general criminal prevention: the establishment of criminal liability along with informing society must lead citizens, first of all the adolescents, to strong belief that such actions are unacceptable.

On 1 April 2025 the Federal Law was adopted “On Creation of State Information System of Countering Violations Committed with the Use of Information and

Communication Technologies". The law foresees several mechanisms to protect users of communications from fraud, including the possibility for a user to refuse to receive mass messages or calls, to create a database for swift information exchange etc.

On 14 August 2025 the Government of the Russian Federation has adopted the plan of activities on realisation of the Concept of State System Countering Illegal Acts Committed with the Use of Information and Communication Technologies. This plan of activities is obligatory for executive authorities rather than courts, but it illustrates the comprehensive nature of the State efforts on combating cybercrimes, and probably will be taken into account by courts in their work.

5. In those legal systems where apart from criminal prevention there is so-called administrative prevention (including Russia), the latter is also, as we believe, capable of punishing, preventing and achieving prophylactics of illegal activities in digital sphere. Administrative norms may be more flexible and casuistic than criminal ones, enabling the authorities to react less severely to less dangerous offences, and stopping illegal and socially dangerous activities early, thus allowing the offenders to make up their minds and stop prohibited activity. Also, in Russia where only natural persons are criminally liable, the administrative jurisdiction provides for prosecuting legal persons, ensuring punishment through large fines, disqualifications and prohibition of certain activities.

6. Where the victims of cybercrimes (largely those in the form of stealing) resort to private law measures, particularly to civil claims, we can speak of claiming damages, demanding return of property from illegal ownership, recovery of unjust enrichment or of court recognition as invalid or null and void contracts concluded under the effect of fraud or cheating, or when a person did not properly understand the consequences of their actions. The latter is all the more relevant for contracts in banking, where obtaining loans (credits) in the name of another person after fraudulently gaining access to personal information became rather widespread.

In the Decision of 13 October 2022 and a number of other decisions the Constitutional Court of the Russian Federation has underlined that in examining such claims special attention must be given to the good faith and due care of banks. In particular, the circumstances demanding increased circumspection of banks include

obtaining of a loan with immediate instructions to the bank to transfer the loaned money to third persons. The position of the Constitutional Court has been taken into account by further practice and instructional rulings of the Supreme Court.

The highest courts are of the opinion that conclusion of a private loan with the use of information and telecommunication services must ensure safety of remote provision of banking services and observing the legally established guarantees of the rights of citizens, including the right to informed choice of financial products. The bank, being a stronger party to a contract, infinitely more capable of countering cybercrime than a consumer, must deploy reasonable and adequate measures to properly identify the contract party and be assured that the latter acts lawfully, reasonably and in his own name.

The practice of highest courts has motivated the legislator to undertake concrete measures aimed to protect the interests of financial services consumers: in September, some provisions that foresee a “cool-down period” in handing out bank loans will come into force. Depending on the loan amount, the loaned money will be available after 4 or 48 hours from the conclusion of the contract. During this period a person with whom a loan is concluded will be able to detect fraudulent activity and take necessary measures to protect his rights. There is also a banking organisation obligation to ensure the identity of a person concluding the loan contract foreseen, as well as the creation of a database for instant information exchange regarding simultaneous or short-timed attempts to obtain loans in different organisations.

7. As it was already said, the special feature of cybercrime is its most wide geographical spread, and readiness to make use of any discrepancy between approaches of national jurisdictions. This demands consideration of the issue of a more serious and effective international cooperation than the one deployed against “general” crime. Here, there is no place for outdated approaches, bureaucratic delays or incorrectly understood political interests. As the well-known concept puts it, crime has no nationality, and given the new capabilities that criminals have gained with their access to borderless world and new technologies, it is our common interest to counteract in a coordinated and effective manner. On our planet, there may be no “quiet harbours” or “grey zones”

for criminals where they could easily hide, blend in, legalise and use the criminal gains. Figuratively speaking, they must have the earth burning under their feet; they must feel constant threat of prosecution and imminent perspective of being captured by justice and put before court; and the illegal actives' transfer to other jurisdictions must become pointless because of synchronised state approach to countering their deployment and legalisation. Increased level of cooperation between financial and banking systems is relevant to prevent criminal withdrawal of money(today it is done as part of partners' relations and business practices); between police and special services – to disclose, expose and destroy criminal schemes and criminal groups; among courts – to ensure extradition, effective criminal prosecution and return of stolen assets.

At that, we must not become similar to criminals in the methods of our fight. However important are the goals and aims of criminal prosecution or recovery of illegally gained assets, the national jurisdictions must not resort to kidnappings, fabrication and falsification of evidence, torture or psychological pressure in order to obtain confession of guilt or a plea bargain, or to applying one's legislation outside its jurisdiction.

Apart from trivial types of criminal activity in new forms and with new capabilities offered by digital medium, there is also an especially dangerous part of cybercrime that must draw most serious concerns and most active counteraction on the part of authorities. It involves truly professional IT-specialists and significant financing, and its final beneficiaries are most likely the most serious influence groups. Mass DoS-attacks and collapse of websites of state authorities, large monopolies, transport and energy companies aimed to disrupting critically important processes up to blockage of vital service systems, to pose obstacles for normal functioning of whole societies; creation of terrorist and extremist networks, systems of recruitment of terrorists and organisation of terrorist attacks, provocation of mass disorders and attempts of state revolts; terrorist attacks and attacks on infrastructure objects: all this today is done with active involvement of digital medium. A special type of illegal activity either creating a background and conditions for other crimes, or aimed to their covering and evading responsibility is the falsification of court evidence, which fabrication in fact may

become industrialised, performed with the newest digital technologies and costly equipment or mass dissemination of fake news. In recent years Russia encounters all these “time stamps”, and we are not alone in this.

As is the case with general criminality, countering evil in this segment calls for systemic analysis, which must be full and verified, without any political engagement, and concern the understanding of present and prospective threats, the aims, possibilities and motives of culprits, the available resources to counter these schemes, and the most effective ways of their deployment.

Most importantly, we must have common understanding and common acknowledgment of the fact that this segment of illegal activities, such ways of achieving of personal political, ideological, but ultimately selfish goals go hand in hand with the most serious risks of normal existence, for lives and health of millions of innocent people. Those who can sacrifice others’ interests and even lives are actively using newest technologies, join forces, and have no burdens in the form of moral or ethical principles. Unlike them, we have law and rule of law at the heart of all our actions, but we must not lose in terms of efficiency. On the contrary, we must surpass international crime both in the means of fighting and in the results of their deployment. However strong, united, armed and dangerous may be the international criminal networks, the states with their powerful enforcement mechanisms and what is more important – with their humanistic goals will be stronger by definition. Everyone needs to understand that fighting for one’s goals with such methods will create no winners, everyone will lose. This is why it is so important to take a sober, balanced, strict and consistent approach with regard to joining forces in fighting cybercrime, and to take specific steps to this end.

Fortunately, international regulations and international cooperation in the sphere of fighting cybercrime has seen some progress lately. International regulatory framework that envisages interstate communication is developing.

Apart from the well-known law enforcement cooperation machinery through Interpol, new options of cooperation are being developed. In September 2018 in Dushanbe (Tajikistan) the Agreement was signed on cooperation of states-participants

to the Commonwealth of Independent States in the Fight against Crimes in the Sphere of Information Technologies; during 2020-2022 this Agreement has entered into force for Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan.

This Agreement recognises as criminally punishable such actions as unauthorized access to information, creation of harmful software, theft of property by way of changing the information in computer systems, as well as dissemination of pornography or extremist materials, and the call for terrorist activities. Cooperation under this Agreement is done mainly through specially defined competent authorities by way of exchange of information sending and fulfilling requests for assistance.

On 24 December 2024 the UN General Assembly after five years of preparations has adopted the UN Convention against Cybercrime; on Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

The Russian Federation was among the initiators of the UN General Assembly Resolution to develop this Convention, and it was our country that has prepared and submitted its draft.

The Convention must become the first universal international treaty, as opposed to regional Budapest Convention of the Council of Europe, to be substantially devoted to a set of measures to fight cybercrime in its different manifestations, as well as to relevant state cooperation.

The Convention provides for criminalising a number of acts committed with the use of computer networks: from hacker attacks to using technical means for deception of citizens with the aim to steal their money assets, or non-consensual dissemination of intimate images.

In its procedural part, the Convention envisages most wide legal assistance between states, including the assistance in judicial procedures in respect of crimes listed in the Convention. Such assistance is foreseen not only for information exchange (e.g. for obtaining testimony or statements, or service of judicial documents), but also for investigation-related activities – for example, collecting traffic data in real time, or

tracing proceeds of crime. Since such measures as interception of messages or traffic result in rather significant interference with the right to respect of private life, the Convention establishes the principle of proportional interference, and also indicates that state parties shall ensure deploying of cooperation procedures subject to conditions and safeguards provided for under its domestic law, including judicial review, the right to an effective remedy etc.

The signing ceremony of the Convention is planned to be held in Viet Nam on 25-26 October 2025, and it will enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. Registration of participants to the Convention signature ceremony is open until 15 September 2025.

It is our belief that the Convention creates a strong foundation for balanced and effective cooperation of law-enforcement authorities in the sphere of fighting cybercrime, and will become an adequate answer to this modern threat to the benefit of security of states and citizens' rights.

Honourable colleagues!

Just 30 years ago many things that we presently consider mundane reality would seem outright fantastic. The world surrounding us is full of new technologies simplifying our actions, communications, and decision-making process. Digital environment itself became independent reality, and the notions of «off-line» and «on-line» are practically equal. Digital technologies and processes are accompanying legal contracts and transactions, and completely new approaches and instruments have entered legal reality. Sometimes, this new reality may look truly frightening: there can be a feeling that traditional law that we became used to seeing and trusting, is incapable and has no chance of catching up with this reality, and to deal with the mass of avalanching problems. I think that despite objective complexity of the situation we must not succumb to panic and pessimism. As said before, new technologies are only serving and facilitating motives and interests that are well known since ancient times. However the contract is concluded, be it through a rite of mancipation, or block chain and cloud

technology, its essence and parties interests remain the same: remuneration-based acquiring or disposal of property subject to agreed type and quality thereof. Behind all the unique and perfect technologies there are features well-known to us: search for happiness and aversion from suffering, charity and selfishness, good and evil, truth and lie. However difficult and diverse, even frighteningly diverse is the world, we still have at our disposal the truths and principles tested by centuries of human civilization, which are enshrined in our constitutions and basic laws, in the systems of our life values that are greatly corresponding to everlasting features of human nature and patterns of social relations, and ensure our universal goals and our best future. If our legal systems in cooperation remain loyal to these principles, I am sure that they will overcome all challenges and threats.

Thank you for your attention.